Functional safety assessment
Setting the boundaries of the FSA, defining the scope and planning the FSA

Power and productivity
for a better world™

Contents

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 Ed 2 and IEC 61511 may not be fully conversant with the specific details of the FSA activity, aware that it is a mandatory requirement 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 within the overall 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.

EC 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, provides the reader with details of an FSA process methodology and FSA reporting mechanism which is in use across ABB's global Safety Execution Centres (SECs). These SECs all have IEC 61508 Ed 2 compliant Functional Safety Management Systems (FSMS) and are progressively being certified by TÜV. 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.

The guide, looks 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, functional safety assessments and functional safety assessment planning.

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 'A functional safety assessment shall be applied to all phases throughout the overall E/E/PE system and software safety lifecycles including documentation, verification and management of Functional Safety'. Similarly, the relevance and importance of the role of other organisations and the interfaces is apparent when read in conjunction with clause 8.2.4 'those carryin out the functional safety assessment shall consider the activities carried out and the outputs obtained during each phase of the overall, E/E/PE system and software safety lifecycles and judge whether adequatte functional safety has been achieved based on the objectives and requirements in this standard'. 8.2.5, all relevant claims of compliance made by suppliers and other parties responsible for achieving functional safety, shall be included in the Functional Safety assessment.

Also, clause 8.2.6, 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 10 and IEC 61511 Phase 4. 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
- Codingstandards 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 has established a Safety Lead Competency Centre (SLCC). This SLCC operates on behalf of ABB senior management and is responsible for:

- developing an IEC 61508 and IEC61511 compliant generic functional safety management system (FSMS)
- rolling this out to each SEC for local implementation
- managing a global third-party IEC 61508 and IEC161511 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 8.2.11 to 8.2.15 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 different 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 61511. Therefore in order to comply with this requirement:

- FSAs shall be performed by approved resources under the direction of the Safety Lead Competency Centre (SLCC) in order to meet the independence and competency requirements of both IEC 61511 5.2.6.1 and cross referenced to the requirements within IEC61511, parts 2 and 3. 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.

3.0 Scope of the FSA

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

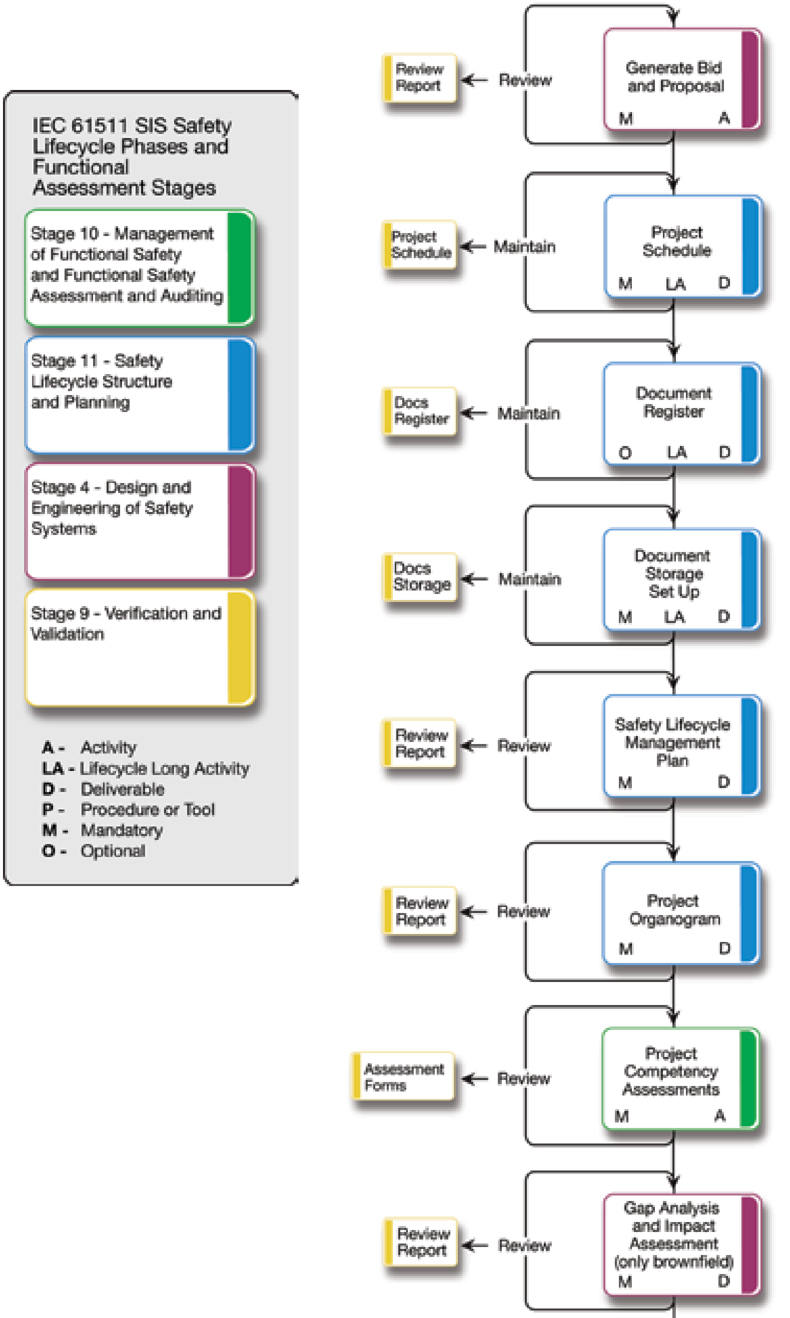
This FSMS specifies a safety lifecycle model for use by each SEC. Integral to this model are the audit and FSA processes. For each compliant item, e.g. safety system logic solver, implemented by an ABB SEC an FSA is a mandatory requirement.

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. It assesses if appropriate methods, techniques, tools and processes have been used to achieve functional safety.

