FUNCTIONAL SAFETY ASSESSMENTS

Guidance on FSA Stages 1, 2 and 3

The 61508 Association, 15 Hillside Road, Knutsford, Cheshire, WA16 6TH, UK
Tel: 07977 441 552 E-mail: info@61508.org **Web:** www.61508.org

Contents

Revision History

Version	Date	Author	Comments
Issue 1.0	01/03/19	D Chauhan	First Publication issue

Disclaimer

These guidelines have been produced by The 61508 Association to assist its members and others on Functional Safety Assessment stages 1 -3. The Association would welcome any comments on this publication, see http://www.61508.org/contact.htm. Whilst every effort has been made to ensure the accuracy of the information contained in this document, neither The 61508 Association nor any of its members will assume liability for any use made thereof.

1 Introduction

1.1 Aim of this guidance

Functional Safety Assessments (FSAs) have an increased profile as Edition 2 of IEC61511 is placing further emphasis on their scheduling within lifecycle phases. FSAs have always been a requirement of the standard, but what the purpose is, how to do it and why they are a good idea is poorly understood.

The aim of this guidance is to provide a basic explanation of FSAs with respect to the definitions provided in IEC61511 and their intent. For FSA stages 1, 2 and 3, it covers who is responsible, when and how they should be carried out as well as highlighting the key information that is required as an input into each FSA stage and the expected outputs.

This guidance is intended to supplement that provided by the Chemical and Downstream Oil Industries Forum (CDOIF) guidelines entitled 'Management of Installed Safety Instrumented Systems' which contains information about FSA stages 4 and 5.

Note that although the intention within this guidance is to focus on IEC61511, relevant clauses and references from IEC61508 have been included for clarity.

1.2 Intended audience for this guidance

IEC 61511 identifies that the Asset Owners or End Users have the responsibility of ensuring that FSAs are undertaken at the specific lifecycle stages of the Safety Instrumented System (SIS). However, the responsibility of complying with the FSA clauses of the standard applies to the entire supply chain. The supply chain may include Engineering Procurement Construction Companies (EPCs), System Integrators (SIs) as well as Original Equipment Manufacturers (OEMs).

This guide is intended for use by personnel who may be aware that FSAs are required but may not be familiar as to what they entail and the benefits of undertaking an FSA.

1.3 Background – The Requirement for Functional Safety Assessments

The basic purpose of functional safety is to provide defined levels of risk reduction in managing specific hazards associated with some sort of equipment. The levels of risk reduction are determined within a company's overall risk management framework to ensure that the overall risk to people and the environment is as low as reasonably practicable.

Functional safety relies on the correct functioning of a SIS and other protection layers. These systems can be complicated and subject to hidden or latent failures. There is always some chance that the systems will not work effectively when a hazardous event occurs.

The fundamental question is this:

How can we be confident that our functional safety system will reliably achieve the risk reduction that we need?

That is the question that FSA is intended to answer. Ultimately the owners of any hazardous equipment have a duty of care in protecting people from harm caused by that equipment. In most developed countries occupational health and safety legislation imposes severe penalties on process owners that are negligent in that duty of care. To protect people and the environment from harm (and to protect ourselves from prosecution) we need to be diligent in our duty of care.

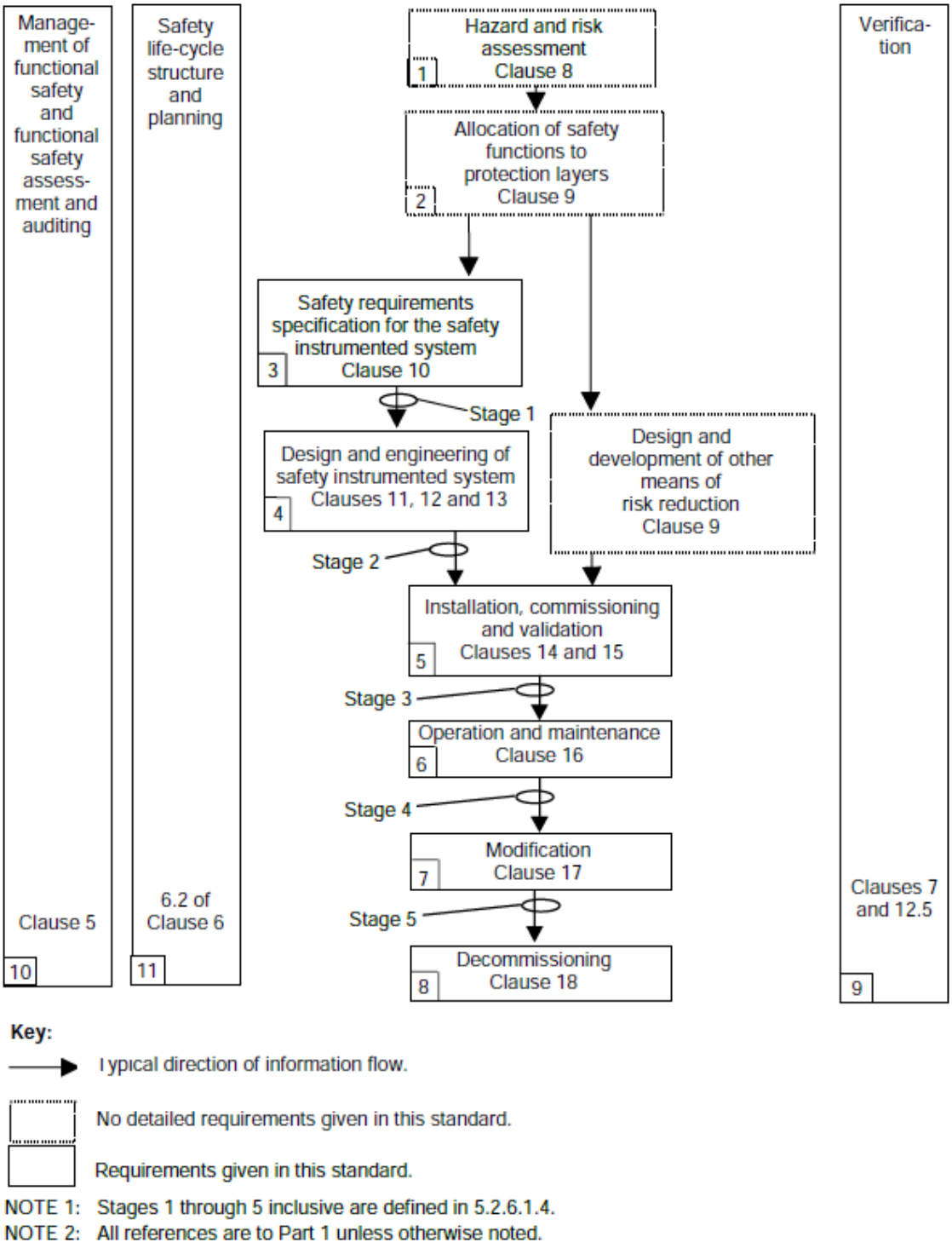
Due diligence requires a demonstration that reasonable efforts have been made to apply appropriate standards and work practices in managing workplace hazards.

