Functional Safety Assessments & IEC 61508 Development of a competency scheme for functional safety assessors

Stuart R Nunns BSc, CEng, FIET, FInstMC
ABB Ltd

1.0 Introduction

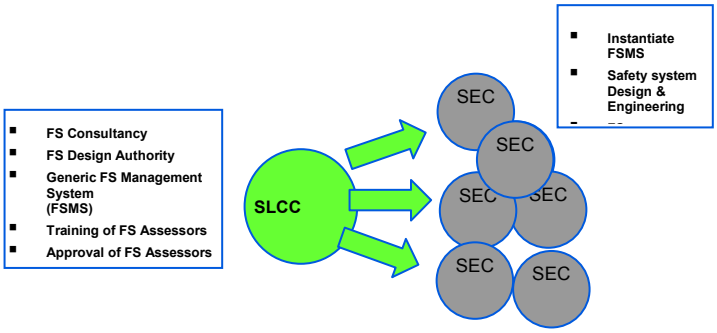
Functional Safety Assessments (FSAs) are undertaken in addition to the traditional safety lifecycle activities of verification, validation and functional safety audits. These safety lifecycle activities are typically planned and executed directly by the safety-related systems project team implementing phase(s) of the safety lifecycle. The purpose of a FSA is to independently ensure that functional safety has been achieved within the specific scope of supply for the organisation(s) in the context of the safety lifecycle.

Performing FSAs requires staff to have a high level of knowledge of IEC 61508 [Ref 1] & IEC 61511[Ref 2] combined with assessment experience who can ensure a careful balance between subjectivity and objectivity. This paper describes the approach taken by ABB in developing a competency scheme for functional safety assessors who operate in ABB's global Safety Execution Centres (SEC's)

2.0 Functional Safety Management within ABB

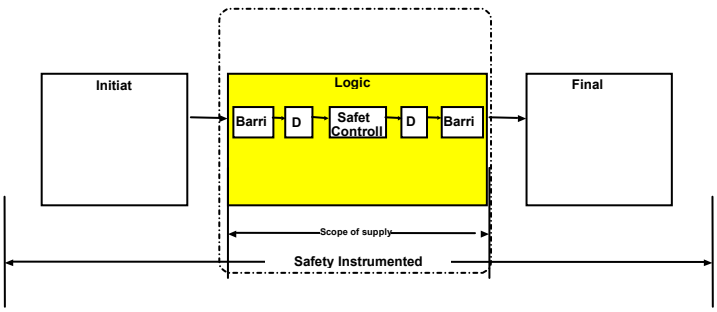
ABB is a global company who engineer safety-related systems through SEC's located in 25 countries around the world. These SEC's work to a Functional Safety Management System (FSMS) that is compliant and certified to IEC 61508/IEC61511. The SEC's are supported by a corporate functional safety authority, the Safety Lead Competency Centre (SLCC). Figure 1 below outlines the relationship between the SEC's and the SLCC.

Figure 1 – SEC and SLCC responsibilities



Recognising the importance of competency as an integral part of this functional safety management system, ABB developed a competency framework for functional safety assessors drawing on *good practice* competency guidance by way of the IET [Ref 3], IET/BCS [Ref 4], HSE [Ref 5] and the CASS Scheme [Ref 6]

Safety-related projects are engineered in accordance with a safety life cycle mapped across to IEC 61508 Phase 5 and IEC 61511 phase 4. In the context of the end-to-end safety instrumented system, the SEC's are typically responsible for the logic solver subsystem as shown in the following figure.



Each safety project is subject to two functional safety audits and a functional safety assessment performed at three stages of the safety design and engineering activities. Safety projects can be 'green field' and 'brown field' and linked to on-going support contracts involving modifications to existing safety systems. The audits are performed by the SEC QA function and form an integral part of the SEC's ISO 9001 certification. The functional safety assessments are performed by competent 'independent-from-project' functional safety assessors in accordance with the requirements of the standards.

3.0 The FS Assessor competency scheme

As stated in section 2 an SEC engineers safety-related systems in accordance with the requirements of IEC 61508 Phase 5 and IEC 61511 Phase 4. However, one of the challenges faced by the company was to develop a competency scheme for FS assessors which could be rolled out across all of the company's 25 SEC's, which was cost effective, easily managed and represented a pragmatic interpretation of the requirements of the standards. It had to have the support and endorsement of each of the SEC's senior management. FS assessments and the responsibilities of the FS assessors had to align to the requirements of the standards. Because the SEC's work predominantly in the Oil, Gas and Petrochemical sectors, the decision was taken to use IEC 61511 as the applicable standard for guidance on performing functional safety assessments.

