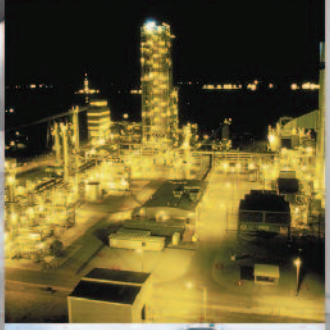
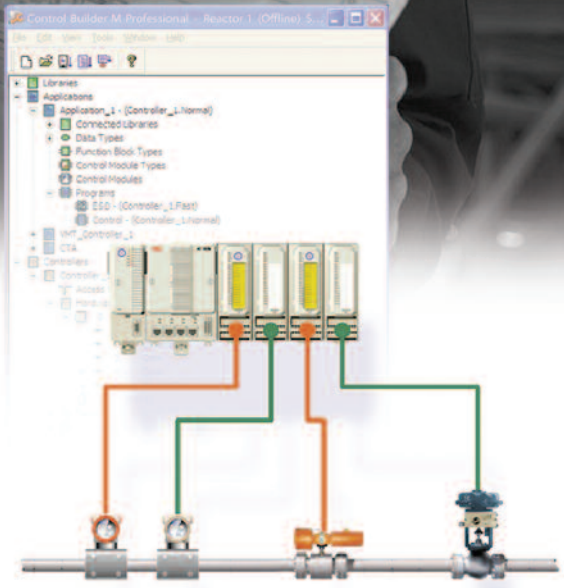


# Functional safety assessment

Part 1 - Setting the boundaries of the FSA, defining the scope and planning the FSA.




ABB

# CONTENTS




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

# 1.0 INTRODUCTION

To many readers, Functional Safety Assessments (FSAs) will be a new topic in the area of functional safety. Even those who have read and understand the key features of IEC 61508 [1] and IEC 61511 [2] may not be fully conversant with the specific details of the FSA activity, aware that it is a mandatory (shall) requirement if one wishes to claim compliance to IEC 61508 or have actually implemented FSAs and reaped the benefits.

FSAs are undertaken in addition to the traditional activities of verification, validation and functional safety audits. These activities are typically planned and executed directly by the Safety-Related Systems project team implementing phase(s) of the safety lifecycle. The FSA is performed and specific to ensuring that functional safety has been achieved within the specific scope of supply for the organisation(s) in the context of the safety lifecycle. For a typical systems integrator this scope of supply is the provision of the logic solver sub-system only within the end-to-end Safety-Related System. For an Engineering Procurement and Construction (EPC) company this is typically the end-to-end Safety-Related System, consisting of the input subsystem, logic solver subsystem and final element (output) subsystem.

IEC 61508 and IEC 61511 both have clauses specific to FSAs; For IEC 61508 this is Part 1 clause 8 and for IEC 61511 Part 1 clause 5.2.6.1. However, there are differences in the approach and recommendations which need careful interpretation by those seeking to implement FSAs. Performing FSAs requires staff with a high level of competency and are more often than not based on subjectivity, particularly when applied to earlier phases of the safety lifecycle. The FSA assesses if appropriate methods, techniques and processes have been used to achieve functional safety.

This guide, consisting of two parts, provides the reader with details of an FSA process methodology and FSA reporting mechanism designed and implemented by the author and in use across ABB's global Safety Execution Centres (SECs). These SECs all have IEC 61508 compliant Functional Safety Management Systems (FSMS) and are progressively being certified by TUV Rheinland. They implement safety system solutions for clients that focus on integration and configuration of the logic solver subsystem. It is a requirement of this compliance and certification that these SECs implement FSAs.

In this first part of the guide, we look at how to define the boundaries of the FSA in the context of the safety lifecycle model, organisational scope and responsibilities and levels of independence. We then move on to discuss the differences between audits and functional safety assessments and then how to plan a functional safety assessment.

# 2.0 SETTING THE BOUNDARIES OF THE FSA

One of the first activities to be performed when developing an FSA methodology is to clearly define the scope of supply for the organisation which wishes to implement FSAs. This scope of supply has to be set in the context of those other organisations involved in the safety lifecycle and in particular, those organisations implementing phase(s) immediately before and after those defined in this scope of supply. In the first instance, this requires a full understanding of the requirements of IEC 61508 Part 1, clause 8 which provides information relating to when, how, who and why in addition to the levels of independence required of the organisation and staff implementing the FSAs.

The relevance and importance of defining this scope of supply for an organisation is obvious when read in conjunction with IEC 61508, Part 1, clause 8.2.3 *'the functional safety assessment shall be applied to all phases throughout the overall E/E/PES and software safety lifecycle'. Similarly, the relevance and importance of the role of other organisations and the interfaces is apparent when read in conjunction with clause 8.2.3 'those carrying out the functional safety assessment shall consider the activities carried out and the outputs obtained during each phase of the overall, E/E/PES and software safety lifecycles and judge the extent to which the objectives and requirements in this standard have been met'.*

*Also, clause 8.2.4, states 'the functional safety assessment shall be carried out throughout the overall, E/E/PES and software lifecycle, and may be carried out after each safety lifecycle phase, or after a number of safety lifecycle phases…….*

The scope of supply of an ABB SEC relates directly to IEC 61508 Phase 9 and IEC 61511 Phase 4 but within these phases is limited to the engineering and configuration of the logic solver subsystem and not the end-to-end safety instrumented system. This scope of supply includes a core set of pre-requisites:

- 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. Analogue Input module, Analogue 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 [3] 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 unauthorised modification
- Hardware consists of Safety-Related System 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 Safety-Related System 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

In addition to ABB's SECs which operate in each continent of the world, ABB established a Safety Lead Competency Centre (SLCC). This SLCC operates on behalf of ABB senior management and is responsible for:

- developing an IEC 61508 compliant generic functional safety management system (FSMS)
- rolling this out to each SEC for local implementation
- managing a global third-party IEC 61508 certification programme for each SEC
- providing functional safety training and consultancy to SECs and external clients
- acting as the independent safety authority for performing FSAs

A further key consideration is the level of independence of the organisation performing the FSA and by implication their assessors. The level of independence is defined in IEC 61508, Part 1, clauses 8.2.12 to 8.2.14 and IEC 61511 part 1, clause 5.2.6.1.2. On reading these clauses it is clear that the requirements in respect of independence are significantly different between the standards. IEC 61508 has very clear and mandatory (shall) requirements for independence based on consequences or SIL, the choice dependent on safety lifecycle phase(s). IEC 61511 proposes a more relaxed approach not dependent on consequences or SIL and not requiring rigidity in terms of organisational or department independence.