The objective of FSA is to make a judgement as to the functional safety and safety integrity achieved by the safety system, or in other words, whether the system will reliably deliver the risk reduction required.

The FSA therefore provides evidence towards demonstrating due diligence in our duty of care. It is a feedback tool that supports management's monitoring and review process and an approach to minimising systematic failures.

FSA is a mandatory requirement of the international standards that govern functional safety. The requirements for FSA are defined in IEC 61508-1:2010, Clause 8 and in IEC 61511-1:2016, Clause 5.2.6.1 which specifically defines 5 stages when FSAs should be carried out. This is shown in the figure below:

Figure 1. SIS safety lifecycle phases and FSA stages



The simpler standards that cover machine safety applications, IEC 62061 and ISO 13849 do not explicitly require FSA. Nevertheless, managers in charge of hazardous machinery are still required to demonstrate due diligence. If FSA is not carried out then some other equivalent form of management monitoring and review will be necessary. The regulator will inevitably want to see evidence that the risks are managed.

FSA assists us in demonstrating that we have done as much as is reasonable.

At the conclusion of the FSA the assessors recommend for acceptance, qualified acceptance or rejection of the systems assessed.

1.4 The purpose / approach of this guidance

This document will provide guidance to the FSA stages as identified by IEC 61511 and will provide the following:

- an aide memoir to the end user for understanding of the requirements for each stage of the FSA;
- the necessary inputs;
- the expected outputs;
- items to review as a minimum;
- conditions for completion of the FSA;
- a sample template associated for each stage of the FSA;
- an explanation of what it means ‘to achieve functional safety and safety integrity’
- the principles for application of FSA;
- the methodology of how the FSAs provide reasonable objective evidence that functional safety and safety integrity have been achieved.

2 Definitions and Abbreviations

The definitions and abbreviations provided within this section provides the end user with more clarity on the terminologies such as assessment, audit, validation and verification.

These terms define a number of checks whose purpose is to ensure that what is produced is complete, consistent and correct, but they each have a different purpose and are implemented at different times and in different ways. Appendix A also contains further detail on the principles of functional safety.

2.1 Functional Safety Assessment

Definitions provided in IEC61508-4:2010 and IEC61511-1:2016 are as follows:

IEC61508-4:2010, 3.8.3 - investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems and/or other risk reduction measures.

IEC61511-1:2016, 3.2.24 - investigation, based on evidence, to judge the functional safety achieved by one or more SIS and/or other protection layers.

What does this imply?

Functional Safety Assessments are judgement made by assessors so as to ensure that functional safety is achieved. The assessments rely more on the awareness and technical competence of the assessor. The FS assessment will focus more on the technical aspects in addition to the procedural aspects.

To 'achieve functional safety' means that the specified levels of risk reduction are achieved by applying electrical, electronic or programmable electronic safety related systems.

To do that we need to demonstrate that the probability of dangerous failures (or the rate of dangerous failures) is sufficiently low to meet the risk reduction target. That means we need to show that the both the probability of random hardware failure and the probability of systematic failure have been controlled.

FSA is a feedback mechanism for senior management. It is a way of monitoring the effectiveness of risk management strategies that rely on automated safety systems (i.e. functional safety).

FSA provides evidence of due diligence in duty of care: Have we made a reasonable effort to reduce the risks that people or the environment are exposed to?

2.2 Functional Safety Audit

Definitions provided in IEC61508-4:2010 and IEC61511-1:2016 are as follows:

IEC61508-4:2010, 3.8.4 - systematic and independent examination to determine whether the procedures specific to the functional safety requirements to comply with the planned arrangements are implemented effectively and are suitable to achieve the specified objectives. Note: A functional safety audit may be carried out as part of a functional safety assessment.

IEC61511-1:2016, 3.2.25 - 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. Note: A functional safety audit may be carried out as part of a FSA.

What does this imply?

The purpose of the Functional Safety Audit is to determine if functional safety procedures are being correctly and effectively implemented during the project execution.

Many companies have developed various functional safety procedures which are in accordance with the functional safety standards, but in order to show compliance, projects need to be following the procedure effectively. The audit provides a useful means of assessing how effectively systematic failures are being controlled by using procedures to prevent errors in design, construction or operation.

Note that it does not provide any judgement on whether functional safety has been achieved or maintained during the project. It typically forms part of the Quality Management System (QMS) of the organisation responsible for the respective phase of the safety lifecycle. The records of the audits are reviewed as part of the FSAs.

Audit is also a feedback mechanism for senior management. Its purpose is to monitor how well people understand and apply procedures, and whether those procedures are practicable and effective.

FSA is more abstract than audit; it takes a wider view. FSA almost always relies on evidence collected by audits.

2.3 Validation

Definitions provided in IEC61508-4:2010 and IEC61511-1:2016 are as follows:

IEC61508-4:2010, 3.8.2 - confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled.

In this standard there are three validation phases: overall safety validation; E/E/PE system validation; software validation. Validation is the activity of demonstrating that the safety-related system under consideration, before or after installation, meets in all respects the safety requirements specification for that safety-related system. Therefore, for example, software validation means confirming by examination and provision of objective evidence that the software satisfies the software safety requirements specification.

IEC61511-1:2016, 3.2.86 - confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled.

In the IEC 61511 series this means demonstrating that the SIF(s) and SIS after installation meet the SRS in all respects.

What does this imply?

Validation is part of the normal engineering quality process and is a fundamental feedback mechanism. Its purpose is to show that a finished product has been built to meet the specified requirements.

Validation is not the same thing as commissioning.

The purpose of commissioning is to make something work. The purpose of validation is to show that it works correctly as required. This may have been demonstrated during commissioning, if the commissioning tests were planned with traceability to the SRS.

FSA goes much further than validation: Not only does it consider (by looking at evidence) whether the requirements were met, but it also considers whether the requirements themselves are complete, consistent and sufficient to achieve the intended level of safety. Furthermore it also examines how effectively error prevention and error detection techniques have been applied.

Validation never considers FSA but in contrast, FSA must always assess the validation process and results.

2.4 Verification

Definitions provided in IEC61508-4:2010 and IEC61511-1:2016 are as follows:

IEC61508-4:2010, 3.8.1 - confirmation by examination and provision of objective evidence that the requirements have been fulfilled.

In the context of this standard, verification is the activity of demonstrating for each phase of the relevant safety lifecycle (overall, E/E/PE system and software), by analysis, mathematical reasoning and/or tests, that, for the specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase.

IEC61511-1:2016, 3.2.27 - confirmation by examination and provision of objective evidence that the requirements have been fulfilled.

In the IEC 61511 series this is the activity of demonstrating for each phase of the relevant SIS safety life-cycle by analysis and/or tests, that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase.

What does this imply?

