COMPREHENSIVE GUIDE TO THE SAFETY LIFECYCLE FOR

SAFETY INSTRUMENTED SYSTEMS

Your essential resource for understanding, implementing, and maintaining functional safety in process industry applications.

Sixth Edition | Document ID: eFS-ebook-SIS-ed6.3

ABOUT THIS EBOOK

Welcome to the sixth edition of our eBook, aimed at industry professionals working to achieve compliance with IEC 61511 - the international standard for functional safety of safety instrumented systems (SIS) in the process industry sector.

Despite functional safety standards guiding industry practices for over two decades, we believe providing a clear, accessible overview remains essential. This guide aims to simplify some complex concepts while delivering comprehensive insights.

For those new to functional safety, we recommend beginning with professional training. On the resources page of this edition, we've provided information and links you may find useful for further learning and practical use in real-world projects.

All the best,
Jon

Jon Keswick, CFSE
Founder - eFunctionalSafety

Contents

eFunctionalSafety® INSIDER

Join our Functional Safety Community

A professional community offering networking, exclusive online events and training resources for functional safety practitioners, with premium options for enhanced benefits.

Register Now

Understanding Risk and Safety in Industrial Environments

> Industrial environments inherently involve risk trade-offs, requiring multiple protective layers beyond PPE. Engineers apply inherent safety principles in equipment design, while functional safety principles ensure appropriate safety integrity levels for critical instrumented systems.

As industry professionals, we accept various levels of risk every day. From commuting to work to operating in inherently hazardous environments, we tolerate some elevated risk in exchange for compensation.

Creating a tolerably safe environment when working with hazardous materials involves significant challenges. While workers in industrial settings wear appropriate personal protective equipment (PPE), this measure alone is insufficient when facing possible events that could lead to significant fire, explosion, or toxic release.

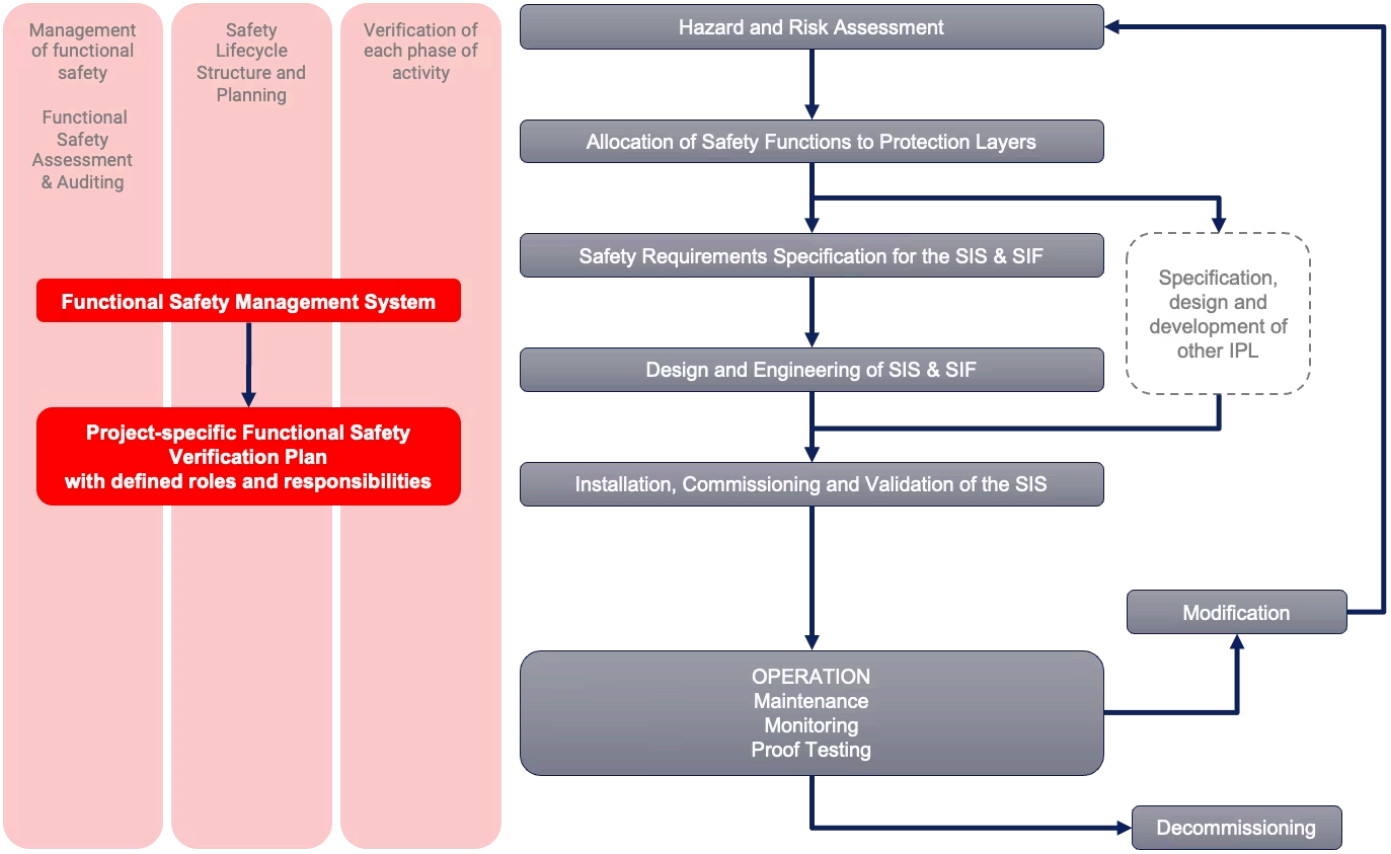
To maximize process safety, engineers apply *inherent safety* principles to ensure pipes, vessels, and process equipment are designed with appropriate materials that can withstand extreme temperatures, pressures, and corrosive substances.

