Safe and sound

Achieving organizational functional safety certification for IEC 61508 and IEC 61511

Stuart R. Nunns, Roger W. Prew

Statistics relating to the performance of major manufacturers are published internationally and incidents, especially those causing injury or death, make headline news. Safety is a major issue and with heightened awareness of contractual rigor and the potential for litigation should something go wrong, organizations need to demonstrate that their functional safety capability is seen as best-in-class.

With this in mind and the increasing globalization of markets, it becomes more and more important to have uniform international safety standards. The IEC 61508 and IEC 61511 international standards are now increasingly used as a measure to demonstrate compliance with legal requirements and justify that the required functional safety has been achieved.

As one of the largest suppliers of safety-related systems to the oil and gas, petrochemical and power industries worldwide, ABB recognizes the importance of compliance. Two years ago, the company embarked on a program to achieve third-party accredited certification in accordance with with the requirements of IEC 61508 and IEC 61511 for 18 of its system integration centers around the globe. This article illustrates the process that the company followed.

Recent inquiries into major industrial incidents [1, 2] reinforced the importance of the international standards IEC 61508 [3] and IEC 61511 [4] and their use as a benchmark of acceptable good practice. In today's world, manufacturers and producers face significant liabilities if they are in breach of or fail to apply required regulations. Such liabilities include direct financial costs arising from the incident itself or from legal costs and fines if found guilty of breaking the law, damages paid to injured parties and a damaged reputation, which can have far-reaching implications on the business. The result is that safety and profitability are inextricably linked.

For ABB, compliance is not only about minimizing liabilities for both the company and its clients, but it is also about leading by example and achieving engineering efficiencies through company-wide common practices and procedures. To explain further, safety systems, like many other automation technologies, are undergoing a revolution. Process protection relies increasingly on networked "smart" equipment, integrated control and safety systems, reprogrammable components and subsystems with automated configuration tools. The application of such technology offers significant economic and safety benefits. However, to exploit this potential the technology must be applied in a compliant and competent manner, and this means the adoption of relevant standards such as IEC 61508 and IEC 61511. In any case, the requirements of these standards cannot be ignored, especially as many major clients are specifying them as a functional safety benchmark and a contractual requirement.

To meet this requirement, the company embarked on a program to achieve third-party accredited certification in accordance with the requirements of IEC 61508 and IEC 61511 for 18 of its system integration centers around the globe. The benefits of certification are outlined in the Factbox.

Establishing the basics

ABB responded to the strategic objective of third-party certification by establishing a Safety Lead Competency Center (SLCC). The SLCC was charged with ensuring that safety applications implemented within ABB Safety Execution Centers (SEC) complied with IEC 61508 and IEC 61511.

For ABB, compliance is not only about minimizing liabilities for both the company and its clients, but it is also about leading by example.

One of its first tasks was to develop a set of core principles for functional safety and a program of work to achieve accredited certification for all the system integration businesses in ABB wishing to achieve SEC status. These core principles, called strategic competency principles, define the minimum requirements needed to demonstrate a commitment to (functional) safety within the businesses. There are four strategic competency principles:

- *Benchmarking current practice* undertakes and documents a "gap assessment" of the existing functional safety management system against IEC 61508 and IEC 61511 to establish the scope of work required.
- *Implementing safety standards* species and implements a work program to achieve accredited certification for each potential SEC's functional safety management system.
- *Establishing individual competency* encourages safety engineers to achieve "certified functional safety engineer" status through the TÜV Rheinland Functional Safety program. Additionally, it ensures that lead and safety engineers working on safety projects have previously attended all the relevant safety system training courses.
- *Managing third-party integrators and channel partners*. Third-party companies invited to carry out safety-related activities for an ABB company will be assessed and approved by the SLCC in the same way as an ABB integrator.