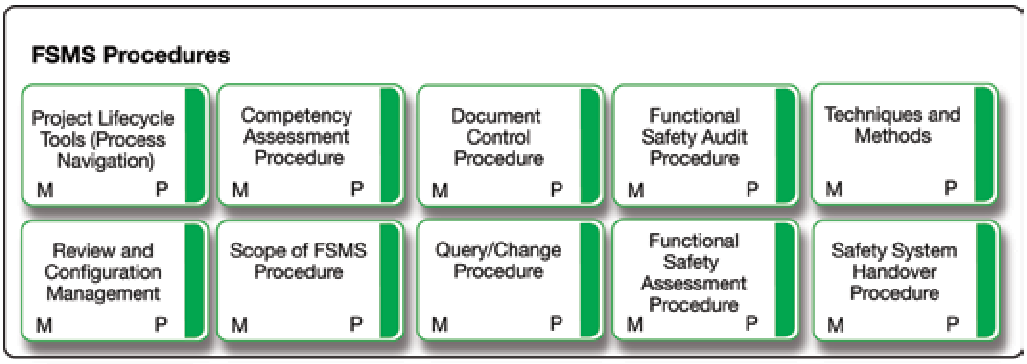
The FSA includes amongst other things an analysis and review of:

- 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

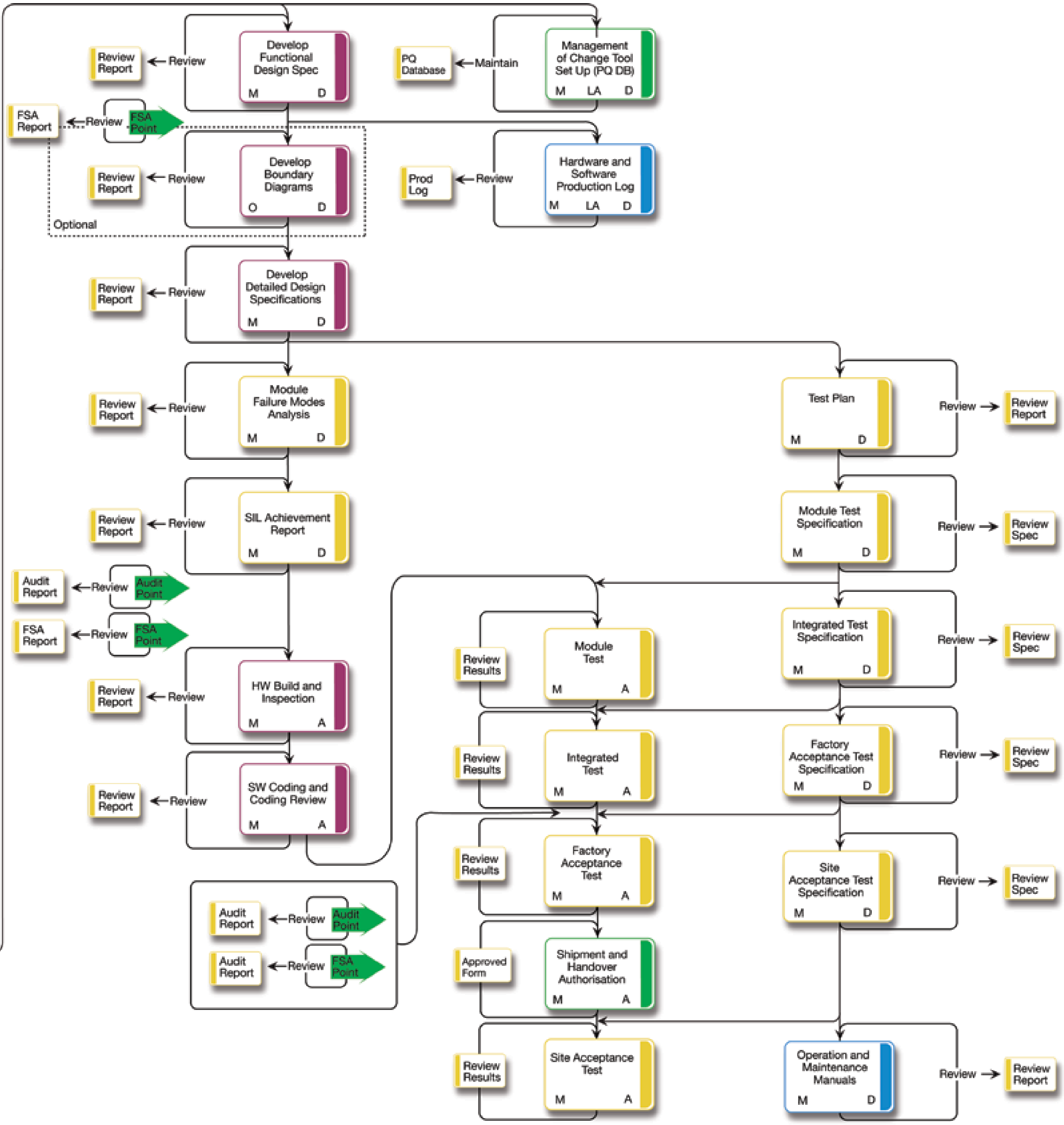
Figure 1 (opposite) provides an overview of this safety lifecycle model:



IEC 61511 SIS Safety Lifecycle Phases and Functional Assessment Stages
Stage 10 - Management of Functional Safety and Functional Safety Assessment and Auditing
Stage 11 - Safety Lifecycle Structure and Planning
Stage 4 - Design and Engineering of Safety Systems
Stage 9 - Verification and Validation
A - Activity
LA - Lifecycle Long Activity
D - Deliverable
P - Procedure or Tool
M - Mandatory
O - Optional
Review Report
Review
Generate Bid and Proposal
M A
Project Schedule
Maintain
Project Schedule
M LA D
Docs Register
Maintain
Document Register
O LA D
Docs Storage
Maintain
Document Storage Set Up
M LA D
Review Report
Review
Safety Lifecycle Management Plan
M D
Review Report
Review
Project Organogram
M D
Assessment Forms
Review
Project Competency Assessments
M A
Review Report
Review
Gap Analysis and Impact Assessment (only brownfield)
M D



FSMS Procedures
Project Lifecycle Tools (Process Navigation)
M P
Competency Assessment Procedure
M P
Document Control Procedure
M P
Functional Safety Audit Procedure
M P
Techniques and Methods
M P
Review and Configuration Management
M P
Scope of FSMS Procedure
M P
Query/Change Procedure
M P
Functional Safety Assessment Procedure
M P
Safety System Handover Procedure
M P


