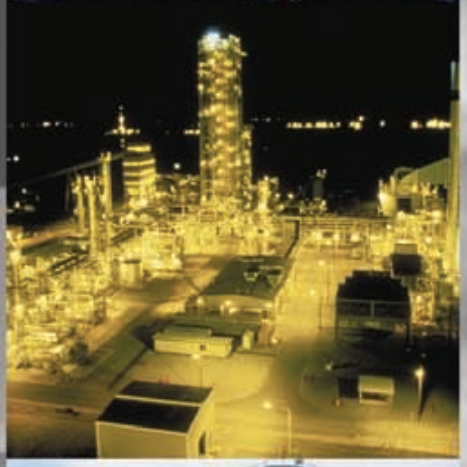
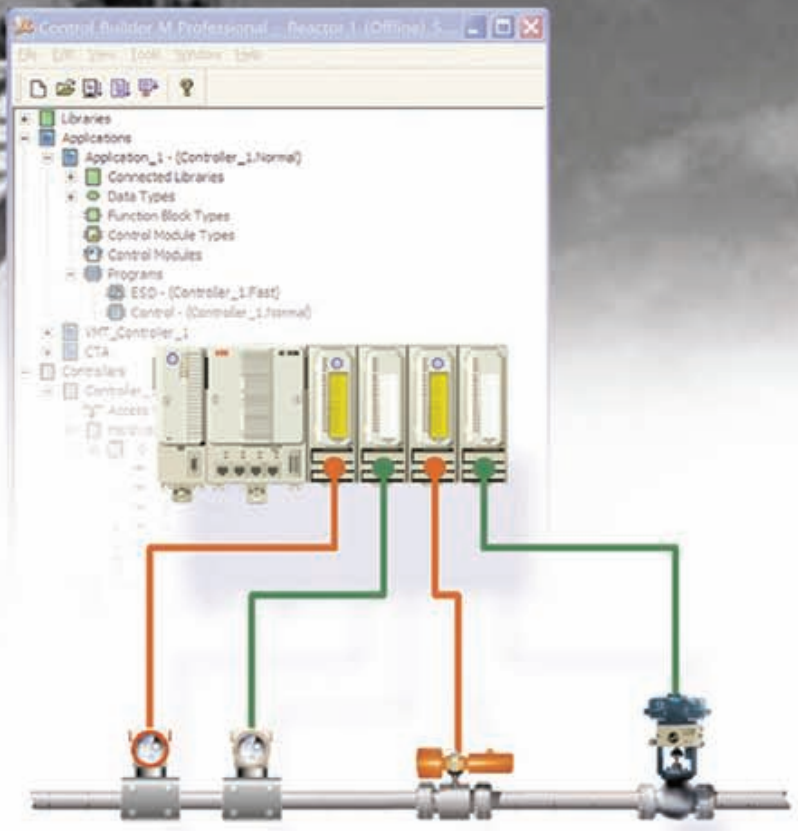
Functional safety handbook





ABB

CONTENTS

For more information, contact Stuart Nunns, UK Safety Lead Competency Centre at
stuart.nunns@gb.abb.com

1.0 INTRODUCTION

The demands of the safety critical systems market are becoming ever more exacting, with international standards being increasingly used to demonstrate compliance with legal requirements and the increasing need to justify that the required functional safety has been achieved. This is not surprising given the increasing dependence on such systems to achieve the specified tolerable risk targets. With increasing contractual rigour and the potential for litigation should something go wrong, organizations need to demonstrate that their functional safety capability is seen as best in class.

Of particular importance in this context is the effectiveness of the competence management arrangements to ensure that those within the organization having responsibility for functional safety are competent to undertake those duties. In order to meet these increasing demands, safety suppliers and integrators are increasingly embarking on more formalized regimes, including certification programmes, to ensure their safety applications are implemented in accordance with IEC61508 [1] and IEC61511 [2].

The author has worked with a number of organizations seeking certification. This *Functional Safety Handbook* provides a case study illustrating how a major automation system supplier (the organization), with world wide systems integration businesses (the integrators) undertook the challenge to achieve third-party accredited certification for its functional safety management system (FSMS) against the requirements of IEC 61508 and IEC 61511.

The generic methodology described and comprising the procedures and processes to achieve certification have been developed by ABB Ltd.

2.0 BACKGROUND

Statistics relating to the performance of large organizations are published internationally and incidents, especially those causing injury or death, make headline news. Recent inquiries into major incidents provide further support of the increasing importance of international standards (IEC 61508 and IEC 61511) where such standards have been used as a benchmark of what constitutes acceptable good practice [3] [4]. Many management incentives are based on the safety performance of their operation. In order to compete or even survive, industry continually strives to improve performance and profitability while maintaining and improving safety. In today's world there are significant costs on an organization if they are not acting in a socially responsible manner. Such costs include direct financial costs arising from the incident itself, from legal costs and fines in the event of being found guilty of breaking the law, damages paid to injured parties caused by negligence and reputation damage which can have far reaching implications on the business. The result is that safety and profitability are inextricably linked.

In summary, there are strong regulatory and social demands for businesses to demonstrate they have exercised their duty of care by providing a safe, reliable operation with full documentation and decision traceability.

2.1 Safety technologies are changing rapidly

In line with all control system technologies, safety systems are undergoing a revolution. Increasing reliance for process protection is being placed on networked 'smart' equipment, integrated control and safety solutions, reusable safety components and subsystems with automated configuration tools. The application of such technology has, potentially, significant economic and safety benefits, but to release its potential, it is vital that such technology is applied by the adoption of current good practice and this means the adoption of relevant standards such as IEC 61508 and IEC 61511. These standards represent current good practice and demand that attention be paid to all safety lifecycle activities within an effective functional safety management system.

2.2 Safety standards are also changing

The publication of the international safety standards IEC 61508 and IEC 61511 for the process sector are setting global benchmarks as "good practices" in functional safety. Safety Regulators and the legal professions world wide are embracing these standards and using them to make judgements as to whether accepted good practice has been applied if negligence is suspected. Ignore them at your peril!

2.3 Globalization

The safety-related market is truly global and increasingly based on international standards. Although companies throughout the supply chain are establishing the capability to ensure compliance with the relevant international standards there are currently differences in the way IEC 61508 and IEC 61511 are being implemented. These differences lead to a lack of cohesion in the supply chain and increase the likelihood of contractual and project disruption. The interface between the supply chain and the end user organization can sometimes be less than ideal as end user organizations have been subjected to right-sizing, downsizing, restructuring and changes of ownership which makes it a challenge for them to retain core competencies in an environment of rapid change.

2.4 Organizational and personal competence

Proven competence at a company, department and individual level is increasingly seen as necessary to meet contractual and regulatory requirements. But which competency scheme is most appropriate and who should it apply to?

2.5 What do the standards say about competency and functional safety?

The following clauses relate to IEC 61508 and IEC 61511 in respect of the "Management of functional safety". In the case study, the

organization had to develop a functional safety management system (FSMS), centrally, in compliance with these clauses as an essential pre-requisite to achieving accredited certification.

The relevant clauses in these standards are:

1. IEC 61508 – Part 1 – clause 6.2.1 states "Those organizations or individuals that have overall responsibility for one or more phases of the overall E/E/PES or software safety lifecycle shall, in respect of those phases for which they have overall responsibility, specify all management and technical activities that are necessary to ensure that the E/E/PES safety-related systems achieve and maintain the required functional safety".

2. IEC 61511 – Part 1 – clause 5.2.2.2 states "Persons, departments or organizations involved in safety life-cycle activities shall be competent to carry out the activities for which they are accountable"

Striving to achieve recognition for organizational and individual functional safety capabilities had to be seen as both a positive and essential requirement for the business as a whole. Also, in the light of many inaccurate and disputed claims (so-called 'claims to fame') relating to compliance of safety-related products in the marketplace it was necessary for the organization to establish an objective and irrefutable means of demonstrating compliance and competence. The organization could not afford to ignore the requirements IEC 61508 and IEC 61511 standards and those of its customers who increasingly specify them as a functional safety benchmark and a contractual requirement.

The additional benefits to the business of achieving certification included:

- Limiting the company's exposure to potential liabilities
- Demonstrating due diligence
- Implementing repeatable and cost effective safety management systems (procedures, techniques, tools etc)
- Reducing unnecessary and costly pre-contract discussions and evidence gathering (which actually benefits both the organization and its clients)
- Winning work cost effectively
- Limiting effort (and cost) in developing so-called bespoke project safety procedures
- Gaining a competitive advantage and as a result securing more business

3.0 PUTTING THE BASICS IN PLACE

In the case study, the senior management of the organization responded to the strategic objectives by establishing an internal Company Safety Authority (CSA). The CSA was charged with the responsibility of ensuring that safety applications were implemented in accordance with IEC61508 and IEC61511.

The CSA was tasked with developing a set of core principles for functional safety and a program of work to achieve accredited certification for the organization as a whole. These core principles endorsed by senior management are collectively referred to as *'Strategic Competency Principles'*. They define minimum requirements designed to reflect a common purpose, shared beliefs and values and a commitment to (functional) safety within all the relevant businesses.

The *'Strategic Competency Principles'* are based on a multi-tiered approach to demonstrating functional safety capability, see Figure 1 below. At the highest level the organization had to demonstrate compliance to good practice by the adoption of international standards IEC 61508 and IEC 61511. A key part of this demonstration was the strategic aim of achieving third party accredited certification. An essential element of this was the organization's competence framework.

The second level relates to individual competence and the requirement to achieve external recognition of an individual's functional safety capability. This recognition complements the organization's competence framework. At the lowest level is the specific requirement to be competent to implement and deliver a specific safety product, package or service.

