Functional Safety for Process Safety Managers: Verifying Risk Reduction Credit for PHA Safeguards

Tuesday, March 31, 2026

12:00pm EDT
11:00am CDT

AcuTech
PROCESS RISK MANAGEMENT

Disclaimer

This webinar is intended solely to provide information. The information presented as part of this webinar, the opinions of the speakers, and any material published in relation to this webinar are provided for general purposes only and should not be construed as professional advice from any of the hosts, the presenters or the sponsors of the webinar, including AcuTech Group, Inc., or any of their respective affiliates, associates, employees or representatives (collectively, the "Presenters"). The content of this webinar may not apply directly to specific circumstances. Professional advice should be sought before any action is taken in relation to information disseminated during the webinar.

This webinar is being recorded. By participating, you consent to the recording and its potential distribution by AcuTech Group, Inc.

Functional Safety Webinar Series

AcuTech
PROCESS RISK MANAGEMENT

Today's Webinar

Functional Safety for Process Safety Managers: Verifying Risk Reduction Credit for PHA Safeguards

Tuesday, March 31, 2026
12:00pm EDT
11:00am CDT

Upcoming Webinars

Beyond PSM Audits: Functional Safety Assessments that Expose Hidden Risks

Tuesday, April 21, 2026
12:00pm EDT
11:00am CDT

From PSM to Performance: Your Functional Safety Deep Dive

Tuesday, May 12, 2026
12:00pm EDT
11:00am CDT

About AcuTech

Since 1994, AcuTech has been a global leader in providing best-in-class consulting, training, and software solutions to manage process risk.

With deep expertise in both the management and technical aspects of risk management, AcuTech is uniquely positioned to support clients ranging from the world's largest companies to specialized private companies to trade organizations and government agencies in improving safety, security, environmental, and operational performance.

This extensive experience across industries and in-depth knowledge of the tools and methods available for managing risk, allows our consultants to be responsive and flexible to meet client needs. In addition, they possess strong project management skills, broad technical expertise, and emphasize high-quality, on-time project work to support safer, more efficient, and, ultimately, more profitable operations.

Functional Safety for Process Safety Managers: Verifying Risk Reduction Credit for PHA Safeguards

Tuesday, March 31, 2026

12:00pm EDT
11:00am CDT

AcuTech
PROCESS RISK MANAGEMENT

Speaker

Charlie Souza, MSEE, PE, PMP, CAP

Functional Safety & ICS Cybersecurity Lead

AcuTech
PROCESS RISK MANAGEMENT

Charlie Souza, PE, PMP, CAP, TUV FS Engineer, IEC61511 SFS, IEC62443 CFS, is the Functional Safety Lead at AcuTech. He has over 25 years of engineering, design, and consulting experience in instrumentation, electrical, controls & automation, functional safety, and industrial cybersecurity.

He is a Professional Engineer (PE), a Project Management Professional (PMP), a Certified Automation Professional (CAP), and a TUV FS Engineer. He is also an IEC 61511 Safety Specialist and an IEC 62443 Cybersecurity Specialist through the International Society of Automation (ISA).

Mr. Souza is the lead for functional safety projects at AcuTech. This includes using exSILentia® and other tools to ensure SIF design meets the SIL target, proof-test procedures to enable optimal proof-test intervals, and functional safety assessments to sign off on SIS implementation. SIL Assignment and Verification activities include developing a Safety Requirement Specification (SRS) that details the functional safety integrity requirements specified in RAGAGEP for SIS implementation.

Mr. Souza is an FBI InfraGard member and a founding member of the ISA Global Cybersecurity Alliance (ISAGCA). He serves on numerous committees of the International Society of Automation (ISA).

A quick poll...

Who is our audience?

Today’s Agenda

- The PSM + Functional Safety Integration Challenge
- Safety Lifecycle: From PHA through SIL Verification
- IEC 61511 Standard & RAGAGEP Compliance
- Connecting MOC, Mechanical Integrity & SIS
- Practical Implementation & Audit Readiness