Candidate FS assessors have to meet minimum eligibility requirements:

- To be actively working within an SEC using the compliant FSMS
- To have previously attended ABB University courses on FS management, IEC 61508/61511 and SIL Achievement
- To have a minimum of 2 years in safety projects

Additional desirable eligibility requirements are:

- TUV FS Eng qualification
- Experience in auditing
- Education to degree level

Candidates are then required to provide a detailed Curriculum Vitae, focussed on functional safety detail including:

- Qualifications
- Training (courses, seminars, conferences)
- Publications
- Additional relevant experience (e.g. control systems, oil & gas, petrochemical, chemical, reviews and auditing)
- A comprehensive list of safety projects undertaken, covering:
    - Project description and scope
    - Responsibilities and key work activities
    - Application (e.g. F&G, ESD, BMS)
    - SIL rating
    - Complexity and novelty of technology

The IET and IET/BCS were used to assist in identifying core competencies relevant to these phases of the safety lifecycle. These were then reviewed and developed into a set of core competencies tailored to the specific role and organisational model in use within the SEC's resulting in the following set of core competency requirements:

- Domain and safety related knowledge
- Project execution and review
- System architectural design
- System hardware realisation
- System software realisation
- Verification and validation
- Safety-related system operation, maintenance and modification

Each of these core competencies has associated *tasks and attributes* – with guidance notes. Candidate FS assessors are required to provide supporting evidence against each of these core competency requirements, in particular their knowledge, experience, training and qualifications.

The information provided by the assessor is reviewed by the SEC manager and also by the company's global FS manager within the SLCC. If required, an interview may be necessary (local or remote) to establish more details of the experience and knowledge.

The tables below provide extracts from the competency proforma

Core Competency – Extract from Domain & safety knowledge		
Associated tasks & attributes	**Description**	**Context statement (supporting information to qualifications, training, knowledge & experience)**
Domain knowledge	Has knowledge and understanding of the oil & gas industry. General knowledge of processes, plants, hazards and operational environment	
Principles of functional safety practices & assurance	Has a basic knowledge and understanding of functional safety practices and principles of functional safety assurance, hazard & risk assessment, ALARP	
Interpreting safety requirements	Can understand and interpret safety requirements in order to devise an implementation strategy and develops functional design specifications based on those requirements	
Core Competency – Extract from system architectural design		
Associated tasks & attributes	**Description**	**Context statement (supporting information to qualifications, training, knowledge & experience)**
Partitioning safety requirements	Can partition safety requirements into individual subsystems and functions so that the overall safety requirements can be met	
Evaluating solutions	Can evaluate architectural design solutions against performance criteria to provide a safety-compliant solution	
Specifying safety-related system architecture	Can specify a system architecture that meets the safety requirements in both hardware and software	
Knowledge of ABB safety technology	Has knowledge of ABB safety technology, safety manual and reliability handbooks, and practical experience in at least one safety platform	

Core Competency – Extract from system software realisation		
Associated tasks & attributes	**Description**	**Context statement (supporting information to qualifications, training, knowledge & experience)**
Interpreting safety requirements for system software design and engineering	Can interpret safety requirements and determine whether these are complete and feasible for transposing into software design	
Transposing requirements into software design	Can produce software design specifications based on safety requirements, that are coherent, clear and testable and recognise software constraints	
Producing and analysing code	Can translate a software functional design specification into modular, understandable and analysable source code using a relevant programming language (e.g LVL(	

Core Competency – Extract from Verification and Validation		
Associated tasks & attributes	**Description**	**Context statement (supporting information to qualifications, training, knowledge & experience)**
Defining safety verification and validation planning incorporating suitable test and analysis activities	Has knowledge of a range of relevant test and analysis methods and measures for safety assurance, and insight for applying them into a general	

	verification and validation plan and specifications. Can develop a V&V plan and produce stage specific specifications for different V&V phases; e.g. IAT, FAT, SAT	
SIL analysis	Can develop and interpret SIL achievement reports congruent with the safety requirements specification, FDS and the scope of supply. Can interpret and analyse SIL achievement reports.	
Specifying software tests	Can produce software test specifications congruent with the test stage, which can detect systematic errors and omissions on the software functionality through the use of appropriate methods and techniques	

On completion of this information and subject to the candidate having achieved a specific threshold, they are nominated as '*Provisional FS Assessors'*.