Review Report
Review
Develop Functional Design Spec
M D
PQ Database
Maintain
Management of Change Tool Set Up (PQ DB)
M LA D
FSA Report
Review
FSA Point
Review Report
Review
Develop Boundary Diagrams
O D
Prod Log
Review
Hardware and Software Production Log
M LA D
Optional
Review Report
Review
Develop Detailed Design Specifications
M D
Review Report
Review
Module Failure Modes Analysis
M D
Test Plan
M D
Review
Review Report
Review Report
Review
SIL Achievement Report
M D
Module Test Specification
M D
Review
Review Spec
Audit Report
Review
Audit Point
FSA Report
Review
FSA Point
Review Results
Module Test
M A
Integrated Test Specification
M D
Review
Review Spec
Review Report
Review
HW Build and Inspection
M A
Review Results
Integrated Test
M A
Factory Acceptance Test Specification
M D
Review
Review Spec
Review Report
Review
SW Coding and Coding Review
M A
Review Results
Factory Acceptance Test
M A
Site Acceptance Test Specification
M D
Review
Review Spec
Audit Report
Review
Audit Point
Audit Report
Review
FSA Point
Approved Form
Shipment and Handover Authorisation
M A
Review Results
Site Acceptance Test
M A
Operation and Maintenance Manuals
M D
Review
Review Report

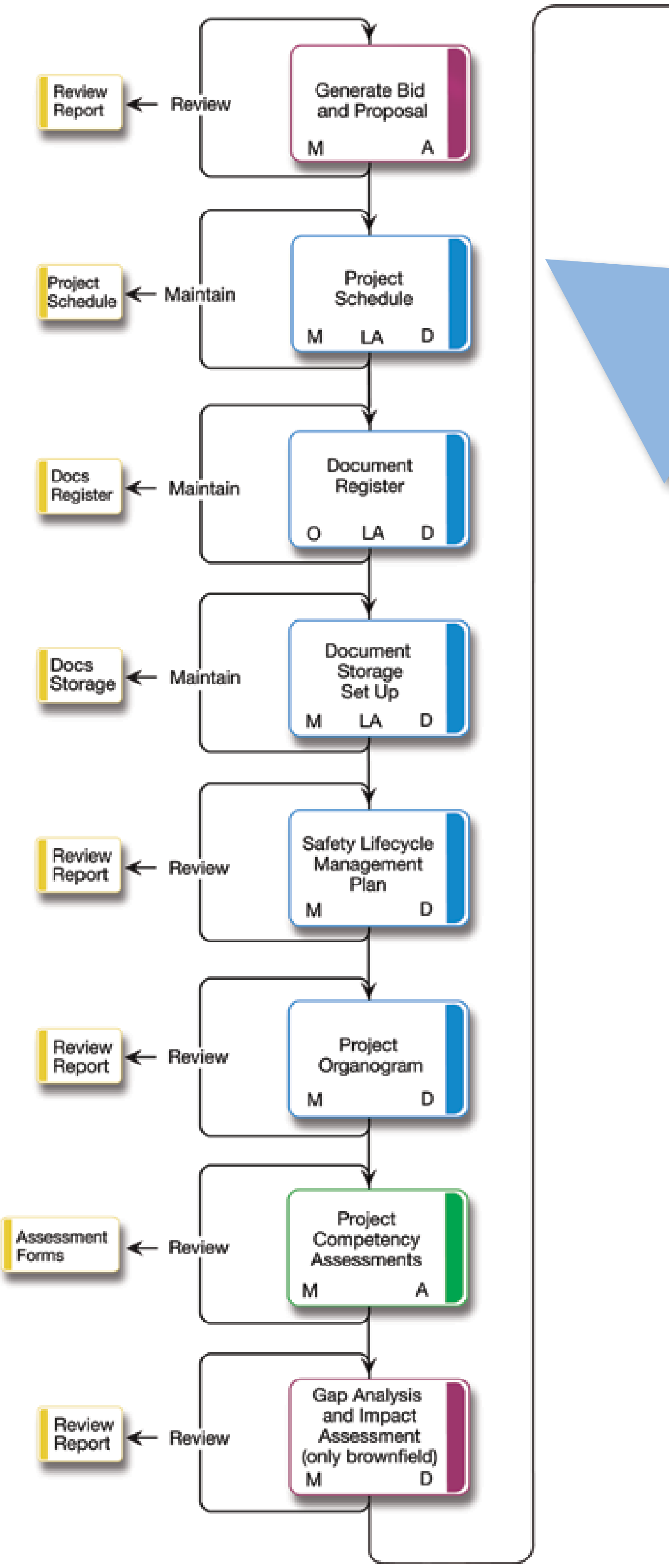
4.0 Planning of FSAS

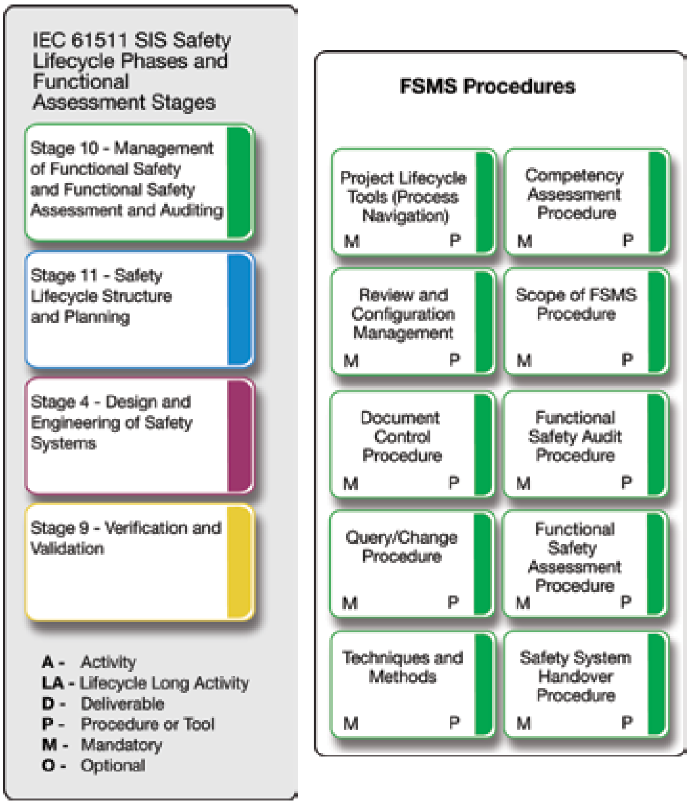
Having specified the scope of supply, specifically Phase 10 of IEC 61508 and Phase 4 of IEC 61511, and documented the policy to comply with IEC 61508 for FSA, the FSA is planned to be performed at three key stages of the safety lifecycle:

Preliminary
Design
Final

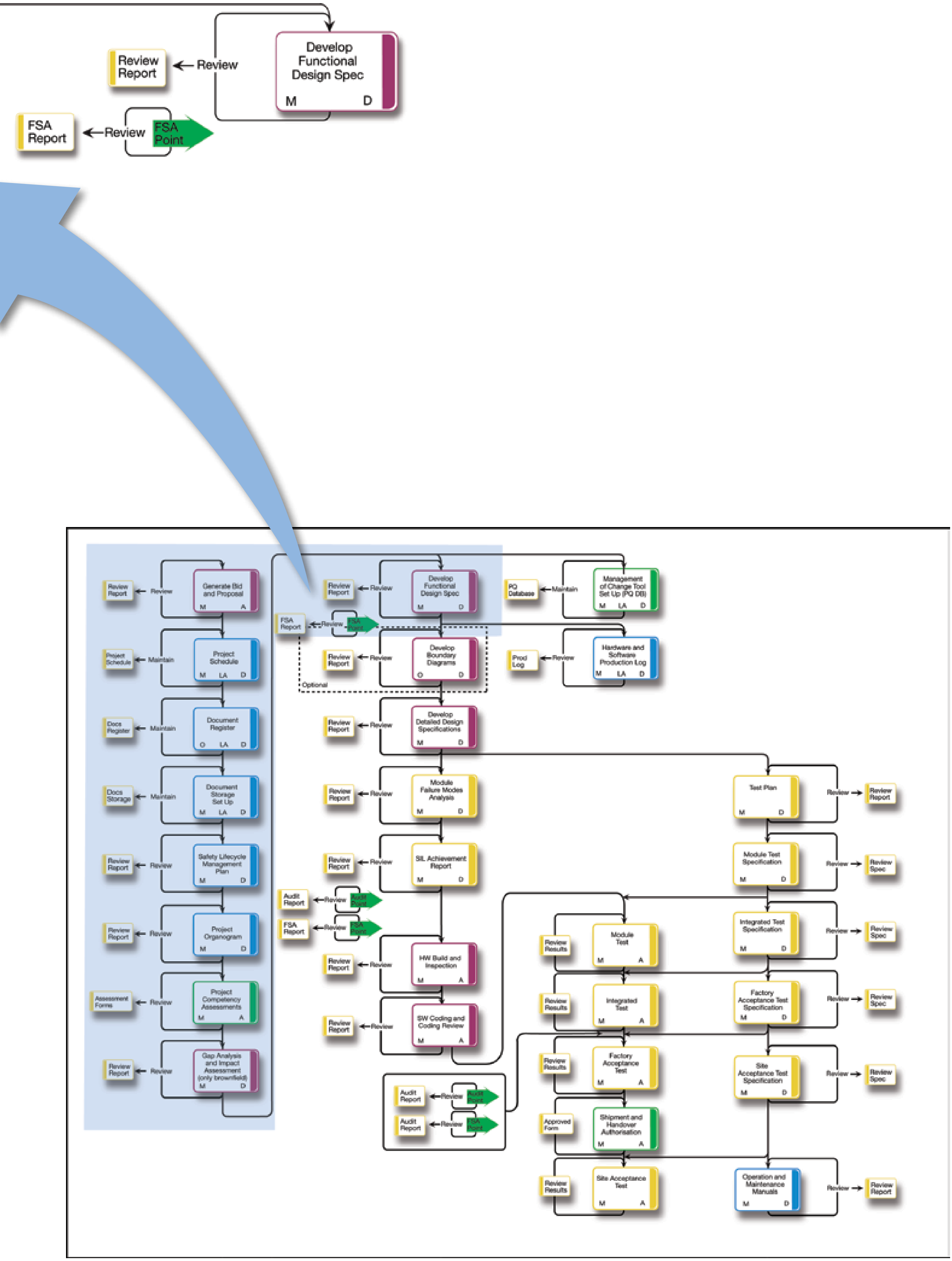
Stage 1 - Preliminary FSA

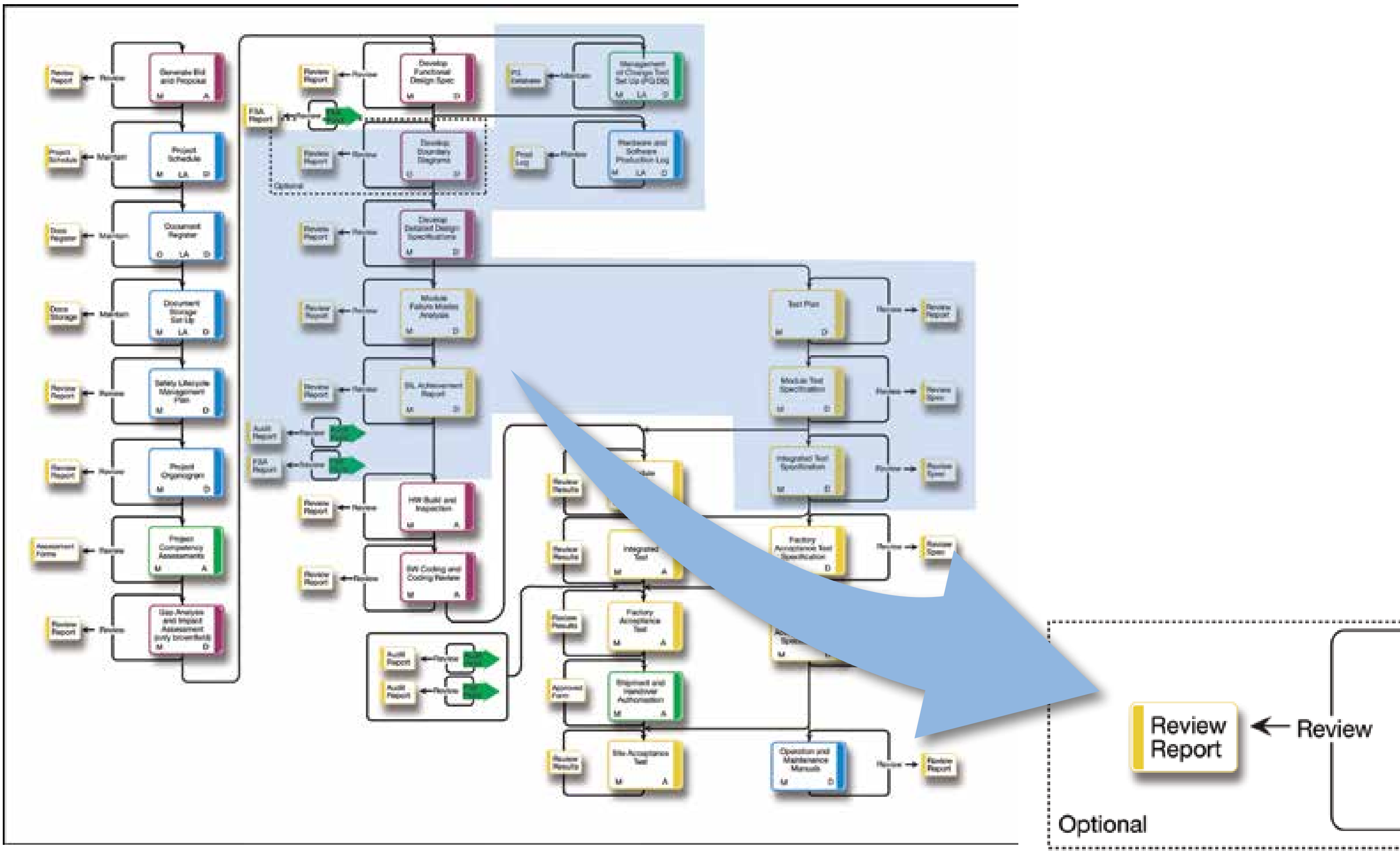
– Following completion of the Safety Lifecycle Management Plan and internal review of the Safety Lifecycle Management Plan. Figure 2 shows the preliminary FSA in relation to the safety lifecycle, processes and deliverables. The shaded area identifies the key inputs to this FSA stage.

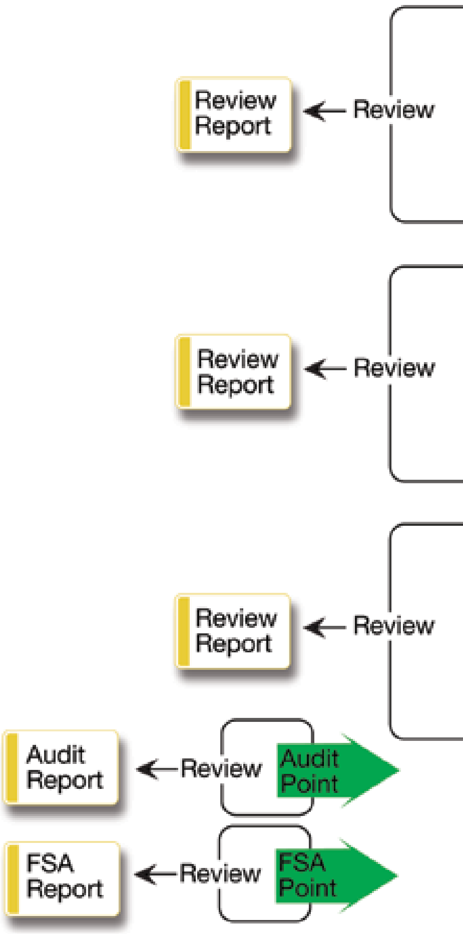




IEC 61511 SIS Safety Lifecycle Phases and Functional Assessment Stages
Stage 10 - Management of Functional Safety and Functional Safety Assessment and Auditing
Stage 11 - Safety Lifecycle Structure and Planning
Stage 4 - Design and Engineering of Safety Systems
Stage 9 - Verification and Validation
A - Activity
LA - Lifecycle Long Activity
D - Deliverable
P - Procedure or Tool
M - Mandatory
O - Optional
FSMS Procedures
Project Lifecycle Tools (Process Navigation)
M P
Competency Assessment Procedure
M P
Review and Configuration Management
M P
Scope of FSMS Procedure
M P
Document Control Procedure
M P
Functional Safety Audit Procedure
M P
Query/Change Procedure
M P
Functional Safety Assessment Procedure
M P
Techniques and Methods
M P
Safety System Handover Procedure
M P