Verification is simply the process of confirming that something (anything at all) has been produced correctly.

Within the safety lifecycle, verification is a functional safety management activity which should be carried out at every stage to ensure systematic integrity. It is part of the normal engineering quality process carried out through checking, review, inspection or testing.

Verification records could include check prints, completed checklists or inspection and test records.

Validation in comparison to verification is a specific lifecycle phase which takes a wider view because it looks at the overall completed system. Validation always relies on verification techniques as a way of showing the system meets all of the specified requirements in every regard. It should be noted that the validation process must also be verified.

Verification is at a lower level and relates to individual components or documents. Verification never relies on validation. FSA looks for evidence that verification has been completed effectively.

3 Functional Safety Assessment Planning

3.1 FSA Planning Requirements

IEC 61511-1 (sub-clauses 5.2.6.1.1 – 5.2.6.1.3) require that FSA must be planned in advance. The initial planning can be part of the project's functional safety management plan. As a minimum the management plan should specify the responsibility for FSA, the FSA outputs and the timing of the FSA activities.

A formal FSA plan or procedure should be prepared when the FSA work starts and be structured to address the requirements for planning specified in IEC 61511.

IEC 61511-1 sub-clause 5.2.6.1.3 requires that planning for FSA shall consider:

- *The scope of the FSA;*
- *Who is to participate in the FSA;*
- *The skills, responsibilities and authorities of the FSA team;*
- *The information that will be generated as a result of any FSA activity;*
- *The identity of any other safety bodies involved in the FSA;*
- *The resources required to complete the FSA activity;*
- *The level of independence of the FSA team;*
- *The methods by which the FSA will be revalidated after modifications.*

The plan should be put together by either those responsible for FSA or those responsible for management of functional safety, or can be shared between them. Prior to a functional safety assessment taking place, the plan should be approved by all parties.

3.2 Assessor Competence

The competency requirements for the assessors need to be considered in the FSA planning. There should be formal evidence to demonstrate that the assessors have the appropriate competence. Refer to the guidelines 'Managing competence for safety-related systems - Part 1&2' produced by the HSE UK (Section 7.2).

The IET publication 'Competence Criteria for Safety-related System Practitioners' includes the competency unit 'Independent Safety Assessment'. An assessment of competence against this unit is appropriate for assessors.

It is essential for assessors to be competent in auditing because audit underpins the process of functional safety assessment. Experience in quality auditing or safety auditing is valuable for FSA.

It is also essential to have sufficient understanding and experience of functional safety principles and practices so that an informed judgement can be made regarding the effectiveness of the functional safety.

In particular, assessors should have a thorough understanding of the principles of both risk management and quality management.

Assessors need to have a sufficiently broad and deep understanding of the specific areas of work covered by the assessment. This enables them to be able to judge the impact of non-conformance. It also enables them to see what is missing. The most serious non-compliances tend to be in the areas which have not been addressed at all. People that take on activities beyond their area of experience often are not aware of their own lack of knowledge.

Persons with overall accountability for FSA should be expected to have an 'expert' level of competence. This means that they are able to think outside and beyond the standard rules and guidelines. They should be capable of abstraction rather than being limited to ticking boxes.

3.3 FSA Staging

The overriding requirement is that FSA must be carried out before hazards are introduced. Apart from that requirement the FSA work can be sequenced or staged in any way to suit the planning.

IEC 61511-1 sub-clause 5.2.6.1.4 suggests stages of FSA in Note 2:

Stage 1	*After the H&RA has been carried out, the required protection layers have been identified and the SRS has been developed.*	Refer to section 4.
Stage 2	*After the SIS has been designed.*	Refer to section 5.
Stage 3	*After the installation, pre-commissioning and final validation of the SIS has been completed and operation and maintenance procedures have been developed.*	Refer to section 6.
Stage 4	*After gaining experience in operating and maintenance.*	Refer to Appendix B.
Stage 5	*After modification and prior to decommissioning of a SIS.*	Refer to Appendix B.

Although the five stages are suggested as above, in practice it is effective to schedule and complete the FSAs as soon as possible to avoid passing faults to the next lifecycle phase. No matter how the FSA is staged, the process and the requirements are exactly the same so delaying FSA until late in the project delivers no benefit at all. The amount of work is the same, but the feedback from the FSA will be too late to prevent wasted effort and rework.

Quite often operators will only plan a single Stage 3 FSA immediately before commissioning, borne out of the misconception that that the mandatory requirement is simply that FSA is carried out before hazards are introduced. For the project to get the full benefit, FSA stages 1, 2 and 3 are equally important and should be scheduled and carried out at the appropriate time. The old adage applies: proper prior planning prevents poor performance.

3.4 FSA Output

IEC 61511-1 sub-clause 5.2.6.1.5 outlines requirements that the FSA shall confirm before hazards are introduced into the process (or before a modification is implemented):

- *the hazard and risk assessment (H&RA) has been carried out fully and correctly;*
- *the recommendations arising from the H&RA that apply to the SIS have been implemented or resolved (and resulting requirements specified in the safety requirements specification, SRS);*
- *project design change procedures are in place and have been properly implemented;*
- *the recommendations arising from any previous FSA have been resolved;*
- *the SIS is designed, constructed and installed in accordance with the SRS, any differences having been identified and resolved;*
- *the safety, operating, maintenance and emergency procedures pertaining to the SIS are in place;*
- *the SIS validation planning is appropriate and the validation activities have been completed;*
- *the employee training has been completed and appropriate information about the SIS has been provided to the maintenance and operating personnel;*
- *Plans or strategies for implementing further FSAs are in place.*

Further to this, the FSA should also confirm that the project has achieved the objectives of IEC 61511-1 Clauses 5, 6 and 7 in the management and planning of functional safety, safety lifecycle requirements and verification activities. The ultimate objective is to ensure that management and planning is sufficient to achieve the required level safety integrity, as required by IEC 6511-1 sub-clause 6.2.3.

3.5 Functional Safety Audit

Many people seem to be confused between functional safety audit and functional safety assessment. They are two different things with different objectives. Both are mandatory. Carrying out FSA does not remove the requirement for functional safety audit.

IEC 61511-1 sub-clause 5.2.6.2.1 explains the purpose of audit:

'The purpose of the audit is to review information documents and records to determine whether the functional safety management system (FSMS) is in place, up to date, and being followed. Where gaps are identified, recommendations for improvements are made.'

Sub-clause 5.2.6.2.2 requires that:

'All procedures identified as necessary resulting from all safety life-cycle activities shall be subject to safety audit.'

IEC 61508-1 sub-clause 8.2.7 makes it clear that functional safety audits are an input into FSA:

'A functional safety assessment shall include assessment of the evidence that functional safety audit(s) have been carried out (either full or partial) relevant to its scope.'

One reason for the confusion is that FSA not only depends on evidence produced by audits, it also usually applies audit techniques to find further evidence. The assessor will look for evidence of clause-by-clause compliance with the relevant standards.