When these extreme conditions could potentially lead to containment breaches, *Functional Safety* principles come into play, ensuring that Safety Instrumented Functions within the Safety Instrumented System (SIS) are assigned appropriate Safety Integrity Levels (SIL).

The Safety Lifecycle

The IEC 61511 standard establishes a functional safety lifecycle for the process industry sector that has gained international acceptance among operating companies and regulators worldwide.

Figure 1: An adapted version of the IEC 61511-1 safety lifecycle



All SIS projects must be conducted according to robust project management principles, incorporating a clear, concise plan, well-documented procedures, and thorough verification and sign-off activities at key stages.

We strongly advocate for developing practical procedures and templates that teams will genuinely utilize. This requires keeping documentation relevant and accessible, preferably incorporating visual elements such as flowcharts and diagrams to enhance understanding and facilitate implementation.

> In practice, the hazard owner must develop a customized lifecycle clearly defining a selection of methodologies and procedures to achieve all functional safety objectives.

Project templates serve a distinct purpose from procedures, providing valuable starting points for professionals new to SIS projects. Well-designed templates and comprehensive checklists significantly contribute to ensuring completeness and compliance, thereby simplifying subsequent assessment processes.

Functional Safety Management

People, Planning & Procedures - FSM

> Functional Safety Management (FSM) is a systematic approach that integrates competent personnel, strategic planning, and standardized procedures to effectively implement and maintain safety instrumented systems throughout their lifecycle, as required by IEC 61511.

Successfully implementing the SIS safety lifecycle requires careful consideration of people, planning, and procedures. The IEC 61511 standard defines this comprehensive approach as *Functional Safety Management* (FSM).

A robust functional safety management system ensures projects are staffed with individuals who possess the appropriate competencies for their specific roles within the lifecycle. The primary objective is to establish effective policies, strategic planning, and standardized procedures to govern specialized functional safety activities. With proper management practices in place, organizations can preserve critical safety knowledge even as personnel change or retire.

When planning lifecycle steps, it is crucial to address the required inputs, detailed procedures, and expected outputs for each specialized activity. While the IEC 61511 standard provides a sample lifecycle framework, this serves merely as a starting point as it is too generalized for direct implementation. Instead, organizations must develop tailored approaches that meet their specific operational needs and safety requirements.