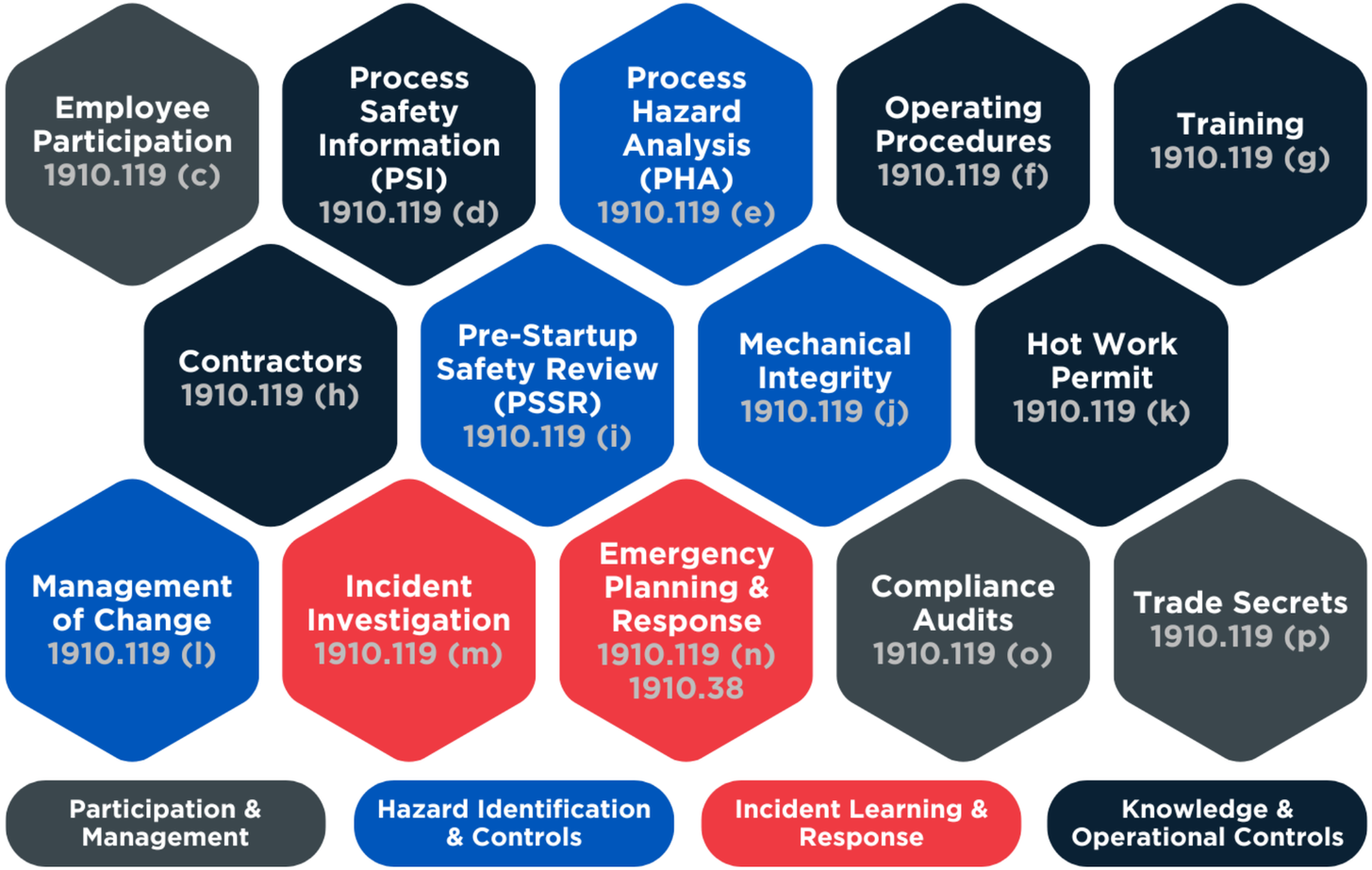
The Challenge We're Addressing

- You have PSM programs, PHAs, LOPAs, and SIS—but are they truly integrated?
- OSHA expects RAGAGEP: How does IEC 61511 fit into PSM?
- Risk reduction must be VERIFIED and VALIDATED in design, testing & operation
- MOC often misses instrumented safeguards—creating gaps
- Auditors ask: "Can you prove your SIS delivers claimed risk reduction?"