It is essential, therefore, before embarking on developing an FSA methodology that a decision is made as to which standard is to be used for compliance in the context of FSA. This decision may also be influenced by:

- which standard is being used for development of the FSMS
- the specific requirements of the third-party certification body if the organisation is seeking to achieve certification of its functional safety management system
- The organisational and management models operating within the company and how these impacts on levels on independence
- Availability of competent resources

In respect of ABB's SECs the policy was to implement FSAs in accordance with the requirements of IEC 61508. Therefore in order to comply with this requirement:

- FSAs shall be performed by resources under the direction of the Safety Lead Competency Centre (SLCC) for safety systems of SIL 3 capability in order to meet the independence and competency requirements of IEC 61508 – 1, Clause 8, Table 5.
- For SIL 1 & SIL 2 safety systems capability, FSAs can be performed by an independent person from within the SEC, provided that the person is independent from the safety system design and engineering team and is deemed competent by the SLCC to perform in the role of Lead Assessor. All FSA reports will be subject to review and approval by the SLCC. If this requirement cannot be met the UK SLCC shall perform the FSA.

In accordance with IEC 61508 Part 1, Table 5, HR1 was deemed appropriate and suitable due to the fact that each SEC:

- Has previous experience with similar designs
- Those safety systems being engineered and configured are based on standard certified safety platform technologies with LVL software and certified function/building blocks
- There is little or no novelty in the degree of design
- Standardised design features and attributes are the norm

# 3.0 SCOPE OF THE FSA

As stated in section 2 above, ABB developed a generic FSMS for local implementation by each SEC.

This FSMS specified a safety lifecycle model for use by each SEC. Integral to this model are the audit and FSA processes.

Figure 1 below provides an overview of this safety lifecycle model:

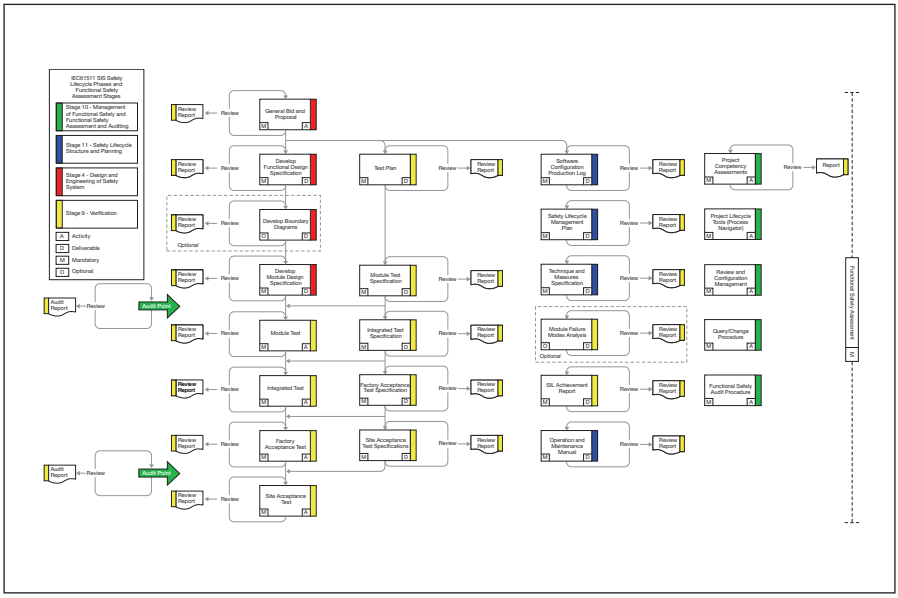



***Figure 1 SEC safety lifecycle model, larger version on pages 14 & 15***

For each compliant item, e.g. safety system logic solver, implemented by an ABB SEC an FSA is a mandatory requirement.

FSAs are performed in addition to verification, validation and functional safety audits, these are planned and executed directly by the SEC. The objective of the FSA is to ensure that functional safety has been achieved within the scope of supply for the SEC, i.e. provision of the logic solver sub-system only within the end-to-end Safety-Related System. It assesses if appropriate methods, techniques, tools and processes have been used to achieve functional safety.

The FSA includes amongst other things an analysis and review of:

- The safety instrumented system logic solver and whether it is designed, constructed, verified and tested in accordance with the safety functional design specification and whether any differences have been identified and resolved
- Whether the safety instrumented system logic solver validation planning is appropriate and the validation activities have been completed
- Project design change procedures to ensure they are in place and have been properly applied
- Whether SIL capability achieves the SIL target requirements
- Whether regulations, mandatory standards and any stated codes of practice have been met
- Development and production tools if used
- Adequacy and completeness of documentation

# 4.0 AUDIT AND FSA

**4.1 What do the standards say?**

An *audit* is a systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives:

- Procedures shall be defined and executed……
- There should be an:
  - Audit strategy
  - Audit programme
  - Audit Plan, reporting and follow-up

In contrast an *assessment* is an investigation based on evidence, to judge the functional safety achieved by one or more E/E/PES SRS:

- In the context of an ABB SEC, this is specific to the logic solver (IEC 61508 Phase 9 and IEC 61511 Phase 4)
- Procedure shall be defined and executed…….
- Judgement shall be made as to the functional safety and safety integrity achieved by the Safety-Related System
- Membership of the team shall include at least one senior competent person

**4.2 What are the differences?**

An *audit* is undertaken to ensure compliance with procedures. It is integral to a Quality Management System and ISO 9000. Auditors are not required to make judgements on the adequacy of the work they are considering and no specific judgement of functional safety and integrity.