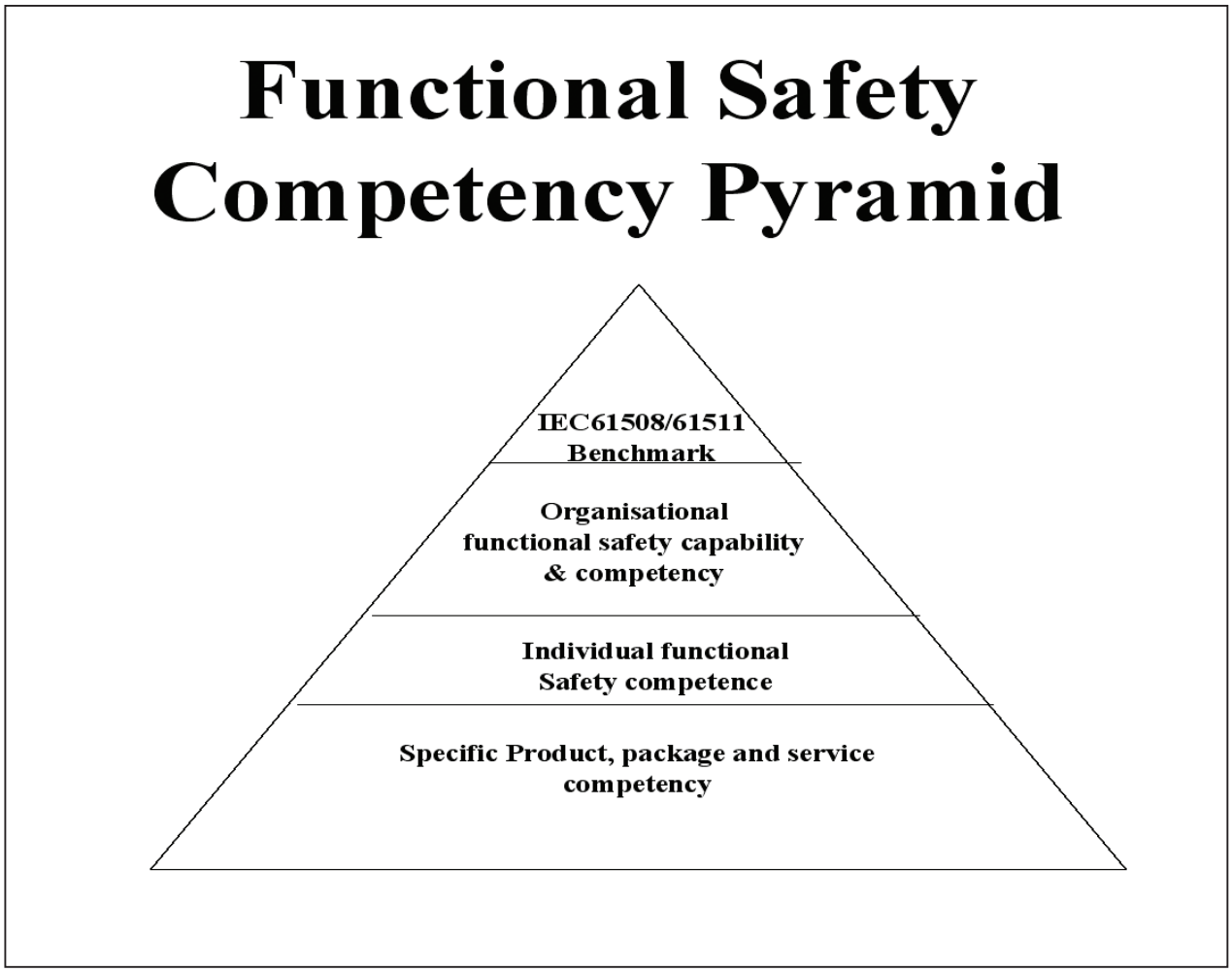


Figure 1

There are four strategic competency principles:

a) Benchmark current practice

Undertake and document a 'gap assessment' of each of the organizations integrator companies' functional safety management system against IEC 61508 and IEC61511 to establish the scope of the task. (See section 6)

b) Implement safety standards

Following the 'gap assessment', specify and implement a program of work to achieve accredited certification for each of the organization's integrator companies' functional safety management systems.

Whilst the organization's integrator companies are seeking accredited certification, they shall produce safety plans covering all their related safety activities.

c) Establish individual Competency

The organization's Safety Engineers shall progress to certified functional safety engineer status through the TUV Rheinland Functional Safety Program.

The organization's Lead Engineers and nominated Safety Engineers working on a safety project shall have attended all the relevant safety system training courses prior to working on a safety project

d) Manage Third Party Integrators and Channel Partners

All Third Party companies invited to carry out safety-related activities on behalf of the organization's integrator companies shall be assessed and approved by the CSA.

This assessment and approval shall be achieved through a gap assessment, project functional safety assessments undertaken by the CSA and project audits undertaken by the integrator. All Third Party Integrators shall have in place a functional safety management system compliant with IEC 61508 and IEC 61511.

The key tenets of these Strategic Competency Principles are:

- To use Certified Products
- To employ Competent (Certified) persons
- To implement safety systems through the certified organization

4.0 DEFINING THE BOUNDARIES

In the case study, prior to the gap assessment a core set of prerequisites had to be agreed for the organization. These not only provided a clear understanding of the organization's safety-related systems supply chain responsibilities but also 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).

This core set of prerequisites are defined below:

- The subsystem used for systems implementation (logic solver and associated I/O modules) is third-party certified in accordance with the requirements of IEC61508
- Safety integrity data (PFD, systematic capability and hardware fault tolerance) exists for all devices
- Safety integrity data for the logic solver is clearly defined in the Safety Manual provided by the supplier of the logic solver
- Reliability data necessary for the integrator to perform their task is provided by supply chain manufacturers to the integrator and is readily available
- Hardware element design (e.g. Analog Input module, Analog Output module) is not undertaken but hardware is configured into overall hardware architecture by development of subsystems
- Software is Limited Variability Language (LVL). This is defined in IEC61131-3 [5] and includes ladder diagram, functional block diagrams, sequential function chart and structured text
- Libraries are available with certified or approved function blocks
- Special (approved) configuration tools are available as part of the logic solver environment
- Development tool support confirms that the downloaded run-time application software is identical to the source application software
- Application software development is facilitated by the use of existing function blocks
- Integration involves the downloading and compilation of the configuration data and application software on the target platform
- Approved libraries and function blocks are protected from unauthorized modification
- Hardware consists of SIS logic solver, cabinets with appropriate termination panels for connecting the process signal to the logic solver I/O modules. Power supplies and power distribution for the logic solver and field devices are also normally included
- A certified application development package is used to configure the SIS logic solver, I/O and communication hardware
- Coding standards are available for each 61131-3 language used, including any specific limitations or restrictions
- The development environment provides version and configuration management facilities
- Process Hazard and Risk Assessment has been performed to ensure systematic development of a Safety Requirements Specification and this has been provided as a key deliverable from the End User/Engineering Procurement and Construction (EPC) organization

With respect to the last bullet point, there are significant variations in the quality and contents of the Safety Requirements Specification (SRS) within the industry. The fundamental requirements are for a clear specification of the safety functions and target safety integrity for each safety function. This information is critical to the integrator, as it enables the integrator to not only provide a detailed and constructive proposal to any bid document, but also, if successful, to engineer a solution which meets the safety functions and target safety integrity required.

Guidance is provided in IEC 61508 Part 2 clause 7.2.3 regarding the content of the Safety Requirements Specification. This is strengthened, for the process industry, in IEC 61511 part 1 clause 10.3.1. In the absence of an SRS at the bid and proposal phase, the integrator established a set of processes to

facilitate a dialog with the client in order to complete, for the bid and proposal phase purposes, the checklist in Table 1. However, this was not a substitute for the delivery of an adequate SRS by the client which would be necessary subsequent to the bid and proposal phase.

There are significant benefits to the parties involved in needing the SRS (the party having responsibility for developing the SRS and the party requiring the SRS in order to undertake the integration process) engaging in a dialog at an early stage. Early dialog facilitates the concept of partnership working and can be of advantage to both parties.

This core set of pre-requisites was also a requirement for defining the certification scope and applied area of each integrators' certification. The certification scope covered:

- IEC 61508 E/E/PE safety related System Integration and IEC 61511 SIS Integration
- Applicable phases – IEC 61508 Phase 9 & IEC 61511 Phase 4
- Specifically:
  - Management of Functional Safety
  - Documentation
  - Functional Safety Assessments

Table 1 Requirements to be addressed

A description of all the safety instrumented functions necessary to achieve the required functional safety
Identification of requirements of common cause failures
Definition of the safe state of the process for each identified safety instrumented function
Definition of any individually occurring safe process states which, when occurring concurrently, create a separate hazard (for example, overload of emergency storage, multiple relief to flare system)
Assumed sources of demand and demand rate on the safety instrumented function
Requirement for proof-test intervals
Response time requirements for the SIS to bring the process to a safe state
Safety integrity level and mode of operation (demand/continuous) for each safety instrumented function
Description of SIS process measurements and their trip points
Description of SIS process output actions and the criteria for successful operation, for example, requirements for tight shut-off valves
Functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives
Requirements for manual shutdown
Requirements relating to energize or de-energize to trip
Requirements for resetting the SIS after a shutdown
Maximum allowable spurious trip rate
Failure modes and desired response of the SIS (for example, alarms, automatic shutdown)
Any specific requirements related to the procedures for starting up and restarting the SIS
All interfaces between the SIS and any other system (including the BPCS and operators)

4.0 DEFINING THE BOUNDARIES

At the outset of the certification program it was necessary to analyze the two relevant standards (IEC 61508 and IEC 61511) to identify differences in interpretation and terminology for those clauses affecting the scope of supply; such as levels of independence for Functional Safety Assessments, Techniques and Measures, Site Acceptance Test (SAT), Verification and Validation.