3.6 Planning for Success

The simplest and easiest way of ensuring a successful FSA outcome is for the project to start out with a clear understanding of what evidence the FSA will need.

This principle holds true for any type of audit. If the procedures stipulate clearly what evidence must be produced and retained then the project team should not be surprised when the auditor asks for that evidence. It also simplifies the auditor's task, because it is much easier to prepare the audit checklists.

Any type and any stage of FSA will start by looking for evidence of compliance to the standards.

If the functional safety management plan clearly defines who is to produce what evidence for each and every sub-clause then compliance is easy to achieve, easy to demonstrate and easy to assess.

3.7 Suggested FSA Process

There is no set way for carrying out FSA. One technique is to apply a conventional audit process. Exactly the same technique can be applied at any stage and in any phase:

- The assessor prepares the FSA plan including the checklists to be applied
- The project team (or operations and maintenance team) assigns a focal point to work with the assessor in identifying and obtaining evidence of compliance
- The assessor meets with the team or with the focal point in an 'entry' meeting to review the planned process and the checklist.
- After the entry meeting, the focal point identifies the likely sources of evidence for each checklist item and collates the evidence for review
- The assessor reviews the evidence in detail against the checklist items to review compliance clause-by-clause and to assess the level of systematic integrity achieved
- The assessor compiles a list of items requiring clarification or discussion
- The assessor meets with the team to discuss and clarify issues
- The assessor produces a report summarising findings for that stage of the FSA
- The team and the assessor review the results in an 'exit' meeting.

FSA should be seen as a constructive and collaborative effort. The aim is to assist people in achieving safety. If the FSA provokes a defensive reaction from the team then the assessor may need to take a less critical, and more understanding and helpful approach.

4 Functional Safety Assessment Stage 1

4.1 Introduction – Purpose of FSA Stage 1

Stage 1 FSA assesses whether the project has solid and robust foundation as a basis.

It reviews the topics outlined in the following table and looks for compliance with the IEC61511 clauses listed here. Note that IEC61508 clauses are provided for reference.

Table 1. FSA Stage 1 Topics

Topic	IEC 61511-1	IEC 61508
Management and safety lifecycle planning, including verification planning and selection of techniques and measures	Phases 9, 10, 11 Clauses 5, 6, 7, 19	All phases Part 1 Clauses 5, 6 Part 2 Clause 7.1 Part 2 Annexes A,B Part 3 Clauses 6, 7.1 Part 3 Annexes A,B, C
Functional safety audit	Phase 10 Clause 5.2.6.2	All phases Part 1 Clause 8.2.7
Concept, scope definition, hazard and risk assessment	**Phase 1** **Clause 8**	**Phases 1, 2, 3** **Part 1 Clauses 7.2, 7.3, 7.4**
Overall safety requirements, safety function allocation	**Phase 2** **Clause 9**	**Phases 4, 5** **Part 1 Clauses 7.5, 7.6**
Safety requirements specification	**Phase 3** **Clause 10**	**Phase 9** **Part 1 Clause 7.10**

Management and safety lifecycle planning is of fundamental importance because it provides the framework for achieving systematic integrity.

Functional safety depends primarily on the prevention and elimination of systematic failures, and that can only be achieved through effective management and safety lifecycle planning.

The hazard and risk assessment, safety function allocation and the SRS provide the technical basis for the whole system. Again, these are of fundamental importance for systematic integrity.

There is a tendency to think operations are problematic, but in the past almost half of serious hazardous incidents have been caused by errors in specification and nearly 60% of errors are specification with consequent errors in design. Refer to the HSE UK paper ‘Out of control: Why control systems go wrong and how to prevent failure’.

The SRS must fully specify performance requirements as well as the functional requirements.

Assessors commonly find that the SRS is incomplete. There are usually several specification topics that the designers have not fully understood. Typical examples are the actual demand rate, requirements for the speed of response required from safety functions and the criteria for successful actuation of functions. It is also common to find inadequate specification of requirements for responding to failures detected within functions.

The assessor should also ask how the performance will be measured during operation. If a limit has been specified on a leakage rate does the design allow the leakage rate to be measured with the equipment installed in position? During proof testing when the system is unavailable, are other layers of protection identified?

4.2 Expected Inputs

During the detailed planning for the Stage 1 FSA the assessor should work together with the project team to identify the inputs that may contain the evidence of compliance.

For Stage 1 the inputs might typically include:

- Project management and quality management:
  - Corporate policies and standards;
  - Functional Safety Management Plan;
  - Project execution plan;
  - Project quality plan;
  - Functional safety management planning documents;
  - Competence assessment system description;
  - Competence assessment records;
  - Competency Records;
  - Safety Validation Plan;
  - Recommendations management procedures;
  - Internal audit and assessment plans;
  - Change management procedure;
  - Configuration management plan;
  - Document and information management procedure;
  - Configuration management procedure;
  - Safety lifecycle plan or equivalent definition of inputs, outputs and responsibilities;
  - Verification (checking) procedures;
  - Techniques and measures plan;
  - Audit plan.
- Conceptual design:
  - Basis of design;
  - Conceptual design report.
- Risk Assessment and safety function allocation:
  - Terms of reference or procedures for hazard and risk studies;
  - Hazard identification and assessment reports;
  - SIL determination reports;
  - Security risk assessment.
- Requirements:
  - Safety requirements specification.

4.3 Expected Outputs

The output from Stage 1 FSA will typically include.

- FSA plan;
- Completed Stage 1 FSA checklists;
- Interim FSA report with conclusions and recommendations;
- FSA Compliance Statement for Stage 1.

4.4 Review – Hazard and Risk Assessment and SIL Allocation

The Hazard and Risk Assessment process is reviewed for implementation and assessment of the reports from this process is undertaken at this stage. The methods of SIL determination and allocation is also reviewed for appropriateness as part of this stage of assessment. Review is performed as to how this information is transposed onto the Safety Requirements Specification and the process of information transfer to the next phase of the safety lifecycle is reviewed. There should be clear traceability between the stages so that each identified hazard can be traced through the SIL determination to the safety requirements specification.

4.5 Review – Safety Requirement Specification

The SRS at this stage is expected to be complete and verified, detailing all the requirements for each SIF, so as to enable a systems integrator to commence the design and engineering phase.

The SRS is reviewed in this context to identify whether all the SIFs have been described adequately including Sensors, Logic, Actuator, Time, target SIL, safe state definition, bypass design, reset design, action on fault, other layers of protection..

In addition the SRS will form the basis of the safety validation later on in the lifecycle so the requirements should be written in a way that a Safety Validation Plan (SVP) can be easily produced from it.

4.6 Completing the FSA Stage 1

FSA Stage 1 is performed against the Conceptual Design information, the Hazard and Risk Assessment and the Safety Requirement Specification. This FSA should be completed before commencing with the detailed design.

Functional Safety Assessment is performed by an approved assessor using FSA checklist template. The assessment will include the handover from sales to the project team (process and information transfer), Safety Requirement Specification, the project Organisation and the competence of the people executing the project.