Factbox The benefits of certification

- Limiting exposure to potential liabilities
- Demonstrating due diligence
- Establishing an efficient, repeatable safety management system (procedures, techniques, tools, etc.)
- Reducing unnecessary pre-contract discussions (a benefit to both ABB and client)
- Cost-effective proposals
- Reducing requirements for bespoke project safety procedures
- Gaining a competitive edge
- Being seen as best-in-class

Defining the boundaries

Prior to the gap assessments, a core set of prerequisites[1)] was agreed for all potential SECs. These provided a clear understanding of the organization's safety systems supply chain responsibilities, and mapped the organization's generic functional safety management system against IEC 61508 part 1, clause 6 and IEC 61511 part 1, clause 5 (Management of Functional Safety).

A Safety Requirements Specification (SRS), based on a Process Hazard and Risk Assessment and developed in a systematic way by the Engineering Procurement Contractor (EPC)[2)], is essential before a project can begin. Even though there are significant variations in the quality and contents of the SRS within the industry, the fundamentals are for a clear specification of what safety functions are required and their target Safety Integrity Level (SIL). This information is critical as it enables a definitive proposal to be prepared against an enquiry, and when the contract is won, it provides the full definition for the safety functions to be engineered.

The prerequisites are also required to define the scope of the certification and how it applies to the SEC. For ABB, the certification scope covered:

- IEC 61508 E/E/PE safety-related system integration and IEC 61511 Safety Instrumented System (SIS) integration

Footnotes

1) These prerequisites detail the activities specifically associated with the logic solver subsystem as part of the overall end-to-end Safety Instrumented System (SIS).

2) The benefits to all parties involved (ie, the system supplier, contractor and end-user) by engaging in dialogue at an early stage to establish a quality SRS are immeasurable.

- Applicable phases – IEC 61508 phase 9 and IEC 61511 phase 4. Specifically:
  - Management of functional safety
  - Documentation
  - Functional safety assessments

Specifying competency requirements

The need for formal evidence of the competency of providers of safety-related products and services is increasing. However, in many cases it is clear that there is little understanding of what competency means. Against this background the SLCC has established processes for both organizational and individual competence. These demonstrate that the organization has competent functional safety staff as part of a functional safety competence scheme. This competence scheme is based on four attributes: knowledge, experience, training and qualifications, which are addressed through the development and introduction of a Competence Management System (CMS).

The CMS introduced additional competences specific to functional safety, over and above the requirements of ISO 9001. It is based on the UK IEE/BCS "Competency Criteria for Safety-related System Practitioners" [5].

1 A TÜV Rheinland certificate showing that ABB Limited (UK) has successfully introduced and applied a Functional Safety and Management System (FSMS) in accordance with the requirements of IEC 61508 and IEC 61511.

The CMS ensures that all personnel having responsibilities for safety-related project tasks are equipped with the correct training, knowledge, experience and qualifications appropriate to the tasks for which they are responsible.

A competence database is used to record the technical capabilities of all personnel and provides data for personnel selection. Project managers consult the database when assigning resources to a safety-related project, to ensure that candidates for the roles have the necessary experience and qualifications appropriate to the task and technology, in addition to the legal and safety regulatory framework. The competency level achieved by an individual is classified as follows:

- *Level 1:* Indicates implementation experience of the system safety platform and/or appropriate training. This is the minimum level required for system implementers and testers.
- *Level 2:* Indicates experience and training to the level required for specifying/designing solutions for the system platform. This is the minimum level required for system designers.
- *Level 3:* Indicates a recognized expert in a specific aspect of the systems platform, demonstrated through appropriate combination of experience, application and training. This is the minimum level required for the reviewers of the system.

Benchmarking current practice

The first of the four strategic competency principles described earlier ("Benchmarking current practice") calls for a gap assessment of the Functional Safety Management System (FSMS) against the requirements of IEC 61508 and IEC 61511 for each SEC. To perform this task, a gap assessment methodology, based on a Conformity Assessment of Safety Systems (CASS) [6] scheme was used. This was developed to align with part 1, clause 6 of IEC 61508 and part 1, clause 5 of IEC 61511.