In addition, this analysis was required as the organization only provides logic solver subsystems and IEC 61511 tends to focus on the complete SIS. As the organization had a requirement for its certification scope to include both IEC 61508 and IEC 61511 it had to reach an agreement with its certification body on interpretation of the standards in specific areas. This resulted in a memorandum of understanding providing interpretation and clarification. For example:

- IEC 61511, Part 1, clause 15.1.1 states that SIS Validation is also referred to as Site Acceptance Test (SAT) which is undertaken on the complete SIS. However in the context of the integrator, Site Acceptance Test (SAT) is an activity performed by the integrator on the customer's site, following Factory Acceptance Test (FAT) on the logic solver (and not the complete SIS) and after delivery of the logic solver to site

- IEC 61511, Part 1, 15.2.2, software validation can be interpreted as applying to the SIS. In the context of the integrator software validation is included in the Factory Acceptance Test (FAT) on the logic solver itself, and not the complete SIS which is out of the scope of supply

- IEC 61511, Part 1, Clause 13.1 refers to Factory Acceptance Test (FAT) and states that Factory Acceptance Test (FAT) is sometimes referred to as integration test and part of validation. In the context of the integrator's Factory Acceptance Test (FAT) this is a separate activity from integration test and is undertaken on the logic solver itself

5.0 SPECIFYING COMPETENCY REQUIREMENTS

There is an increasing trend in the marketplace for client organizations to demand formal evidence of the competency of those providers of safety-related products and services. Many of these requirements are colloquially referred to as 'one liners' (for example 'must have competent people' or 'must have certified engineers'), and it is clear in many cases that the originators of such statements do not fully understand the requirement or how to respond to questions relating to what is exactly meant by such statements.

In any well-run organization, staff are required to be competent to perform the tasks assigned to them. Organizations dealing with safety-related systems increasingly find that their customers need assurance that the organization's personnel can be shown to meet the necessary standards of competency. This includes the designers and implementers of such systems. Professionals, with responsibility for design and/or supervision, will also, for example, be expected to have a detailed working knowledge of all relevant legislation, codes of accepted good practice which affect their work, together with knowledge of working practices in similar establishments and awareness of current developments in their field.

Against this background the case study company established processes for both organizational and individual competence. The ability to demonstrate that the organization had competent functional safety staff called for the establishment of a functional safety competence scheme. This competence scheme was based on four attributes:

1. Knowledge
2. Experience
3. Training
4. Qualifications

One of the objectives of the CSA was set to establish a group of functional safety practitioners within the organization.

Strategic Competency Principle (c) (see section 3) addresses training (attribute 3) in functional safety and specific safety platforms. The CSA chose a respected third party specialist as the provider of training leading to TUV certified functional safety engineer status.

The other three attributes above on which the competence of persons was based, namely knowledge, experience and qualifications, were addressed through the development and introduction of a Competence Management System (CMS).

The CMS introduced a further level of competence specific to functional safety, over and above that required by the company's ISO 9001 QMS. The CMS was based on the UK IEE/BCS "Competency Criteria for Safety-related System Practitioners" [6].

The key requirement was for all personnel having responsibilities for specified tasks on a safety-related project to have their training, knowledge, experience and qualifications assessed in relation to the particular tasks for which they were responsible.

Although IEC61508 does not make a direct correlation with the required level of rigour and competence, the following factors were taken into consideration:

- The consequences in the event of failure of the Electrical/Electronic/Programmable Electronic (E/E/PE) safety related system; the greater the consequence, the more rigorous the specification and assessment of competence.
- The safety integrity levels of the Electrical/Electronic/Programmable Electronic (E/E/PE) safety related system; the higher the safety integrity levels, the more rigorous the specification assessment of competence.
- The novelty of design procedures or application; the newer or more untried the designs, design procedures or application, the more rigorous the specification and assessment of competence should be.

- Previous experience and its relevance to the specific duties to be performed and the technology being employed. The greater the required competence levels, the closer the fit should be between competencies developed from previous experience and those required for the specific duties to be undertaken.

A competence database, in existence at the organization, and used to record the technical capabilities of personnel was used as the basis for personnel selection. That is, the responsible Project Manager consults the database when assigning resources to a safety-related project, to ensure that candidates have the necessary experience and qualifications appropriate to the application area and technology, as well as knowledge of the legal and safety regulatory framework. The classification of the level of competence achieved, with respect to specific competence, is as follows:

Level 1:
Has experience of the system safety platform in an implementation capacity and / or has attended appropriate training courses. This is the minimum level required for the relevant activities of the implementers and testers of the system.

Level 2:
Has experience and training to the level of specifying/designing solutions for the systems platform. This is the minimum level required for the relevant activities of the designers of the system.

Level 3:
A recognised expert in his/her application of the systems platform, demonstrated through appropriate combination of experience, application and training. This is the minimum level required for the relevant activities of the reviewers of the system.

A set of supplementary guidelines assists those undertaking the assessment of an individual in order to produce an assessment profile and the level of competence achieved. This information was subsequently recorded in the competence database.

The supplementary guidelines cover such areas as:

- Engineering knowledge appropriate to the industry domain
- Safety system knowledge applicable to the application and technology
- Principles of Functional Safety Assurance
- Specifying, witnessing & performing tests
- Transposing safety requirements to design
- Analysing design and code (in terms of software and hardware architecture and including various forms of definition notation)

Completion of the assessment of competence not only facilitates the mapping of the individual's competence to the specific project tasks and activities they are required to perform but also identifies those areas where mentoring and supervision is required and any additional training necessary.

6.0 BENCHMARKING CURRENT PRACTICE

Strategic Competency Principle a) (see Section 3) called for a gap assessment to be performed of the functional safety management system against the requirements of IEC 61508 and IEC 61511 for each of the organization's integrators involved in functional safety activities. In order to undertake this task, a gap assessment methodology, based on the CASS (Conformity Assessment of Safety Systems) [7] scheme was used. The CASS assessment templates were developed to align with clause 6 of IEC 61508 Part 1 and clause 5 of IEC 61511 Part 1.

IEC 61511 rather than IEC 61508 was used to develop the detailed gap assessment methodology, simply because its terminology was more readily understood and relevant to the case study organization that operates predominantly in the process sector. The gap assessment methodology was aligned to those phases of IEC 61511 and mapped across to the core set of pre-requisites of the organization (see Section 3. 2 – Defining the boundaries), namely:

- Phase 4 SIS Design & 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 the above phases.

For each gap assessment module, and for completeness, all relevant clauses of both standards were reviewed and a series of gap assessment tables developed to include:

- Targets of Evaluation (TOE) i.e.) evidence expected
- Summary of the clause
- Sub clause reference identifier
- Supplementary assessor guidance (Assessor prompt list)
- Assessor findings

An example is provided in table 2 below.

As a result of performing the gap assessment common areas for improvement were identified, which in turn helped to prioritize the later development of the functional safety management system.

Table 2 Example Gap Assessment Target of Evaluation

Target of Evaluation	**Purpose of TOE**	**IEC 61508 Clauses/tables**	**Assessment prompt list**	**IEC 61511 Clauses/purpose**
Competence assessment process	To define procedures for ensuring that applicable parties involved in any of the overall, E/E/PES or software safety lifecycle activities are competent to carry out the activities for which they are accountable; in particular, the following should be specified: the training of staff in diagnosing and repairing faults and in system testing, the training of operations staff, the retraining of staff at periodic intervals;	1/6.2.1 h) Figs 2,3,4 and 1/Table 1 as framework.	• There is evidence that the functional safety tasks to be done have been assigned – the competency required for the task and a gap analysis between the competencies of the individual allocated to the task have been undertaken. • There is evidence of a logical process that documents who is responsible for deciding why an individual has been allocated to the task. • This element will be explored in greater detail within the overall competency assessment TOES (Annexe C)	5.2.2.2 Persons, departments or organisations involved in safety lifecycle activities shall be competent to carry out the activities for which they are accountable. • What evidence is available demonstrating this • Does it take into account, specific technology, safety engineering, regulations, management and leadership skills, consequences, SIL, complexity, novelty • Knowledge – how do you show this • Training – generally records in place (part of ISO9001) • Experience – traditionally poorly recorded • How are these assessed / recorded / updated • How are the competency needs identified • How is the 'gap' between needs and skills assessed / bridged

7.0 SELECTING THE CERTIFICATION BODY

The organization chose to achieve accredited third-party certification as its ultimate goal. Accredited certification provides transparency, credibility, international recognition, objectivity and independent scrutiny.

A short list of accredited certification bodies was drawn up by the Company Safety Authority (CSA) and invited to participate in a pre-qualification exercise to provide information to demonstrate their capability and competency.

The information requested included:

- Appropriate evidence of operation as an accredited certification body including
  - national accreditation bodies to which accredited
  - scope and date of accreditation
  - details of applicable standards and certificates relevant to the accreditation

- Pedigree, including a description of the experience, capability and competence of the certification body and its auditors to perform these specific third-party assessments (functional safety management as opposed to product assessment)

- Global presence of the certification body including countries in which they operate

- Whether dependent on agencies in specific countries and if so their details

- Reciprocal arrangements including:
  - Memoranda of Understanding (MOR)
  - Mutual Recognition Arrangements (MRA)

- CVs of assessors

- List of organizations including those that have been assessed, their scope of assessment and contact details within the organization

- Description of:
  - the assessment methodology
  - the assessment process
  - guidance notes for the assessed organization

- Typical work program (including labor costs) for a third party functional safety assessment, including man-days effort

- Any current limitations envisaged in undertaking the third party assessment program

- Company accounts for the last accounting period

- Organizational structure

It was then necessary to establish an impartial and independent panel representing the organization to review the responses resulting in the selection of a global third-party accredited certification organization. In the case study this was the Company Safety Authority (CSA).