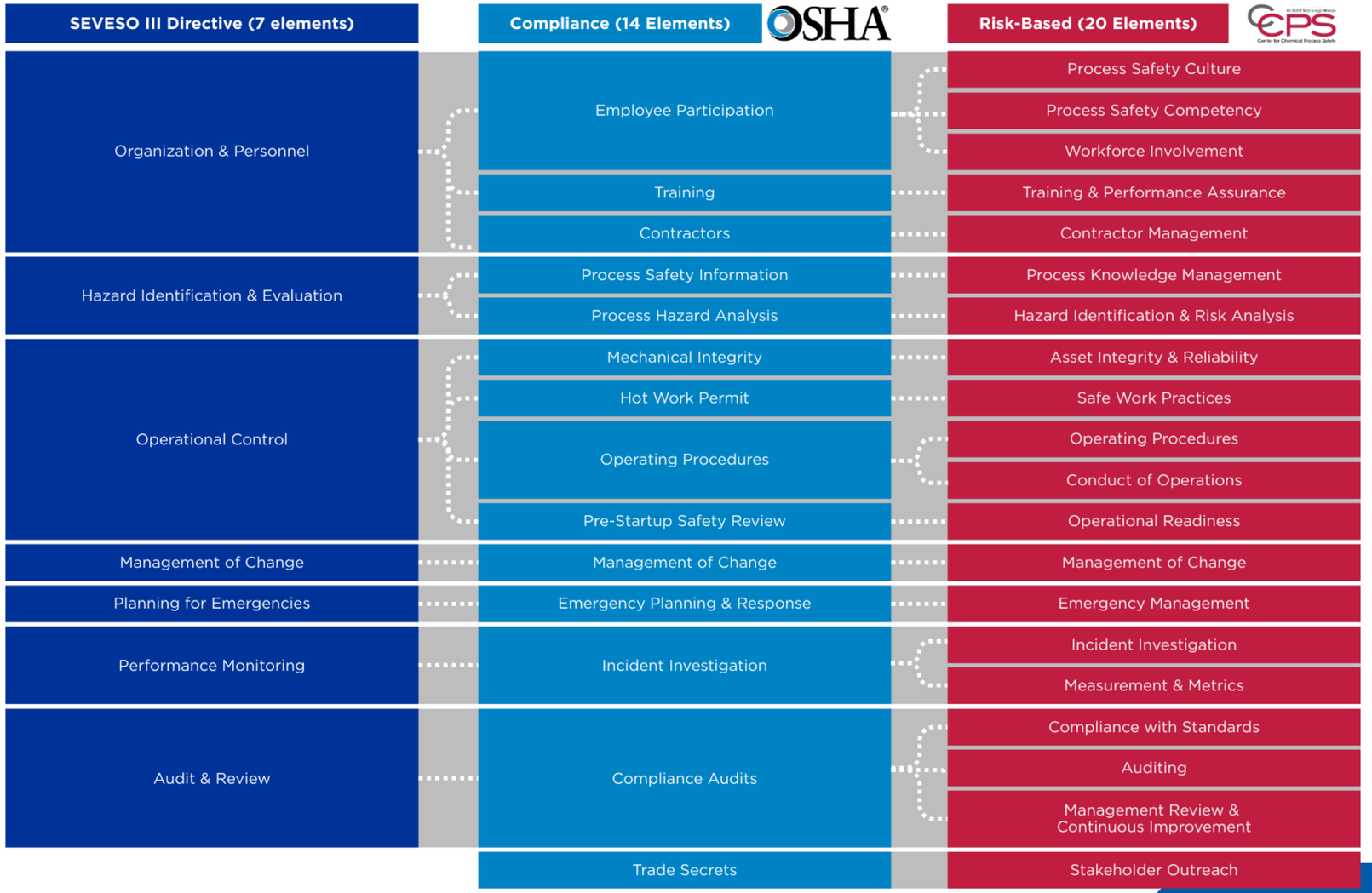
RAGAGEP in PSM: What OSHA Requires

- RAGAGEP = Recognized And Generally Accepted Good Engineering Practice
- For SIS: IEC 61511 is the recognized standard
- OSHA's expectation: SIS design, implementation & verification follows standard
- Audit reality: Inspectors review for functional safety lifecycle documentation
- Compliance strategy: Demonstrate lifecycle adherence + design verification

The 14 PSM Elements



SEVESO vs OSHA vs RBPS Elements



The Safety Lifecycle: Big Picture (IEC 61511)