IEC 61511, rather than IEC 61508, was used to develop the detailed gap assessment methodology because its terminology was more relevant to companies like ABB that operate predominantly in the process sector. The gap assessment methodology was aligned to the following phases of IEC 61511, and mapped to the core set of prerequisites defined earlier:

- *Phase 4:* SIS design and engineering
- *Phase 9:* Verification
- *Phase 10:* Management of functional safety and functional safety assessment and auditing
- *Phase 11:* Safety life-cycle structure and planning

A gap assessment module was developed specifically for each of these phases. For completeness, each module was reviewed against all relevant clauses of both standards, and a series of gap assessment tables were developed, which included:

- Targets of Evaluation (TOE)
- A summary of the clause
- A sub-clause reference identifier
- A supplementary assessor guidance (assessor prompt list)
- Assessor findings

By performing the gap assessment in a number of ABB integrators, common areas for improvement were identified, which helped to prioritize the development of the generic FSMS.

Selecting the certification body

Accredited third-party certification – ABB's goal from the outset – provides transparency, credibility, international recognition, objectivity and independent scrutiny. A shortlist of accredited certification bodies, compiled by the SLCC, were invited to participate in a pre-qualification exercise to demonstrate their capability and competency. A panel from within the SLCC reviewed the responses and selected TÜV Rheinland as being the most appropriate third-party accredited certification organization 1.

Model and function

Developing the safety life-cycle model and FSMS was the most significant activity undertaken. It followed the gap assessments and entailed defining a comprehensive safety life-cycle model by mapping the requirements of each phase of the project to the relevant clauses defined in IEC 61508 and IEC 61511. This safety life-cycle model 2 is fully supported by procedures, framework documents (basic

default information for a safety project to be customized to meet any specific project variations) and skeletons (a template consisting of all necessary headers to be completed) – collectively known as the FSMS.

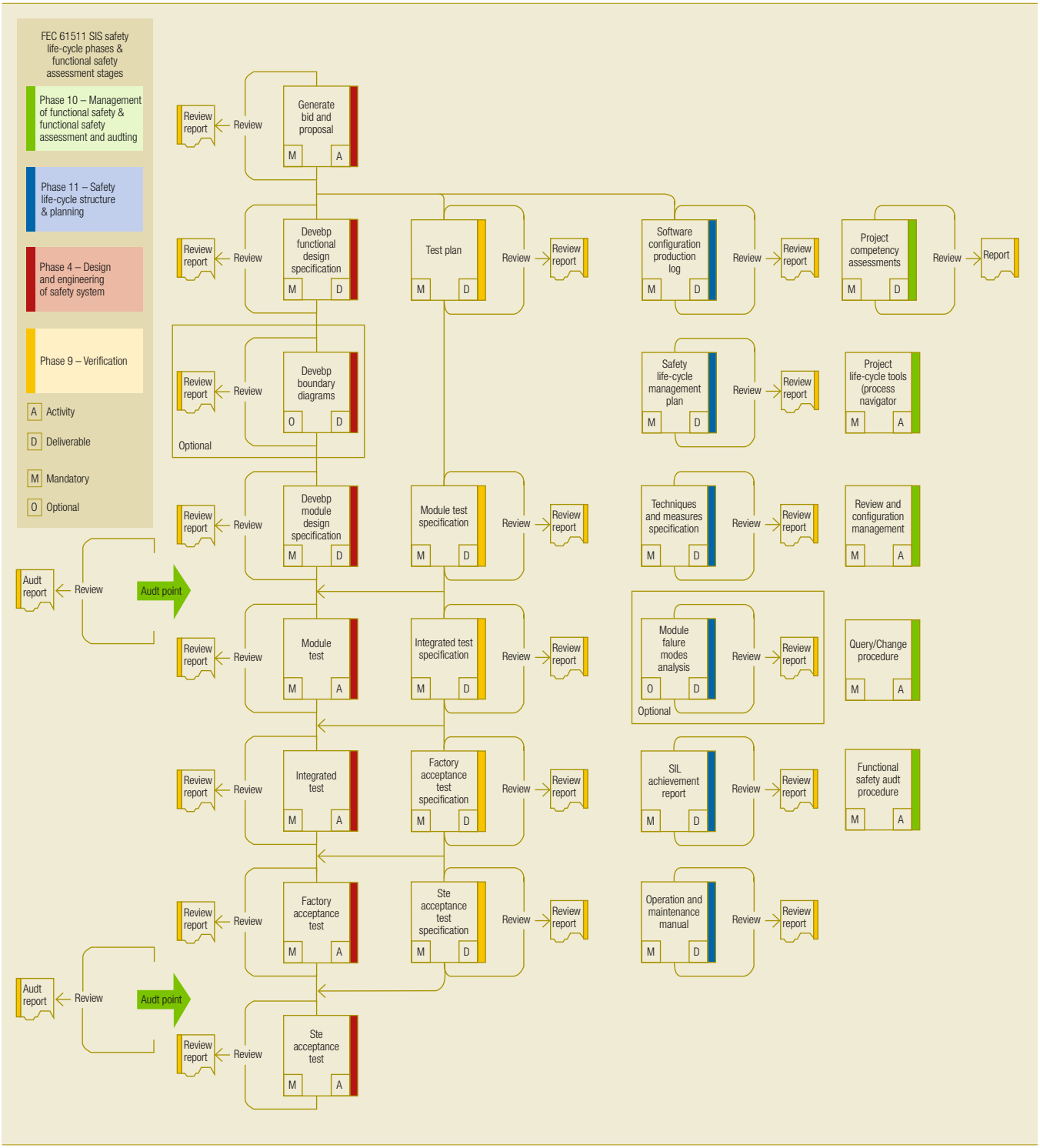
In addition, the FSMS documentation covers all aspects of the life cycle, including the management system, policy, competency, assessments and audits, modification and impact procedures, verification procedures and reporting. It also includes skeleton documents for all the main working documents such as FDS, SDS, Testing, FAT, SAT and operational manuals.