8.0 DEVELOPING THE SAFETY LIFECYCLE MODEL AND FUNCTIONAL SAFETY MANAGEMENT SYSTEM

This was the most significant activity undertaken. It followed the gap assessment and entailed defining a comprehensive safety lifecycle model mapping the relevant phases of IEC 61508 [1] and IEC 61511 [2] in respect of the core set of pre-requisites described in section 4 – 'Defining the boundaries'. This safety lifecycle model was 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).

The development of this safety lifecycle model had in addition to make full use of the existing quality management processes and procedures. Figure 2 below details the model.

An explanation of the deliverables specified in the model is provided below in sections 8.1 to 8.5.

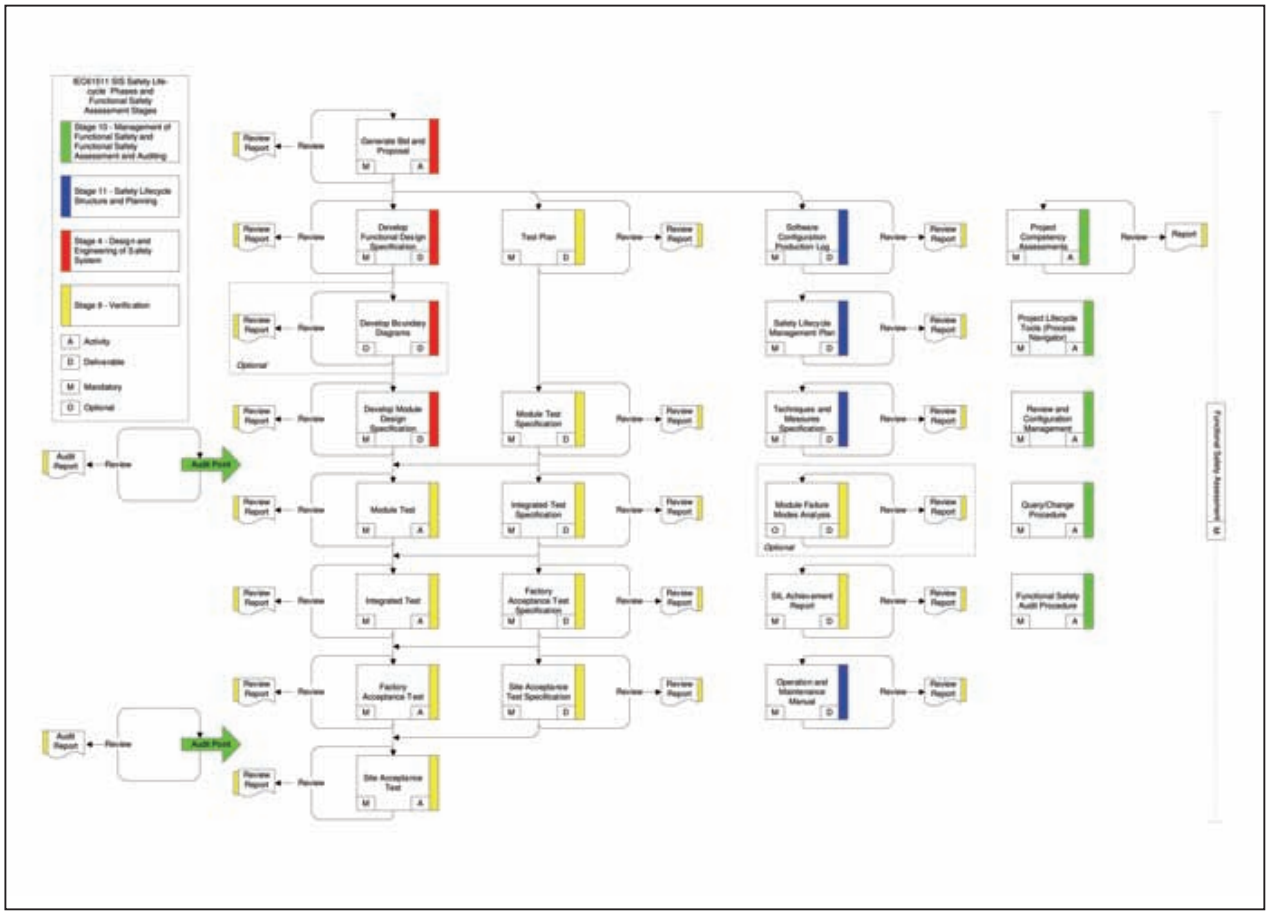


Figure 2: The Safety Lifecycle Model (see Appendix, page 32 for full version)

8.0 DEVELOPING THE SAFETY LIFECYCLE MODEL AND FUNCTIONAL SAFETY MANAGEMENT SYSTEM

8.1 Design Documentation

8.1.1 Functional Design Specification

The Functional Design Specification (FDS) is the key design document produced by the integrator. It is also the key, controlling document for the system design and contains all the rationale as to why the design has taken the specified approach. It takes the client's Safety Requirement Specification (SRS) as input data, and develops them through the FDS, detailing the platform to be used, system layout (often in the form of a system block diagram), interfaces, and functional and operational design considerations. The FDS, once approved, confirms the basis of design and traceability of the ensuing design to the client's requirements. It also sets up the rollout of the Hardware Design and Software Design Specifications. The FDS provides the key acceptance criteria for the system Factory Acceptance Testing (FAT), and is used by the integrator to measure the success of the project from the results of FAT.

8.1.2 Module Design Specification

This is the lowest level of detailed design document produced on the project. The primary function of the Module Design Specification is to show clear design intent, to communicate that design in a clear fashion, and to allow for approval before its implementation. The Module Design Specification defines in detail the inputs, outputs and functionality for the operation of a particular software module in pseudo code or structured English. It will also define all variables used (global or local), other modules called, the result and error conditions, parameters passed and interfaces/relationships with other modules or systems.

The second function of the document is to enable any trained programmer to code to the programming language and standards defined in the document and in accordance with the relevant project programming standards. The approach to the Module Design Specification is of particular importance where there is more than one programmer on the project team producing modules that affect the overall functionality of the system.

Examples of modules are as follows:

- Generic analog input module
- Generic digital output module
- Cause and effect mimic
- Firewater pump logic
- Evacuation criteria

8.1.3 Boundary Diagram

The purpose of the Boundary Diagram is to graphically identify which components form part of the Sensor, Logic Solver and Final Element, and is of use as a reference point for the SIL verification report.

Boundary Diagrams are an optional requirement and only need be produced if they are a requirement / necessity of the project.

8.2 Verification documentation

8.2.1 Test Plan

The Test Plan defines the verification process for the System. This includes an outline of the tests and test criteria, test environment and test phase prerequisites necessary to verify and validate the system against the appropriate reference documents and standards.

Refer to the Review and Configuration Management Procedure in respect of the verification activities which encompass documentation and code reviews.

8.2.2 Module Test Specification

Once a software module has been coded, and reviewed, it is subjected to formal testing defined by the Module Test Specification. As many module test specifications can be produced as necessary.

The functionality of each module will be verified by the use of this document and the approved Module Design Specification specific to the module under test.

8.2.3 Integrated Test Specification

The Integrated Test Specification is used to demonstrate that each application software module produced integrates correctly with other software modules and interfaces correctly with the system target hardware and system firmware, all being an integral part of the deliverable system. Testing will include both functional safety and non-safety aspects of the system to verify that the system performs its intended functions and does not perform unintended functions.

8.2.4 Factory Acceptance Test Specification

The Factory Acceptance Test Specification is used to demonstrate to the client that each application software module produced integrates correctly with other software modules, and interfaces correctly with the system target hardware and system firmware, all being an integral part of the deliverable system. Testing will include both functional safety and non-safety aspects of the system, to verify that the system performs its intended functions and does not perform unintended functions.

8.2.5 Site Acceptance Test Specification

The Site Acceptance Test Specification is used to demonstrate to the client that the entire system, including all networks, function correctly after re-assembly and installation on site. In addition the SAT verifies that the software loaded is that which was demonstrated at the FAT stage, this is achieved by functionally testing specific elements of the control system, previously verified at the FAT.

8.2.6 SIL Achievement Report

The purpose of the SIL Achievement Report is to demonstrate that the system meets the systematic and hardware fault tolerances required by the SIL specified by the Safety Requirements Specification. The SIL Achievement Report provides the quantitative evidence in the form of PFD and architectural constraints (a combination of Hardware Fault Tolerance (HFT) and Safe Failure Fraction (SFF)).

8.2.7 Module Failure Modes Analysis

The purpose of the Module Failure Modes Analysis is to provide a report of the hardware failure modes performed on the System.

This analysis attempts to discover and analyze all potential failure modes of the hardware sub-system, the effects these failures have on the system, and what measures have been engineered to correct and or mitigate the failures or effects on the system.

The analysis supports the Reliability and Availability calculations in the SIL Verification Report, in providing evidence that the ESD system conforms to the availability requirement of the SIL, as identified in the Safety Requirement Specification.

Note that the Failure Modes Analysis is an optional requirement and should only be produced if they are a requirement/necessity of the project.

8.3 Safety Lifecycle Structure and Planning Documentation

8.3.1 Safety Lifecycle Management Plan

The purpose of this document is to demonstrate how the integrator intends to manage the realization sections of the safety lifecycle of the project and defines how the user manages the subsequent operational and maintenance parts. This is in order to show its alignment with the recommendations laid out in IEC 61508 and IEC 61511.

Compliance with this safety lifecycle management plan, and thus conformance with the recommendations of IEC61508 and IEC61511, is demonstrated by means of assessment (Functional Safety Audits) and verification (Module, Integrated and Factory Acceptance Testing) of the outputs from each phase of the safety lifecycle model.

8.3.2 Software Configuration Production Log

The purpose of the software configuration production log is to modularize and categorize the software elements, for example, generic loop types, graphics, and logic. The production log is then used to track the progress of each module as it goes through design, build and stage stages, according to the safety lifecycle model.