In contrast, *assessment* involves assessors undertaking an evaluation and making a judgement, whether provisions are adequate for the achievement of functional safety and integrity. Assessments are outside the normal ISO 9000 scope and rely heavily on assessor judgements and competency. One of the inputs to the assessment process will be the audit processes and findings.

Assessments can span several organisations and the FSA activities can drill down to technicalities, reserving the right to redo activities.

Assessments performed in accordance with IEC 61508 demand prescriptive independence.

Having specified the scope of supply of an SEC, specifically Phase 9 of IEC 61508 and Phase 4 of IEC 61511 and documented the policy to comply with IEC 61508 for FSA, then the decision was made for one FSA to be performed for each safety system or logic solver. However, this FSA is performed at three key stages of the safety lifecycle:

- ***Preliminary FSA*** - Following completion of the Safety Lifecycle Management Plan and internal review of the Safety Lifecycle Management Plan. Figure 2 shows the preliminary FSA in relation to the safety lifecycle, processes and deliverables. The shaded areas identify the key inputs to this FSA stage.

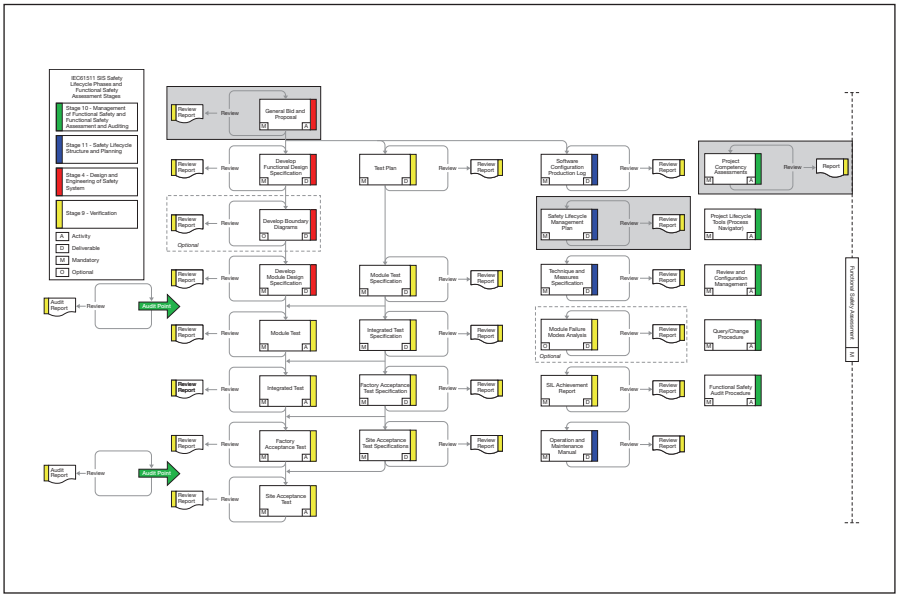



***Figure 2 Preliminary FSA, larger version on pages 16 & 17***

- ***Design FSA*** - Following completion of the Functional Design Specification (FDS), internal review of the FDS, and prior to approval by the client. Figure 3 shows the Design FSA in relation to the safety lifecycle, processes and deliverables. The light shaded areas identify the key inputs to this FSA stage and dark shading indicates activities/deliverables that are revisited following the preliminary FSA.

- ***Final FSA*** - Following Factory Acceptance Testing (FAT). Figure 4 shows the Final FSA in relation to the safety lifecycle, processes and deliverables. The light shaded areas identify the key inputs to this FSA stage and the dark shading indicates activities/deliverables that are revisited following the Preliminary and Design FSAs.

With respect to safety projects involving more than one logic solver/safety system, more than one FSA is likely to be required dependent on the:

- Duration of the project
- Number of safety systems implemented within the project
- Degree of commonality across the logic solvers

This would therefore require additional Design and Final FSAs.

The Lead FSA Assessor has the responsibility for preparing a Functional Safety Assessment Plan for the safety project. The plan is written to enable a systematic and comprehensive FSA to be performed and specifies the:

- Membership of the assessment team at each FSA stage. As a minimum, it shall include a competent Lead FSA Assessor and the Lead Engineer from the specific safety project
- Scope of the FSA. See section 2 of this guide for minimum requirements
- The skills, responsibilities and authorities of the assessment team
- The information that will be generated as a result of the functional safety assessment
- The identity of any other safety bodies and ABB Groups/departments involved in the assessment
- The means by which any follow-up recommendations shall be progressed
- The stage(s) within the safety life cycle when the FSA(s) will occur
- Degree of Independence in accordance with IEC 61508
- Schedule and estimated duration of the assessment
- Documents referenced at each FSA stage
- Checklist utilised at each FSA stage
- Findings and recommendations from each FSA stage

The plan is approved by the local SEC Manager and issued to all parties prior to the assessment-taking place. Only one plan is developed for the specific project FSA and this plan is effectively a 'living document' in that as each stage is completed the evidence reviewed, findings, conclusions and recommendations are added to the plan.