4.7 Example Template for FSA Stage 1

The following table provides some typical FS assessment prompts during this stage of FSA. This should be considered as an aide memoir and the assessor may prepare a specific assessment questionnaire using these questions depending on the project assignment in scope.

Table 2. FSA Stage 1 Example Questions

Item	Completion Measure	Evidence
Assignment of project team		
1	Has the PM identified the SIS project members and updated the FSM plan?	
2	Are the persons assigned to the project competent to perform the SIS related activities?	
3	Is there sufficient independence in the team assignment for the V&V and assessment?	
Review of SRS, H&RA and customer information		
4	Is the SRS adequate for commencement of project design? Does the SRS represent the requirements of the H&RA?	
Basic Design		
5	Has a basic software/hardware architecture been designed to consider the required SIL integrity?	
6	If there are any non-safety elements, have they been suitably segregated in the design?	
7	If the basic design reveals the customer specified SIL target cannot be met, has this been communicated to the customer?	
Functional Safety Management		
8	Is the FSM plan for the project adequate for the required SIL?	
9	Is there a safety validation plan initiated and reviewed for the project?	

5 Functional Safety Assessment Stage 2

5.1 Introduction – Purpose of FSA Stage 2

Stage 2 FSA assesses whether the 'design and engineering' or the 'system realisation' has proceeded as planned. It looks for evidence of **traceability** both to the SRS and to the standards. It also looks for evidence of **Systematic Safety Integrity (Systematic Capability),** evidence that the planned procedures, techniques and measures have been applied effectively.

FSA stage 2 reviews the detailed design of the SIS. The following topics outlined in the table below are reviewed and evidence is sought for compliance with the clauses listed here.

Table 3. FSA Stage 2 Topics

Topic	IEC 61511-1	IEC 61508
Application program safety requirements specification	Phase 3 Clause 10	Phase 10 Part 3 Clause 7.2
System design specifications Systems engineering	Phase 4 Clause 11	Phase 10 Part 2 Clauses 7.2, 7.4
Application program / software development	Phase 4 Clause 12	Phase 10 Part 3 Clause 7.4
Integration / factory acceptance test planning	Phase 4 Clause 13	Phase 10 Part 2 Clause 7.5 Part 3 Clause 7.5
Preliminary planning for operations and maintenance (this may be covered later in Stage 3)	Phase 4/6 Clauses 16, 17	Phase 6 Part 1 Clause 7.7 Part 2 Clause 7.6 Part 3 Clause 7.6
Validation planning	Phase 4 Clause 15	Phase 7 Part 1 Clause 7.8 Part 2 Clause 7.3 Part 3 Clause 7.3
Installation and commissioning planning	Phase 4/5 Clause 14	Phase 8 Part 1 Clauses 7.9
Verification	Phase 9 Clauses 7, 12.5	Phase 10 Part 1 Clause 7.18 Part 2 Clause 7.9 Part 3 Clause 7.9
Functional safety audit	Phase 10 Clause 5.2.6.2	All phases Part 1 Clause 8.2.7

5.2 Expected Inputs

The stage 2 inputs might typically include, but not to be limited to the following:

- Detailed design:
  - Safety Requirement Specification
  - Application program safety requirements specification;
  - Design specifications;
  - Design datasheets;
  - Design drawings;
  - Device and system safety manuals;
  - Evidence of suitability of devices based on analysis of data obtained from prior use;
  - Evidence of suitability of devices based on independent assessment of compliance with IEC 61508;
  - Quantification of random hardware failure rates and probabilities;
  - Application program documentation;
  - Application program code;
  - Configuration management records;
  - Installation specifications;
  - Inspection and test plans (overall validation planning);
  - Detailed validation planning;
  - Equipment test procedures;
  - Unit or module test procedures;
  - Integration test procedures;
  - Factory acceptance test procedures;
  - Site acceptance test procedures;
  - Verification records;
  - Functional safety audit reports;
  - Factory Acceptance Test Specification;
  - Factory Acceptance Test Records;
  - Functional Design Specification;
  - Application Program.
- Operations and maintenance planning:
  - Functional safety management plan for operations and maintenance;
  - Proof test planning;
  - Spares planning.

5.3 Expected Outputs

The output from Stage 2 FSA will typically include:

- Completed Stage 2 FSA checklists;
- Interim FSA report with conclusions and recommendations, updated for Stage 2;
- SIL verification results;
- FSA Compliance Statement and / or Certificate for Stage 2.

5.4 Review – SIS Design

The review includes assessment of the design of the SIS, the techniques applied for each stage of the design, the independent reviews performed on the documentation, application program code and personnel competency. All the Test Specifications, records and review of records shall be subject to this stage of the FSA.

Perform SIL verification on completed system to ensure it meets the target SIL level after design and engineering. This should include an assessment of the systematic capability and compliance with the safety manual of all the components which form part of the SIF.

5.5 Completing the FSA Stage 2

This FSA considers all project phases up to and including Factory Acceptance Testing. The relevant sections of the FSA checklist will be addressed in this assessment. All intermediate project SIS documents will be used as supporting evidence. The completed checklist may be signed by the project SIS Lead Engineer, the Project Manager and the Functional Safety Assessor.

5.6 Example Template for FSA Stage 2

The following table provides some typical FS assessment prompts during this stage of FSA. This should be considered as an aide memoir and the assessor may prepare a specific assessment questionnaire using this template depending on the project assignment in scope.

Table 4. FSA Stage 2 Example Template

Item	Completion Measure	Evidence
SIS Design and Engineering		
1	Have requirements for segregation of SIF and non-SIF functions been applied in the segregation of software and hardware design?	
2	Does the system reset philosophy hold the SIS outputs in a safe state until a reset has been performed?	
3	Where voting groups exist, have they been designed to minimise common cause failures such as by allocating them on independent cards?	
4	Have the architecture and design requirements for the SIL been met as instructed in the safety manual of the SIS logic solver such as having EOL resistors, duplex cards etc.?	
5	Does the application program shut down the system automatically after a fault if the fault is not resolved within the MTTR?	
6	If fault action on a safety critical IO is not set to trip the system, has the fault alarm been designed as a safety critical alarm with operator action clearly defined in the operators procedures?	
7	Has the systematic capability of the system design been assessed considering the measures to avoid failures and measures to control failures?	
8	Have the hardware fault tolerance and architecture requirements for the SIL been met by the proposed design?	
9	Has the system response time been calculated and found to be within the lowest response time required by any SIF being implemented by the SIS?	
10	Has the verification confirmed that the safety functions are fully testable for both validation and regular proof testing, and accessible for inspection and maintenance?	
Application program		
11	Does the application program contain comments to explain complex functionality and cross reference SIFs?	
12	Does the FDS contain a detailed description of application specific user defined function blocks?	
13	Does the FDS contain or reference IO listing, Modbus listing etc.?	
14	Does the application program contain diagnostics for the detection, annunciation and management of faults?	
15	Have the application program requirements for the SIL been met as instructed in the safety manual of the SIS logic solver including watchdog configuration and PLC card configurations?	
16	Has the application program been implemented in a modular design?	

