CDOIF

Chemical and Downstream Oil Industries Forum

Guideline

Functional Safety Management of Installed Safety Instrumented Systems

Foreword

In promoting and leading on key sector process safety initiatives, CDOIF has developed through its members this guideline to assist operators in understanding and applying IEC 61511 *Functional safety. Safety instrumented systems for the process industry sector* to installed Safety Instrumented Systems (SIS).

It is not the intention of this document to replace any existing corporate policies or processes.

There are no limitations on further distribution of this guideline to other organisations outside of CDOIF membership, provided that:

1. It is understood that this report represents CDOIF's view of common guidelines as applied to the functional safety management of installed SIS.
2. CDOIF accepts no responsibility in terms of the use or misuse of this document.
3. The report is distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "CDOIF Guideline – Functional Safety Management of Installed Safety Instrumented Systems".
4. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the report except that it is believed to be substantially correct at the time of publication.

It should be understood that this document does not explore all possible options for demonstrating compliance of installed SIS with IEC 61511, nor does it consider individual site requirements – Following the guidance is not compulsory and duty holders are free to take other action.

Contents

1. EXECUTIVE SUMMARY

Safety Instrumented Systems (SIS), where installed within the process industry sector, are an important measure in reducing the risks of harmful events. They provide a layer of protection to prevent plant or process entering a state which could result in harm to either people or the environment.

They are typically implemented together with other measures which can be used to demonstrate that the site operator has done all that they reasonably can to reduce the risk of a hazardous event occurring. Demonstrating this risk reduction can be part of an *As Low As Reasonably Practicable* (ALARP) demonstration.

The design, operation and maintenance of SIS are particularly important because they provide a significant risk reduction. The international standard that has been adopted for SIS as applied to process industries is the current version of IEC 61511 *Functional safety - Safety instrumented systems for the process industry sector*.

The purpose of this guidance is to provide a common framework by which SIS that are already installed and operational can be managed and how they can be demonstrated to align with IEC 61511 so far as is reasonably practicable. A definition of what is meant by an installed SIS can be found in Section 2.2 *Definition of an Installed SIS*.

This guidance provides a reference by which existing site procedures, practices and standards can be reviewed or developed to ensure that installed SIS are appropriately managed. Further information on the applicability and audience for this publication can be found in Section 2.

2. INTRODUCTION AND SCOPE

CDOIF guidance is primarily written for and on behalf of site operators and therefore this publication aims to be short, concise and use common terminology that would be understood by this audience and who are already familiar with IEC 61511 requirements. Practitioners may also find this publication to be a useful reference.

This document describes how suitable management systems could be adopted to ensure and demonstrate that the objectives of the installed SIS are achieved and maintained so far as reasonably practicable.

Management systems for SIS are referred to as Functional Safety Management Systems (FSMS).

The activities required for functional safety management will normally be best achieved if they are integrated with the site operator's wider management systems which could include Safety Management Systems (SMS) and Competency Management Systems (CMS). The overall policy and strategy for achieving functional safety should be defined providing references to these wider management systems where relevant.

This guidance includes information on:

1. the basic management and lifecycle activities required. For example; policy, planning procedures, auditing, competence assurance and monitoring for installed SIS.

2. key considerations for operation and maintenance of installed SIS.

3. the processes required to assess if the functional safety requirements of the installed SIS are adequate through review and periodic functional safety assessment in a proportionate manner.

4. demonstrating that the requirements of the installed SIS are maintained during modification and decommissioning.

NOTE: the examples provided in the appendices are generic and would need to be modified to make them relevant to a specific site.

2.1 Background

Functional safety management is a key requirement to ensure that the Installed SIS will operate correctly when required. Correct application of functional safety management ensures that faults that could have be introduced or occur through the design, installation, maintenance, operation or modification of the SIS are detected and minimised throughout its life – functional safety management is therefore considered an essential safety risk and environmental major accident risk control measure.

IEC 61511 includes management requirements and describes a life-cycle approach for SIS. However, it is sometimes difficult to apply these requirements to installed SIS particularly where the earlier stages of the life-cycle are unknown or have been delivered through a separate corporate entity or third party. Refer to Section 3.1 for further information.

2.2 Definition of an installed SIS

The term *Installed SIS* used within this guidance implies any instrumented function that provides significant safety risk reduction (SIL 1 or higher) which would meet the definition of a Safety Instrumented System in IEC 61511 irrespective of when it was installed.

This guidance has been developed specifically to address Safety Instrumented Functions (SIF) operating in low demand mode systems, but the broad requirements apply equally to high demand and continuous systems.

It is recognised that site operators may have a range of operational installed SIS including those:

1. installed not in compliance with any version of IEC 61511, sometimes referred to as legacy SIS, and hence unlikely to comply with the latest version of the standard.

2. installed in accordance with earlier versions of IEC 61511 and compliant with the standard at that time. The SIS may or may not comply with the latest version of the standard.

3. installed in accordance with IEC 61511 but were not fully compliant with the standard or may not have sufficient documentation in place to demonstrate ongoing compliance.

For the management of instrumented systems providing safety functions of low / undefined safety integrity, refer to HSE Operational Guide (OG) 46 *Management of instrumented systems providing safety functions of low/undefined safety integrity.*

2.3 Regulatory approach for installed SIS

The view of the Health and Safety Executive (HSE) regarding installed SIS and compliance with IEC 61511 (adopted in the UK as BS EN 61511) is summarised as follows:

- Health and Safety law in Great Britain requires that risks are reduced to ALARP. Where applicable the Control of Major Accident Hazards (COMAH) regulations also require that all necessary measures are taken to reduce major accident risks (interpreted to mean that risks are reduced to ALARP), and that this is demonstrated.

- HSE Inspectors will refer to relevant good practice when making judgements about a site operator's compliance with the law. IEC 61511 is recognised by the HSE as relevant good practice for SIS and is used by the HSE to benchmark site operators.

- Site operators can demonstrate ALARP by other equivalent means than demonstration of compliance with IEC 61511, but this demonstration of equivalence could be a challenging and lengthy process.

- For installed SIS, it is recognised that retrospective application of the full requirements of the current version of IEC 61511 may not be reasonably practicable (whether or not the SIS was originally compliant with previous versions) and therefore it is not expected that SIS hardware / software be upgraded or replaced to seek full compliance with the current version of IEC 61511 but instead decisions are made based upon whether improvements would deliver risk reduction in a reasonably practicable way.

- The law also requires that site operator's put in place management systems to determine, implement, maintain and monitor the risk reduction requirements - this applies to installed SIS.

For the full range of operational installed SIS described in section 2.2, the HSE shall consider the overall approach taken by the site operator to ensure that the risks are being managed in a proportionate manner.

2.4 Using this guidance

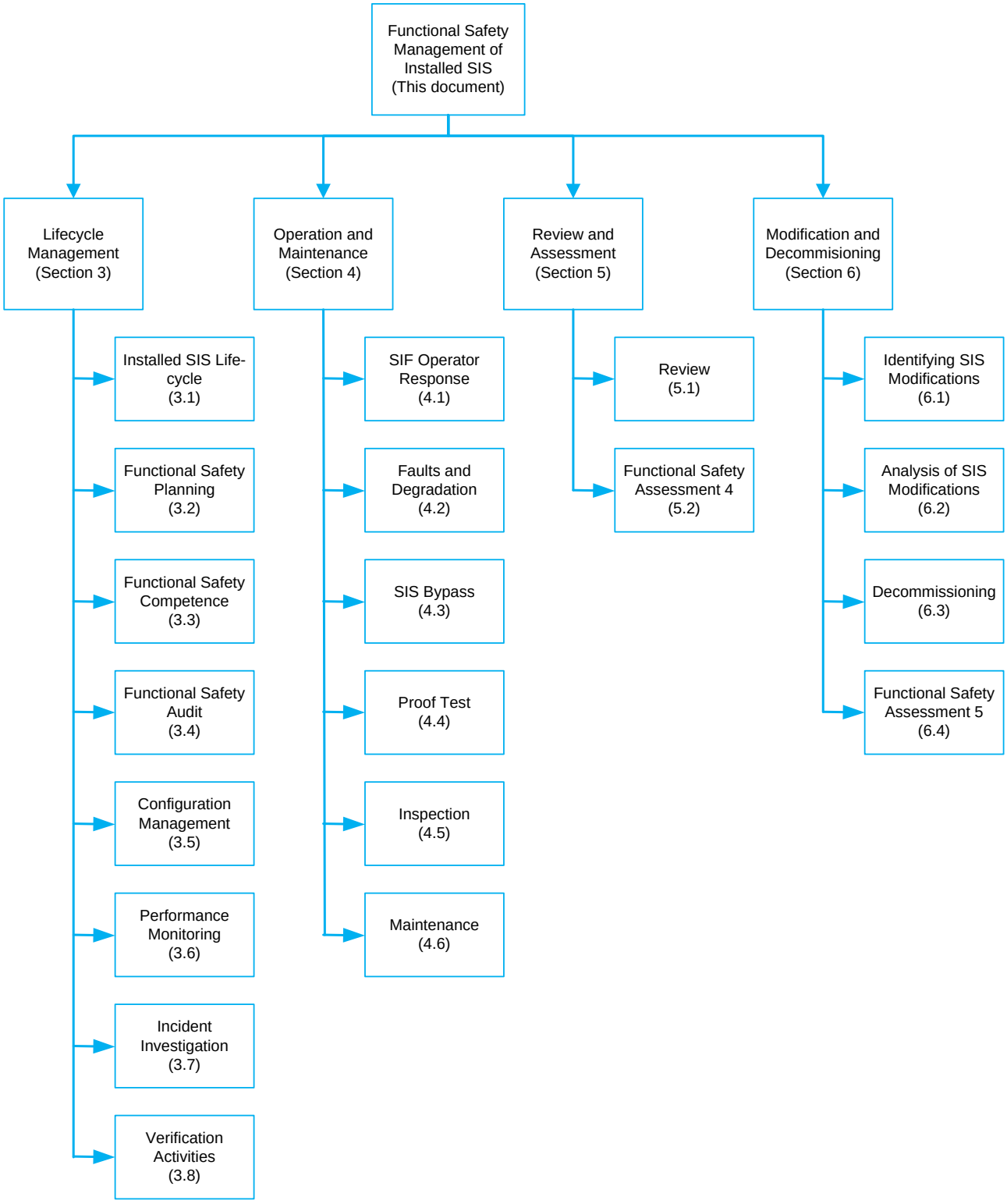


Figure 1 – Using this guidance

3. LIFE-CYCLE MANAGEMENT

Functional safety management is a process by which the functional integrity of the installed SIS can be reviewed, measured and maintained. The FSMS may be integrated into existing systems such as the overarching safety management systems and competency management systems to provide an overall safety management system for the site.

Regardless of this integration, a functional safety plan should be developed for the installed SIS – this may include references to existing procedures or processes that are utilised. Further information on the safety planning can be found in Section 3.2.

Functional safety management policy and procedures should be in place for all relevant life-cycle activities for installed SIS.

3.1 Installed SIS life-cycle

The concept of a safety life-cycle is very important since it facilitates the adoption of a systematic approach to ensuring that all relevant factors that have an impact on the achievement of functional safety are addressed on a phase by phase basis.

The scope of this guidance covers any Installed SIS in the operation and maintenance phase.