1 **Hazard & Risk Analysis**

- PHA/HAZOP + LOPA

2 **Safety Requirements Specifications**

- SRS documents SIFs & functional requirements

3 **SIS Design**

- Hardware/ software verified to meet requirements

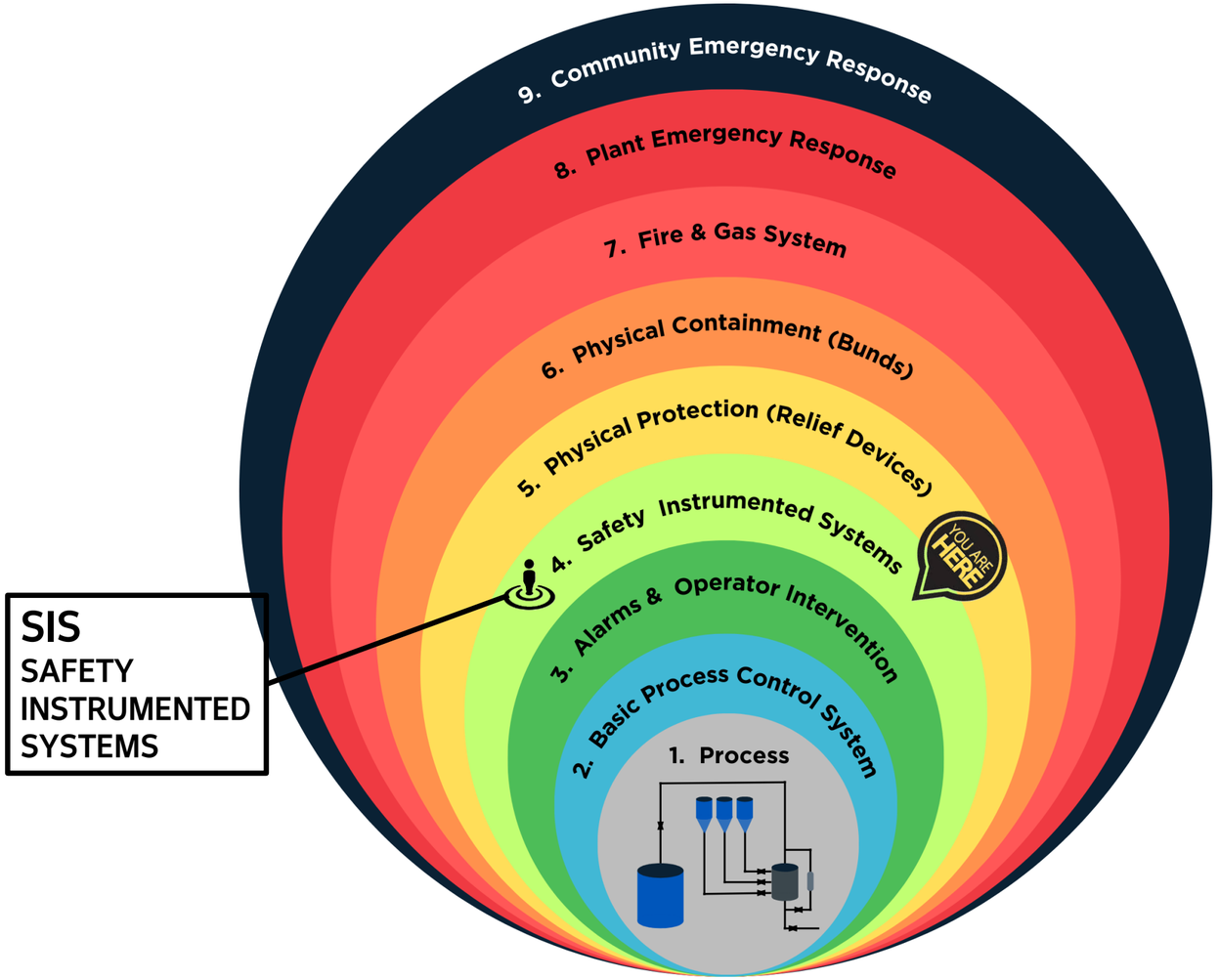
4 **Installation & Commissioning**