Item	Completion Measure	Evidence
17	Does the application program have documentation that provide the purpose of each program, traceability to input documents, identify SIFs, order of processing, explain how correctness of signals sent over communications is ensured?	
Application program testing		
18	Have the different modules and components of the SIS application program been tested independently?	
19	Have the different modules and components of the SIS application program been tested integrated?	
20	Does the application test specification cover 100% logic paths?	
21	Has the startup/operations procedure for the SIS been considered for the application test?	
22	Has the IO mapping been verified including its range and trip settings?	
23	Has the application been tested as per the test specification and all errors identified closed?	
Validation and Verification		
24	Has the application program been verified?	
25	Has the application program been validated against the SRS?	
Functional Safety Assessment		
26	Have all the punch list items identified in FSA1 been closed satisfactorily?	
27	Has the project FSM report been updated to reflect the phase gate approvals?	

6 Functional Safety Assessment Stage 3

6.1 Introduction – purpose of FSA Stage 3

Stage 3 FSA assesses the following, but not to be limited as to whether:

- The installation, commissioning and validation have proceeded as planned and with clear traceability to the SRS, the design and to the standards
- The operations and maintenance team is ready to accept handover of the systems
- The dossier of information about the system is complete

It reviews the topics outlined in the following table and looks for compliance with the clauses listed here.

Table 5. FSA Stage 3 Topics

Topic	IEC 61511-1	IEC 61508
Installation and commissioning completion	Phase 5 Clause 14	Phase 12 Part 1 Clauses 7.13
Validation completion	Phase 5 Clauses 15.2.4 to 15.2.8	Phase 13 Part 1 Clauses 7.14 Part 2 Clause 7.7 Part 3 Clause 7.7
Operations and maintenance procedures	Phase 6 Clause 16	Phases 6, 14 Part 1 Clauses 7.7, 7.15 Part 2 Clause 7.6 Part 3 Clause 7.6
Modification procedures (including decommissioning)	Phases 7, 8 Clauses 17, 18	Phases 15, 16 Part 1 Clauses 7.7, 7.16 Part 2 Clause 7.8 Part 3 Clause 7.8
Verification	Phase 9 Clauses 7, 12.5	Phase 10 Part 1 Clause 7.18 Part 2 Clause 7.9 Part 3 Clause 7.9
System information	Clauses 11.2.13, 19	Part 1 Clause 5 Part 2 Annex D Part 3 Annex D
Functional safety audit	Phase 10 Clause 5.2.6.2	All phases Part 1 Clause 8.2.7

6.2 Expected Inputs

The stage 3 inputs might typically include, but not to be limited to the following:

- Installation, commissioning and validation:
  - Updated SRS;
  - Design Manual;
  - Completed inspection and test plans (overall validation planning);
  - FAT punch list;
  - Site Acceptance Test Specification;
  - Site Acceptance Test Records;
  - Validation reports: including completed validation procedures or specifications;
  - Configuration management records;
  - Equipment test records;
  - Unit or module test records;
  - Integration test records;
  - Factory acceptance test records;
  - Installation inspection and test records;
  - Commissioning records;
  - Site acceptance test records;
  - Confirmation of validation of other layers of protection against the safety requirements for those layers (e.g. relief valves, bunds, pressure vessel certification);
  - Verification records;
  - Functional safety audit reports.
- Operations and maintenance planning and procedures:
  - Functional safety management plan for operations and maintenance;
  - Operation procedures;
  - Preventive maintenance procedures;
  - Corrective maintenance procedures;
  - System performance data collection and analysis procedures;
  - Incident recording and analysis procedures;
  - Bypass and override procedures;
  - Periodic inspection procedures;
  - Periodic proof test procedures;
  - Spares inventory management;
  - Operator training and competence;
  - Maintainer training and competence.

6.3 Expected Outputs

The output from Stage 3 FSA will typically include.

- Completed Stage 3 FSA checklists;
- Final FSA report with conclusions and recommendations, updated for Stage 3;
- FSA Compliance Statement for Stage 2;

6.4 Review – Validation of specific items against SRS

It is regrettably very common for project teams to assume that successful commissioning is synonymous with validation and to assume that many aspects of performance do not need to be tested. Validation requires demonstration that the SIFs and SIS after installation, meet each specific requirement outlined in the SRS.

The assessor must establish that there is reliable evidence that compliance with all of the performance requirements for the SIFs has been demonstrated after installation. For example this might include testing the stroking time of valves, the leakage rate and the time to vent pressure to the specified level.

The assessor must also confirm that the records show exactly which version and which serial numbers were tested. Many experienced commissioning engineers do not appreciate that serial numbers must be recorded as otherwise there is no way of telling exactly which items were tested.

6.5 Review – Proof Testing

It is important to appreciate that validation and proof testing have different objectives.

The primary objective of validation is to test that the safety functions achieve the requirements of the safety requirements specification. Site acceptance testing is primarily concerned with proving that the system functions correctly.

The basic objective of regular proof testing and inspection during operation is to reveal dangerous failures that have not been detected by diagnostics.

Procedures for periodic inspection and proof test can be developed from a subset of validation procedures but particular attention must be paid to finding all of the undetected failures. The procedures should be based on some form of failure mode analysis.

Unrevealed dangerous failures can accumulate with time if the proof testing procedures do not provide complete coverage.

6.6 Review – Management of Change

The assessor should confirm that the operations and maintenance team has a clear understanding of types of changes may have an impact on functional safety.

Any change that affects the hazard rate, the demand rate, the consequences or the dynamic response of the equipment under control must be controlled. Seemingly simple changes may impact the risk reduction requirements, such as:

- Adjusting controller setpoints or tuning
- Changing valve trim size or characteristic
- Increasing velocity
- Increasing occupancy levels
- Changing fluid density

Any change that affects safety lifecycle outputs must be controlled. This includes changes to specifications.

There must be evidence that the persons authorised to approve modifications are competent to do so.

6.7 Review – Reliability

The assessor should confirm that the operations and maintenance team has a clear understanding of how failure rates are estimated and how causes of failures must be analysed.

The analysis of failures should be determining which failures are avoidable or preventable and should determine whether the failure rates are reasonably constant and consistent with the failure rates assumed in the design.

The assessor should confirm that the operations and maintenance team has a clear understanding of how demand rates are associated with alarm rates and process excursion frequency and duration.

6.8 Review – Operation and Maintenance

The assessment shall review the requirements for enabling appropriate Operation and Maintenance provisions of the SIS.

6.9 Completing the FSA Stage 3

The review shall assess that the Installation, Commissioning and Validation of the SIS does not compromise functional safety and that it satisfies clauses 14 and 15 of IEC 61511 standard.