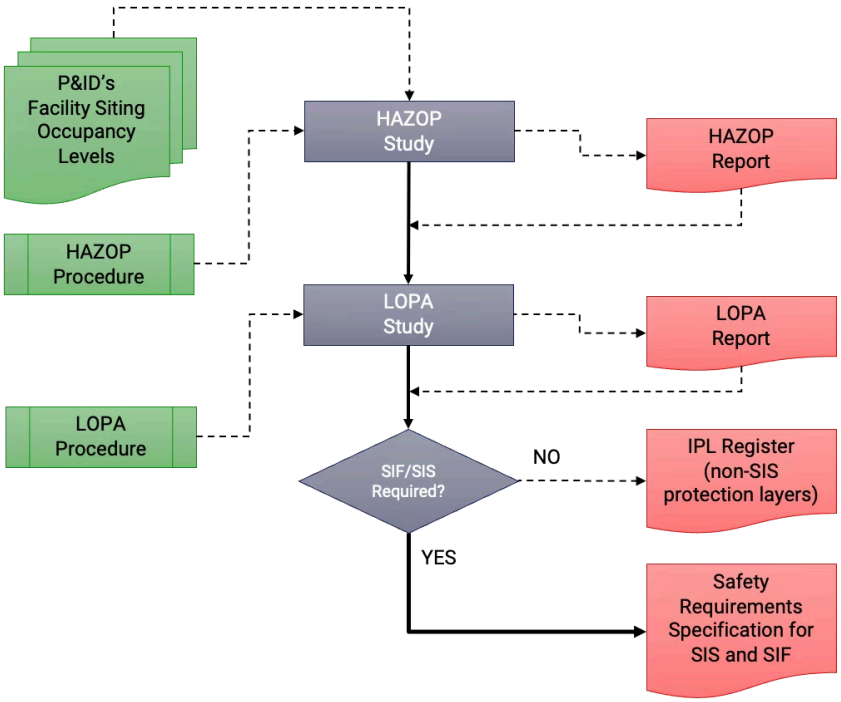
Hazard, Risk and SIL Assessment

> Process safety requires systematic hazard identification and risk assessment. HAZOP studies serve as a foundation, followed by LOPA to evaluate protection layer effectiveness and determine SIL targets for critical safety functions.

Organizations operating systems, processes, or machinery that could potentially result in loss of life or significant environmental damage must conduct thorough hazard identification and risk assessment. For most process facilities, this primarily involves identifying events that could result in the "loss of containment" (LOC) of hazardous materials.

There are numerous methodologies for conducting process hazard analysis (PHA), with HAZOP (Hazard and Operability studies) being a typical starting point. Regardless of the chosen methods, the key to success lies in employing a systematic approach with a multi-disciplinary team.