In IEC 61511, the objectives to be achieved and the requirements to meet those objectives, are specified for each phase of the safety fife-cycle. Refer to Appendices 1 and 2 for further information.

Although the focus of this guidance is on the later life-cycle phases, it is essential that there is full traceability from all previous phases back to the Hazard and Risk Assessment phase to ensure that all the assumptions affecting functional safety maintain their validity. Once traceability is lost then the basis on which the SIF can be managed is undermined and could lead to decisions being taken on an invalid basis. For some installed SIS, this traceability may have been lost and will require re-establishing at the first review point – refer to section 5.

The site operator should generate a safety life-cycle that defines:

1. the phases required to establish and organise the requirements for the life-cycle activities for the Installed SIS.

2. the objectives of each life-cycle phase for the installed SIS.

3. the documented inputs and outputs for each life-cycle phase for the installed SIS.

4. the verification activities for each life-cycle phase for the installed SIS.

An example of a safety life-cycle for installed SIS is shown in Appendix 1. This has been slightly modified from IEC 61511 to separate the earlier lifecycle phases in order to emphasise the scope of this guidance which is the operation and maintenance, modification and decommissioning phases and associated functional safety management and verification phases.

Examples of the installed SIS objectives and documentation inputs and outputs is provided in Appendix 2.

3.2 Functional safety planning

IEC 61511 *Safety Planning* requires that safety planning shall take place; this includes activities associated with installed SIS. The Functional Safety Plan (also known as the SIS Safety Life-cycle Plan) is a document or compilation of documents that shall be updated throughout the life-cycle of the SIS. It should be used as an integral part of the functional safety management system to control safety planning of the SIS.

The site operator should take ownership of the existing safety life-cycle plan, if created during earlier life-cycle phases or create and maintain a functional safety plan which:

1. defines the activities required for each life-cycle phase for the installed SIS along with criteria, techniques, measure and procedures required. This should be of sufficient detail to define the tasks to be completed and the competence requirements.

2. defines the persons and/or organisations responsible for conducting the activities of the life-cycle phases for the installed SIS.

3. sets out timescales for the life-cycle activities for the installed SIS.

3.3 Functional safety competence

Of importance to functional safety management is that persons, departments or other organisations (including contractors and sub-contractors) having responsibility for functional safety of installed SIS are identified and informed of the responsibilities assigned to them; and are competent to carry out those responsibilities.

The purpose of this activity is to ensure that the individual and team competence required to undertake defined life-cycle activities for the installed SIS, and the tasks that form part of these activities, are in place.

A Competency Management System (CMS) is required for staff at all levels of responsibility within an organisation. The CMS needs to match the technical and personal aspects of the individual and team competences that are required for functional safety at the relevant life-cycle phases. For this the site operator should:

1. have a CMS in place for functional safety. The CMS may be part of a wider CMS system, or a standalone system.

2. have a process in place to ensure that those responsible for installed SIS life-cycle activities (including any third parties) are informed of their responsibilities

3. specify and document the competencies required for each life-cycle activity task for the installed SIS, considering the components of competence described in Appendix 3; For example:

- 'Manage functional safety' could require the competencies 'knowledge of the company FSMS, risk assessment etc., relevant experience and managerial and leadership of the FS team'

- 'Proof testing' could require the competencies 'knowledge of the plant and systems, technical skills, qualifications and experience'.

4. define and document the level of competency (e.g. beginner, supervised practitioner, practitioner, expert) required for each life-cycle activity task.

5. assess and document the level of competence achieved of the person, team or other organisation relevant to each life-cycle activity task;

6. compare the required (step 4) and achieved (step 5) competence. This comparison will facilitate an objective judgement to be made as to whether the person, team or organisation is competent to undertake the defined life-cycle activity task.

7. carry out and document necessary instruction, training and experience to manage competency including where necessary periodic refresher training and assessment.

8. understand that for other organisations, competence may be managed by that organisation. The site operator should gather sufficient evidence through review / audit etc. of their quality / functional safety management system to ensure that competence is assured and that this evidence is recorded and available to the site operator.

9. manage any organisational changes that may impact individual or team competence.

Additional guidance on competence management can be found in the following publications:

- HSE and IET Code of Practice: Competence for Safety-Related Systems.

- IChemE Safety Centre Guidance; Process Safety Competency – a model 2015

- The 61508 Association: Conformity Assessment of Safety-related Systems (CASS) - (Assessing compliance to IEC 61508 and related standards)

Note that the above guidance contains important concepts in terms of defining competence requirements and levels of competence. A proportionate approach should be taken in determining the amount of detail to be included, for example the number of tasks defined for each role.

3.4 Functional safety audit

Functional safety audit is a review of the processes and procedures that have been developed to manage the SIS throughout the functional safety life cycle and is therefore applicable to installed SIS. Typical audits include:

- verification that functional safety management procedures are current and valid.
- verification that personnel are following the procedures.
- verification that the latest version of the procedures is in use.
- verification that changes to procedures are managed appropriately.

The site operator should develop procedures for carrying out audits of the installed SIS functional safety management systems. The procedures should also cover the periodicity of the audit and the management of any corrective actions that may be identified. The periodicity of the audit could be aligned (and carried out together) with that of existing management system audits. They should be carried out by an independent person who is familiar with carrying out audits, for example the site quality manager. Functional safety audits may also be integrated and carried out with functional safety assessment, so long as the requirements are addressed.

Refer to Appendix 4 for an example checklist for a functional safety audit.

3.5 Configuration management

IEC 61511 requires that procedures for configuration management of the SIS during any SIS safety life-cycle phase shall be available and therefore applies to installed SIS.

The site operator should develop and maintain an asset register which provides a method by which:

- all SIS related devices, components and documentation are uniquely identified, e.g. by tag.
- SIS device and component hardware and firmware model, version and serial numbers etc. are recorded.
- SIS software configuration (application program) versions are recorded.
- actions arising for example from observations on site or the Original Equipment Manufacturer (OEM) can be tracked.
- devices and versions can be controlled during, for example, modification and repair activities.
- documentation relating to the SIS and its components can be controlled and subject to management of change.

3.6 Performance monitoring

3.6.1 Evaluation of SIS performance

IEC 61511 includes specific requirements to evaluate the performance of the SIS with respect to systematic failures, SIS reliability data and SIS demand rates for the purposes of ensuring that assumptions made during the early lifecycle phases remain valid.

For installed SIS, some of the assumptions made during the earlier lifecycle phases may not be available; for example, if no Probability of Failure on Demand (PFD) calculation is available it will not be clear what failure rates have been assumed of the SIS components, or the hazard and risk assessment may not have been sufficiently detailed to determine what demand rate on the SIS was assumed. In these cases, it will be necessary to re-establish the assumptions – see section 5.1.

Often the causes of SIS component failures are assumed to be random hardware failure. However, in many cases if they are properly analysed the causes are systematic in nature and are predictable and preventable. There is a requirement to analyse all failures and condition monitoring data of the installed SIS to identify if systematic failures so that further failures can be prevented.

Note that the requirements of this section should be completed periodically. In this guidance, it is recommended that SIS performance evaluation is completed as part of the wider review and assessment of Installed SIS (see section 5) or integrated as part of the process safety performance indicators for the site (see section 3.6.2).

The site operator should implement procedures to gather information for analysis and review of the following:

1. SIS equipment condition monitoring data and details of all SIS failures (safe or dangerous) revealed or detected during operation, maintenance, inspection or test and analysis. This data can help in the identification of systematic failures (e.g. suitability of the component in the conditions it is working under, installation or environmental issues etc.) and requirements for rectification and prevention of these systematic failures.

2. Actual reliability data of SIS components experienced during operation and maintenance. This should be compared to the assumptions made in the PFD calculation.

3. Actual SIS activations i.e. the demand on each SIF. This should be compared to the assumptions made at the Hazard & Risk Assessment life-cycle phase.

The outcome of the analysis and review should be recorded.

The outcome of the analysis and review may require that the SIF and other similar SIFs are required to be modified to make the actual performance reflect the intended design performance, or to eliminate a systematic failure. If a modification is required, then it should be conducted within management of change procedures (see section 6).

See Appendix 5 for further guidance on the assumptions that may have been made and how data can be gathered and analysed.

3.6.2 Process safety performance indicators

Process Safety Performance Indicators (PSPIs) are used to monitor the ongoing effectiveness of specific risk controls. Functional safety including the associated management systems may be one such risk control.

Monitoring the performance of the functional safety risk controls for installed SIS can be typically achieved by focusing on three main areas:

1. PSPIs related to the SIS equipment; such as SIF failures during operation and maintenance, use of defeats, spurious trip rates, demands on other protection layers (e.g. pre-alarms) etc.

2. PSPIs related to the development and upkeep of competence within the organisation; such as training and assessment progress;

3. PSPIs related to compliance to the systematic processes in place to ensure the continued and successful application of the safety lifecycle; such as proof test compliance, review and Functional Safety Assessment (FSA) progress, functional safety audit progress, failure rate collation, failure investigation and management of change completion;

The site operator should define appropriate PSPIs for the SIS alongside other indicators for other risk controls. These indicators should assess information from specific activities to determine the performance level of each of the indicators against the expected practice whilst having:

- consideration of the required level of functionality and performance to achieve the risk reduction assumed within the hazard and risk assessment;
- defined actions and trigger points/criteria for action.

Further information on developing PSPIs can be found in the following publications:

- HSG254 Developing process safety indicators - A step-by-step guide for chemical and major hazard industries, 2006
- EI High level framework for process safety management, 2010
- CCPS Process Safety Leading and lagging metrics, 2011

3.7 Incident investigation

Where an incident or near miss occurs associated with a SIF, a follow-up investigation should be carried out so that the root cause is understood and corrective action can be taken where necessary to prevent reoccurrence.

The site operator should implement procedures to:

1. identify and carry out a suitable investigation to determine the causes when any of the following events occur:
    - Correct activation of a safety function which prevented an incident occurring.

- Correct activation of a safety function, but a hazardous consequence still occurred.
- Spurious activation of a safety function.
- Incomplete activation of a safety function – i.e. one or more elements did not perform as intended during a genuine or spurious demand on the system.
- Detection of a hidden/latent fault or failure during routine proof testing, visual inspection or maintenance activities (including electronic diagnostics) which would have prevented the correct operation of the system.
- A revealed / evident fault or failure occurring during operation.
- Condition of components was much worse than expected during a scheduled component inspection or replacement task, e.g. accelerated corrosion or wear in component scheduled to be replaced.

2. identify any issues or deficiencies and put in place solutions to ensure that the SIF can fulfil its design intent to the correct level of availability.
3. identify any wider issues or deficiencies and put in place solutions to ensure that the findings are applied across site, and where applicable across other business units and the wider industry. This should include a systematic failure review if appropriate (refer to section 5.1.5).

The level of investigation should be proportionate to the potential consequences and the level of risk reduction expected from the SIF.

Examples of investigation team make-up, information required to support an investigation, and prompts to assist an investigation are provided in Appendix 6.

3.8 Verification activities

Verification is the process of checking that the outputs are correct and consistent with respect to the inputs. Verification is fundamental to finding and correcting errors and thereby preventing systematic failures. It is essential to keep complete and fully detailed records of exactly what was checked, how it was checked, what issues were found and how they problems were rectified. If the records are not available it is as if the work was never checked at all because the checkers will not be able to remember what was checked and what was not checked.