- As-built tested per procedures

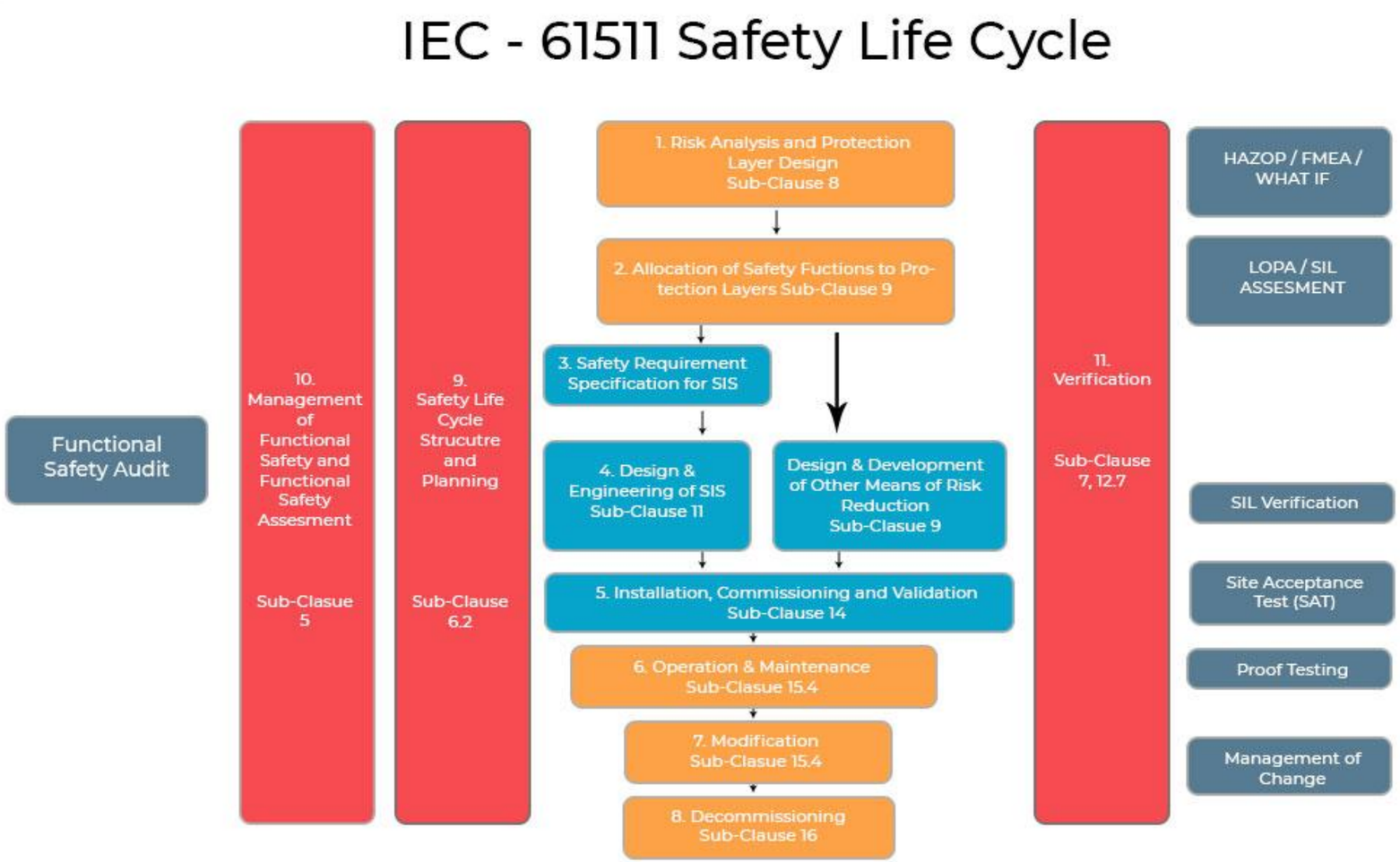
5 **Operational Verification**

- Proof testing & maintenance

Process Safety Onion Diagram



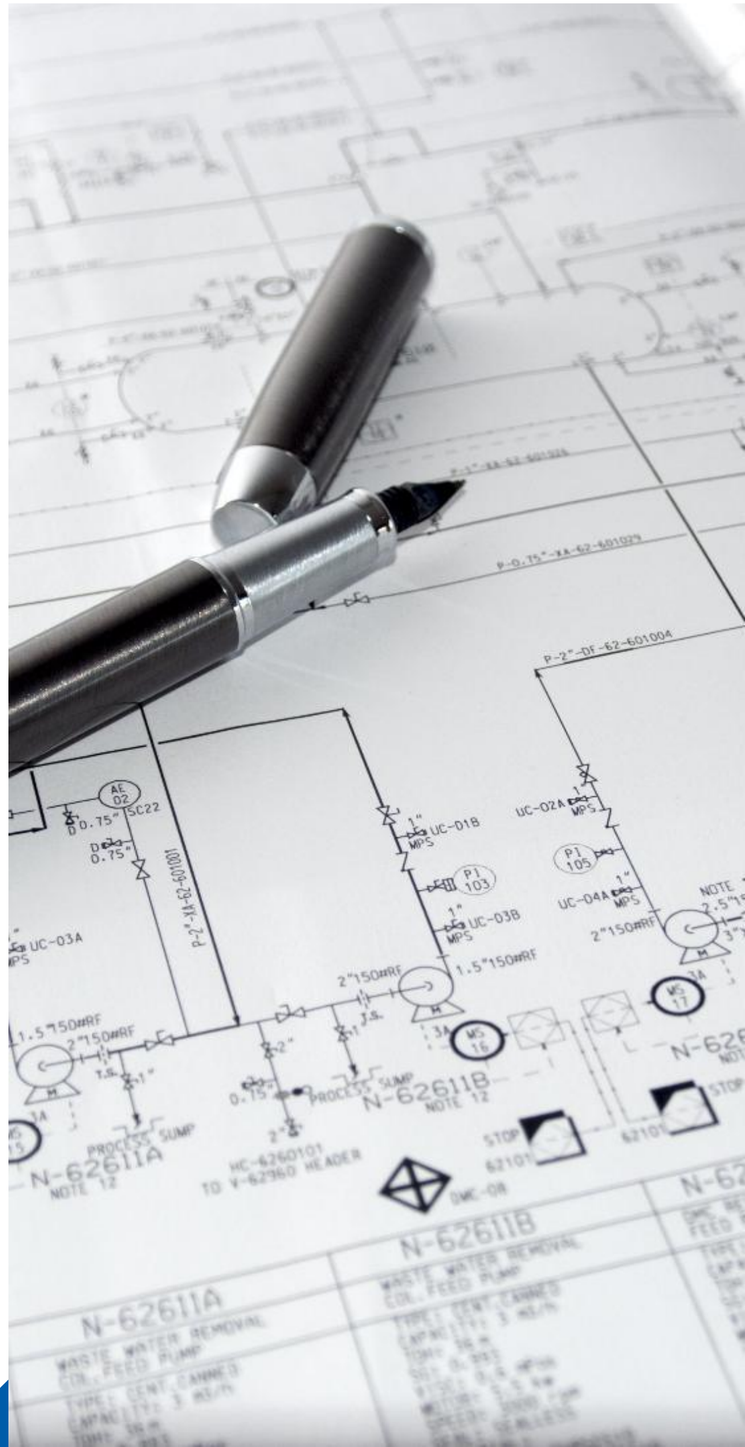
IEC 61511 Functional Safety Lifecycle



Source: NIST Global Pvt. Ltd.