8.3.3 Techniques and Measures Specification

The purpose of this document is to define the techniques and measures, and where applicable supporting tools, necessary to align with the requirements of IEC61508, Part 2 (Annexes A and B) and Part 3 (Annexes A and B) for each phase of the E/E/PE and Software Safety Lifecycles. In order to demonstrate compliance to the requirements of IEC 61508 it was necessary for the organization to specify those techniques and measures used in order to avoid and control systematic faults, see IEC 61508 Part 2, clause 7.4.2.2.

Table 3 - Recommendations to avoid faults and failures during E/E/PES integration

Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4	SIS	Techniques and Methods
Functional testing	B.5.1 mandatory	HR mandatory	HR mandatory	HR mandatory	HR	Y	In-house 'Process Navigator' Safety Lifecycle Management Plan Test Plan Module Test Specification Integrated Test Specification Factory Acceptance Test Specification
Project Management	B.1.1 Low	HR Low	HR Medium	HR High	HR	Y	ISO9001 'Process Navigator' Safety Lifecycle Management Plan
Documentation	B.1.2 Low	HR Low	HR Medium	HR High	HR	Y	'Process Navigator' Safety Lifecycle Management Plan
Black box testing	B.5.2 Low	R Low	R Medium	R High	R	Y	Validation and Test Plan
Field experience	B.5.4 Low	R Low	R Medium	R High	R	N	
Statistical testing	B.5.3 Low	- Low	- Medium	R High	R	N	

All techniques marked "R" in the grey shaded group are replaceable, but at least one of these is required.
For the verification of this safety lifecycle phase, at least one of the techniques or measures shaded grey in this table or listed in table B.5 shall be used.
NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding this table.
NOTE 2 The measures in this table can be used to varying effectiveness according to table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.
NOTE 3 The overview of techniques and measures associated with this table is in annex B of IEC 61508-7. Relevant sub-clauses are referenced in the second column.

In the case study, this was an extensive exercise. The tables of Techniques and Measures within IEC 61508 cover the complete E/E/PES and Software Safety Lifecycles. The first step was to identify only those tables associated with the integrator's core set of pre-requisites (see section 3.2 above) related to IEC 61508 Phase 9 and IEC 61511 Phase 4. Having identified the sub-set of tables the decision was made to benchmark the assessment of the organization against the requirements for SIL 3. The aim of the certification would be to provide the third party evidence that the integrator had demonstrated, for the logic solvers within the scope of the certification, a functional safety capability of SIL 3. In respect to the techniques and measures used, the Highly Recommended 'HR' option was selected and then tables populated with:

- cross references to organization procedures
- certificates of compliance
- use of certified logic solvers

Examples are shown in Tables 3 and 4 below

A 'Y' in the SIS column within the table against a specific technique identifies the technique as being selected for the project.

Table 4 – Software design and development: support tools and programming language

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4	SIS	Techniques and Methods
1	Suitable programming language	C.4.6	HR	HR	HR	HR	Y	Certified Control Language, with a subset of function blocks is certified for use, constrained by certified logic solver Certified Control Language
2	Strongly typed programming language	C.4.1	HR	HR	HR	HR	Y	Certified function blocks are utilized, constrained by certified logic solver Certified Control Language
3	Language subset	C.4.2	-	-	HR	HR	Y	Certified Control Language is a component of certified logic solver. Safe subset dictated by the safety manual and certified logic solver
4a	Certified tools	C.4.3	R	HR	HR	HR	Y	Certified Control Language, with a subset of function blocks is certified for use. Safe subset dictated by the safety manual and certified logic solver Certified Control Language
4b	Tools: increased confidence from use	C.4.4	HR	HR	HR	HR	Y	
5a	Certified translator	C.4.3	R	HR	HR	HR	N	Not used for LVL
5b	Translator: increased confidence from use	C.4.4	HR	HR	HR	HR	Y	Certified Control Language has >5 years proven in use
6	Library of trusted/verified software modules and components	C.4.5	R	HR	HR	HR	Y	Only certified function blocks, or modules constructed from these blocks, are utilized in this application. Refer to the Safety Manual

* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. Only one of the alternate or equivalent techniques/measures has to be satisfied.

8.3.4 Operator Manual

The Operator Manual is developed from the FDS and the Module Design Specifications and is written to ensure that plant personnel are provided with all relevant information on the operation of the System.

8.3.5 Maintenance Manual

The Maintenance Manual is developed from the FDS and the Module Test Specification and is written to ensure that plant personnel are provided with all relevant information on the maintenance of the System.

The Maintenance Manual makes reference to, and use of, the standard integrator Document Reference Set. This is a collated set of individual, standard instruction booklets (IBs) for the company's generic Safety system (in the case of the case study 800xA HI) (which includes the safety manual), covering both hardware and software.

The Maintenance Manual indicates, where applicable, the verification tests that the user must undertake to proof test the Logic Solver. This includes, but is not limited to, the action to be taken when abnormal conditions are indicated by the system (either via LED on the module, or software diagnostic).

The Maintenance Manual provides information to the end user to enable them to ensure functional safety performance is maintained.

8.4 Management of Functional Safety Documentation

8.4.1 Query/Change Procedure

The Query/Change Procedure provides guidance in the use of project queries, and defines the impact assessment form to be used to assess each change or variation to the Safety Instrumented System.

8.4.2 Review and Configuration Management Procedure

The Review and Configuration Management Procedure ensures that, through review and assessment, application software code and supporting documentation is produced to be consistent, maintainable, of acceptable quality, satisfying user requirements, and is safe.

8.4.3 Project Competency Assessment Procedure

The purpose of the Project Competency Assessment Procedure is to provide a formal means of assessing personnel involved in any Safety Lifecycle Electric / Electronic / Programmable Electronic Systems (E/E/PES) and software activities, to ensure that they possess the necessary experience, knowledge, training and qualifications to carry out the activities for which they are accountable and, where necessary, to identify any additional training requirements.

8.4.4 Functional Safety Audit Procedure

The purpose of the Functional Safety Audit Procedure is to provide additional guidance to the project auditors in order to verify correct implementation.

8.4.5 Functional Safety Assessment (FSA)

Functional Safety Assessments are undertaken in accordance with the requirements of IEC 61508 Part 1 Clause 8.

In the case study, the CSA acted as the 'Independent Department' in performing functional safety assessments of the integrator's safety-related projects in accordance with the requirements of IEC 61508 Part 1, Table 5 for Safety Integrity Level (SIL) 3. An assessor drawn from the CSA plans, schedules and executes these functional safety assessments in accordance with a CSA procedure ('Functional Safety Assessment Process').

Acting as an Independent Department for undertaking FSAs enables the CSA to perform a similar role for other business units within the organization planning for future accredited certification.

The FSA should provide, amongst other things, confidence that the following have been achieved:

- The safety instrumented system logic solver is designed, constructed, verified and tested in accordance with the safety functional design specification; any differences have been identified and resolved
- The safety instrumented system logic solver validation planning is appropriate and the validation activities have been completed
- Project design change procedures are in place and have been properly applied
- SIL capability achieves the SIL target requirements
- Regulations, mandatory standards and any stated codes of practice have been met
- Where development and production tools are used they shall be included in the FSA
- Adequate and complete documentation is provided

At least one Functional Safety Assessment (FSA) is performed during the project's safety lifecycle. The FSA is split into three phases:

- Preliminary FSA – trigger point completion of Safety Lifecycle Management Plan
- Design FSA – trigger point completion of Functional Design Specification
- Final FSA – trigger point completion of Factory Acceptance Test

Additional FSAs may be required depending on criteria such as:

- Duration of project
- Number of safety systems implemented within the project
- Safety regulatory requirements
- Degree of complexity

Each phase of the FSA is supported by checklists drawn directly from IEC 61508 and designed to assist the assessment team in ensuring that the FSA is conducted in accordance with the requirements of the standard.

Table 5 (see page 22) provides an example of a checklist to be used during the final FSA. The white cells are the clauses from the standard setting out the objectives to be achieved whereby compliance will be measured and findings recorded. The blue cells are the clauses from the standard setting out the requirements to meet the objectives.

Table 5 Example of a Final FSA checklist

Item	Clause	Objectives & Requirements	Recommendation *Accept (A); Reject (R); Qualified Acceptance (QA); Not Applicable (NA)*
1	IEC 61508-1 Clause 5 Documentation	**5.1** Objectives **5.1.1** The first objective of the requirements of this clause is to specify the necessary information to be documented in order that all phases of the overall, E/E/PES and software safety lifecycles can be effectively performed. **5.1.2** The second objective of the requirements of this clause is to specify the necessary information to be documented in order that the management of functional safety (see clause 6), verification (see 7.18) and the functional safety assessment (see clause 8) activities can be effectively performed. **Assessor Note:** In respect of the Preliminary FSA this will seek evidence that the key deliverables are identified within the SLMP and the SLMP has itself undergone formal review and approval. During the Design and Final FSA the results of the functional safety audits will be reviewed.	
1.1	IEC 61508-1 Clause 5.2 Requirements	**5.2.1** The documentation shall contain sufficient information, for each phase of the overall, E/E/PES and software safety lifecycles completed, necessary for effective performance of subsequent phases and verification activities. **5.2.2** The documentation shall contain sufficient information required for the management of functional safety (clause 6). **5.2.3** The documentation shall contain sufficient information required for the implementation of a functional safety assessment, together with the information and results derived from any functional safety assessment. **5.2.4** Unless justified in the functional safety planning or specified in the application sector standard, the information to be documented shall be as stated in the various clauses of this standard. **5.2.5** The availability of documentation shall be sufficient for the duties to be performed in respect of the clauses of this standard. **5.2.6** The documentation shall be – accurate and concise; – be easy to understand by those persons having to make use of it; – suit the purpose for which it is intended; – be accessible and maintainable. **5.2.7** The documentation or set of information shall have titles or names indicating the scope of the contents, and some form of index arrangement so as to allow ready access to the information required in this standard. **5.2.8** The documentation structure may take account of company procedures and the working practices of specific application sectors. **5.2.9** The documents or set of information shall have a revision index (version numbers) to make it possible to identify different versions of the document. **5.2.10** The documents or set of information shall be so structured as to make it possible to search for relevant information. It shall be possible to identify the latest revision (version) of a document or set of information. **5.2.11** All relevant documents shall be revised, amended, reviewed, approved and be under the control of an appropriate document control scheme.	