6.10 Example Template for FSA Stage 3

The following table provides some typical FS assessment prompts during this stage of FSA. This should be considered as an aide memoir and the assessor may prepare a specific assessment questionnaire using this template depending on the project assignment in scope.

Table 6. FSA Stage 3 Example Template

Item	Completion Measure	Evidence
Installation		
1	Are there specifications and procedures for the materials, work, inspection and testing?	
2	Have personnel carrying out the installation been trained to the level appropriate for their assigned tasks?	
3	Are installation procedures designed and managed to reduce CCF?	
4	Is there sufficient independence between those carrying out the work and inspecting it?	
5	Have adequate standards been specified for the installation phase?	
6	Is the SIS inspected to reveal damage caused by the installation phase?	
7	Are installation and inspection procedures sufficiently explicit in their detail so that they do not leave important decisions or interpretations to be made by installation personnel?	
8	Is the installation consistent with the SRS?	
SIF Validation		
10	Are there specification and procedures for validation of each SIF?	
11	Are proof test procedures for each SIF device defined?	
12	Are test records maintained?	
13	Do the tests adequately cover the SIS in accordance with the requirements defined in the SRS?	
14	Has appropriate training been given to the personnel involved?	
15	Have discrepancies in expected results been resolved?	
16	Are SRS modifications reviewed through management of change?	
Operations Planning		
17	Has an adequate plan for the Operations and Maintenance phase been developed?	
Functional Safety Assessment		
18	Have all the punch list items identified in FSA1 and FSA2 been closed satisfactorily?	
19	Has the project FSM report been updated to reflect the phase gate approvals?	

7 References

7.1 References used in this guidance

[1] Functional safety of electrical / electronic / programmable electronic safety-related system - IEC61508 Edition 2.0, 2010.

[2] Functional safety – safety instrumented systems for the process industry sector - IEC61511 Edition 2, 2016.

[3] CDOIF, Chemical and Downstream Oil Industries Forum, Guideline, Functional Safety Management of Installed Safety Instrumented Systems, v1.0.

7.2 Further Reading

[1] Health and Safety Executive, Managing competence for safety-related systems Part 1: Key guidance (http://www.hse.gov.uk/humanfactors/topics/mancomppt1.pdf).

[2] Health and Safety Executive, Managing competence for safety-related systems Part 2: Supplementary material (http://www.hse.gov.uk/humanfactors/topics/mancomppt2.pdf).

[3] HSE UK paper 'Out of control: Why control systems go wrong and how to prevent failure'. (http://www.hse.gov.uk/pubns/books/hsg238.htm).

[4] Conformity Assessment of Safety-related Systems (CASS) Targets of Evaluation (TOEs) for Functional Safety Management and Overall Lifecycle Assessment against the requirements of IEC61508 and IEC61511 (https://www.61508.org/downloads/index.php). Further information on CASS can be found at https://www.61508.org/cass/index.php.

Appendix A – Principles of Functional Safety

A.1 Hazard and Risk Assessment

Functional safety starts with identification of each hazardous scenario associated with an item of equipment. The risk of harm being caused by each hazardous scenario is characterised in terms of consequence and likelihood.

The estimated risks are compared with the levels of risk that are considered to be tolerable by that business, in the context of the values generally held in the society. The risk reduction required from the safety related systems is then determined for each hazardous scenario.

The risk reduction is always based upon other layers of protection and not just the SIF. The SIF is handling the remaining gap. Therefore the Hazard & Risk Assessment must reference all the other layers of protection that have been considered when calculating the gap for the SIF (if any of these change then the gap changes with it and so the SIL rating and PFDavg for the SIF also change).

We can only achieve functional safety by basing it on a reasonably objective analysis of the hazards and risks of the process or equipment under control.

To make a judgement about the functional safety achieved, an FSA must first establish that a reasonable effort was made in the hazard and risk assessment and the targets for tolerable risk are reasonable in the context of society's values.

A.2 Risk reduction requirements

The risk reduction required from a safety related system depends on:

- The demand rate on the safety related system for each hazard (depending on effectiveness of other preceding risk controls)
- The consequences of the hazard if all of the risk controls were to fail
- The tolerable frequency of those hazardous consequences

The safety integrity level (SIL) depends directly on the risk reduction required. The SIL can be interpreted as representing the approximate order of magnitude of the risk reduction required.

A SIL 1 demand mode safety function is designed to reduce risk by at least one order of magnitude. A SIL 1 continuous mode safety function is designed to fail at a rate at least one order of magnitude lower than a non-safety rated function.

SIL 2 corresponds to a reduction of at least two orders of magnitude and SIL 3 corresponds to a reduction of at least three orders of magnitude.

In practice, functional safety can only distinguish risk reduction in terms of orders of magnitude. The uncertainty in the assumptions made and in the data available prevents a more precise characterisation.

To make a judgement about the functional safety achieved, an FSA must review how the risk reduction targets were allocated to the safety related systems and other layers of protection.

In context of the hierarchy of hazard controls, functional safety depends on a combination of engineering controls and administrative controls.

The FSA must ask the question why was hazard elimination or substitution not possible? Could 'safety by design' not have been achieved at a reasonable cost?

A.3 Safety Integrity

Functional safety maintains safety integrity of assets in two ways:

- **Systematic safety integrity** deals with preventable failures. These are failures resulting from errors and shortcomings in the design, manufacture, installation, operation, maintenance and modification of the SIS.
- **Hardware safety integrity** deals with controlling random hardware failures. These are the failures that occur at a reasonably constant rate and are completely independent of each other. They are not preventable and cannot be avoided or eliminated.

In practice at least 90% of failures in safety functions are preventable to some degree, though it may not be practicable to eliminate them completely. For this reason systematic safety integrity is (arguably) far more important than hardware safety integrity, and **functional safety is primarily to do with the prevention of failure.**

A.4 Hardware Safety Integrity

The risk reduction achieved by a safety function depends on the probability of random hardware failure of the safety function.

By definition, random failures are those that occur at a reasonably constant rate and are independent of other failures. The probability of failure can be estimated from the failure rate by using the principles of random or 'stochastic' processes.

The probability of failure due to random failure of components is directly proportional to all of these factors:

- Component failure rates
- The proportion of failures that share a common cause (though many common-cause failures are systematic in nature)
- The time interval between periodic inspection and testing
- The proportion of dangerous failures that cannot be found by testing
- The time period during which protection is out of service due to failure or deliberate bypass.

To make a judgement about the functional safety achieved, the FSA must review how the random hardware failure rates were managed and how the probability of failure was reduced to meet the targets.