Step 1: Hazard Identification (PHA/HAZOP)

- Purpose: Identify hazards, causes, consequences & safeguards
- Key output: Safeguard requirements—which ones are instrumented (SIFs)?
- Integration: Link each hazard-consequence to the proposed SIF
- Best practice: Conduct PHA/LOPA with the same team (integrated approach, although separate in the lifecycle)
- Documentation: Traceability from scenario to SIF requirement



Step 2: Risk Quantification (LOPA)

- Purpose: Quantify risk & verify safeguard adequacy
- Output: Required SIL (1–4 scale) for each Safety Instrumented Function
- Critical: LOPA links PHA findings directly to SIL assignment
- Reality check: Verifies that the proposed SIF can deliver risk reduction
- SRS: Documents target SIL for the design team

Step 3: Safety Requirements Specification (SRS)

- The document that bridges PHA/LOPA to SIS design
- Specifies: SIL target, response time, inputs, logic, outputs, proof test strategy
- Ensures: Design team understands hazard context—not just requirements
- Quality: SRS errors propagate through the entire design lifecycle
- Governance: MOC and proof testing must reference SRS

Step 4: SIS Design to SIL

- Design team selects sensors, logic, outputs based on SIL target
- Calculation: Component reliability
- Verification: Design reviews confirm hardware meets SIL
- Documentation: Design rationale, FMEA, testing plans per IEC 61511, and manufacturer's safety manuals
- Quality: Design errors undermine the entire risk reduction claim

Steps 5–6: Verification & Validation, Testing & Maintenance

- Commissioning: As-built SIS tested per documented procedures
- Operational verification: Periodic functional tests confirm SIL
- Proof testing: Full-stroke tests per RAGAGEP intervals
- Maintenance records: Document tests, anomalies, and corrective actions
- Continuous feedback: Test results inform ongoing risk assessment

IEC 61511: The RAGAGEP Standard

- International standard for functional safety in process industries
- Coverage: SIS lifecycle (FSM, FSMP, SIL Assignment, SIL Verification, documentation requirements, FSAs on new and old units, etc.)
- Recognized by OSHA as RAGAGEP for SIS compliance
- Three-part structure: Definitions, framework, design & implementation
- Compliance approach: Performance criteria + lifecycle documentation

OSHA's Compliance Approach: Performance Criteria

- OSHA expects to demonstrate performance as required per RAGAGEP
- Key criteria: Lifecycle management, SIL verification, testing discipline
- Audit focus: Complete lifecycle documentation + design traceability
- Red flags: No SRS, no SIL calcs, inadequate proof test procedures or records, inaccurate or missing PSI documents, discrepancies in general
- Success: Comprehensive documentation package reviewed by the auditor

Connecting MOC to Functional Safety

- Problem: MOC reviews often miss instrumented safeguards
- Risk: Changes bypass SIL verification, creating uncontrolled gaps.

  e.g.: Does the proposed change introduce any additional demands on the SIF (new valve, etc.)? If so, the LOPA should be revisited, the target PFD/SIL re-established, and SIL verification revisited to confirm that the achieved performance still meets the target.
- Solution: MOC checklist explicitly addresses SIF impact
- Key question: Does change affect any SIF? Require re-verification?
- Governance: MOC coordinator trained on functional safety

Mechanical Integrity & SIS Instrumented Systems

- MI scope: Sensors, logic solvers, final elements performing safety function
- Testing: Proof testing ≠ maintenance—both required per RAGAGEP
- Intervals: Proof test intervals determined by SIL verification, design assumptions in SRS for the SIF, and maintenance records.

  e.g.: If a proof test interval of 6 months is required, it must be performed; if the device needs to be overhauled in 5 years, that must be done as well.

- Records: Document all tests, failures, and repairs with traceability
- Training: MI personnel must understand SIL implications of their work

Complete PSM + Functional Safety Integration

- PHA/HAZOP: Identify hazards + safeguards (SIF candidates)
- LOPA: Assign SIL to each instrumented safeguard
- SRS: Document functional and integrity requirements for design
- SIS Design: Verify SIL is achieved
- MOC: Review changes for SIF impact + re-verification triggers
- MI + Proof Testing: Maintain SIS and SIL per documented strategy

Remember, RAGAGEP compliance is required for all items!