8.5 Safety Project Activity Plans

The project safety lifecycle model, as defined above, is further supported by a detailed Activity Plan, which specifies for each stage of the project, its inputs, outputs and review responsibilities. The intention is that each integrator will populate the business process model reference and activity references with local procedures. An extract of the Activity Plan is provided in Table 6 below.

Although Activity Plan activities are in their respective logic sequence, this does not constitute the actual order in which activities may be completed. Therefore reference should be made to each specific safety project schedule.

Table 6 Safety Project Activity Plan

Activity Number	Business Process Model reference	Activity	Activity related procedure or document	Acceptance criteria	Prime responsibility for activity	Activity deliverable	Inspection schedule		
							ABB	Client	VB
1.12		Preparation, Submission, Review and up-date of Competency Assessment Procedure	Safety Lifecycle Management Plan Review and Configuration Management Procedure	Conformity to ABB quality system requirements	SIS Lead Engineer Project Manager Independent Verification Body	Client Approved Project Competency Assessment Procedure	H	A	R
1.13		Assessment of Safety Team Members	Project Competency Assessment Procedure	Conformity to Safety Lifecycle Management Plan	Project Manager Independent Verification Body	Completed Safety Team Member Assessment Forms	H	R	R
1.14		Preparation, Submission, Review and up-date of Query/Change Procedure	Safety Lifecycle Management Plan Review and Configuration Management Procedure	Conformity to ABB quality system requirements	SIS Lead Engineer Project Manager Independent Verification Body	Client Approved Query/Change Procedure	A	A	R
1.15		Preparation, Submission, Review and up-date of Review and Configuration Management Procedure	Safety Lifecycle Management Plan Review and Configuration Management Procedure	Conformity to ABB quality system requirements	SIS Lead Engineer Project Manager Independent Verification Body	Client Approved Review and Configuration Management Procedure	A	A	R

Further clarification of some of the cells is provided on the following page

Verification Body (VB)
Verification is only applicable to those activities within the Quality Plan that relate to the design, hardware build, software configuration, functional test and validation of safety-related systems, that is Phase 9, Realization, of the Safety Lifecycle recommended by IEC61508 and IEC61511, and Phase 4, SIS design and engineering within IEC61511.

The field marked 'VB' is used to indicate (and demonstrate to the client or Verification Body (VB)) that each applicable activity has been formally assessed and verified in terms of meeting the required Safety Integrity Level (SIL), for the particular item of safety-related equipment, to which the activity relates.

The Verification Body will be a person that has the required competency, skills and independence from the project to undertake the assessment of the particular activity. In line with the recommendations of IEC61511, Independence is defined as follows:

Independent Person – a competent person who is separate and distinct from the activities which take place during the specific phase of the safety lifecycle and does not have direct responsibility for those activities

Inspection Schedule Codes
The inspection / documentation schedule codes listed in the Activity Plan are defined as follows:

H: Hold Point
This is an inspection or test that is considered vital to the quality and integrity of the equipment and services being supplied.

A hold point cannot be passed unless the specified acceptance criteria have been met (unless a concession is raised and approved). Where a hold point is also specified by the client, the point cannot be passed without written authorization from the client.

W: Witness Point
This is an inspection or test that may be as important as a hold point (and must be notified to the client), but which can be responsibly carried out after the point has been passed.

Witness points may be attended by the client, but authorization from the client is not required to allow work to proceed beyond that point (following expiry of the seven days notice).

M: Monitor Point
This is a point in the programme of work where a check may be made to verify that a specified action has taken place, and that the correct documentation records exist. Such checks can be retrospectively made.

A: Approval Point
(documentation and/or records)
Approval points are those which require documentation and/or records to be reviewed and approved by the integrator and the client, and beyond which work cannot proceed until the appropriate approval is given.

R: Review Point
Review points are where design reviews and / or walkthroughs are to be performed for the specified activity or activities that require verification.

Review points may be attended by the client, but authorization from the client is not required to allow work to proceed beyond that point (following expiry of the seven days notice).

Full adherence to the safety lifecycle model required the development of a set of supporting procedures, framework documents and skeletons defined below. Tables 7, 8, 9 and 10 provide titles for all of these additional documents including those specific to the integrator's QMS.

Table 7 QMS Document list

- New Supplier Assessment
- Contract Review and Order Processing
- Internal Kick-off Meeting Preparation
- Quality Plan/Safety Plan
- Query Management Process
- Configuration Management
- Competency and Training Work Practice
- Complete Functional Description
- Software Production
- Complete Test Specification
- Module Test
- Integrated Test
- Factory Acceptance Test
- Management System Audits
- Bid and Proposal Guideline
- Safety Requirements Checklist
- Product Alert Handling
- Management System Review

Table 8 Supplementary FSMS Document list

- Functional Safety Management System Overview
- Functional Safety Policy (UK-SEC)
- Project Competency Assessment
- Project Competency Assessment Form
- Review and Configuration Management Document Review Form
- Code Review Form
- Project Query Handling Supplementary Instruction & Guideline
- Query Change Impact Analysis Form
- Functional Safety Audit & Assessment Procedure
- Safety Lifecycle Management Plan
- Software Production Log
- Techniques and Tools
- Verification and Test Plan
- SIL Verification Report

Table 9 Supplementary FSMS specific Skeletons Document list –

- Functional Design Specification
- Software Design Specification
- Module Test Specification
- Integrated Test Specification
- Factory Acceptance Test Specification
- Site Acceptance Test Specification
- Operator Manual
- Maintenance Manual
- FMEA
- Boundary Diagrams

Table 10 FSMS Framework Documents –

- Safety Lifecycle Management Plan
- Software Production Log
- Techniques and Tools
- Verification and Test Plan
- SIL Verification Report

9.0 EXECUTING THE CERTIFICATION PROCESS

A generic certification process model is necessary for the integrators to identify roles and responsibilities of all parties. It is also used as the basis for the CSA Assessor to provide support and consultancy to each integrator in order to assist them to achieve certification. The model shown below was used during the case study.

9.1 Training in Functional Safety Management and Recommended Lifecycle Procedures

The purpose of this training module is to present the recommended safety lifecycle model, FSMS procedures and specific examples to the integrator such that they have a clear understanding of the intent and purpose

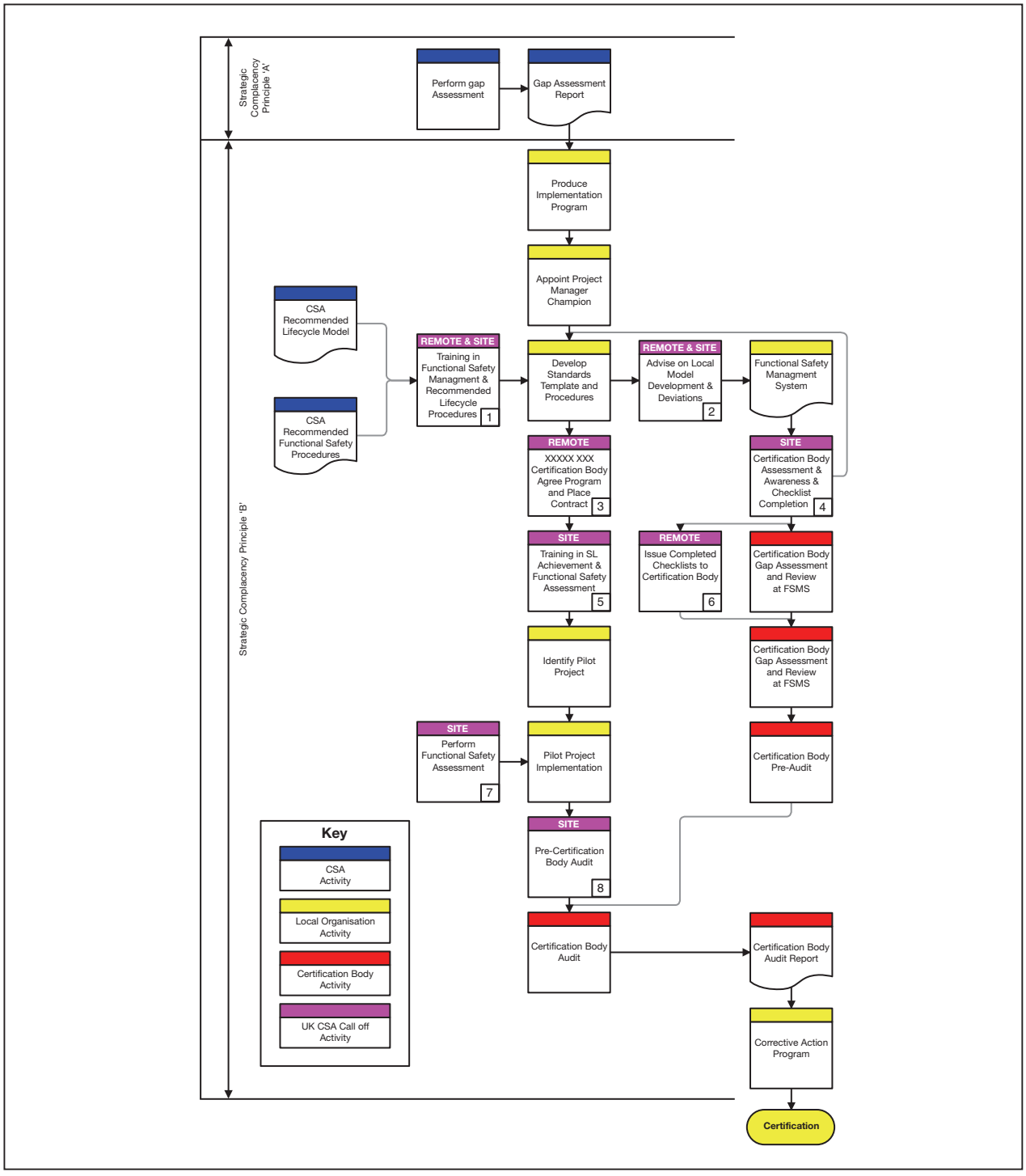


Figure 3: The Certification Process (see Appendix, page 31 for larger version)

of the FSMS and its implementation within their organization. This allows the integrator to develop their local procedures based on a working model. It will also cover the certification process and alignment to IEC 61508 and IEC 61511. (See section 10 below for a description of the training modules).