Verification activities should be carried out throughout the life-cycle and are therefore relevant to installed SIS. Verification planning for each life-cycle activity should be addressed under life-cycle planning – refer to section 3.2.

The site operator should implement procedures for the verification activities identified in the installed SIS life-cycle to describe the requirements, timescales and responsibilities for verification.

In many cases verification activities for later life-cycle phases are achieved through review of the life-cycle outputs, for example a review by the responsible SIS engineer of use of defeats.

4. OPERATION AND MAINTENANCE

Site operators should have procedures in place for operation of the SIS during normal and abnormal process operation. This should also include SIS start-up / reset procedures as well as recovery procedures in the event of power / utility failure.

Special consideration should be given to the following cases.

4.1 SIF operator response

Where an operator response is required to achieve the safety requirements rather than automatic executive function, the site operator should ensure that any special requirements needed in terms of design and management are implemented to verify the required SIL of the SIF is achieved.

Further information on the use of operators as part of a SIF can be found in the following publications:

- EEMUA 191
- HSE Operational Guidance (OG) OG47.

4.2 Faults and degradation

Degradation of the SIS occurs when dangerous failures of the SIF are present but the SIF remains able to carry out its safety function, for example a dangerous failure of a single channel of a voting system.

Where a SIF has completely failed, or has degraded, it no longer provides the same integrity that it was designed to have. It is recommended that this SIF is considered 'defeated' at this time (see below) unless it can be demonstrated that it still provides the required level of risk reduction, or that other management systems are in place to ensure continued safe operation.

Faults or degradation may be revealed during operation, maintenance, inspection or proof testing. The site operator should define what actions are to be taken in the event of faults or degradation to achieve or maintain a safe state. Any faults identified should be restored within the stated Mean Time To Restoration (MTTR).

Actions required in response to a dangerous failure of the SIS are described in IEC 61511 *Requirements for system behaviour on detection of a fault*.

4.3 SIS bypass (override, defeat)

IEC 61511 *Operator interface requirements* states:

> 'the design of the SIS shall minimize the need for operator selection of options and the need to bypass the system while hazards are present. If the design does require the use of operator actions, the design should include facilities for protection against operator error'.

However, installed SIS may not have been designed in this way and bypass functions may be available.

The site operator should adopt suitable management systems for the authorisation, control, mitigation (i.e. compensating risk reduction measures during bypass), assessment and monitoring of bypasses.

The level of authorisation and the integrity of the compensating measures should be commensurate with the integrity of the SIF being bypassed.

4.3.1 Planned bypasses

Use of bypass functions for normal operation and maintenance should be covered within the relevant operating and maintenance procedures. The procedures should describe the other compensating risk reduction measures that must be in place for the duration of the bypass.

These measures and the maximum permitted time (typically the defined 'mean time to restoration') of the operation or maintenance bypass should be based upon an assessment of the risk, SIS design and other protection available to continue to reduce risks to ALARP.

The duration of these bypasses should be limited to the defined maximum permitted assumed within the PFD calculation otherwise the bypass should be considered as unplanned.

4.3.2 Unplanned bypasses

Unplanned bypasses are those that are not envisaged during normal operation and maintenance.

The use of SIF bypass for unplanned reasons (typically due to faults, degradation etc.) should be subject to risk assessment to determine the compensating risk reduction measures to be taken to ensure continued safe operation.

Procedures should be provided to describe the other risk reduction measures that should be in place for the duration of the bypass or to ensure operational personnel conduct initial risk assessments to determine these.

The procedure should also require that if the duration of the bypass exceeds the defined 'maximum repair time' then more comprehensive risk assessment and authorisation process should be adopted to ensure and demonstrate continued safe operation or that action is taken to place the process in a safe state. Continued use of the bypass should be periodically reviewed to determine if safe operation can be continued.

4.4 Proof test

SIS are designed to provide a level of integrity that reduces the risk of a hazard to a defined tolerable level.

During normal operation, components of the SIS are subject to deterioration and failure from a number of causes. These failures may be safe failures that could lead to spurious

trips or dangerous failures that may prevent the SIS operating correctly when required. If the dangerous failures are not revealed by diagnostic functions, then they are termed as undetected.

Over time, the probability that an undetected dangerous failure has occurred increases. Therefore, the probability that the SIS will not operate as required (often called probability of failure on demand - PFD) also increases over time until the SIS has been proof tested, and any failure has been revealed and repaired. If testing is delayed the probability of failure will increase in proportion to the time since the last test.

IEC 61511 requires that a PFD calculation is performed to show that the integrity, i.e. the average PFD, of the SIS is sufficiently low to achieve the level of risk reduction required based upon assumptions including:

- The reliability of the components being used.
- How often undetected dangerous failures are revealed by proof test.

The site operator should implement written proof test procedures for all installed SIS to reveal undetected faults, and have a suitable management system in place to schedule the proof tests at the frequency specified in the PFD calculation, record the proof test results, and identify any failures for further analysis.

Any proof test deferrals should be subject to review and risk assessment and monitoring. Review should consider the impact of deferral against the PFDav calculations and manufacturer's recommendations.

Reference should be made to HSE Operation Guidance (OG) 54, *Proof Testing of Safety Instrumented Systems in the Onshore Chemical / Specialist Industry* for further information.

If no PFD calculation exists then a default frequency should be adopted and the PFD calculation completed, for example as part of the Functional Safety Assessment (FSA) 4 review process.

4.5 Inspection

IEC 61511 requires that inspection is implemented to reveal deterioration and unauthorised modifications.

The site operator should ensure requirements for inspection are captured within procedures. This could be completed as part of the proof test procedures or other inspection procedures.

The inspection procedure should identify all SIS components to be inspected and all items of equipment within the SIF (i.e. end-to-end inspection of transmitters, impulse lines, valves, junction boxes, heat tracing, equipment panels). The procedure is not required to identify every inspection task for each component – standard inspection checklists can be used.

To reveal unauthorised modifications the inspection should require that components are checked against approved drawings / asset registers so that issues such as missing links and unconnected cables can be found.

4.6 Maintenance

Failure to follow manufacturer's guidance and any exclusions stated may impact on the design parameters of the system and may mean that the target SIL level is not achieved or cannot be maintained.

The site operator should implement maintenance regimes for SIS components to ensure that:

- components are maintained considering the manufacturer's instructions, safety manual (where available) and certificate (where available).
- any exclusions identified within the manufacturer's guidelines are understood and taken account of as part of the maintenance regime.
- guidance in relation to other replaceable elements of the component, for example filters, are understood and taken account of as part of the maintenance regime.

5. REVIEW AND ASSESSMENT

IEC 61511 requires that installed SIS (i.e. those not designed and constructed in accordance with the latest version of the standard) are designed, maintained, inspection, tested and operating in a safe manner. This will therefore require the installed SIS to be reviewed against the latest version of the standard to determine that it is safe.

During the operational and maintenance phase of the installed SIS lifecycle (refer to section 3.1) IEC 61511 requires a periodic functional safety assessment (FSA 4). FSA 4 ensures that the installed SIS is being operated and maintained according to the assumptions made during its design and that safety management requirements are met.

In meeting these requirements, it is recognised that:

1. It is not reasonably practicable to review all installed SIS immediately a new version of the standard is issued.

2. Some aspects of such a review and of FSA 4 may already be addressed, or partially addressed, by existing processes that a site operator may have in place (for example periodic evaluation of risk assessments as part of a periodic COMAH Safety Report revision or hazard study 6 / PHR).

3. For installed SIS the existing documentation may not be sufficient or readily available for the purpose of review and FSA 4.

4. There may be other reasons for review or FSA 4, such as outcomes of incident investigation or maintenance and operating experience, or changes to company risk targets or standards etc.

This guidance therefore recommends that these requirements are captured within an ongoing process of review and assessment with continuous improvement where reasonably practicable.

FSA 4 need not repeat requirements that are already covered by existing processes, but instead should act as an independent check that the necessary requirements were completed to the required standard and that the necessary documentation has been produced such that assessment completed and a judgement made.

Note that stage 1, 2 and 3 FSAs are carried out during the initial system design phases (project safety lifecycle) and are therefore not covered within this guidance.

5.1 Review

The site operator should develop a plan and procedure to describe the review scope, activities, responsibilities and timing.

The procedure should ensure that as reviews are completed, they consider:

1. Any changes brought about by new versions of IEC 61511, company standards and risk targets.

2. Other processes completed on site, e.g. hazard and risk assessment reviews.

3. Up to date operation and maintenance experience, outcomes from incident investigations (both on site and from wider industry), outcomes from previous SIS reviews / FSAs.

The following sub-sections describe the review requirements – if these are not completed by review processes then they should be covered at FSA 4.

5.1.1 Hazard and risk assessment and SIF allocation review

Installed SIS will have been specified to reduce the risk of specific hazards. Existing hazard and risk assessments may be sufficient to define the functionality and integrity requirements of each SIF within the SIS, for example if Quantitative Risk Assessment (QRA) Hazard Analysis (HAZAN) techniques were utilised.

However, if the existing assessments are not in place or sufficient to specify the SIS then a review process should be completed to generate new or updated assessments.

This should include a procedure implemented describing the risk assessment process(es) in use (e.g. LOPA, QRA etc.) that includes site specific application of risk targets, event frequencies, layer of protection integrity, ALARP demonstration etc. For further guidance see - EI guidance "Guidance on Safety Integrity Level (SIL) Determination".

Once suitable assessments are in place to specify SIS functionality and integrity, the purpose of later reviews (either ahead of or as part of FSA 4) should be to confirm that assumptions made within the assessments remain consistent with operational and maintenance data such that the assessments and associated demonstrations that risks are reduced to ALARP remain valid.

The review requirements for a SIS hazard and risk assessments are shown in Appendix A7.1.

5.1.2 Safety requirement specification review

The Safety Requirement Specification (SRS) is a pivotal document for the SIS.

For installed SIS which were designed to IEC 61511, it should have been created at the outset of the life-cycle following the Hazard & Risk Assessment (HRA) and allocation phases, before the detailed design commenced and would have been written such that it provided the designer with the safety requirements of the system.

For other installed SIS, it is probable that documents under different titles were created to describe the SIS. Typical examples of documentation include; Basis of Design, User Requirement Specification or other descriptive document together with supporting documentation such as Cause & Effect Diagram, Trip Matrix, Level of Concerns Document and System Structure and/or Overview Drawings.

In order to ensure that the requirements of the installed SIS are sufficiently specified to allow ongoing maintenance, operation, assessment, modification etc., the site operator should ensure that a suitable SRS is available either as a single document or range of documents.

The minimum information required for a suitable SRS is described in Appendix A7.2.

For installed systems which do not have the minimum required SRS or equivalent documentation, or where those documents are not readily available or of sufficient detail, or where those documents do not meet current standards, then a review should be conducted to generate or update the SRS by either:

1. creating a retrospective SRS document using existing documents with the SRS now becoming the master, or
2. creating a signposting document or system that links to existing documents where the SRS information is present, or
3. creating documents that cover information currently missing from the SRS to sit alongside the existing documents (may be useful for information that is consistent across site such as process and environmental conditions or defeats and bypasses), or
4. a combination of the above.

Once a suitable SRS is in place for the SIS, the purpose of later reviews (either ahead of or as part of FSA 4) should be to confirm that the SRS is consistent with the requirements within the risk assessment. The SRS should be kept up-to-date with any changes subject to management of change – see section 6.