From PSM-Compliant to Functionally Safe & Verifiable

Current State: "We have PSM procedures and an SIS contractor.“

Future State: "We verify SIL through integrated lifecycle management.“

- PHA/LOPA integration with SRS ownership by the PSM team
- Design verification + SIS independence documented
- MOC explicitly addresses SIF impact + re-verification triggers
- Proof testing governance owned by PSM (not just OT/operations)

Functional Safety Assessments: Planning & Budget Reality

Gap: FSAs are often unplanned, under-budgeted, or deferred

- Project phase: FSA can add 4–8 weeks; budget impact unknown upfront

  High Cost: Skipping FSAs 1 and 2, waiting until PSSR to conduct FSA 3 translates to a higher cost to close findings/gaps

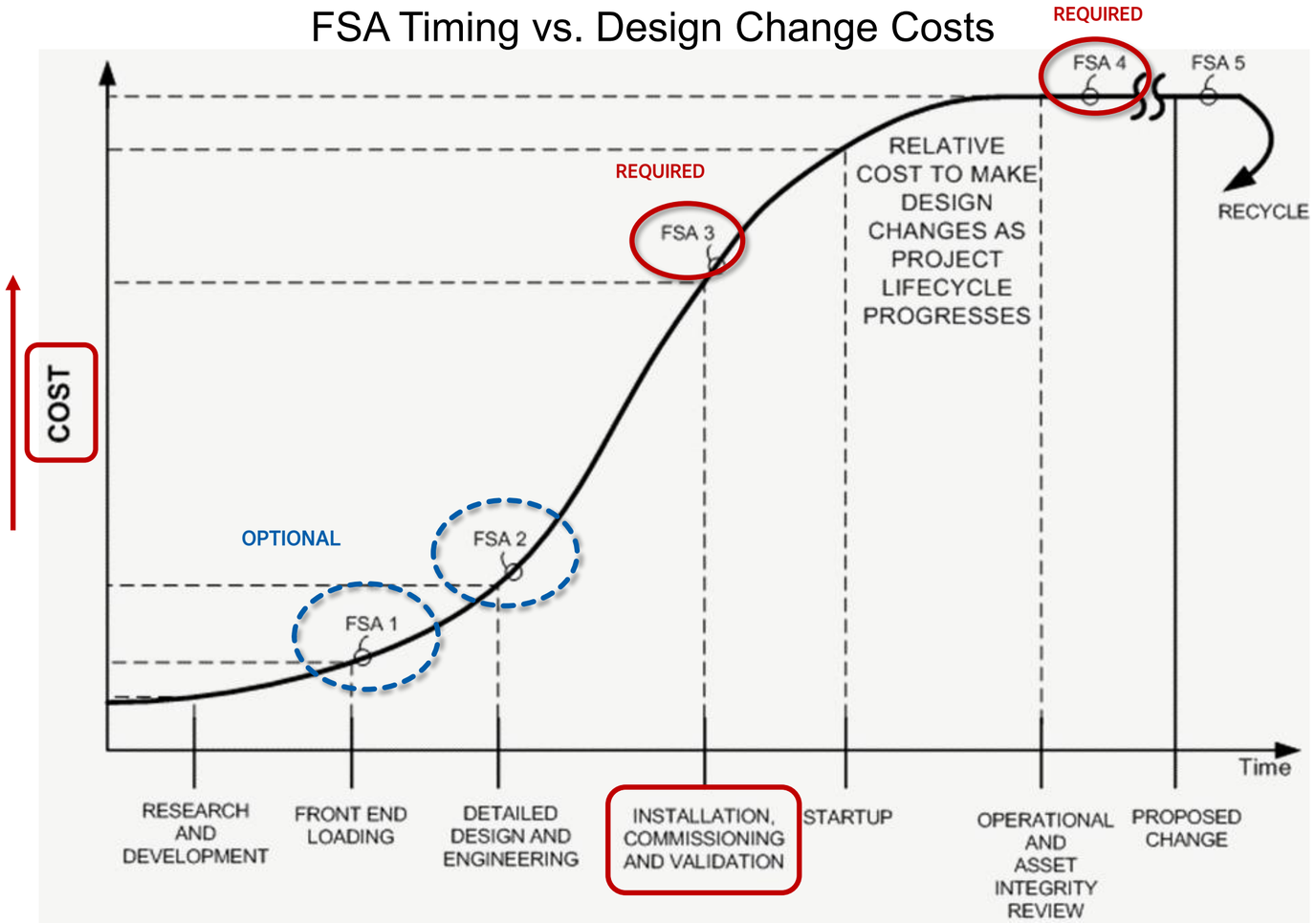
- Operations phase: Proof testing & maintenance compete with production schedules
- Staffing: FSA requires specialists; most plants lack functional safety expertise

  Competency: Shall use Certified Functional Safety Engineers (ISA, TUV, exida, are most common – refer to AcuTech Training Institute for TUV FS Engineer training and certification)

  Independence: FSA Team independence is required based on SIL and process complexity. Outsourcing FSAs is usually best practice, but may also be required at times

Solution: Budget FSA as a capital project cost, not an afterthought

IEC 61511 Functional Safety Assessments



Source: ISA-TR84.00.04-2020

IEC 61511 FSA and Cyber Requirements

ANSI/ISA-61511-1:2018 Clause 5.2.6.1.2 requires at least one senior, competent, independent (from the work being assessed) person to take part in the FSA.