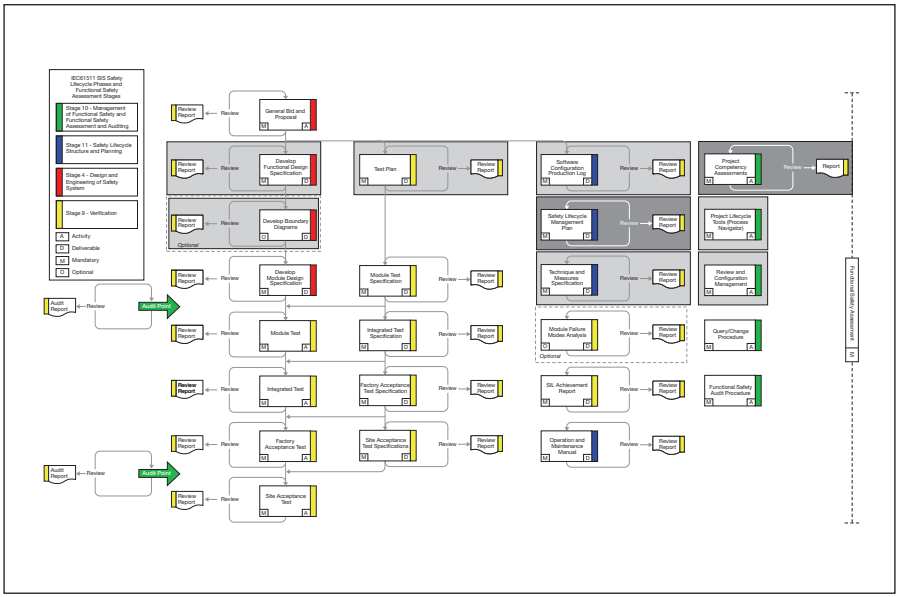



*Figure 3 Design FSA, larger version on pages 18 & 19*

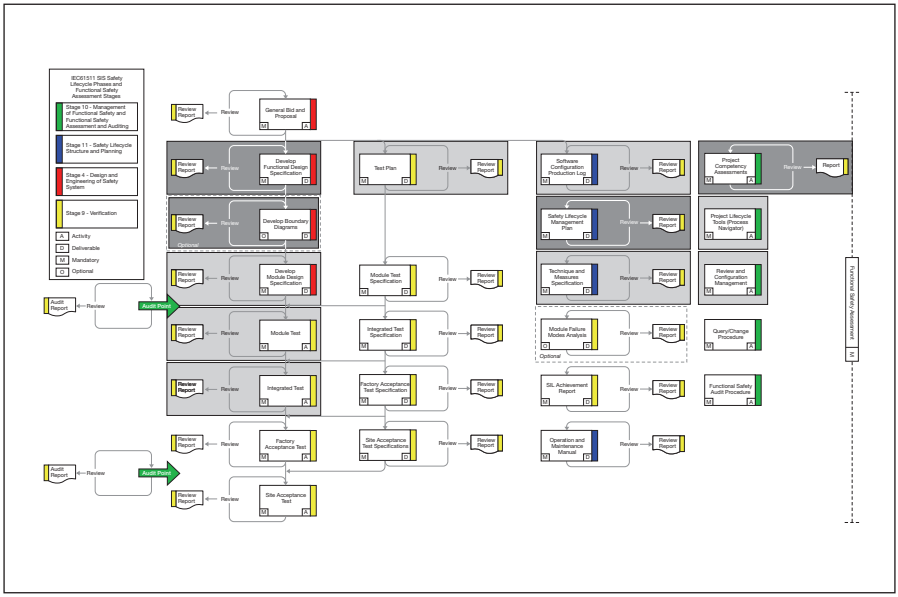



*Figure 4 Final FSA, larger version on pages 20 & 21*

# ALSO AVAILABLE

This document is the first of a two part series focusing on planning creating and implementing a Functional Safety Assessment programme. The second part is also available, covering:

**PART 2:** *Performing the Functional Safety Assessment, reporting and follow-up.*

# APPENDICES

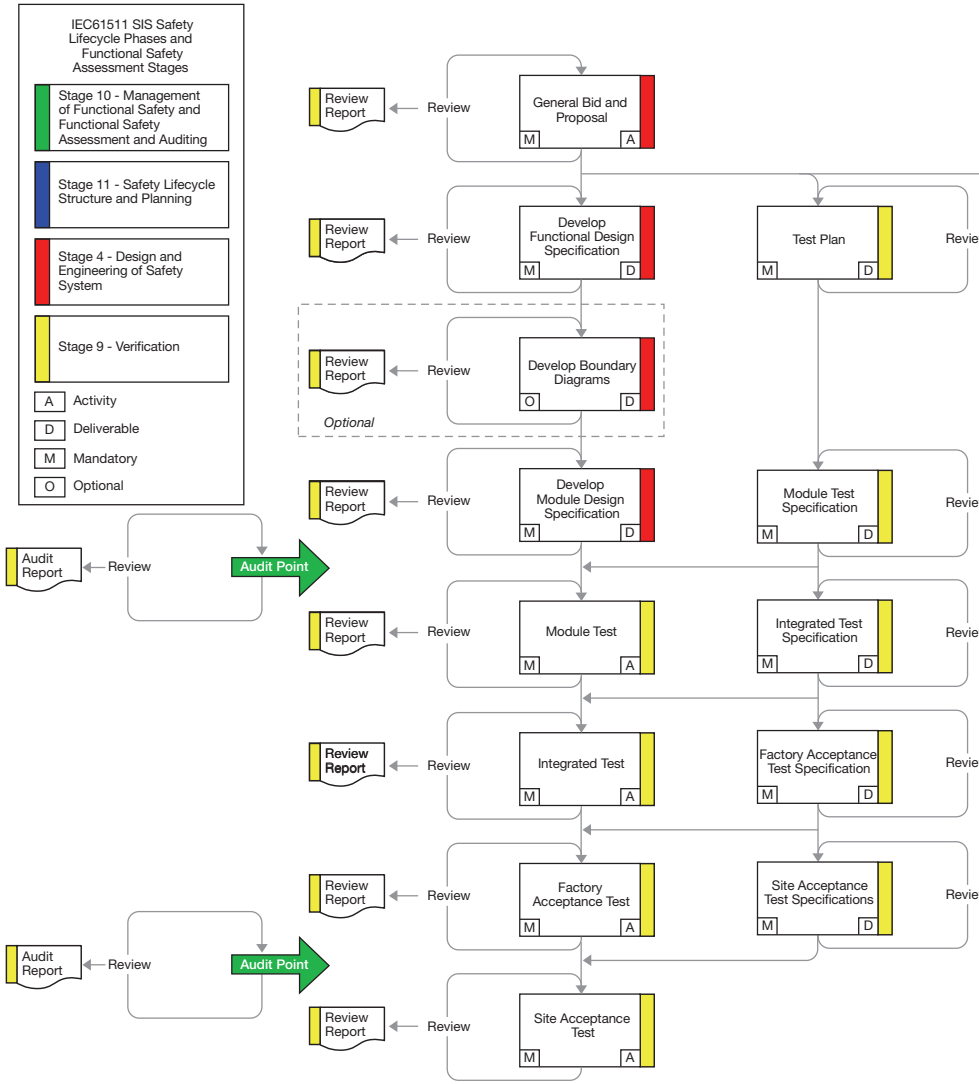
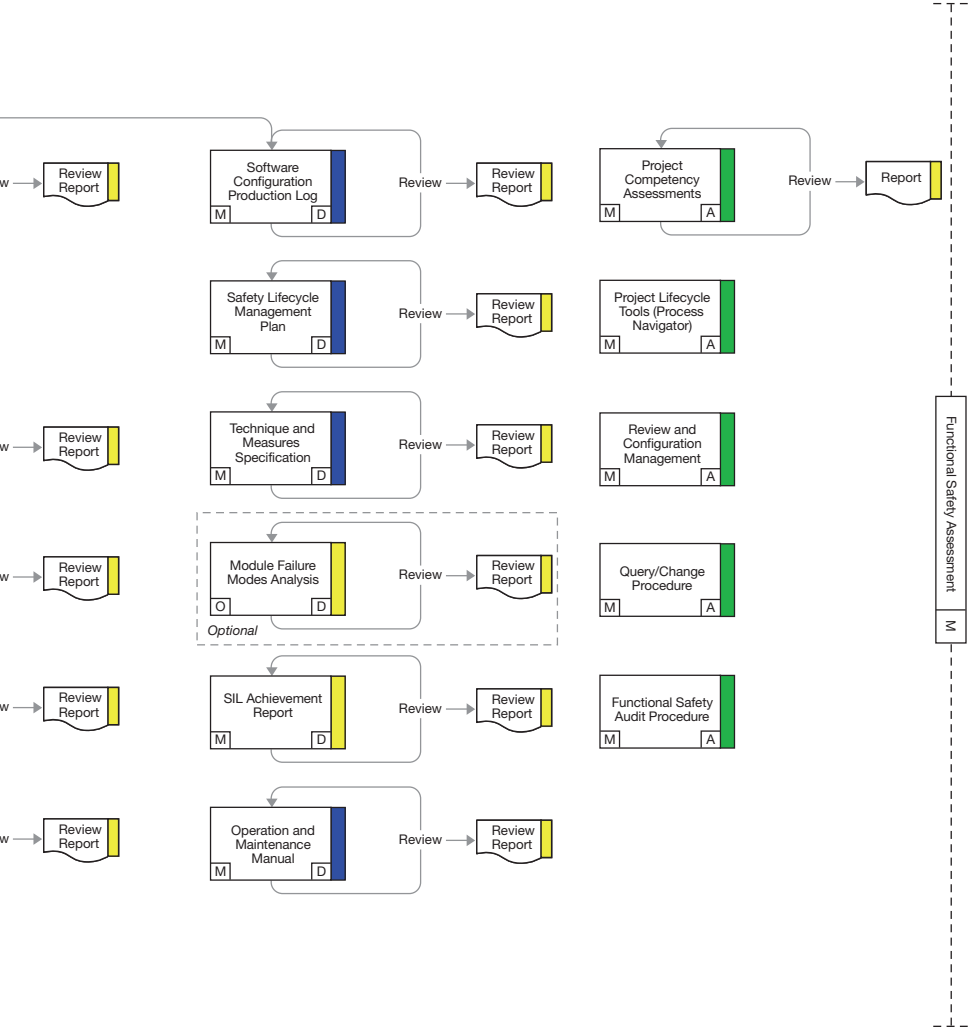



***Figure 1 SEC safety lifecycle model***


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
Technique and Measures Specification
M
D
Review
Review Report
Review and Configuration Management
M
A
Review Report
Module Failure Modes Analysis
O
D
Optional
Review
Review Report
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