5.1.3 SIS design review

The purpose of the SIS design review is to determine if the Installed SIS remains fit for purpose and provides the necessary level of risk reduction, which will depend upon the degree of compliance it has with IEC 61511.

For installed SIS that are compliant with the latest version of IEC 61511, this will be demonstrated by the existing documentation, e.g. PFD calculations, prior-use evidence, safety manuals, design documents and drawings etc. as described in IEC 61511 *Information and documentation requirements*.

For installed SIS that are not compliant with the latest version of IEC61511, similar documentation may be available to show that the SIS remains fit for purpose and provides the risk reduction required of it. If such documentation is not available, a review should be conducted to generate sufficient documentation to allow assessment of the adequacy of the SIS design including PFD calculations. Prior use evidence, design documents and drawings etc. The review should be completed on a per SIF basis although a sampled approach may be appropriate where common architectures are in use on the site.

The review requirements for an installed SIS are shown in Appendix A7.3.

Once suitable documents are in place for the design of the SIS, the purpose of later reviews (either ahead of or as part of FSA 4) should be to confirm that the design assumptions remain valid with current operational and maintenance experience and that the SIS design reduces risk to as assumed within the relevant risk assessment.

When considering if the SIS design reduces risk to as low as reasonably practicable it should be noted that:

1. where gaps are identified within the SIS design compared to the latest version of the standard, the effect of these gaps on the integrity achieved should be considered. For example, if hardware fault tolerance requirements are not met then the PFD achieved may be limited to a lower SIL than indicated by the calculation.

2. if the SIS does not meet integrity requirements and it has been shown and documented that it is not reasonably practicable to upgrade it, the hazard and risk assessment and SRS should be updated to reflect the achieved integrity and functionality of the installed SIS such that the ALARP demonstration for the relevant hazard scenario is consistent with actual risk reduction achieved.

3. it may be that improvements become reasonably practicable when the SIS is next updated, e.g. due to obsolesce replacement or other upgrade – such projects should consider any outstanding gaps at that time and therefore it is important that work done to identify gaps is documented and retained.

5.1.4 Systematic capability review

Systematic capability (SC) is a measure and statement of confidence of the systematic safety integrity that a device provides with respect to preventing systematic failures. Systematic capability is an essential part in determining the suitability of a device to be used in a SIS.

For new devices, the manufacturer of a SIL certified device will provide not only a SIL rating but also a systematic capability figure, this is expressed as SC1 to SC4 which can then be utilised in the selection and inclusion of the device within the SIS.

Reference should be made to IEC61508 Part 2, Appendix D – *Safety Manual for Compliant Items* for further information.

For installed SIS the devices may not have a defined systematic capability. In such cases the devices should be assessed to determine if they are suitable for use based upon prior use as part of the SIS design review - refer to section 5.1.3 for further information.

5.1.5 Systematic failures review

Whereas systematic capability discussed above is associated with the SIS devices themselves, systematic failures may also be introduced during the integration of the SIS devices into the overall system.

Systematic failures are related to pre-existing faults or errors within the SIS that may only occur under particular conditions (as oppose to random failures which occur randomly due to degradation mechanisms in the hardware).

Most systematic failures are created by human intervention and although the likelihood of the failures cannot be predicted, the causes of them can be and step can to taken to detect and eliminate them. To minimise systematic failures, techniques for the avoidance and control of systematic faults are used during the specification, implementation and validation phases. These techniques used are generally procedural, such as requiring structured specification and documentation, application of standards,

analysis, testing and verification, and a systematic approach to dealing with complexity (see IEC 61508 part 2 Annex B).

For installed SIS, systematic failures may have been introduced during earlier parts of the lifecycle, e.g. due to human error during specification or design – see Appendix 8 for further examples.

For Installed SIS that were designed in compliance with IEC61511, evidence should already be available (e.g. project documentation showing that a systematic and structured approach to specification, design and implementation etc.) that such techniques were employed during the specification, implementation and validation phases.

If this evidence is not available or for other Installed SIS that were not designed in compliance with IEC61511 a review should be undertaken and documented:

1. Determine if suitable techniques were employed during the specification, implementation and validation phases with respect to minimise the likelihood of systematic failures.

2. Where suitable techniques were not employed, and therefore there is a higher likelihood for systematic failures to be present, the review should identify what further remedial work should be carried out to identify and address these.

The review need not be completed per SIF but grouped, e.g. into those systems that were originally installed by a single project. A sampled approach may be appropriate where it is known that SIS or groups of SIS were installed to similar standards or by specific vendors.

The level of effectiveness in techniques needs to be in proportion to the SIL. Though the probability of systematic failure cannot be calculated accurately, it should be considered that SIL 3 SIFs need to perform about 100 times more reliably than SIL 1 SIFs. The level of attention to detail in specification, checking and testing needs to be commensurately higher.

An example of a method for reviewing and addressing systematic failures of installed SIS is given in Appendix 9.

It is recommended that the reviews are completed in a prioritised way, starting with systems or groups of systems that:

- have higher levels of risk reduction within, and / or
- are more complex, and / or
- are less understood (i.e. black box, no documentation etc.).

Once higher priority systems have been completed, the remaining systems should be worked through in priority order until it becomes clear that further work is not adding value and some confidence can be demonstrated that systematic failures have been minimised.

Once suitable documents are in place (i.e. original project documents for SIS designed to IEC 61511 or reviews and remedial measures for other SIS as described above) to

show that systematic failures have been minimised, the purpose of later reviews (either ahead of or as part of FSA 4) should be to address any systematic failures that have been identified during subsequent operation and maintenance, or following investigations.

5.2 Functional safety assessment 4

The purpose of a stage 4 FSA as described in IEC 61511 is to ensure that the installed SIS is being operated and maintained according to the assumptions made during design and that safety management requirements are met.

The outcome of FSA 4 will also be a key part of demonstrating that risks are reduced to ALARP.

For FSA 4 the site operator should develop a procedure including a plan for when these activities take place based on the installed SIS diversity, age, complexity and Major Accident Hazard (MAH) potential. For example, an older more complex system may require an FSA 4 more frequently than a new less complex system.

The procedure and plan need not repeat requirements covered by review processes, if these meet the requirements shown in Appendix 7.

The outcome of the assessment should be documented and include a judgement of the functional safety and safety integrity achieved by every SIF of the SIS.

The FSA shall be carried out by a multi-disciplined team, relevant to the appropriate FSA, representing the necessary disciplines involved in the design, operation, maintenance and management of the SIS. It is important that the FSA team have the necessary competence relevant to the assessment. The FSA team should include at least one senior competent person with sufficient independence from the operation and maintenance of the SIS in order that they can conduct the assessment in a manner where their judgement is not pre-conceived by detailed operational and maintenance knowledge of the SIS. The FSA may be assisted by third parties where an operator does not have sufficient resource in-house.

Refer to Appendix 7 for an example template for a Stage 4 FSA.

6. MODIFICATION AND DECOMMISSIONING

Before making any changes to the SIS, Management of Change (MOC) procedures must be in place that define how changes will be identified, authorised, assessed and controlled. This guidance assumes MOC procedures are already in place and focuses on how modifications to SIS are identified, analysed and managed.

A typical process for management of change is shown in Appendix 10.

6.1 Identifying SIS modifications

When assessing the impact of any proposed site modification, e.g. to the process, equipment or the organisation, the site operator should ensure that the MOC process identifies both modifications to the SIS itself and modifications that impact upon the SIS:

- Modifications to the SIS itself are those that result in a modification to the SIS hardware or application program or other software and associated management systems or utilities.
- Modifications that impact upon the SIS are those that that affect the assumptions made during the SIS hazard and risk assessment, SRS or design. For example:
    - If the hazard and risk assessment took credit for other protection layers (e.g. BPCS alarm function, mechanical relief, bunds etc.) to reduce demand on the SIS, modification to, or decommissioning of, these protection layers may impact on the SIS requirements.
    - Changes to operation (e.g. number of road tankers loaded) or organisational change (e.g. availability of operators to respond to alarms) may affect the demand rate on a SIS.

Once a potential SIS modification (direct or indirect) has been identified, the site operator should ensure that MOC processes require that before the modification is put into operation:

- there is authorisation from appropriate personnel, in most cases this will include operations, engineering, SHE and management.
- an analysis is conducted to determine the impact upon functional safety and functional safety plan for the modification.
- any outstanding findings from previous functional safety assessment have been considered.
- an FSA 5 is completed.

Note: It is easy for the impact of organisational changes to be overlooked. Fundamental changes driven from the board level down may bypass the MOC process. These changes may have an adverse impact on process safety and on the effectiveness of functional safety.

6.1.1 Like-for-like modifications

Like-for-like modifications to the SIS are those where a SIS hardware element is being replaced and it has been deemed that there will be no impact on the functional safety of the SIS and therefore the modification process is not followed.

A modification should not be considered as like-for-like:

1. If the element is not an exact duplicate or an approved (by an independent functional safety competent person) substitution from the same manufacturer and does not change the ability of the system to either respond on demand or during faults and that does not require modification to the SIS as installed.
2. If the replacement process has potential to introduce a modification to the SIS, for example due to different embedded software versions, rewiring, configuration, reconnection of the device etc.
3. If the process of specification of a substitute element requires development of a specification.

If in doubt, an analysis of the proposed modification should be conducted by an independent competent person (see section 6.2 Analysis of SIS modifications) to determine if earlier life-cycle phases could be impacted.

If the modification is a 'like-for-like' replacement of equipment or a part of equipment; this could be covered under a maintenance procedure and / or MOC. However, note that re-validation (not proof test) would still be required following replacement.

If the modification is not a 'like-for-like' replacement of equipment or a part of equipment, then it should be treated as a direct modification to SIS and managed under the MOC procedures.

6.2 Analysis of SIS modifications

Once a change to the SIS has been identified, an analysis (impact assessment) should be conducted by a competent person to determine which specific life-cycle phases are affected (see section 6.4) and therefore what activities are required to complete the modification and what documentation will need to be updated.

For example, if a modification affects assumptions made in the risk assessment phase then modification will need to complete this and all subsequent phases. However, if a modification affected only the SIS design, then the life-cycle phases before this would not need to be revisited.

If any proposed change could have a negative effect on safety, then a life-cycle and hazard analysis review will be required.

6.3 Decommissioning

Decommissioning of a SIS should be completed as a SIS modification and covered under management of change. Where SIS equipment is decommissioned but left in place, consideration should also be given to the long-term management of any decommissioned process and electrical equipment.

6.4 Functional safety assessment 5

The purpose of a stage 5 FSA as described in IEC 61511 is to consider the impact assessment and to ensure that the modification is carried out in compliance with the standard.

For FSA 5 the site operator should develop a procedure setting out requirements for FSA 5, within or linked to the SIS management of change procedures to ensure that FSA 5 is planned and completed at the appropriate points of the modification or decommissioning process.

FSA 5 should be completed at least prior to the modification or decommissioning 'going live'. However, it is often advantageous to complete FSA 5 in parts, e.g. with the first part completed after the Impact Assessment to minimise the impact of any issues identified by FSA 5. For larger modifications, the FSA5 may be split into three parts (similar to FSA1-3 for new SIS).