ANSI/ISA-61511-1:2018 Clause 8.2.4 A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS.

Source: ANSI/ISA-61511-1:2018

Integrating FSA into Project & Operations Schedules

Project Phase Strategy:

- Front-load FSA with PHA/LOPA (start HAZOP, not end)
- Allocate 6–12 weeks design review + SIL verification (number of weeks depends on the number of SIFs, complexity, etc.

Operations Phase Strategy:

- Schedule proof tests during planned maintenance windows
- Establish SIS governance with MI—not separate activities

Key Questions for Your Teams

- ✓ For each SIF: Do you have a valid SRS tracing to PHA/LOPA?
- ✓ Can you demonstrate SIL was verified in design & commissioning?
- ✓ Do you follow documented proof test procedures and intervals per RAGAGEP?
- ✓ Does your MOC checklist explicitly address SIF impact?
- ✓ Does your MI team understand SIL implications of their work?

PSM Audit / SIS Assess Readiness: What Inspectors Are Looking For

- Documentation package: PHA → LOPA → SRS → Design → Test procedures and test records
- Traceability: Hazard scenario → SIL requirement → design elements
- SIL verification: Calculations, FMEA, i.e., design review evidence that SIF achieves Risk Reduction Factor (RRF), Hardware Fault Tolerance (HFT), and Systematic Capability (SC)
- Proof testing: Records show adherence to RAGAGEP intervals and procedures per manufacturer's safety manuals
- MOC governance: Examples of reviews referencing SIF impact

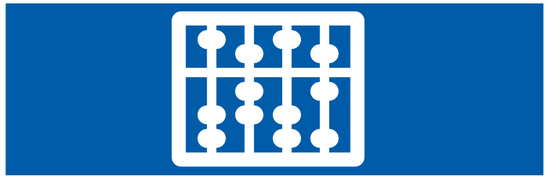
Common Integration Failures & Solutions

Gap 1: "LOPA done, but SRS doesn't match" → Single integrated team

Gap 2: "Never reviewed SIS contractor's design for SIL achievement" → Design review mandatory

Gap 3: "MOC never asks about SIS impact" → Updated checklist + PSM

Gap 4: "Proof tests missed 3 years" → SIS governance in MI budget



Implementation Roadmap: 90–180 Days

Phase 1

30 days

- Audit SIS portfolio—identify gaps + SRS deficiencies + FSA-identified open gaps

Phase 2

60 days

- Update MOC + MI procedures for functional safety + training

Phase 3

90 days

- Establish SIF lifecycle file governance + proof test calendar

Phase 4

120-180 days

- Design reviews + FSA-identified gaps closed + documentation completion

Key Takeaways

- Functional safety lifecycle provides validation that the PSM claimed risk reduction was achieved and its integrity has been maintained
- RAGAGEP requires IEC 61511 lifecycle discipline—not optional
- PHA → LOPA → SRS → Design → Verification creates coherent chain
- MOC & MI must explicitly own instrumented safeguards
- FSA must be budgeted, scheduled, and resourced—not deferred
- Lifecycle documentation + traceability = audit confidence + reduced risk

Another quick poll…

Let us know what you'd like covered in this series' next webinar.

Questions?

Submit questions using the Q&A box.

THANK YOU

Need a PDH certificate or want to follow up with us? Reach out at **contact@acutech-consulting.com**

AcuTech
PROCESS RISK MANAGEMENT

Upcoming Webinars

Beyond PSM Audits: Functional Safety Assessments that Expose Hidden SIS Risks

Tuesday, April 21, 2026

12:00pm EDT
11:00am CDT

https://meet.zoho.com/qydu-bxn-cde

From PSM to Performance: Your Functional Safety Deep Dive

Tuesday, May 12, 2026

12:00pm EDT
11:00am CDT

https://meet.zoho.com/jbey-szx-pmt

AcuTech

PROCESS RISK MANAGEMENT

HEADQUARTERS

1750 Tysons Blvd, Suite 200
McLean, VA 22102
USA

EMAIL ADDRESS

contact@acutech-consulting.com

WEBSITE

www.acutech-consulting.com