Figure 2: Typical workflow from HAZOP to LOPA and SIL determination



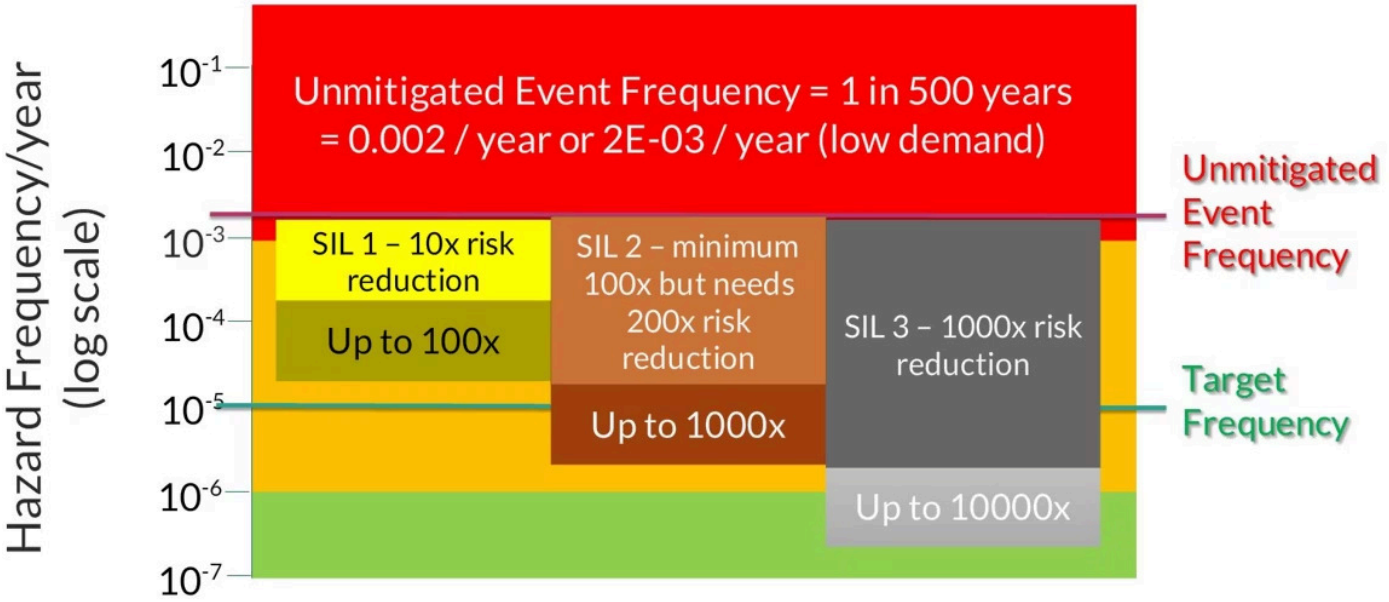
When properly executed, a comprehensive HAZOP should provide:

- Credible information on possible causes of hazards
- Estimated consequences of hazardous events
- Safeguards or protection layers that can prevent event occurrence or mitigate escalation
- Actions for safety and operational improvement

LOPA and SIL targets

Following initial hazard identification, a more detailed assessment of Independent Protection Layers (IPLs) is often required for the most severe hazards. Layers of Protection Analysis (LOPA) is a widely accepted semi-quantitative methodology for this purpose.

> LOPA requires a consistent methodology based on established risk criteria to determine if Safety Instrumented Functions (SIFs) are needed. When properly conducted, LOPA identifies appropriate Safety Integrity Level (SIL) targets for risk reduction.



To understand more about the above figure, join our **SIS & Functional Safety online course** for a full narrated explanation.

Since there are no universally standardized techniques for conducting LOPA, each organization must establish clear, consistent rules within their tolerable risk guidelines to ensure methodical application across all assessments.

LOPA implementation requires well-defined risk criteria as a foundation. These typically include a company-approved risk matrix and established numerical targets specifying maximum acceptable frequencies for various consequence scenarios, particularly those with the highest severity.

After evaluating all available IPLs, it frequently becomes apparent that one or more Safety Instrumented Functions (SIFs) will be necessary to reduce risk to tolerable levels. When proper analytical procedures are followed, the LOPA study can effectively determine the appropriate Safety Integrity Level (SIL) target required for each SIF, establishing the performance standard necessary for risk reduction.