The FSA shall be carried out by a multi-disciplined team, relevant to the appropriate modification or decommissioning, representing the necessary disciplines involved in the specification, design, operation, maintenance and management of the SIS. It is important that the FSA team have the necessary competence relevant to the assessment. The FSA team should include at least one senior competent person with sufficient independence from the SIS modification or decommissioning process in order that they can conduct the assessment in a manner where their judgement is not pre-conceived by detailed knowledge of the SIS modification or decommissioning.

Refer to Appendix 11 for an example template for FSA 5.

ABBREVIATIONS

Abbreviation	Description
ALARP	As Low As Reasonably Practicable
BPCS	Basic Process Control System
CASS	Conformity Assessment of Safety-related Systems
CCPS	Center for Chemical Process Safety
CDOIF	Chemical and Downstream Oil Industries Forum
CMS	Competency Management System
COMAH	Control of Major Accident Hazards
EEMUA	Engineering Equipment and Material Users Association
EI	Energy Institute
FMEDA	Failure Mode, Effects and Diagnostic Analysis
FPL	Fixed Programming Language
FSA	Functional Safety Assessment
FSMS	Functional Safety Management System
HAZAN	Hazard Analysis
HAZOP	Hazard and Operability study
HFT	Hardware Fault Tolerance
HRA	Hazard and Risk Assessment
HSE	Health and Safety Executive
IACS	Industrial Automation and Control Systems
IChemE	Institute of Chemical Engineers
IEC	International Electrotechnical Commission
LOPA	Layer of Protection Analysis
MAH	Major Accident Hazard
MOC	Management of Change
MTBF	Mean Time Before Failure
MTTR	Mean Time To Restoration
OEM	Original Equipment Manufacturer
OG	Operational Guidance
PFD	Probability of Failure on Demand
PHA	Process Hazard Analysis
PSPI	Process Safety Performance Indicators

Abbreviation	Description
QRA	Quantitative Risk Assessment
RRF	Risk Reduction Factor
SC	Systematic Capability
SFF	Safe Failure Fraction
SHE	Safety, Health and Environment
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SMS	Safety Management System
SRS	Safety Requirement Specification
TSA	Tank Storage Association
UKPIA	United Kingdom Petroleum Industry Association

OTHER RELEVANT PUBLICATIONS

Further information relating the compliance of SIS with IEC 61511 can be found in the following publications:

Reference	Description
IEC 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)
IEC 61011	Functional safety - Safety instrumented systems for the process industry sector
CCPS	Process Safety Leading and lagging metrics 2011
CDOIF	Demonstrating prior use of elements of a safety instrumented function in support of BS EN 6151
EEMUA 191	Alarm systems - a guide to design, management and procurement
EEMUA 222	Guide to the application of IEC 61511 (edition 1) to safety instrumented systems in the UK process industries
Energy Institute	EI High level framework for process safety management 2010
HSG 254	Developing process safety indicators - A step-by-step guide for chemical and major hazard industries 2006
HSE and IET Code of practice	Competence for Safety-Related Systems
IChemE	Safety Centre Guidance; Process Safety Competency – a model 2015
NAMUR NE 93	Verification of the Safety-Related Reliability of SIS based on Field Experience.
OG 46	HSE Operational Guide (OG) 46 Management of instrumented systems providing safety functions of low/undefined safety integrity
OG 47	HSE Operational Guide (OG) 47 Operator Response within Safety Instrumented Systems in the Chemical, Oil & Gas, and Specialist Industries
OG 54	HSE Operation Guidance (OG) 54, Proof Testing of Safety Instrumented Systems in the Onshore Chemical / Specialist Industry
OG 86	HSE Operation Guidance (OG) 86, Cyber Security for Industrial Automation and Control Systems (IACS)
PSLG	Process Safety Leadership Group, final report – Safety and Environmental Standards for Fuel Storage Sites
The 61508 Association	Conformity Assessment of Safety-related Systems (CASS)

ACKNOWLEDGEMENTS

This document was created as part of the Chemical and Downstream Oil Industries Forum Process Safety work stream.

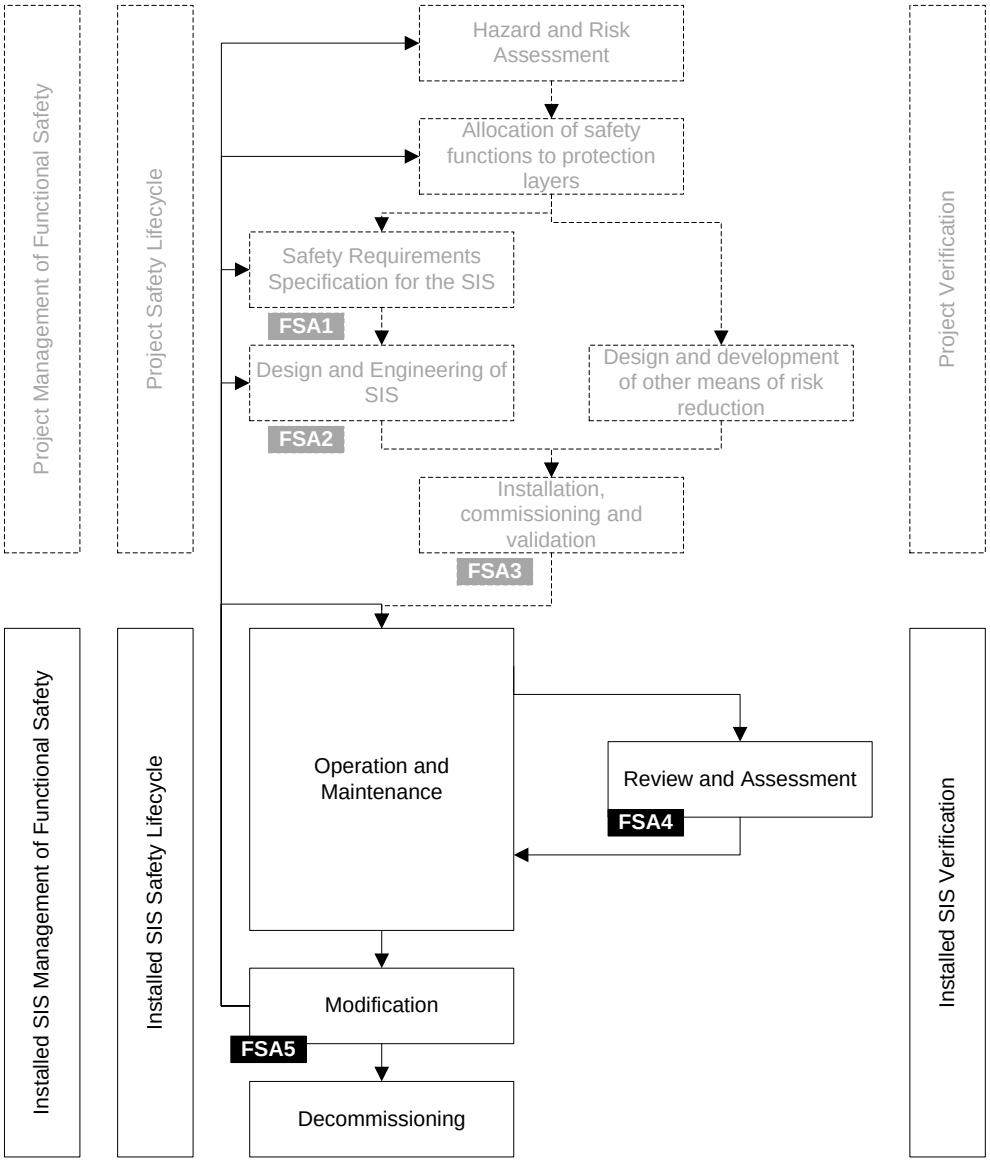
CDOIF wish to record their appreciation to the working group members who were responsible for creating this guideline:

Name	Organisation
Peter Davidson (Chair)	Tank Storage Association
Dave Ransome	P&I Design Ltd.
Barrie Salmon	Tank Storage Association
Jamie Walker	United Kingdom Petroleum Industry Association
Edward Kessler	Engineering Equipment and Material Users Association
Ray Martin	EEMUA Control & Instrumentation Working Group
Nic Butcher	Health and Safety Executive
Sarabjit Purewal	Health and Safety Executive
Paul Cram	Essar Oil UK
Pep Monk	ExxonMobil
Ron Bell	ESC (representing the Energy Institute)
Paulo Oliveira	ESC
Sean Sexton	Greenergy
Neil Campbell	Greenergy
Wayne Brickle	Valero

REVISION HISTORY

Rev.	Section	Description	Date	Changed By
0	All	First Issue	13-Jun-2016	Peter Davidson
0.6	All	Final Committee Draft - HSE	27-Oct-16	Peter Davidson
0.7	All	Final Committee Draft - Committee	December 16	Peter Davidson
0.8	All	Final Committee Draft – for Stakeholder Review	25-Jan-17	Peter Davidson
1.0	All	Updated with stakeholder comments	03-Jul-17	Peter Davidson

APPENDIX 1. EXAMPLE SAFETY LIFE-CYCLE FOR AN INSTALLED SIS



APPENDIX 2. INSTALLED SIS EXAMPLE LIFE-CYCLE OBJECTIVES AND INPUTS / OUTPUTS

This table defines example objectives for each of the life-cycle phases typical to installed SIS. This may be useful as a roadmap to assist the site operator to produce and maintain a functional safety plan for the installed SIS (refer to section 3.2) describing the activities, timing and responsibilities for the installed SIS.

Installed SIS Safety Life-cycle Phase or Activity	IEC 61511 clause	Section in this Document	Inputs	Objectives	Outputs
Management of Functional Safety	5	3	Existing policy and procedure	To identify the management activities that are necessary to ensure that the functional safety objectives are met for the installed SIS	Overall policy and strategy for the installed SIS Procedures for the installed SIS
Safety Life-cycle	6, 5.2.4	3.1	Existing functional safety plans	To establish how the relevant life-cycle steps are to be accomplished for the installed SIS	Functional Safety Plan for installed SIS
Verification	7	3.8	Plan for the verification of the Installed SIS for each phase	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	Results of the verification of the SIS for each phase
Operation and Maintenance	16	4	SIS SRS documents SIS documentation Plan for operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	SIS operational data SIS maintenance, inspection and test records Maintenance data
Modification	17	6	As-built SIS documentation Change request	To make corrections, enhancements or adaptations to the SIS, ensuring that the required SIL is achieved and maintained	Management of change records Updated SIS documentation Results of FSA 5

Installed SIS Safety Life-cycle Phase or Activity	IEC 61511 clause	Section in this Document	Inputs	Objectives	Outputs
Decommissioning	18	6	As-built SIS documentation Decommissioning request	To ensure proper review, authorisation, and ensure SIS remains appropriate	Management of change records SIF placed out of service and / or removed Updated SIS documentation Results of FSA 5
Hazard and Risk Assessment and SIS allocation Review	8, 9	5.1.1	Process design and operation documents and data SIS Operational Data SIS Documentation Existing hazard and risk assessments and allocation documents Safety Targets	To determine that installed SIS is being operated and maintained according to the assumptions made during design and that the SIS requirements have been determined to reduce risks to tolerable levels.	Updated hazard and risk assessments and SIS allocation documents. Revised SRS (where required)
Safety Requirements Specification Review	10	5.1.2	Hazard and risk assessments and SIS allocation documents Existing SIS SRS documents	To determine that sufficient and accurate information is available for those who will utilise the information at any phase of the Installed SIS life-cycle.	Updated SIS SRS documents
Design, Installation, Commissioning and Validation Review	11 - 15	5.1.3 5.1.4 5.1.5	SIS SRS documents SIS Documentation	To determine that installed SIS is being operated and maintained according to the assumptions made during design and that the installed SIS design, installation and validation meets good practice requirements so far as is reasonably practicable.	Updated SIS documents Installed SIS in conformance with the SIS safety requirements
Functional Safety Assessment Stage 4	5.2.6.1	5.2	Planning for SIS FSA SIS safety requirements	To investigate and arrive at a judgement on the functional safety achieved by the Installed SIS	Results of SIS FSA

Table 1 – Installed SIS Life-cycle Objectives

APPENDIX 3. COMPETENCE

Competence comprises of several generic components. The following four components should be addressed in defining the specified competencies required to undertake the defined tasks.