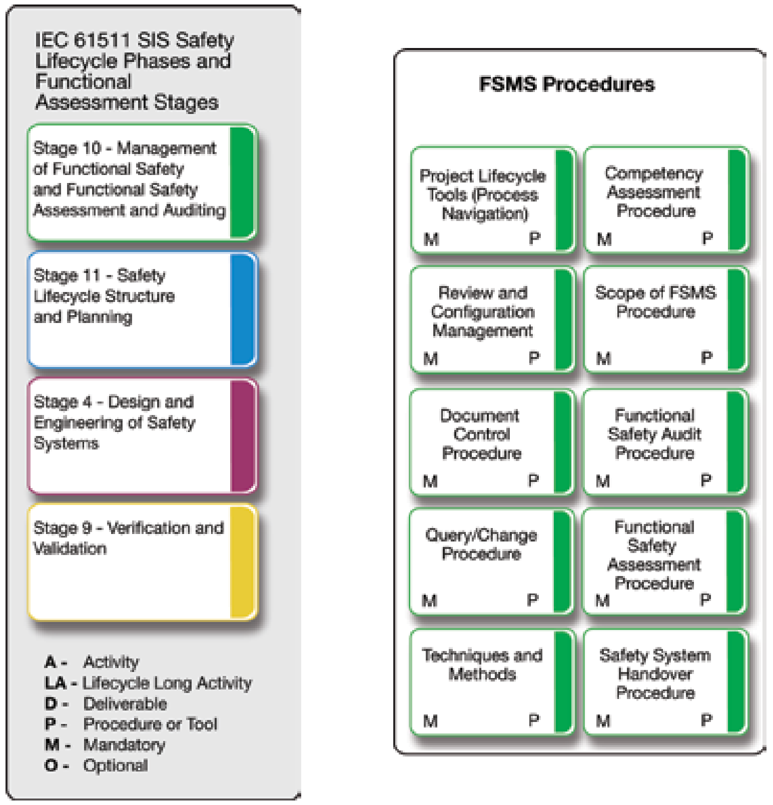

Review Report
Review
Develop Functional Design Spec
M
D
FSA Report
Review
FSA Point
Review Report
Review
Generate Bid and Proposal
M A
Project Schedule
Maintain
Project Schedule
M LA D
Docs Register
Maintain
Document Register
O LA D
Docs Storage
Maintain
Document Storage Set Up
M LA D
Review Report
Review
Safety Lifecycle Management Plan
M D
Review Report
Review
Project Organogram
M D
Assessment Forms
Review
Project Competency Assessments
M A
Review Report
Review
Gap Analysis and Impact Assessment (only brownfield)
M D
Review Report
Review
Develop Functional Design Spec
M D
FSA Report
Review
FSA Point
Review Report
Review
Develop Boundary Diagrams
O D
Optional
Review Report
Review
Develop Detailed Design Specifications
M D
Review Report
Review
Module Failure Modes Analysis
M D
Review Report
Review
SIL Achievement Report
M D
Audit Report
Review
Audit Point
FSA Report
Review
FSA Point
Review Report
Review
HW Build and Inspection
M A
Review Report
Review
SW Coding and Coding Review
M A
Audit Report
Review
Audit Point
Audit Report
Review
FSA Point
PQ Database
Maintain
Management of Change Tool Set Up (PQ DB)
M LA D
Prod Log
Review
Hardware and Software Production Log
M LA D
Test Plan
M D
Review
Review Report
Module Test Specification
M D
Review
Review Spec
Integrated Test Specification
M D
Review
Review Spec
Factory Acceptance Test Specification
M D
Review
Review Spec
Site Acceptance Test Specification
M D
Review
Review Spec
Operation and Maintenance Manuals
M D
Review
Review Report
Review Results
Module Test
M A
Review Results
Integrated Test
M A
Review Results
Factory Acceptance Test
M A
Approved Form
Shipment and Handover Authorisation
M A
Review Results
Site Acceptance Test
M A