The development of this safety life-cycle model also had to make full use of the existing quality management processes and procedures.

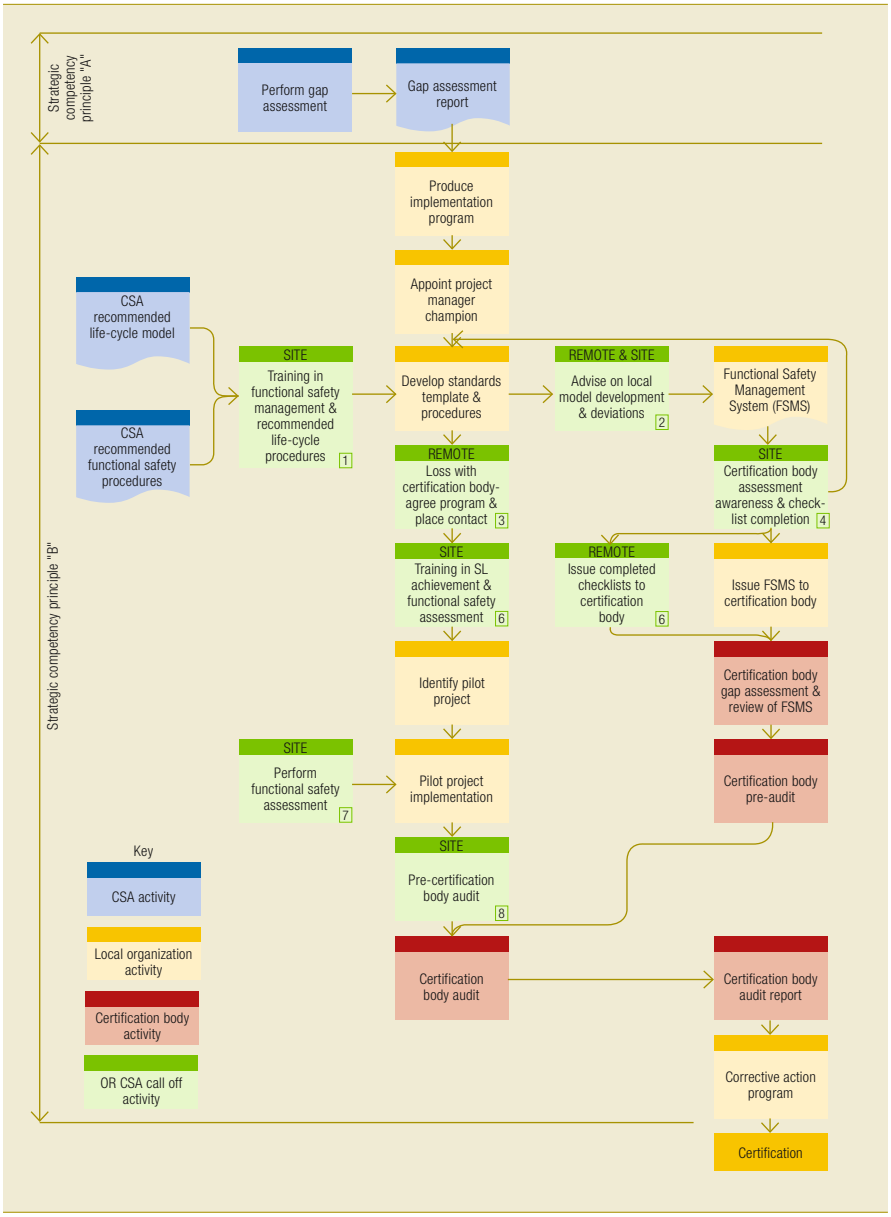
Executing the certification process

A generic certification process model is necessary for the SEC to identify the roles and responsibilities of all the

2 Safety life-cycle model



3 A generic certification process model



parties concerned 3. It is also used by the SLCC to provide assistance in achieving certification.

Establishing supporting activities

Prior to the global certification program, ABB had a large internal network of safety practitioners with different objectives and operational safety standards. Some businesses had already developed plans for certification that had not been completed. Consequently, it was important to establish, early on, a common repository for information exchange. This repository came in the form of a safety database containing the following information:

- Third-party certificates of safety products
- Lists of certified functional safety engineers and functional safety technology engineers
- Improvement themes
- Technical papers and articles
- The latest FSMS procedures
- External functional safety standards
- Sales and technical product material
- Case study progress and program updates

Partners and integrators

To minimize company liabilities, the same rigorous approach to functional safety must apply to any third-party integrators using ABB products. A program of work is required to perform a gap assessment of third-party integrators and to work with them to develop a compliant functional safety management system, preferably in line with that of the main system vendor. This process benefits the third parties in that they can also achieve certification and thereby gain all the advantages.