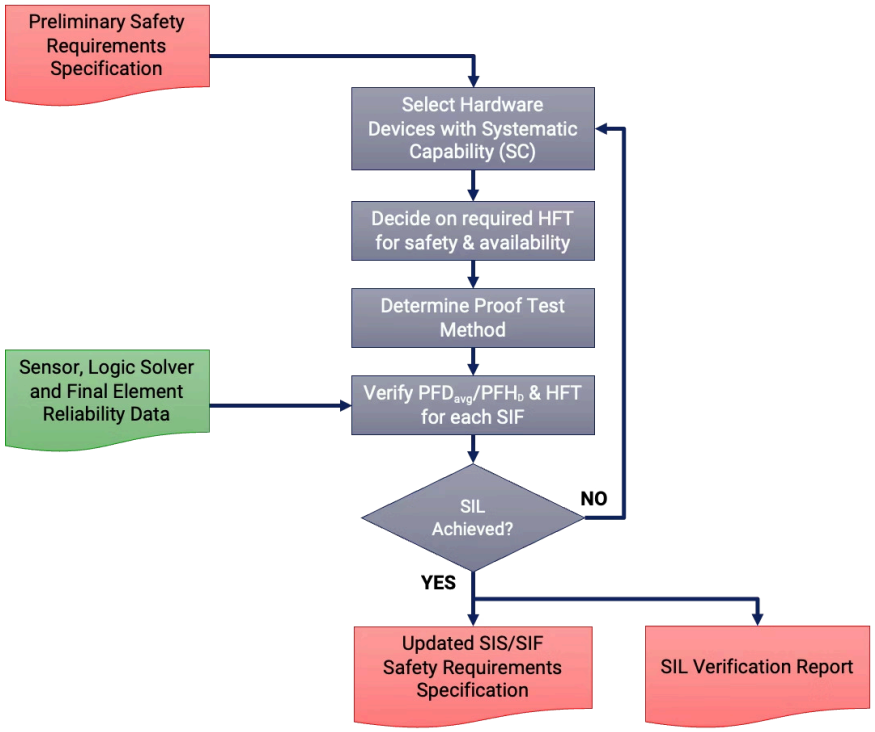
Safety Requirements Specification

Once it has been determined that a Safety Instrumented System (SIS) is required, a comprehensive Safety Requirement Specification (SRS) must be developed.

Functional requirements must clearly define the purpose of each Safety Instrumented Function (SIF), identify the specific hazard it protects against, and detail the required actions. These functionalities can be effectively represented through Cause and Effect diagrams that clearly link the sensed conditions with their corresponding required actions.

While the Safety Integrity Level (SIL) target is a critical integrity requirement for each SIF, it is just one of many things to manage. Other important requirements include Probability of Failure on Demand (PFD) or Probability of Failure per Hour (PFH), Hardware Fault Tolerance (HFT), and Systematic Capability (SC).

Figure 3: Development of the SRS and SIL verification



During the early design or modification stages, the hazard owner must define approximately thirty different integrity and functional requirements to describe each function in hardware terms. This constitutes the "preliminary SRS" as shown in the diagram above.

As the design or modification of a SIS progresses, additional requirements must be meticulously developed to fully specify the overall system, application program (software), and interfaces with other systems.

In practice, the hardware and software SRS may ultimately comprise multiple documents that progressively detail the SIS and SIF devices and software with increasing specificity as the project advances.