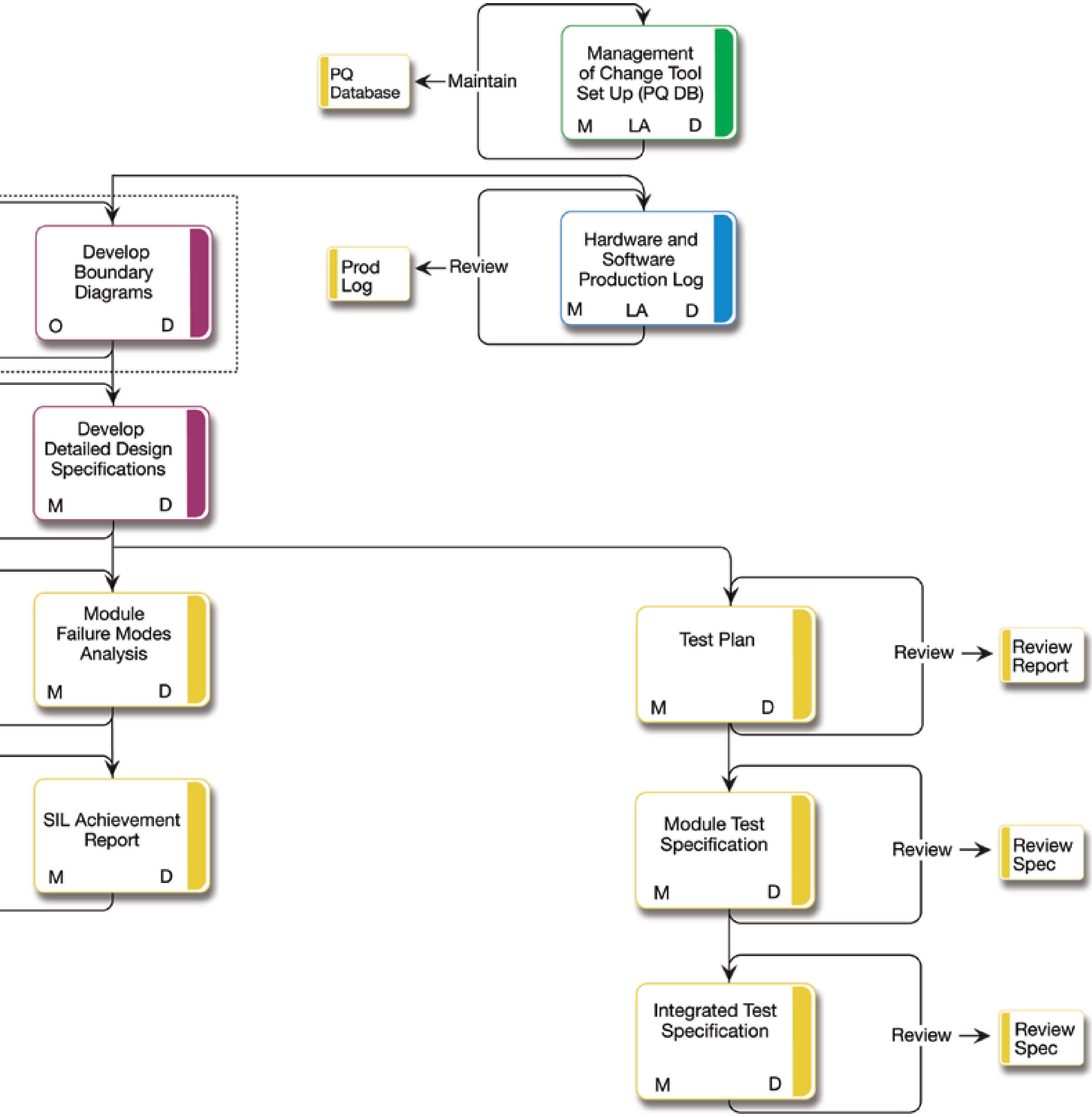




Stage 2 - Design FSA

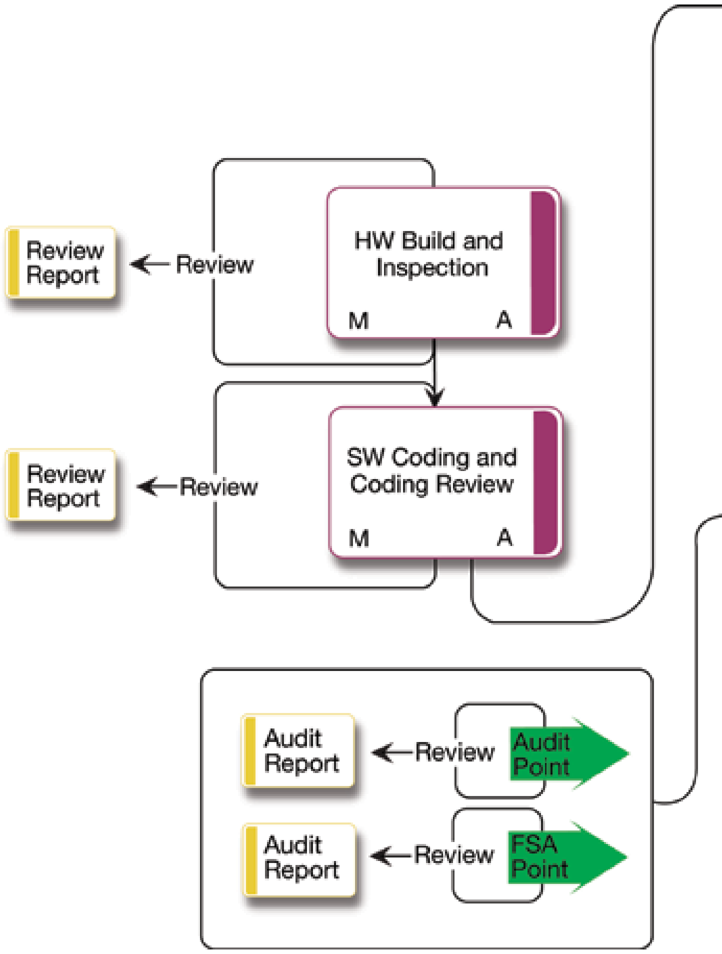
– Following completion of the Functional Design Specification (FDS), internal review of the FDS, and prior to approval by the client. Figure 3 shows the Design FSA in relation to the safety lifecycle, processes and deliverables. The shaded area indicates activities/deliverables that are revisited following the preliminary FSA.

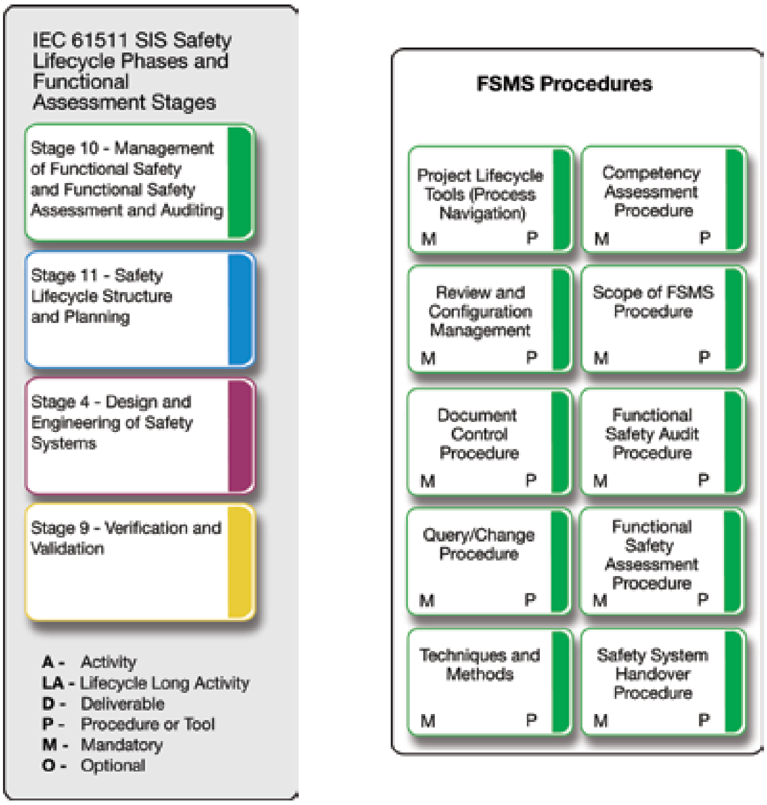

IEC 61511 SIS Safety Lifecycle Phases and Functional Assessment Stages
Stage 10 - Management of Functional Safety and Functional Safety Assessment and Auditing
Stage 11 - Safety Lifecycle Structure and Planning
Stage 4 - Design and Engineering of Safety Systems
Stage 9 - Verification and Validation
A - Activity
LA - Lifecycle Long Activity
D - Deliverable
P - Procedure or Tool
M - Mandatory
O - Optional
FSMS Procedures
Project Lifecycle Tools (Process Navigation) M P
Competency Assessment Procedure M P
Review and Configuration Management M P
Scope of FSMS Procedure M P
Document Control Procedure M P
Functional Safety Audit Procedure M P
Query/Change Procedure M P
Functional Safety Assessment Procedure M P
Techniques and Methods M P
Safety System Handover Procedure M P