A.5 Systematic Safety Integrity

The rate or probability of systematic failures cannot easily be quantified. In functional safety the main focus is on preventing systematic failures by applying conventional **quality management:**

- Clear statement of policies, standards and objectives for safety and risk management
- Definition of organisation, responsibilities and interfaces with respect to safety integrity
- Ensuring that those involved in any functional safety activities are competent to carry out the activities for which they are accountable
- Ensuring that the hazard and risks associated with the process have been identified and risk reduction requirements determined
- Complete and consistent statement of requirements for the safety related system and its safety functions (i.e. the SRS), traceable to the hazard and risk analysis and to the owner's policies, standards and objectives
- 'Safety Lifecycle Planning':
    - Definition of the activities to achieve and maintain risk reduction and the outputs that will be produced from those activities
    - Definition of those responsible for the activities and outputs
    - Planning of the checking, review, inspection and testing (i.e. verification) to ensure that the outputs are correct

    - Planning of the techniques, measures and procedures to be used in order to prevent or eliminate failures
- Preparation of specifications and instructions for design and implementation of the safety related system, traceable to the SRS
- Design and implementation of the safety related system hardware and software in accordance with the approved specifications and instructions, and with demonstration of systematic capability
- Verification (checking, review, inspection and testing) of the outputs as planned in order to find and eliminate preventable failures
- Keeping detailed auditable records of the verification so that there is clear evidence of what was actually checked
- Validation of the installed (or modified) systems to demonstrate that all of the requirements are fulfilled
- Control of changes and modifications so that safety integrity is maintained
- Management of recommendations and actions through to resolution
- Control of information relating to the system
- Periodic independent audit to review compliance with procedures and standards
- Periodic independent FSA to determine if functional safety is achieved and maintained.

Systematic integrity cannot easily be quantified in terms of order of magnitude.

Conceptually, the level of quality management for a SIL 3 safety function needs to be at least two orders of magnitude better than for basic non-safety functions. The effort put into preventing, finding and eliminating preventable failures needs to be something like at least 100 times better than for 'ordinary' quality control (though of course we cannot quantify it). Even for a SIL 1 function the quality management needs to be demonstrably better than for non-safety.

To make a judgement about the functional safety achieved, an FSA must review how quality management procedures, techniques and measures were selected and applied.

What evidence is available to show that enough effort was made to eliminate preventable failures?

This judgement is highly subjective. The effectiveness of the quality management cannot be precisely quantified. Ultimately it is a question of whether there is evidence that a reasonable effort was made, given the assessor's experience of best practice in the industry.

Appendix B – Functional Safety Assessment Stage 4 and 5

B.1 Introduction

The UK Health and Safety Executive (HSE) tasked the Chemical and Downstream Oil Industries Forum (CDOIF) with setting up a working group to provide guidance specifically for installed systems. A guideline published by the working group entitled 'Management of Installed Safety Instrumented Systems' contains sections which focus on FSA stages 4 and 5 which are applicable to installed systems. The sections below provide a brief overview of these. For further information refer to the CDOIF guidelines.

B.2 FSA Stage 4

Stage 4 FSA assesses whether:

- The operations and maintenance have proceeded as planned
- Periodic inspections and proof tests were completed as planned and demonstrate that safety integrity (functionality and reliability) has been maintained with clear traceability to the SRS and to the standards
- System and equipment performance and incident statistics have been collected and analysed
- Modifications have been controlled
- Systems configuration has been managed
- Maintenance records are complete
- Functional safety audits have been completed as planned
- Hazard and risk assessments have been reviewed and maintained
- The dossier of information about the system is complete and up to date

It reviews the topics outlined in the following table and looks for compliance with the clauses listed here.

Table 7. FSA Stage 4 Topics

Topic	IEC 61511-1	IEC 61508
Installation and commissioning completion	Phase 5 Clause 14	Phase 12 Part 1 Clauses 7.13
Operations and maintenance	Phase 6 Clause 16	Phases 14 Part 1 Clauses 7.7, 7.15 Part 2 Clause 7.6 Part 3 Clause 7.6
Modification procedures (including decommissioning)	Phases 7, 8 Clauses 17, 18	Phases 15, 16 Part 1 Clauses 7.7, 7.16 Part 2 Clause 7.8 Part 3 Clause 7.8
Verification	Phase 9 Clauses 7	Phase 10 Part 1 Clause 7.18 Part 2 Clause 7.9 Part 3 Clause 7.9
System information	Clause 19	Part 1 Clause 5
Functional safety audit	Phase 10 Clause 5.2.6.2	All phases Part 1 Clause 8.2.7

The stage 4 inputs might typically include, but not to be limited to the following:

- Operations and maintenance planning and procedures:
  - Functional safety management plan for operations and maintenance;
  - Operation procedures;
  - Preventive maintenance procedures;
  - Corrective maintenance procedures;
  - System performance data collection and analysis procedures;
  - Incident recording and analysis procedures;
  - Bypass and override procedures;
  - Periodic inspection procedures;
  - Periodic proof test procedures;
  - Spares inventory management;
  - Operator training and competence;
  - Maintainer training and competence.
- Operations and maintenance records:
  - Completed work order records;
  - Competence and training records;
  - Performance analysis reports;
  - Alarm analysis reports;
  - Incident analysis reports;
  - Bypass logs;
  - Configuration management records;
  - Hazard and risk assessment reviews;
  - Functional safety audit reports.

The output from Stage 4 FSA will typically include:

- Completed Stage 4 FSA checklists;
- Stage 4 FSA report with conclusions and recommendations.

B.3 FSA Stage 5

Stage 5 reviews the control, authorisation and implementation of modifications, revisiting stages 1, 2 and 3. Refer to the sections above for Stages 1, 2 and 3. Further to those stages, Stage 5 FSA reviews the topics outlined in the following table and looks for compliance with the clauses listed here:

Table 8. FSA Stage 5 Topics

Topic	IEC 61511-1	IEC 61508
Modification procedures (including decommissioning)	Phases 7, 8 Clauses 17, 18	Phases 15, 16 Part 1 Clauses 7.7, 7.16 Part 2 Clause 7.8 Part 3 Clause 7.8
Verification	Phase 9 Clauses 7	Phase 10 Part 1 Clause 7.18 Part 2 Clause 7.9 Part 3 Clause 7.9
System information	Clause 19	Part 1 Clause 5
Functional safety audit	Phase 10 Clause 5.2.6.2	All phases Part 1 Clause 8.2.7

The FSA of a simple minor modification may be conducted in one single phase. For any complex or large modification or any modification that takes longer than several months consider staging the FSA as Stage 5.1, 5.2 and 5.3.

The Stage 5 FSA must start before modification work starts on site. The assessor must establish that the modification has been planned and designed to address hazards and failures that may occur during the modification work.

The Stage 5 FSA can only be completed after the modification work has been completed on site and the system has been re-validated to the extent that it was modified.

Complete validation of the modified safety functions may be impracticable if the changes are made without interrupting operation. The assessor will need to make a judgement as to whether the validation has been sufficient according to the risks.

The stage 5 inputs are defined in FSA stages 1, 2 and 3.

The output from Stage 5 FSA will typically include:

- Completed Stage 5.1, 5.2 and 5.3 FSA checklists;
- Stage 5 FSA report with conclusions and recommendations.