- Knowledge (Know what); for example,
  - Operating Environment/Sector knowledge;
  - Sector Regulatory and Approval Requirements;
  - Relevant Technologies;

- Understanding (Know why); for example:
  - Principles of Safety and Risk;
  - Historical accidents, their causes and contributing factors;

- Personal Qualities (Attitudes & Behaviours); for example:
  - Personal integrity;
  - Methodical attitude in undertaking tasks;
  - Team Player;
  - Professional standing.

- Skills (Know how); For example:
  - Technical skills (Hazard Analysis, Report Writing);
  - Managerial skills (Team Leadership);
  - Behavioural skills (Effective communication).

In defining the required competence there are several key items that need to be addressed and documented as defined in BS EN 61511:

- Engineering knowledge, training and experience appropriate to the process application;
- Engineering knowledge, training and experience appropriate to the applicable technology used (e.g., electrical, electronic or programmable electronic);
- Engineering knowledge, training and experience appropriate to the sensors and final elements;
- Safety engineering knowledge (e.g., process safety analysis);
- Knowledge of the legal and regulatory functional safety requirements;
- Adequate management and leadership skills appropriate to their role in the SIS safety life-cycle activities;
- Understanding of the potential consequence of an event;
- The SIL of the SIF;
- The novelty and complexity of the application and the technology.

APPENDIX 4. FUNCTIONAL SAFETY AUDIT CHECKLIST

The purpose of the audit is to ensure that a FSMS is in place, up to date and being followed. The audit should include reviewing that the procedures are appropriate, and that associated records and forms are completed correctly.

Typical Audit questions include but are not limited to:

- Is there a suitable lifecycle and functional safety plan in place for the installed SIS?
- Is there a competence management system in place for functional safety?
- Are roles and responsibilities for life-cycle activities documented and understood?
- Are competence requirements defined and met for the lifecycle tasks and activities and being managed?
- Are procedures and plans in place for the installed SIS to cover:
    - Future functional Safety Audits
    - Developing and maintaining a configuration asset register
    - SIS Monitoring
    - Incident Investigation
    - Verification activities
    - Operation (including bypasses)
    - Maintenance, Inspection and Proof Tests at the set intervals and procedures for managing repair
    - Periodic Review and Assessment
    - Review of Hazard and Risk Assessment (including company risk targets and demonstration of ALARP)
    - Modification and Decommissioning including identifying changes, approval, review and FSA 5
    - Stewarding of actions from the reviews, FSAs, audits effectively

The audit should ensure that all procedures are current, auditable and operational.

APPENDIX 5. PERFORMANCE EVALUATION GUIDANCE

SIS Demand Rate

For installed Safety Instrumented Systems assumptions may have been made about SIS demand rates during the hazard and risk assessment phase.

For example, if risk graphs were used these often have a 'W' parameter which defines the assumed demand rate on the SIF. It is also often possible to determine the assumed demand rate on a SIF by analysis of fault trees or LOPA's, although this may require consideration of the order in which protection layers will occur as a scenario develops.

Demand rates are difficult to measure in practice because the rates are typically low (e.g. 0.1 per year). It may be useful to implement leading indicators for demand rate such as:

- Alarm rate and duration,
- Magnitude and duration of excursions outside normal process operating envelopes

For instance, a SIF pre-alarm rate is typically expected to occur ten times more frequently than the SIF demand rate. Similarly, minor excursions from setpoint occur more frequently than alarms. Any increase in process excursion or in alarm frequency may provide early warning of an incipient hazard.

SIS Reliability Data

For installed Safety Instrumented Systems assumptions may have been made regarding the failure rate of the components used within it. The type of data the designer/integrator may have used could vary depending on when the design was performed and what reliability information was available at that time. Typical data formats are:

- BS EN 61508 Certified component with a safety datasheet containing PFD_{av} – Average Probability of Failure on Demand with SIL capability;
- Failure data expressed as Failures in Time and normally given as Dangerous Failures (Detected and Undetected) and Safe Failures (Detected and Undetected);
- MTBF – Mean time between failures.

In most cases the assumptions will have come from data failure rates contained in component databases such as OREDA or from component modelling using methods such as failure mode, effects and diagnostic analysis (FMEDA). It is important to remember that the data used may have been selected without any regard to the process or environmental duties of the component and may be optimistic.

It is also possible that the components were chosen on a basis of proven in use or prior use, where the same components had been used in similar process applications. This data, if well founded, often provides more realistic data as it considers in service applications. However, the accuracy of this data is related to the volume of components monitored and their time in service. IEC61511 requires that failure data used is credible (within 90% confidence levels), traceable, documented, justified and shall be based on field feedback from similar components used in a similar operating environment.

As components used in SIS are chosen for their safety reliability, this inevitably means that they have a high safe failure fraction (SFF), thus most failures will be to a safe state. These failures will result in spurious activations, often called nuisance tripping.

SIS components such as sensors and final elements are often used for non-SIS duties on site, i.e. within the BPCS. It can be useful to gather the overall failure rates (which will include safe and dangerous failures) of this wider population to improve confidence in the data as the SIS population is often relatively small.

Analysis of failures on the SIS population should be conducted to determine if a failure was safe or dangerous and if the failure was a result of systematic cause.

Gathering and analysing the data will require that some form of calculation needs to be performed to compare the results to the original assumptions. Guidance is available on these calculations, for example within CDOIF guidance document *Demonstrating prior use of elements of a safety instrumented function in support of IEC 61511*.

However, ultimately, whatever data was used should be monitored to ensure that the SIS is performing within the assumptions made.

APPENDIX 6. INCIDENT INVESTIGATION

A6.1. Investigation Team

Relevant discipline expertise for the investigation may include representatives of the Operations, Maintenance, Process, and Technical teams depending upon the scope of the investigation.

At least one of the members of the investigation team has a level of competence in managing functional safety.

Consideration should be given to including at least one senior person not involved in the operation and maintenance of the plant area under investigation.

A6.2. Information to support an investigation

The following information may be used to support an investigation associated with a SIS:

- Current Process Hazard Assessment (e.g. Process Hazard Analysis [PHA], Hazard and Operability study [HAZOP] etc.) for the process system being investigated.
- Any Safety Requirements Specification or Functional Specifications relating to the system being investigated.
- Risk assessment (e.g. Layer of Protection Analysis [LOPA]) documentation and SIL analysis defining maximum proof-testing intervals to achieve the required system availability.
- Any availability calculations (e.g. SIL calculations) for the system being investigated.
- Details of the proof testing, visual inspection and maintenance activities which are carried out on the system – including tasks completed and frequency of execution.
- Results of previous planned proof testing, visual inspection and maintenance activities.
- Details of previous equipment failures – e.g. maintenance system work order history and condition reporting.
- Details of any previous investigation into this or similar systems.
- Manufacturers report following a failure

A6.3. Prompts to assist investigations

Typical investigation prompts include but are not limited to:

- Confirm that all required actions successfully executed.
- Confirm if the activation successfully mitigated against the hazard.
- Confirm if there is any significant increase in spurious failure rate.
- Confirm that all root causes of the system activation or equipment failure been identified.
- Have appropriate actions been assigned to adequately address root causes to prevent recurrence?
- Did the incident or near miss cause other protection layers to be called upon?
- Did the proof testing, maintenance inspection or maintenance activities fail to identify the failure mode that occurred?
- Is significant degradation being observed each time the proof test procedure or a visual inspection PM procedure is performed on an asset?
- Have there been multiple incidents or near-misses associated with the safety instrumented function and is the system demand rate is still within the range of the initial assumptions made during the initial system design?
- Is there a requirement to perform a Functional Safety Assessment (Stage 4) to confirm the validity of initial PHA & design assumptions, and check that the installed system can fulfil its design intent to the correct level of availability? i.e. outcome of investigation may trigger FSA 4
- Is the incident or near-miss a result of a systematic failure and, if so, could this failure affect other SIS?

APPENDIX 7. FUNCTIONAL SAFETY ASSESSMENT 4 CHECKLIST

Many aspects of this checklist should and may have been covered by previous FSAs,

- FSA 1 – Review of the HRA and SRS
- FSA 2 – Review of the SIS Design
- FSA 3 – Review of the installed SIS prior to process duty

Where these previous FSAs exist, the FSA 4 should ensure that all actions from previous FSAs have been completed and that the findings and conclusion of those FSAs are still current, valid and relevant. Where previous FSAs have not been conducted, it will be necessary to consider all aspects of the SIS life-cycle whilst conducting the FSA 4.

With respect to the Functional Safety Management element of the FSA 4, this may be assisted and less onerous if Functional Safety Audits are conducted and available for review.

A7.1. Hazard and Risk Assessment and Allocation

Validity of Hazard and Risk Assessment / Allocation

1. Is a hazard and risk assessment for the SIS in place and has it been reviewed and where necessary updated to ensure assumptions remain valid and consistent with operating and maintenance experience and the assessment is consistent with good practice with any differences being identified and resolved?

2. The review of the hazard and risk assessment against operating and maintenance experience should cover:

    a. Is the link between the hazards and risk control measures established and valid? i.e. is it possible to determine which hazards the SIF is protecting against?

    b. Is the Hazard and Risk Assessment still valid?

    c. Are the initiating events valid (e.g. number of operations / duration)?

    d. Are the initiating event demand rates valid and reviewed against the observed demand rate of the SIS?

    e. Are the risk reduction measures, protection layers and barriers claimed within the assessment in place and maintained?

    f. Are the conditional modifiers valid (e.g. occupancy, probability of ignition etc.)?

    g. Are there any changes to the assumed process safety time?

    h. Have any changes been made to operation of the process that might affect the Risk Assessment?

i. Are all the SIS identified in the risk assessment recorded in the SIS register (or equivalent).

j. Are there any changes to the required SRS, for example changes to the SIL or safety functionality requirements?

k. Does the assessment demonstrate that all necessary measures have been taken? for example by including an ALARP demonstration where necessary.

3. The review of the hazard and risk assessment against good practice should cover:

   a. The assessments are adequate to determine the functional and integrity requirements of the SIFs for the hazardous events being considered.

   b. Risk reduction credit taken for BPCS should be limited to 10^{-5} hours (continuous functions, typically initiating events) or PFD=0.1 (demand functions).

   c. No more than one BPCS function may be credited, unless the BPCS is not the initiating source in which case two BPCS protection functions may be credited.

   d. Common cause, common mode and dependent failures between the protection layers and between the protection layers and initiating events have been identified and assessed. This could result in confirmation that these failures are sufficiently low in comparison to the overall safety requirements or that a protection layer in the risk assessment may need to be removed.