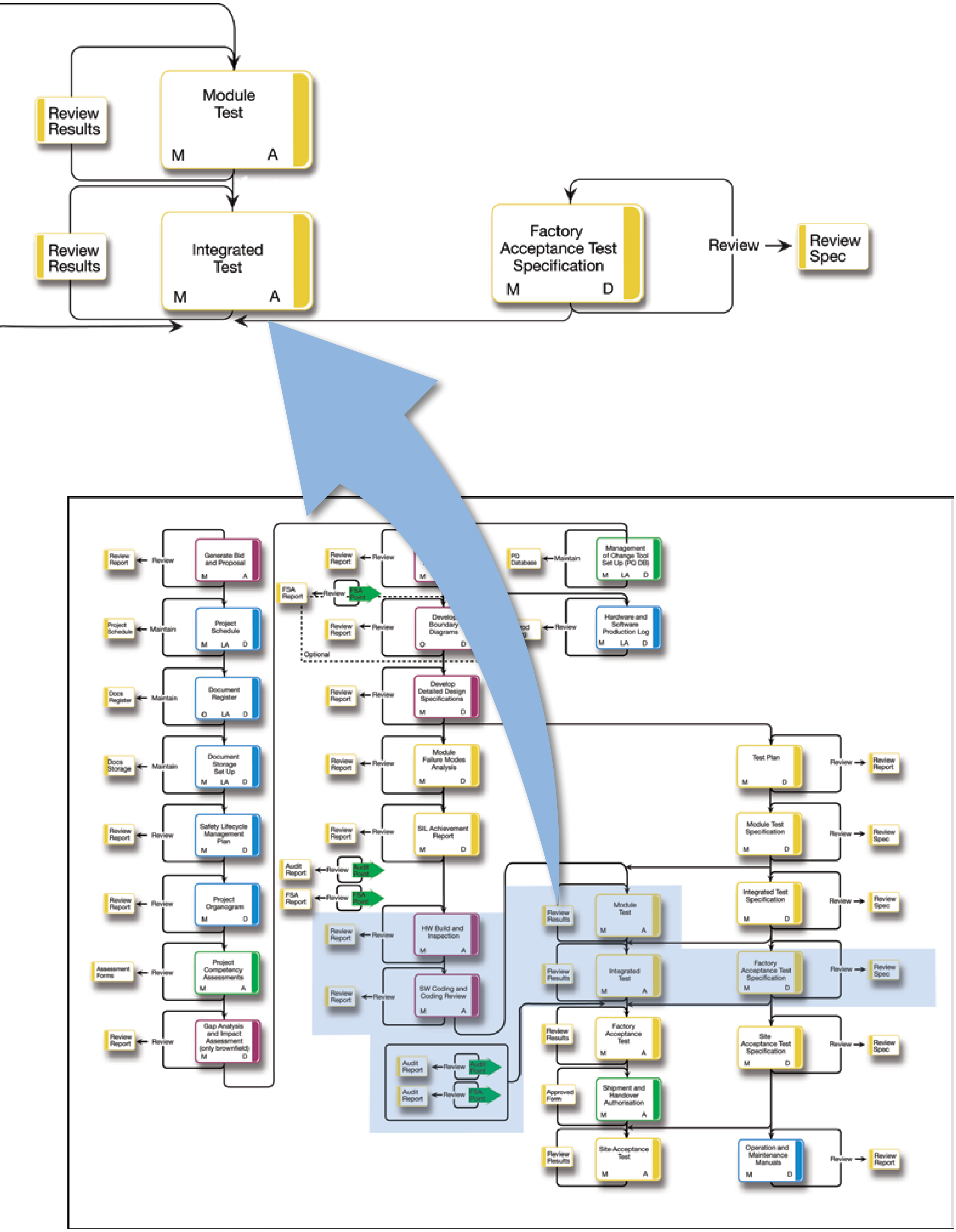

PQ Database
Maintain
Management of Change Tool Set Up (PQ DB)
M LA D
Develop Boundary Diagrams
O D
Prod Log
Review
Hardware and Software Production Log
M LA D
Develop Detailed Design Specifications
M D
Module Failure Modes Analysis
M D
SIL Achievement Report
M D
Test Plan
M D
Review
Review Report
Module Test Specification
M D
Review
Review Spec
Integrated Test Specification
M D
Review
Review Spec

Stage 3 - Final FSA

– Following Factory Acceptance Testing (FAT). Figure 4 shows the Final FSA in relation to the safety lifecycle, processes and deliverables. The shaded area indicates activities/deliverables that are revisited following the Preliminary and Design FSAs.




IEC 61511 SIS Safety Lifecycle Phases and Functional Assessment Stages
Stage 10 - Management of Functional Safety and Functional Safety Assessment and Auditing
Stage 11 - Safety Lifecycle Structure and Planning
Stage 4 - Design and Engineering of Safety Systems
Stage 9 - Verification and Validation
A - Activity
LA - Lifecycle Long Activity
D - Deliverable
P - Procedure or Tool
M - Mandatory
O - Optional
FSMS Procedures
Project Lifecycle Tools (Process Navigation) M P
Competency Assessment Procedure M P
Review and Configuration Management M P
Scope of FSMS Procedure M P
Document Control Procedure M P
Functional Safety Audit Procedure M P
Query/Change Procedure M P
Functional Safety Assessment Procedure M P
Techniques and Methods M P
Safety System Handover Procedure M P


Module Test
M A
Review Results
Integrated Test
M A
Review Results
Factory Acceptance Test Specification
M D
Review
Review Spec
Review Report
Review
Generate Bid and Proposal
Project Schedule
Maintain
Docs Register
Document Register
Docs Storage
Document Storage Set Up
Safety Lifecycle Management Plan
Project Organogram
Assessment Forms
Project Competency Assessments
Gap Analysis and Impact Assessment (only brownfield)
FSA Report
FSA Point
Optional
Develop Boundary Diagrams
Develop Detailed Design Specifications
Module Failure Modes Analysis
SIL Achievement Report
Audit Report
Audit Point
HW Build and Inspection
SW Coding and Coding Review
PQ Database
Management of Change Tool Set Up (PQ DB)
Hardware and Software Production Log
Test Plan
Module Test Specification
Integrated Test Specification
Factory Acceptance Test
Approved Form
Shipment and Handover Authorisation
Site Acceptance Test
Site Acceptance Test Specification
Operation and Maintenance Manuals
M LA D
O LA D

FSA planning continued

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 the assessment
- The means by which any follow-up recommendations shall be progressed
- The stage(s) within the safety life cycle when the FSAs 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.

5.0 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:

- 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 between an audit and an assessment?

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.

Contact us

Assured and certified products, services, delivery and execution.

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

www.abb.com/oilandgas

Power and productivity
for a better world™