A move in the right direction

The international safety market is undergoing many changes driven by technology, standards, legislation and incidents. Those organizations working in this demanding and highly competitive arena seek to differentiate themselves, secure market advantage and demonstrate competence and due diligence. Many organizations see accredited certification as a positive step forward.

Accredited certification for an organization is a significant undertaking. It requires management commitment at the highest level, as well as a comprehensive work program involving not only that part of the organization selected for certification, but other groups within the organization itself.

References

[1] Recommendations on the design and operation of fuel storage sites. Buncefield Major Incident Investigation Board. http://www.buncefieldinvestigation.gov.uk/reports/recommendations.pdf

[2] The Report of the BP U.S. Refineries Independent Safety Review Panel. (concerning the Texas City incident). http://www.csb.gov/completed_investigations/docs/Baker_panel_report.pdf

[3] IEC 61508 – Functional safety of electronic/electrical/programmable electronic safety-related systems.

[4] IEC 61511 – Functional safety – Safety instrumented systems for the process sector.

[5] Safety, Competency & Commitment – Competency Guidelines for Safety-Related System Practitioners 1999 (ISBN 0 85296 787 X).

[6] CASS – Conformity Assessment of Safety-related Systems certification scheme – Functional Safety Capability Assessment (FSCA).

Stuart R. Nunns
Roger W. Prew
ABB Process Automation
St. Neots, UK
stuart.nunns@gb.abb.com
roger.w.prew@gb.abb.com