The next stage is for the candidate to attend a three-day training course on performing functional safety assessments. The objectives of the course are to:

- Develop core competencies in functional safety assessment
- Train candidates in the ABB functional safety assessment process, methodology and reporting
- Provide an understanding of the impact FS assessments have on a safety project
- Introduce the techniques used in performing FS assessments
- Overlay the FS implementation points to the safety lifecycle model and the specific processes and deliverables to be assessed at implementation points

The course is intended to reinforce the attendees' knowledge in the FSMS and to develop the following safety assessment related skills.

Skills	**Description**
Scope and context appreciation and strategy selection	Can identify the safety scope of the project and its context, and determine the best assessment strategy
Assessment Planning	Can develop plans for assessing a project based on its scope, size and context
Safety auditing & eliciting information	Can perform an assessment using audit techniques using a non-confrontational but tenacious style for soliciting evidence
Reviewing safety documentation	Can review systematically and accurately safety-related documentation, identifying the main features and issues
Forming a judgement	Can make an unambiguous judgement with a reasoned argument on whether safety objectives have been achieved
Report writing	Can produce reports with accuracy, logical structure and a plain comprehensible style
Assessing safety analysis	Can assess safety analysis documents in order to judge safety compliance, identify issues and the need of further safety analyses. Can make a judgement and constructing logical arguments for safety compliance
Managing outcomes & monitoring compliance	Can manage and track effectively results of a safety assessment, such that necessary corrective actions and recommendations are implemented
Knowledge of safety regulations and standards (regulatory and legal compliance)	Has knowledge of relevant safety regulations, focussed on IEC 61508/61511 compliance, and can determine whether requirements have been met, included lifecycle management, hardware and software realization
Principles of functional safety practices & assurance	Has a knowledge and understanding of functional safety practices and principles of functional safety assurance (hazards, risk, ALARP, safety principles, etc.)
Principles of functional safety management specific to SEC	Has a knowledge and understanding of the SLCC recommended safety lifecycle and FSMS
Methodical approach	Can select and apply relevant methods to plan, execute and complete the assessment process
Team working	Works well within a team, leading assessment meetings and creating a collaborative environment
Professional standing and personal integrity	Has a level of personal standing sufficient to give credibility to judgements on safety assessments, and a verifiable record of personal independence and integrity
Attention to accuracy and detail	Recognize incomplete, inaccurate and misleading pieces of information design and test specifications and reports

The course duration is three days, two thirds of this time requires attendees to work in break-out groups performing functional safety assessments on an actual safety project (sanitised and seeded with errors and omissions) and to feedback their findings. In addition there are a number of individual multi-choice exercises for course candidates to complete to a satisfactory level.

Candidates are provided with checklists and guide-words to assist them in performing future assessments. However, these are provided as an aide memoir and should not be used to drive the assessment.

Following attendance at the training course a mentoring process commences whereby the global FS Manager and his core team of FS

Assessors will act as observers at an agreed number of FS assessments undertaken by the individual assessors within their SEC. This process will provide feedback on the planning, performance, analysis and recording of findings. After an agreed number of mentoring assignments the FS Assessors will have there status changed from '*Provisional FS Assessor'* to '*FS Assessor'*. This allows the assessor to undertake FS assessments within their local SEC and also if required within other SEC's operating as a cluster within defined regions of the world.

Finally, it is planned to organise annual meetings of FS Assessors to enable them to exchange experiences, findings and suggestions for improvements to the process itself.

4.0 Conclusions

When operating in the safety-related systems domain, organisations need to recognise the importance and relevance of the competency of individuals and teams. The competency of those involved in the assessment of functional safety is equally, if not more important, as the competency of those engineering such systems. FS Assessors operate with a high level of independence and impartiality and need to demonstrate professionalism and integrity in the tasks they are asked to perform. Their recommendations on the achievement of functional safety of a safety-related system and project can have significant impact on not only the project but the organisation as a whole. Independent FS Assessments provide an additional level of assurance to clients and regulatory authorities.

This paper is designed to provide the reader with an overview of the approach taken in the development of a competency framework for FS Assessors within the global safety organisation. It is a major exercise in its own right and requires commitment of resources and support from senior management. Measure need to be put in place to ensure continuous feedback from the FS Assessors enabling improvements to be made to the implementation of these assessments.

References

1	**IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems**
2	**IEC 61511 Functional safety – Safety instrumented systems for the process industry sector**
3	**IET Competence criteria for safety-related system practitioners**
4	**IET/BCS Competency Framework for Independent Safety Assessors (ISAs)**
5	**HSE Managing competence for safety-related systems**
6	**The CASS Assessor Competency Scheme**