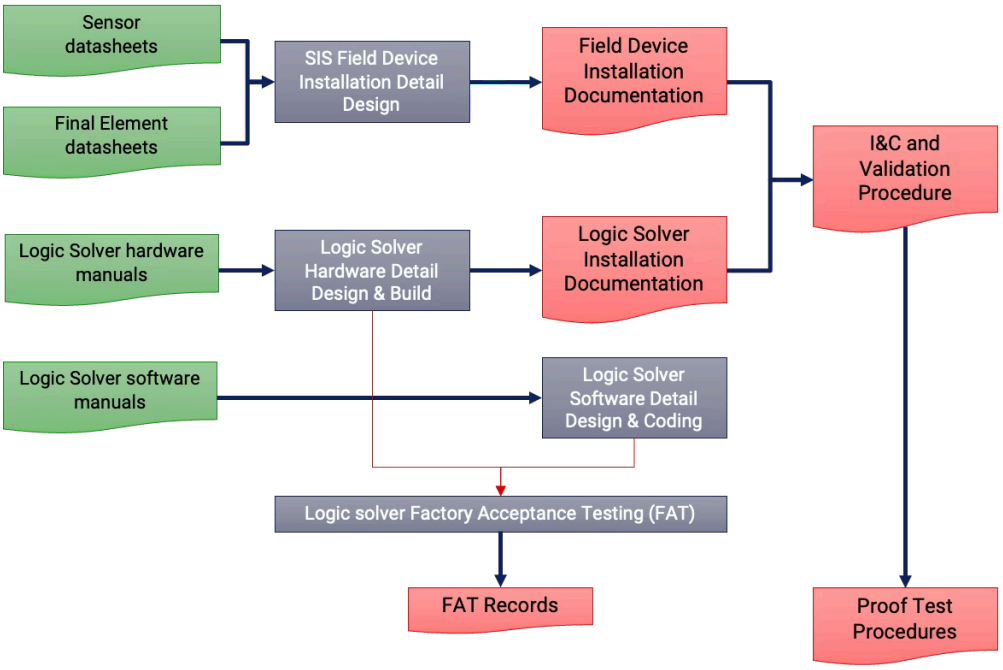
SIS Design & Engineering

> Safety Instrumented System design requires selecting appropriate SIL-capable equipment, developing rigorous application programs following manufacturer guidelines, and conducting comprehensive verification through design reviews and Factory Acceptance Testing.

The specifier of an SIS can select appropriate equipment once the safety requirements are sufficiently complete and stable. Long-lead items such as final element valves and actuators are typically among the first components to be considered for procurement.

IEC 61511 requires all equipment used in the SIS to be justified. Typically, this involves ensuring that only SIL-capable devices from reputable suppliers are utilized. In cases where SIL-capable devices are unavailable, the company responsible for equipment selection and engineering will need to justify the use of alternative equipment on another basis, such as documented "prior use" evidence.

Figure 4: Simplified workflow for typical detailed design of a Safety Instrumented System



Logic solver application programs (software) must also be developed with rigor. When using SIL-capable Safety Programmable Logic Controllers (Safety PLCs), the software coding rules are often specified in a safety manual provided by the Safety PLC manufacturer. When developing the Application Program (AP), it is critical to follow the manufacturer's "do's and don'ts" guidance meticulously.

Verification through comprehensive design review and integrated hardware/software Factory Acceptance Testing (FAT) will typically occur towards the end of this stage. It's important to note that FAT alone is insufficient for complete validation, as field devices are typically not integrated at this stage of testing.

Installation & Commissioning (SAT)

> The installation and commissioning phase includes mechanical installation, commissioning, SIS validation, and documentation. This critical final stage requires rigorous testing of all Safety Instrumented Functions against the Safety Requirements Specification.

The final stage of the design and engineering lifecycle is known by various names in industry. Many refer to this entire phase as Site Acceptance Testing (SAT), which encompasses multiple stages of mechanical completion at the installation site before any testing activities commence.

Phase	Key Activities	Documentation
Mechanical Installation	Physical mounting of equipment, wiring, and connections	Installation records
Commissioning	Power-up, configuration, and calibration of instruments	Commissioning procedures, Calibration records
SIS Validation	End-to-end physical testing of every SIF	Validation plan based on SRS
Documentation	Complete test records, verification against SRS	Validation report, Test records, As-built drawings

Validation testing of the SIS at the hazard location requires comprehensive end-to-end physical testing, from the installed sensors through to the installed final elements, for every Safety Instrumented Function (SIF) documented in the Safety Requirements Specification (SRS).