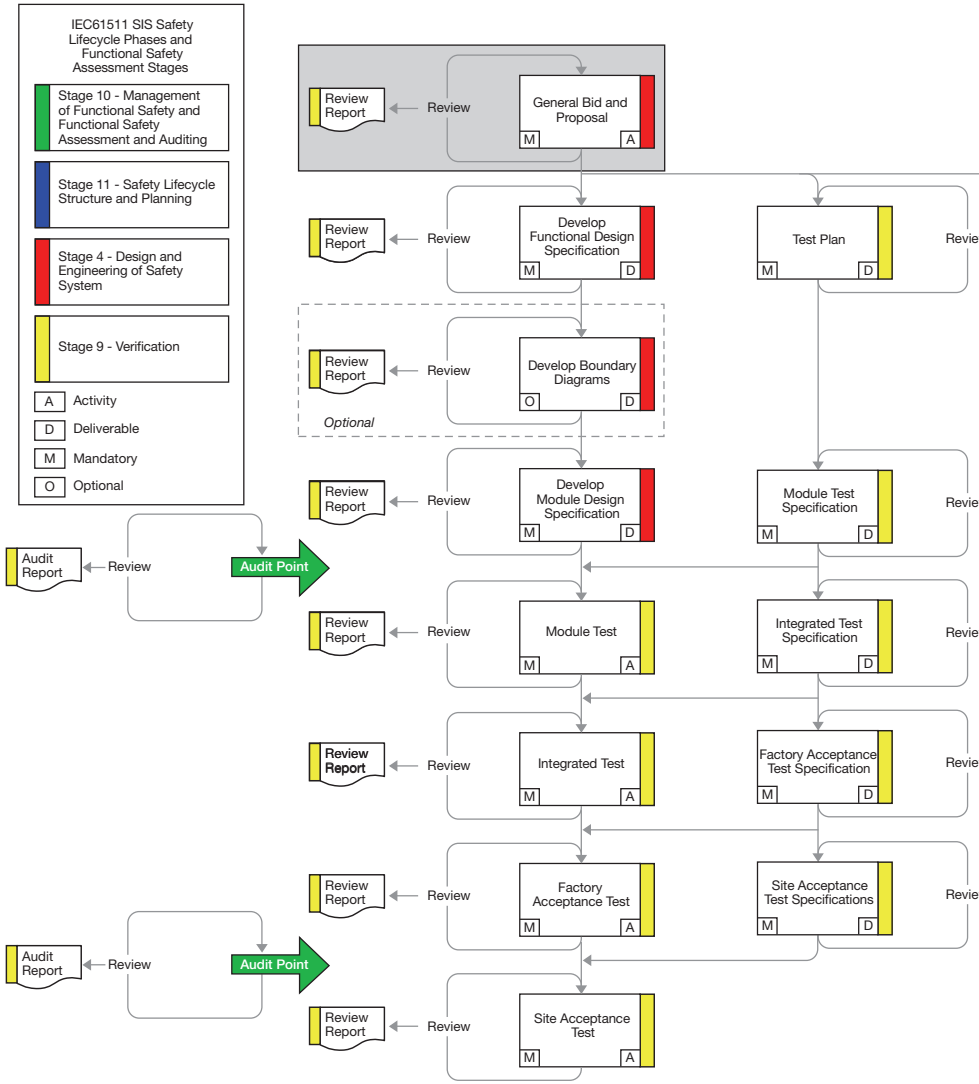
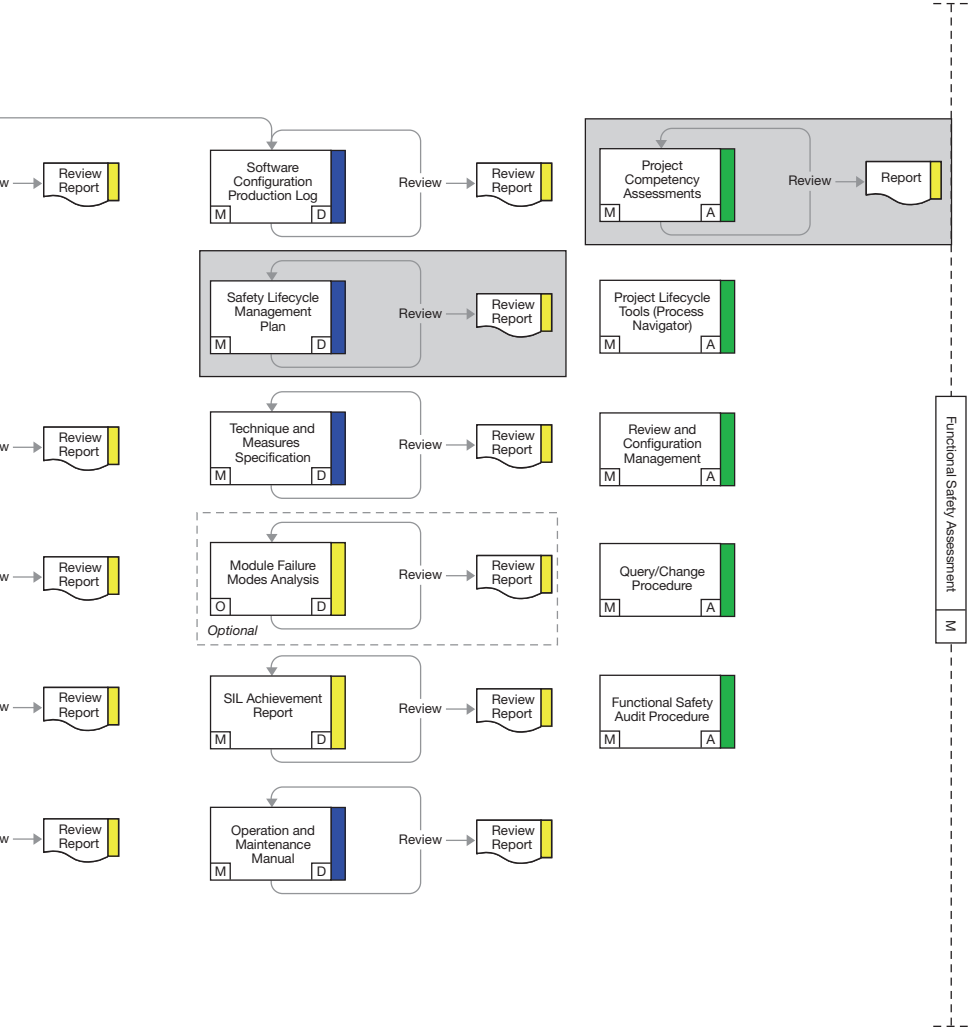



***Figure 2 Preliminary FSA***


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
Technique and Measures Specification
M
D
Review
Review Report
Review and Configuration Management
M
A
Review Report
Module Failure Modes Analysis
O
D
Optional
Review
Review Report
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