At the conclusion of the training module, the integrator is presented with a copy of the training material, the recommended safety lifecycle model, and the suite of generic procedures. (See section 3.8).

9.2 Advise on development / deviations for integrators' use of procedures
The CSA provides advice to the integrator on the implementation of the FSMS, development of their own FSMS procedures and answers technical queries on procedures, templates and other documents.

The integrator then has the option of making alterations to the generic suite of FSMS procedures to align with existing requirements and local business systems. The CSA will provide advice on the impact of these deviations on the FSMS and the recommended certification process.

9.3 Liaison with the Certifying Authority
The CSA directly liaises with the certification body to agree a formal program of work and place a contract on behalf of the organization for the agreed scope of work. The scope and program is confirmed and agreed with the organization prior to order placement.

9.4 Certification Body Assessment Awareness and Checklist Completion
The purpose of this training module is to provide the organization with an overview of the certification body's own detailed certification process.

Following on from the training module, the CSA and the integrator prepare the certification body's compliance checklists (including any deviations), which are required as part of the certification process.

Once completed, the CSA will issue the checklists to the certification body Lead Assessor for review. At the same time, the organization will issue its FSMS procedures to the certification body. In parallel, the integrator identifies a pilot project or projects to demonstrate that the safety lifecycle and FSMS is being implemented in its entirety. The pilot project(s) will be audited by the certification body.

9.5 Training in SIL Achievement and Functional Safety Assessment
The purpose of this training module is to provide the integrator with a detailed understanding of the methodology adopted in order to prepare a SIL Achievement Report for a safety project. This will include several worked examples, and prepare the safety engineers for the pilot project implementation.

The training module will also address the scope and purpose of Functional Safety Assessments and Audits, and commence development of a plan of the assessment activity for the pilot project (see section 10, page 28).

9.6 Perform Functional Safety Assessment
As part of the CSA's responsibilities, a functional safety assessment is performed on the pilot project.

9.7 Pre-Certification Body Audit
In order to ensure the success of the certification site audit, the CSA will perform a pre-audit to identify any potential risks or omissions from the FSMS and/or the pilot project. This gives the integrator the opportunity to correct these deficiencies before the official certification audit, hence ensuring that the certification audit results in a successful outcome.

10.0 TRAINING COURSES

Technical training was an essential part of the implementation program and the competency management system for the organization. Training is one of the four attributes of competence (see Section 5). Two technical training courses were developed by the CSA suitable for delivery to business units working to the core set of the pre-requisites earlier defined (see Section 4).

In the case study, these technical training courses were delivered to the organization with a period of six weeks separating them. The contents of these courses are set out below:

10.1 Functional Safety Management & recommended lifecycle procedures

A two day course consisting of the following topics:

- The certification process
- Overview of IEC 61508 and IEC 61511
- Functional Safety Management and links to QMS
- Safety lifecycle planning and management – the safety lifecycle model, inputs, outputs, deliverables
- Requirements and design
- Overview of SIL Achievement
- Verification & Validation
- Functional safety audit and functional safety assessment
- Course exercises

10.2 SIL achievement & Functional Safety Assessment

A 1.5 day course consisting of the following topics:

- Safety function and safety integrity requirements
- Design essentials of IEC 61508, hardware safety integrity and systematic safety integrity
- SIL compliance to IEC 61508
- SIL achievement procedure, worked example and exercise
- Functional safety assessments in the context of SIL achievement

11.0 ESTABLISHING SUPPORTING ACTIVITIES

Prior to and during the case study, there was already in place a large internal company network of safety practitioners with different safety objectives and operational safety standards.

Other internal businesses had developed future plans for certification.

Consequently it was essential to establish, at an early stage in the process, a common repository for information exchange.

This was achieved 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
- Latest FSMS procedures
- External functional safety standards
- Sales and technical product material
- Case study progress and program updates

12.0 MANAGING CHANNEL PARTNERS AND THIRD-PARTY INTEGRATORS

The same rigorous approach to functional safety had to apply to any third-party integrators being used by any of the company's integrators. This ensured the safety and quality of the third-party integrator. A program of work was required to perform a gap assessment on third-party integrators and to subsequently work with them to ensure that they developed a compliant functional safety management system, preferably in line with that of the main system vendor. This process has been seen to benefit the third-parties in that they can also achieve certification and capitalize on the achievement in the safety market place.

13.0 FINAL COMMENTS AND CONCLUSIONS

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 of the organization as a positive step forward.

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

The case study described above provides details relating to implementation of an organization's generic processes, methodologies and procedures and then how these were applied to a specific safety integration group within the organization. It outlines a step-wise approach covering:

- Strategy
- Benchmarking and gap assessment
- Developing the functional safety management system
- Selecting the certification body
- Implementing the functional safety management system
- Rolling out the certification process

Successful implementation of a certification program provided advantages to the organization, not least:

- Limiting the company's exposure to potential liabilities
- Demonstrating due diligence
- Implementing repeatable and cost effective safety management systems (procedures, techniques, tools etc)
- Reducing unnecessary and costly pre-contract discussions and evidence gathering – actually benefiting both the organization and its clients
- Winning work cost effectively
- Limiting effort (and cost) in developing so-called bespoke project safety procedures
- Gaining competitive advantage and as a result securing more business

The author hopes that the information provided in this chapter will benefit other organizations and individuals with an interest in functional safety management and certification.

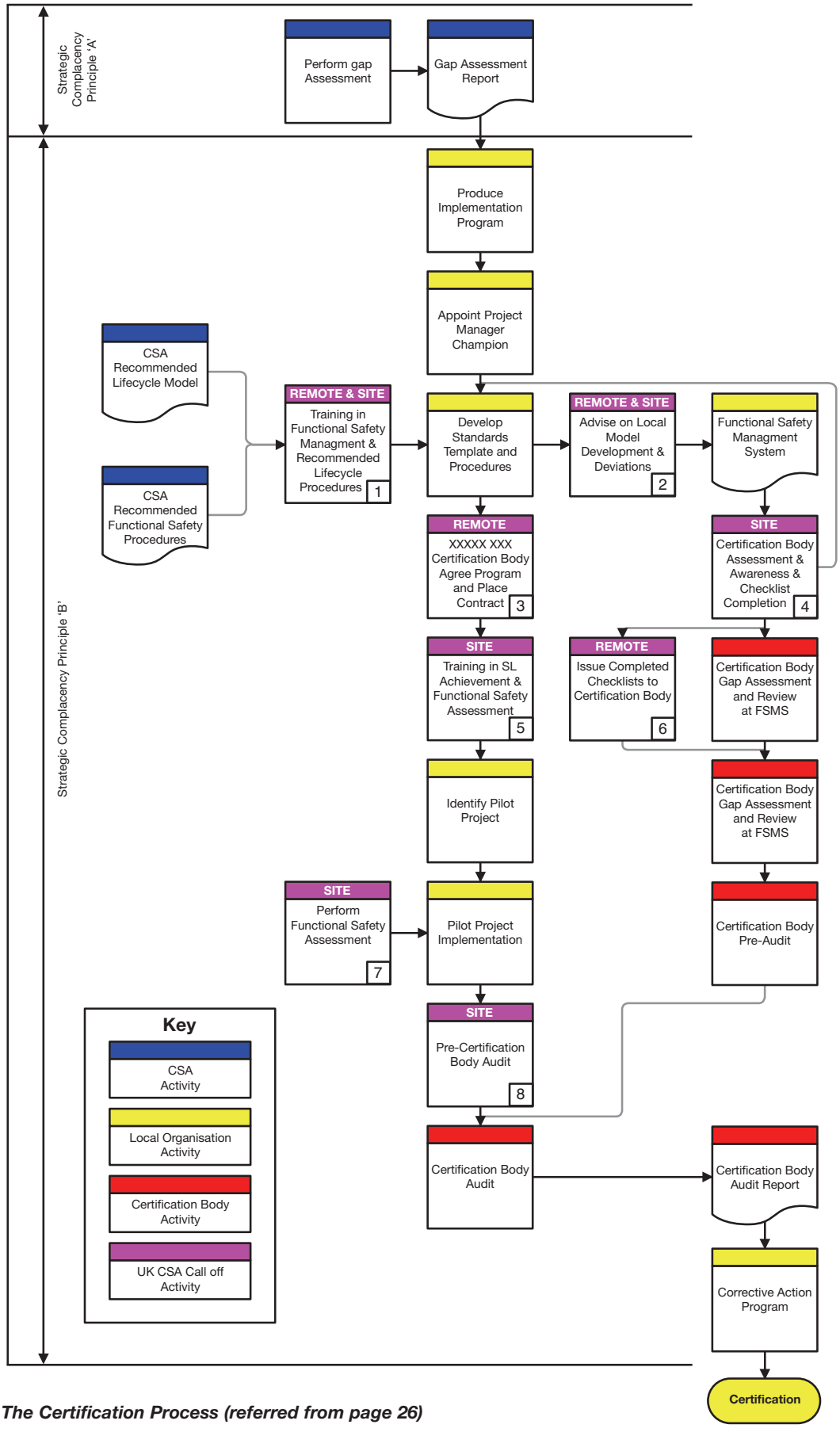


Figure 3: The Certification Process (referred from page 26)