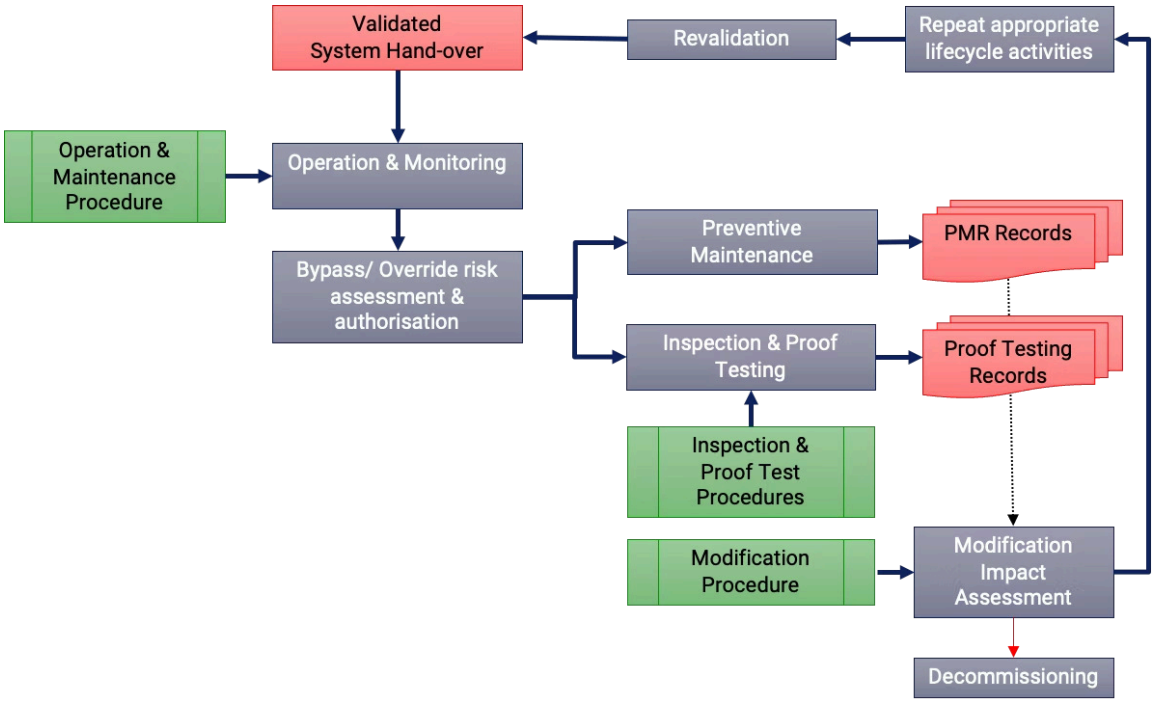
Operation & Maintenance

> SIS operation requires thorough personnel training, documented inspection protocols, scheduled proof testing aligned with plant turnarounds, special bypassing procedures, and systematic tracking of system activations to maintain safety integrity.

Comprehensive training on all SIS and Safety Instrumented Function (SIF) aspects must be provided to operation and maintenance personnel before system startup. This training is especially critical when implementing novel systems or unfamiliar equipment.

Inspection and proof test procedures should be fully developed and documented for the SIS and each individual SIF in readiness for periodic inspection and proof testing.

Figure 5 - Monitoring, maintenance, inspection and proof testing during operation



For optimal safety and efficiency, inspection and proof tests should be scheduled to coincide with planned turnarounds, allowing for safe offline testing. Operations must maintain detailed inspection and test records, which are essential for future assessments, audits, and root cause analysis of equipment failures.

Continuous process plants may require special procedures for bypassing a SIF or SIS during operation. These procedures must include comprehensive risk assessments of safety function bypassing and incorporate appropriate technical reviews and authorization protocols.

Operations personnel should systematically track and analyze SIS activation events (demands) over time to identify potentially negative trends that might indicate the need for plant or system modifications.

Change Management

> SIS modifications require strict change control protocols, independent assessment, thorough documentation, and implementation by competent personnel to maintain system integrity.

Once a Safety Instrumented System (SIS) becomes operational, it must be protected by strict change management protocols. No modifications should occur without following proper change control procedures.

The primary goal of SIS change management is to preserve the integrity of previously validated systems. All change requests must identify and revisit the relevant lifecycle phases to fully understand potential impacts before implementation.

Effective modification planning requires documenting the justification for change, conducting a thorough impact analysis, and performing a functional safety assessment (FSA 5) of this analysis. The FSA must be conducted by a competent individual who is independent from those implementing the changes.

System re-validation and comprehensive documentation updates are mandatory following modifications. The only exemption applies to strictly like-for-like replacements that involve no changes to software or embedded firmware.