4. Is the Security Risk Assessment valid and consistent with operating and maintenance experience (refer to HSE Operation Guidance (OG) 86, Cyber Security for Industrial Automation and Control Systems (IACS))? i.e.

   a. Assumptions made in the assessments are consistent with current operations in terms of the devices in place, requirements for data transfer between devices, current experience knowledge regarding threats and vulnerabilities of the system.

   b. The assessment demonstrates that all necessary measures have been taken.

5. Have any recommendations or changes arising from the risk assessment reviews been implemented or resolved?

A7.2. Safety Requirements Specification

Validity of the SRS

1. Are accurate and up-to-date safety requirements specifications for the SIFs available, consistent with the risk assessments and correctly stored?

2. If a Safety Requirements Specification is not available, a review shall be conducted to ensure that the requirements are sufficiently specified by collating data or generating requirements documents.

3. The review of the SIF safety requirements should ensure that the following information is available:

    a. Functional description of the SIFs (e.g. a cause and affect diagram, logic narrative etc.) including input and output voting logic arrangements

    b. Functional description of the SIFs (e.g. a cause and affect diagram, logic narrative etc.)

    c. Links to the relevant hazard and risk assessment showing which hazardous scenario(s) the SIF is provided for.

    d. Integrity requirements, e.g. SIL level, PFD requirements, risk reduction factor

    e. The mode of operation, energise to trip or de-energise to trip

    f. The demand on the SIS – High / Low Demand or Continuous.

    g. The safe state required of the process following activation

    h. The inputs and outputs of the SIS, including definition of SIF actions that are carried out by the SIF but are not required for functional safety (often known as tidy-up actions)

    i. The actions required to achieve Safe State

    j. The Process Safety Time[1]

    k. Response time requirements of each SIF within the SIS including any slow closing requirements of the final element[2]

    l. Tight shutoff valve maximum leakage rate / shutoff class requirements to achieve functional safety. (Note that this is different to the standard of valve that might be specified)

    m. Settings and ranges of measuring instrumentation including activation points

    n. Process and environmental operating conditions

[1] The time period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed.

[2] SIS Response Time </= Process Safety Time / 2

o. Interface with other control systems and other protection layers

p. Start-up, restart and reset functionality

q. Manual shutdown facilities

r. Overrides and bypass philosophy

s. Maximum acceptable spurious trip rate

t. A system model or similar describing the system architecture and independence

u. Consideration of anticipated failures, such as common cause and systematic failures

v. Software safety requirements for any programmable devices (other than components such as sensors with a fixed programmable language).

A7.3. SIF design

Validity of the Design

1. Has the SIS been reviewed to ensure that it is designed, constructed and installed in accordance with the safety requirements specification and good practice, with any differences being identified and resolved?

2. The review of the SIS design, construction and installation against the safety requirements specification good practice should cover:

    a. Are the integrity requirements met for example by a documented PFD calculation that is relevant to the SIF?

    b. Do the PFD calculations correctly consider the input and output voting arrangements?

    c. Is the architecture of the system in terms of its independence and fault tolerance documented and consistent with the safety requirements specification?

    d. Are the instrument ranges and settings valid and recorded correctly?

    e. Is there independence between layers of protection, consider other layers for which risk reduction credit has been taken within the hazard and risk assessment?

    f. Are the SIS devices components suitable for use based upon prior use or in accordance with IEC 61508 parts 2 and 3? Reference should be made to IEC 61511 clauses *Requirements for the selection of devices based on prior use, Requirements for selection of FPL programmable devices based on prior use, Requirements for selection of LVL programmable devices*

based on prior use, Requirements for selection of FVL programmable devices and CDOIF guidance 'Demonstrating prior use of elements of a safety instrumented function in support of IEC 61511'. Note that this assessment need only be completed per device?

g. Does application software and configuration meet requirements?

h. Are support systems (instrument air, power etc.) adequate and common cause failure addressed?

i. Have the differences between the SIS design and current standards (e.g. IEC 61511 clauses *SIS design and engineering* and *SIS application program development*) been identified and documented? Note where installed SIS are known to be to a historical standard then the assessment could be completed against this historical standard rather than the SIS design?

j. Does the SIF design meet the functional and other requirements in the SRS?

k. Do operating or maintenance records show any problems with the design or suggest that the design is not adequate?

l. Are any obsolesce and spares issues being managed?

m. Are the SIS components within their design life or else being managed appropriately?

3. Have any issues identified by the review of the SIS design, construction and installation been resolved (e.g. by improvement where reasonably practicable and/or by modifying the hazard and risk assessment and ALARP demonstration to reflect the integrity and functionality achieved by the SIS)?

A7.4. Proof Testing

Effectiveness of Testing

The proof test design will be reviewed to confirm that it gives sufficient test coverage to confirm all relevant aspects of the SRS.

1. Are the proof tests being completed in a timely fashion?

   a. Is there a maintenance management system (paper or electronic) in place to schedule proof tests?

   b. Is the proof test interval set correctly according to the PFD calculations?

   c. Is the SIS being tested in-line with the set test interval and any deferrals being managed and monitored appropriately?

2. Are the proof test procedures adequate?

    a. Are the proof test procedures sufficient to reveal all undetected faults in the SIS, considering any assumptions made within the PFD calculation (for example partial test strategies or assumptions about test coverage)?

    b. Have the proof test procedures been developed to cover all elements of the SIF

    c. Are the test procedures updated when new information is available?

    d. Are the SIF test procedures being followed?

    e. Are tight shutoff valves being leak tested prior to overhaul and their leakage rates being recorded / reviewed?

    f. Is the oversight of the proof test outcomes such that wider issues are acted upon, for example SIS response time not within required limits at every test (rather than just repaired)?

A7.5. Management of Change

1. Are management of change procedures in place for the SIS?
2. Have any modifications been carried out to the SIF and have they been completed, documented and reviewed correctly? – review any projects / management of change requests.
3. Were modifications subject to an impact assessment prior to modification?
4. Were modifications authorised prior to implementation?
5. Do the current revisions of FS documentation reflect the modification changes?
6. Is application software under management of change control and version tracking?

A7.6. Reliability

1. Is the reliability of protection layers other than the SIF function sufficient (such as pre-alarms, non-return valves [NRVs] etc.) and are they being maintained?
2. Is the reliability of the SIF in line with the failure rates assumed in the original design?

A7.7. Operation and Maintenance

1. Are Operating, Maintenance and Emergency Procedures pertaining to the SIS available and correct?

2. Is system performance adequate? (Review loss and near miss incident investigations and/or operational experience) – see also sections 3.6 and 3.7
3. Are procedures in place and being followed for control of bypasses of the SIS?

A7.8. Functional Safety Management

1. Are the requirements for safety management and verification being met (refer also to FS Audit)?
2. Is competence managed appropriately for all personnel and organisation involved in the SIS life-cycle.
3. Are there any outstanding actions from previous FSAs, HAZOP or any other process safety reviews?
4. Are the plans in place for the next FSA review?

A7.9. Conclusion and Summary of assessment findings

1. Clearly state if the SIS meets the design specification or not, if it is maintaining the correct level of functional safety and safety integrity, identify any gaps that need to be addressed.
2. Make a judgement about the functional safety achieved and consider if risks are reduced to ALARP including:
    a. What more could be done to improve the SIS?
    b. What is the basis for not doing it at this time?
    c. Could the SIS be improved during modification or future new installations?
3. Summarise actions and recommendations and system for stewarding.

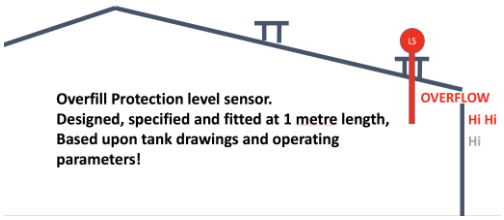
APPENDIX 8. EXAMPLE OF A SYSTEMATIC FAILURE

The following are examples of systematic failures relative to each life-cycle phase:

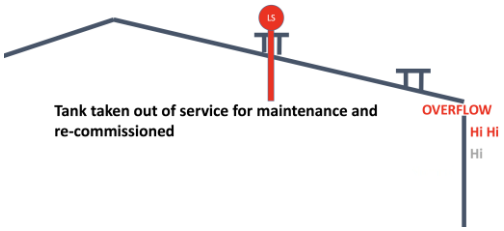
- specification – Human error in providing inaccurate basis of design e.g. miscalculation of activation points for the SIF.
- design – Human error during the design process (e.g. due to a misinformed assumption), incorrect design resulting from interpretation of requirements or simple copy and paste errors providing the wrong information. Software induced systematic failures during programming.
- Inappropriately specified materials or devices may deteriorate and fail due to environmental factors such as corrosion, contamination, vibration, temperature, moisture.
- manufacture - software and hardware errors built into the device by the manufacturer.
- installation - incorrect installation, not following the safety manual for the devices.
- operation and maintenance - Poor or no inspection, incomplete testing, incorrect use of testing devices, failure to return SIS to operational mode following maintenance or testing, inappropriate use of bypasses or failure to remove bypass.
- Age and wear - failure rates gradually increase with age and wear. As equipment approaches the end of its useful service life the failures are no longer random. A program of condition monitoring and renewal or replacement is necessary to prevent these failures.
- modification - Following any modification to the SIS there is a possibility that any of the failures above can be introduced into the system.

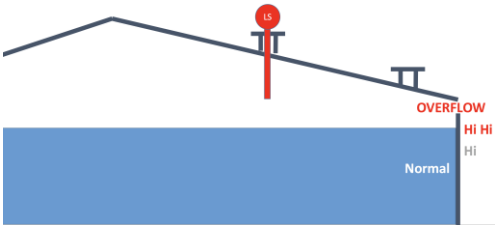
Random hardware failures and recurring faults may indicate that there is a systematic failure present.

The following figures illustrate how a systematic fault can be introduced into a SIS following a maintenance activity, the error may not be noticed throughout further inspection or proof testing regimes.

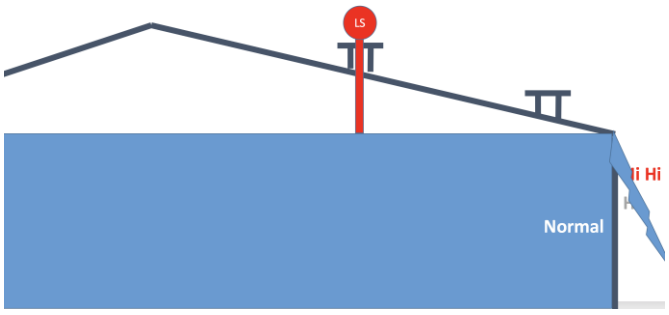


Operational procedures and other protection layers should prevent a demand on the SIS, such that the error may not be noticed, even during future maintenance.





However, if the other protection layers fail, the SIS will not operate as designed leading to overfill:



APPENDIX 9. METHODS FOR REVIEWING AND ADDRESSING SYSTEMATIC FAILURES

This appendix provides a question set to assess each section of an installed SIS life-cycle so as to form a judgement about the measures taken to minimise systematic failures (broadly based around IEC 61508-7 Annex B). Also provided is potential remedial work that could be undertaken to retrospectively identify systematic failures if judged that there is insufficient evidence that the systematic failures were managed in the earlier life-cycle steps.