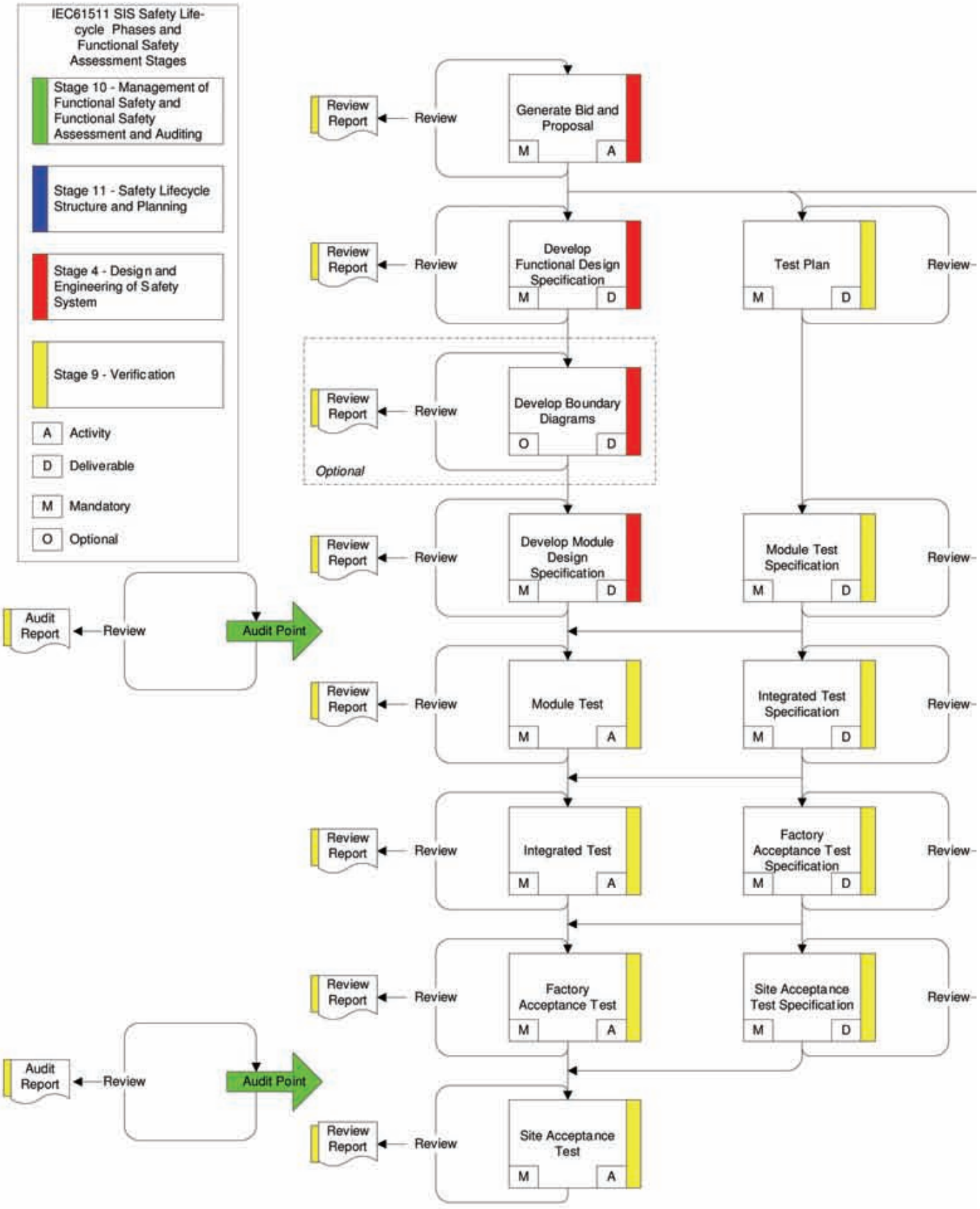
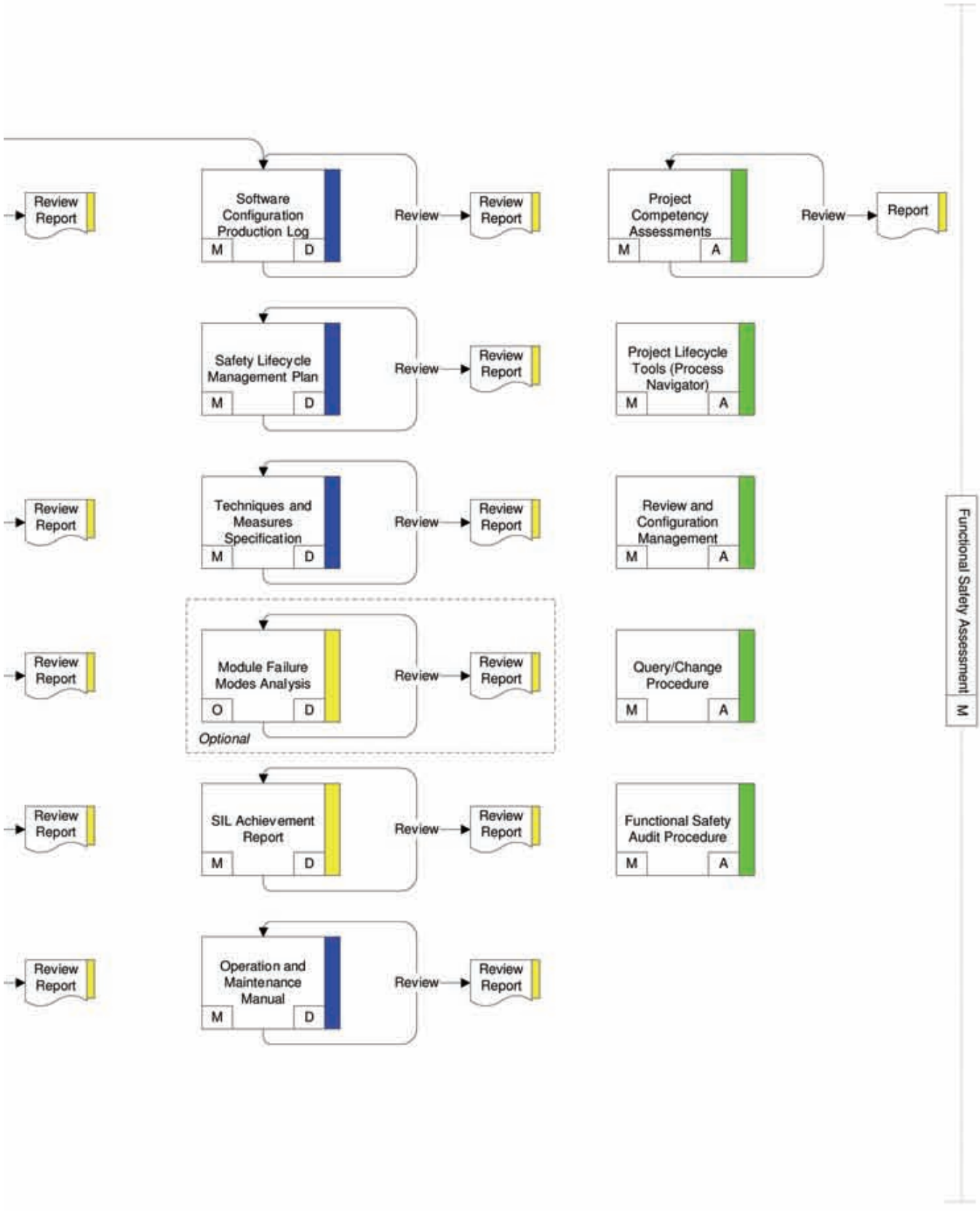


Figure 2: The Safety Lifecycle Model (referred from page 15)


Review Report
Software Configuration Production Log
M
D
Review
Review Report
Project Competency Assessments
M
A
Review
Report
Safety Lifecycle Management Plan
M
D
Review
Review Report
Project Lifecycle Tools (Process Navigator)
M
A
Review Report
Techniques and Measures Specification
M
D
Review
Review Report
Review and Configuration Management
M
A
Review Report
Module Failure Modes Analysis
O
D
Review
Review Report
Optional
Query/Change Procedure
M
A
Review Report
SIL Achievement Report
M
D
Review
Review Report
Functional Safety Audit Procedure
M
A
Review Report
Operation and Maintenance Manual
M
D
Review
Review Report
Functional Safety Assessment
M

REFERENCES

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

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

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

[4] “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

[5] IEC 61131 – Programmable Controllers

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

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

ABOUT THE AUTHOR

Stuart R Nunns CEng, BSc, FIET, FInstMC - Principal Safety Consultant ABB Ltd

Stuart Nunns has thirty-six years' experience in automation and safety within the oil & gas, chemical, steel and electricity generation sectors and is a Principal Consultant within the Safety Lead Competency Centre of ABB's Process Automation Division. Nunns is a member of ABB's Safety Steering Team, responsible for identifying and managing the development of functional safety products and services, mapping the total safety lifecycle. He is currently leading a global work program within ABB to establish TUV certified Safety Execution Centres.

Nunns is a TUV Functional Safety Expert and member of the IET Functional Safety Professional Network Executive Group and the InstMC's Safety Panel. He has written and presented papers and led international safety-related systems workshops. He was project manager of both the CUIG (Framework IV) European safety group and the F/W V SIPI61508 EC Framework V project developing guiding principals for the implementation of IEC 61508.

Within the UK he was the instigator and project manager of the CASS (conformity assessment of safety systems to IEC 61508) scheme and served as a Director of CASS Ltd.

Functional safety handbook/June 08

ABB Limited
Howard Road
Eaton Socon
St Neots
Cambridgeshire
PE19 8EU
Tel: 01480 475321
Fax: 01480 217948
www.abb.com