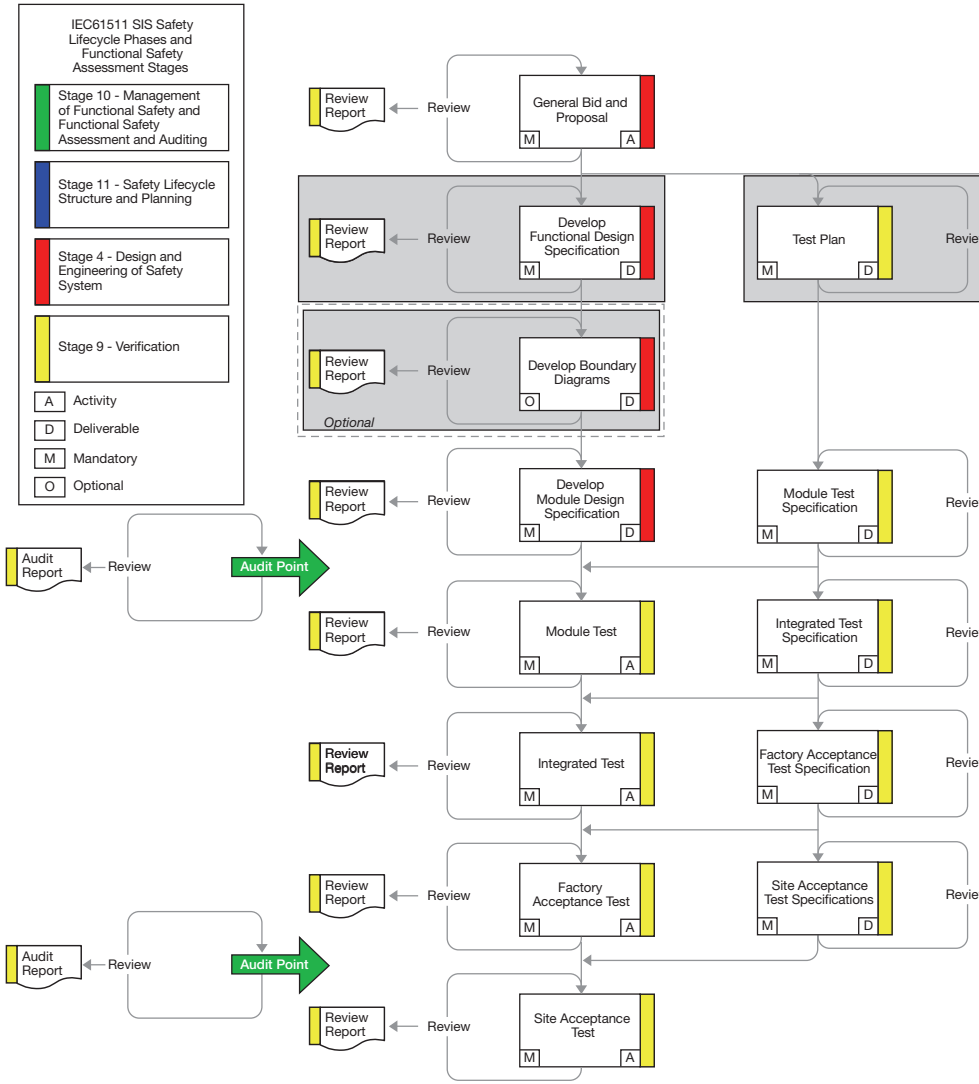
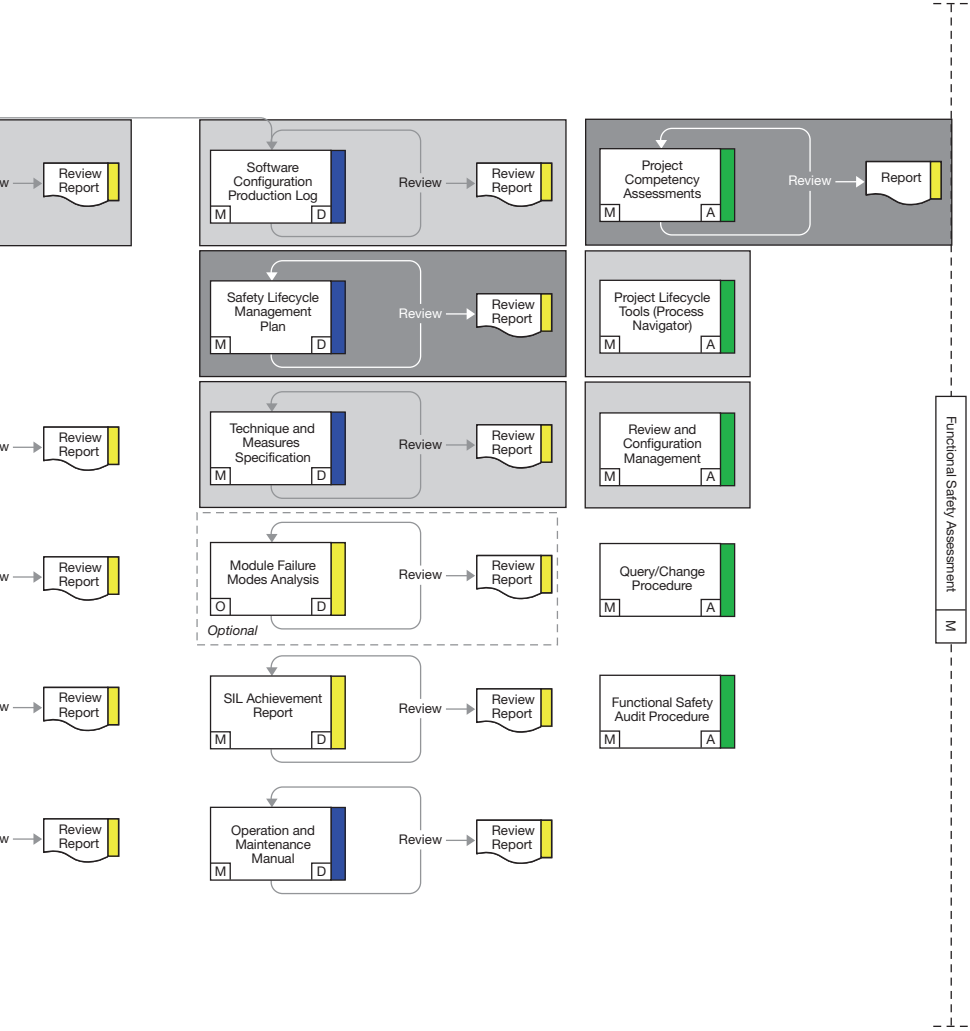



***Figure 3 Design FSA***


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
Technique 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