Implementation of SIS changes must occur only under pre-authorized conditions and established work-permit protocols. As with all safety-critical tasks, changes must be executed by personnel with demonstrated competence, with detailed completion records maintained. All affected personnel must receive appropriate training on the modifications.

Any decommissioning of a Safety Instrumented Function (SIF) or System (SIS) must adhere to formal change management procedures, with comprehensive justification records preserved to document the removal of safety functions from service.

Functional Safety Assessment & Audit

> Functional Safety Assessment (FSA) is a mandatory, independent technical evaluation conducted at specific lifecycle stages of Safety Instrumented Systems.

Functional Safety Assessment (FSA) is a critical technical evaluation required to be conducted at several stages in the Safety Instrumented System (SIS) lifecycle. IEC 61511 mandates that an FSA must be performed at least once before SIS startup and at regular intervals during operations.

A senior competent professional who is independent from the stages being evaluated must lead the FSA. This independence ensures objective assessment without bias from those who designed or implemented the system.

FSA planning should begin at project inception whenever an SIS is anticipated. For existing systems, schedule an operations and maintenance FSA 4 after a period of operation, and implement FSA 5 for all subsequent modifications.

While often confused, Functional Safety Assessment (FSA) and FS Audit are distinct requirements in IEC 61511. The key difference lies in required expertise: FSA demands functional safety technical competence, whereas audits can be conducted by professionals with management and auditing expertise but without specialized safety system knowledge.

1 Verification

Independent-person check of any lifecycle step or deliverable.

2 Validation

Physical on-site end-to-end test of a safety system and all SIL rated functions, including integrated hardware and software.

3 Assessment

An independent, senior and technically competent person checks that functional safety has been achieved.

4 Audit

Somewhat like a quality audit, this is a management check that functional safety procedures are being followed.

SIS Documentation

> Properly maintained safety system documentation is critical for compliance and operational safety. Changes to systems require updates across multiple interconnected documents from different lifecycle phases, making paper-based management inefficient and potentially risky to safety integrity.

Maintaining safety system documentation that is accurate, current, comprehensible, and fit for purpose is not just good practice; it's essential for operational safety and regulatory compliance.

In reality, this presents significant challenges. Modifications often necessitate updates across multiple documents created during different lifecycle phases. These changes occur both during project implementation and throughout operational phases.

Consider a scenario where a contractor installed the SIS over three years ago, and the process hasn't undergone any hazard revalidation. A modification to this SIS requires revisiting the Safety Requirements Specification (SRS) and may impact Hazard and Operability studies (HAZOP), Layer of Protection Analysis (LOPA), Safety Integrity Level (SIL) determination, SIL calculations, Proof Test Procedures, and probably more.

When managed through traditional paper-based archives, achieving consistency across all these interconnected documents becomes extraordinarily time-consuming and prone to error, potentially compromising safety integrity.

Fixing the Documentation challenge with Digitalization

1

Reasons for Digitalization

Juggling the myriad interconnected parameters and information at different lifecycle stages poses a significant challenge in effectively managing even small quantities of IPL and SIF.

2

Recommended Software

We recommend aeShield; the elite choice for safety lifecycle software. aeShield is renowned for its unmatched ability to bulk import data from your existing records, and then automatically revision-control that data across a plant or enterprise.

3

Start the Digitalization Journey

You can start your digitalization journey by joining us for an online demo.

Use the link below to book a demo time in our live diary.

Book a Demo

Other Resources

Download A Brochure

Join A Webinar

eFunctionalSafety INSIDER

SIS & Functional Safety for IEC 61511

Self-paced online training for IEC 61511-related safety instrumented systems. Learn about functional safety principles in process industry...

eFunctionalSafety INSIDER

Functional Safety Assessment Checklist

The eFunctionalSafety FSA checklist is an original Microsoft Excel (.xlsx) file that encompasses over 350 cross-referenced prompts for anyone leading an IEC 61511 functional safety assessment and/or functional safety audit.

eFunctionalSafety INSIDER

Video Hub | eFunctionalSafety INSIDER

Explore the Video Hub space in eFunctionalSafety INSIDER