A9.1. General Measures and Techniques

1. Project management - Is evidence available that the SIS was implemented in a structured way including: quality assurance, project planning, configuration management, oversight and formal acceptance at each stage, for example as part of a project process?
2. Documentation – Is documentation available showing how the SIS was developed and decisions recorded?
3. Competence – Is evidence available that the SIS was implemented by competent personnel and organisations?
4. Separation of the safety and non-safety functions – Is the SIS physically separate from the non-safety functions?
5. Diverse hardware – Has diverse hardware been used for the SIS?
6. Complexity – is the overall installed SIS being considered complex or simple (and well understood)?
7. Integrity – what is the highest SIL and number of SIFs within the SIS being considered.
8. Operating experience – Is there significant and documented operating experience that gives confidence that systematic failures are not present, for example evidence that the SIS has operated on demand?

Potential Remedial Work:

1. The findings of this section should be used to weigh the findings of the later sections, and used as part of the judgement as to what further work would be necessary.

A9.2. Specification

1. Structured Specification – is there evidence that a requirements specification (e.g. URS) was produced to set out user requirements for the SIS during the project?
2. Is it clear which hazardous scenario(s) the SIS was designed to prevent and is this consistent with current requirements.
3. Are the SIS requirements complex or unique? For example, requiring sequential operations, conditional based actions etc.?

4. Was a hierarchical framework approach to specification used, i.e. breaking down complex requirements into simple requirements and minimising interfaces?
5. Were recognised methods (e.g. cause and effects, function block diagrams, ladder logic, state graphs etc.) used for specifying functionality requirements?
6. Is there evidence that the specification documents were subject to review / analysis / verification and approval mechanisms?
7. Are differences between the original and current specification traceable through management of change forms?

Potential Remedial Work:

1. Detailed review of current SIS functional specification against current requirements (linked to current hazard and risk assessments and to re-define functionality from first-principles).
2. Analysis of differences between original and current specification to identify modifications and to ensure that these modifications were appropriately managed.

A9.3. Design

1. Were guidelines / standards (of the day) followed and are these standards known and differences to current standards understood?
2. Is there evidence of a structured design process with known methods and development tools, for example described within functional design specifications and detailed design specifications?
3. Is the design documented and understood, for example as-built loop and system design documents?
4. Were well-tried / well-known hardware components used?
5. Are the hardware components or overall hardware design complex or unique?
6. Is there evidence of a modularised software design, e.g. using standard blocks / configurations?
7. Were standard tools / methods for design used?
8. Is there evidence that design reviews / analysis / walkthroughs and approvals were completed?
9. Is there evidence of integration or software module testing?
10. Are differences between the original and current design traceable through management of change forms?

Potential Remedial Work:

1. Complete design review / analysis (e.g. FMEA) / walkthroughs of hardware and software design.
2. Review of component manuals (or testing) to understand their operation and limitations.

3. Analysis of differences between original and current design to determine basis to ensure modifications made are appropriate.

A9.4. Installation, Commissioning and Validation

1. Is there evidence of installation and commissioning being completed in a structured way to known procedures?
2. Is there evidence of validation completed, e.g. FAT and SAT?
3. What was the coverage of validation completed – e.g. were techniques such as fault insertion, simulations, black box testing etc. completed?
4. Does field experience and testing outcomes indicate problems with the SIS design / limitations?

Potential Remedial Work:

1. Targeted, e.g. simulation tests, black box testing of complex software etc., or sampled validation testing (note validation testing is not proof testing) against current specifications.
2. Analysis / review of field experience to gain confidence in installed SIS.

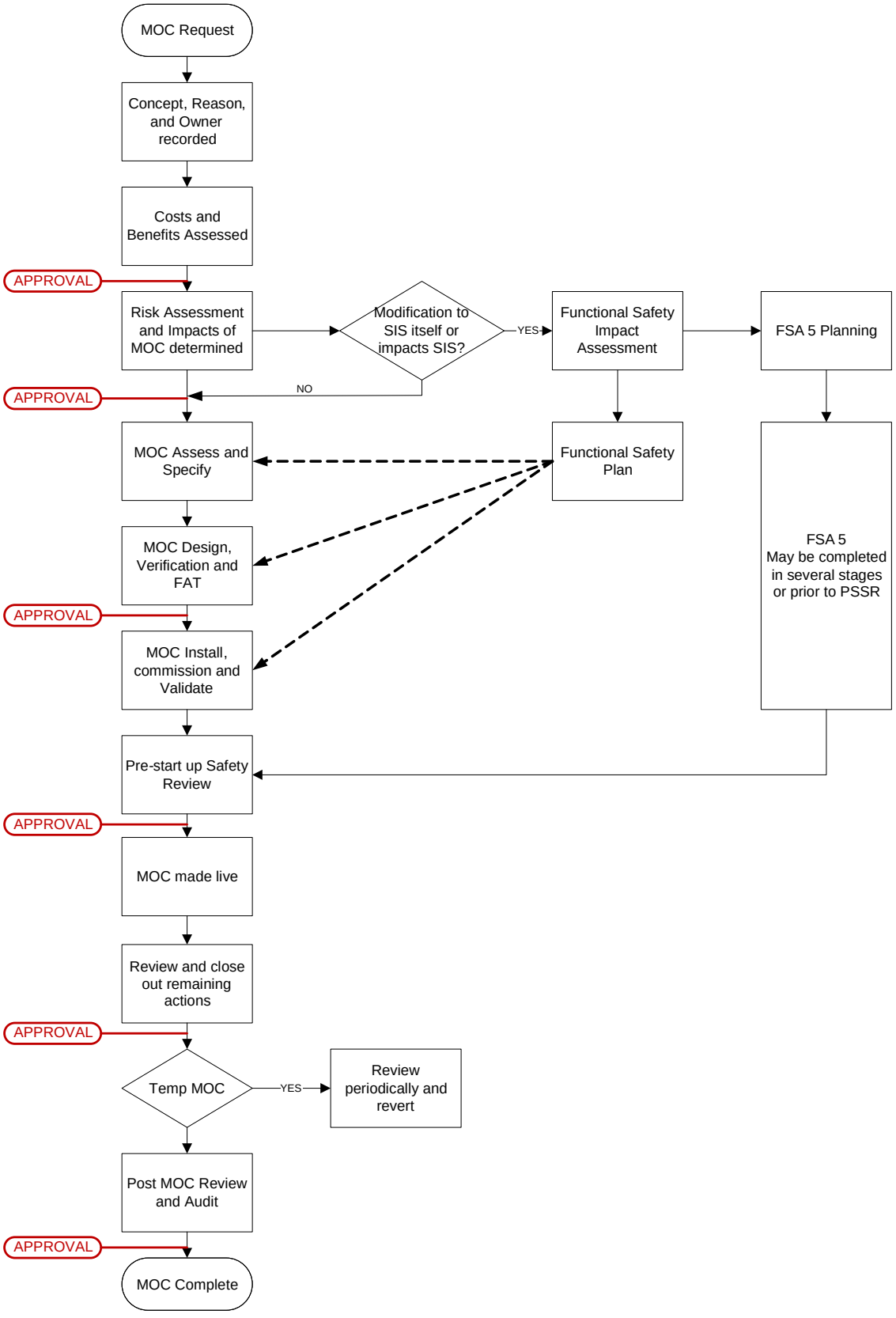
A9.5. Operation and Maintenance

1. Have operation and maintenance procedures been in place and implemented since SIS installation?
2. Evidence that changes have been subject to MOC?
3. Is the operation and maintenance complex (e.g. not user-friendly)?
4. Are there limited operation possibilities (e.g. special operating modes, number of operating elements and modes)?
5. Are operator errors captured, e.g. protection against inputting wrong data, making modifications etc.
6. Are operators trained to operate the SIS correctly and is this training refreshed?
7. Any evidence of issues that have the potential to cause a failure (systemic failures, operational problems etc.)?

Potential Remedial Work:

1. Review operation procedures against current specification and design requirements.
2. Review maintenance procedures against current specification and design requirements and any relevant manufacturers manuals.
3. Operator training.
4. Consider modifications for any identified issues.

APPENDIX 10. TYPICAL PROCESS FOR MANAGEMENT OF CHANGE



The MOC should ensure that any relevant documentation is updated or produced, this could include:

- A description of the modification.
- The reasons for the modification.
- Modification impact analysis by assessment of all relevant risk and design parameters (e.g. new hazards identified) and relevant risk assessments.
- Functional Safety Impact Assessment, i.e. how the modification will impact the SIS and a resulting functional safety plan for the modification.
- Functional safety documents (depending upon the scope of the modification and as defined in the functional safety plan) – for example:
    - Competence records
    - Hazard and risk assessment and SIS allocation documents
    - SRS
    - Design documents, verification records, validation records, PFD calculations
    - Installation and commissioning records
    - Updated / new operating and maintenance procedures etc.
    - FSA 5 outcome
- Other records that require updating (including secondary documentation i.e. spares information).
- Approvals
- Actions.

APPENDIX 11. FUNCTIONAL SAFETY ASSESSMENT 5 CHECKLIST

Note that the FSA could be completed in 1, 2 or 3 (or more parts) depending upon the complexity of the modification made. The example below includes two parts.

A11.1. FSA 5 Part 1 – Prior to commencing the modification

1. Have the hazards been identified?
2. Is the Impact Analysis[3] on the SIS modification adequate?
3. Have the appropriate parts of FSA 5 been planned?
4. Have the appropriate life-cycle phases been completed based upon the impact analysis?
5. Is there any impact on the Hazard and Risk Analysis?
6. Is the definition and reason for the SIS modification adequately documented?
7. Have instrument trip settings been verified against master data / SRS?
8. Have instrument range settings been verified against master data / SRS?
9. Has Management of Change documentation been completed and approved?
10. Is the SIS modification proposed in compliance with IEC 61511?
11. Have all SIS Components impacted by the change been identified?
12. Are all SIS Modification activities to be carried out by appropriately qualified personnel?
13. Have all necessary re-verification activities been included in the Safety Plan?
14. Do verification checks include tests to ensure the change does not adversely impact parts of the SIS which are not intended to be modified?
15. Has the SIS modification been reviewed approved by appropriately qualified personnel?
16. Have all changes been checked against requirements of SRS document?

A11.2. FSA 5 Part 2 – Prior to introduction of the hazard / prior to handover)

1. Have the verification checks been successfully completed?
2. Does the modified SIS perform as required?

[3] An impact analysis assesses the impact the change has on functional safety and where in the safety life-cycle the modification needs to return to

3. Has adequate validation been completed?
4. Have on going proof testing / operating / emergency procedures and plans been updated?
5. Have all relevant affected personnel been trained / informed of SIS modification?
6. Has all documentation / configuration been updated and stored correctly?
7. In summary is SIS ready to be brought into service?
8. Are there plans for an FSA 4 in place once operating experience has been gathered.?

A11.3. FSA 5 - Decommissioning

To include an assessment of:

1. That either:
    a. Hazards are reduced/eliminated due to changes in the process conditions and the SIS is no longer needed; or
    b. There is a progressive and systematic reduction control of the existing hazards and safety reducing dependency of protection layers on the SIS. (e.g. controlled by other means (non-SIS) of protection)
2. The impact on functional safety as a result of the proposed decommissioning activity.
3. The impact both during and after execution of the proposed decommissioning or disposal activities on the functional safety of any other SIS associated with the plant and plant control system.
4. The update of the hazard and risk analysis sufficient to determine the necessary breadth and depth of subsequent overall safety lifecycle activities as identified in this procedure.