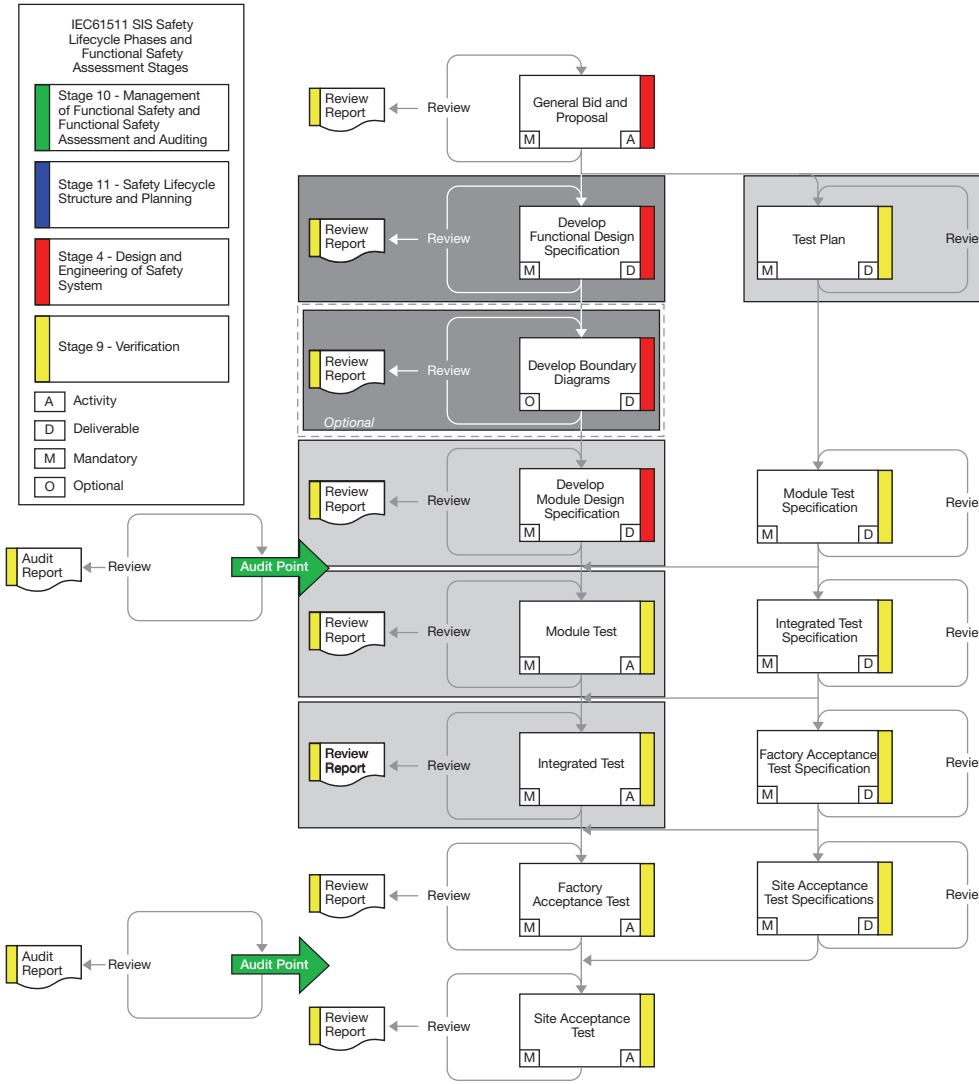
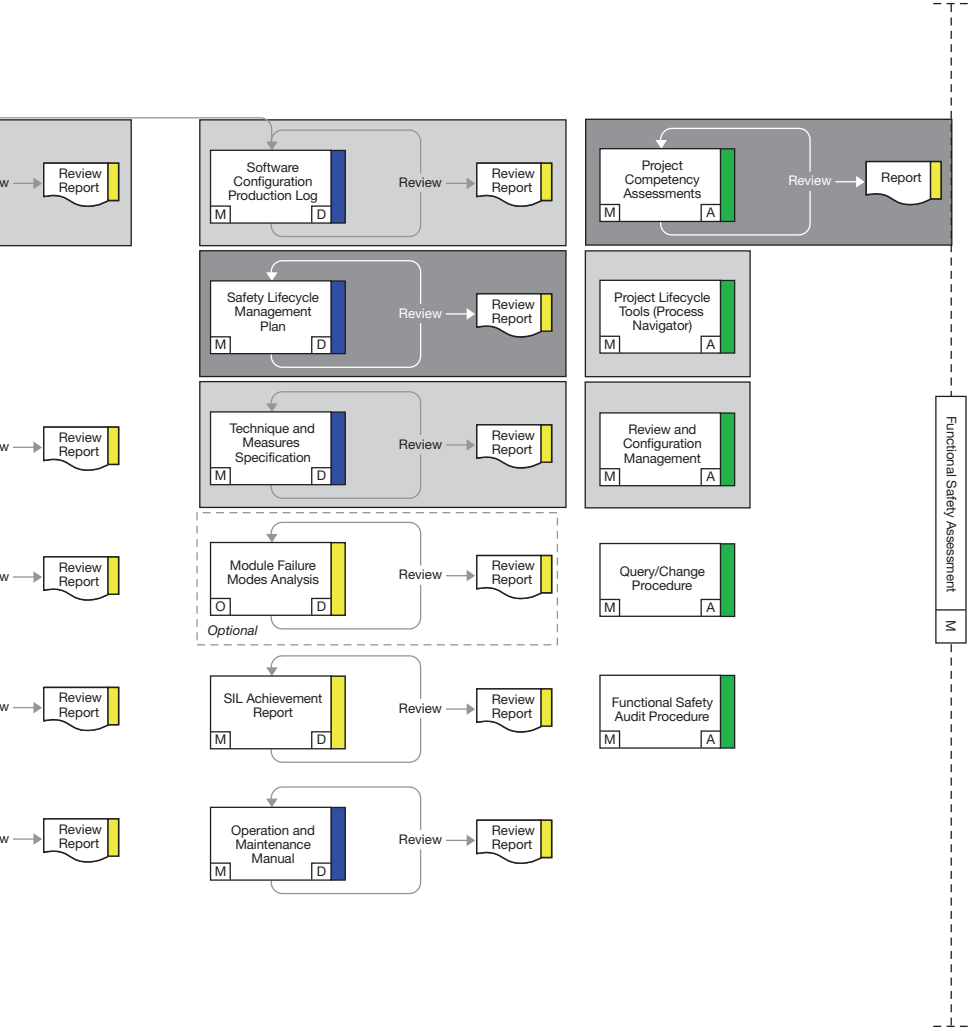



*Figure 4 Final FSA*


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
Technique 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] IEC 61131 – Programmable controllers

# 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 assessments/March 09

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