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

Tuesday, April 21, 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

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

Tuesday, April 21, 2026

12:00pm EDT
11:00am CDT

Upcoming Webinar

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.

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

Tuesday, April 21, 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, IEC61511 SFS 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. Mr. Souza is trained in SIL studies (SIL Assignment, Verification, SRS).

He is a Professional Engineer (PE), a Project Management Professional (PMP), and Certified Automation Professional (CAP). He is also an IEC61511 Safety Specialist and an IEC62443 Cybersecurity Specialist through the International Society of Automation (ISA).

Mr. Souza is the lead for SIL Verification projects at AcuTech. This includes using exSILentia® and other tools to ensure SIFs meet SIL Assignment targets (verified/ achieved with instrumentation design) and proof testing intervals. SIL Verification activities include developing Safety Requirement Specification (SRS) that details the functional and safety integrity requirements listed in the IEC 61511-2016 standard 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

- Why this matters to PSM managers
- What an FSA is – and is not
- Where FSAs fit in the lifecycle
- Misconceptions that keep sites exposed
- What hidden SIS risks FSAs expose
- Capital projects: why late FSA discovery is expensive
- What good looks like
- Takeaways to leave with

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

Why this Matters to PSM Managers

PSM programs often touch SISs across the board—yet still leave hidden lifecycle weaknesses untested.

What PSM managers already own

- PHA / LOPA decisions that assign risk reduction to safeguards and SIS functions
- MI, testing, and procedures that must keep credited protection real in the field
- MOC and training systems that can either preserve or erode lifecycle integrity
- Audit and governance expectations after incidents, near misses, or insurance scrutiny

What this webinar will clarify

- What a Functional Safety Assessment actually is—and what it is not
- Why a PSM audit and an FSA answer different questions
- What kinds of subtle SIS gaps FSAs expose at operating sites and projects
- How to recognize when a site likely needs an FSA gap assessment or SIS health check

Beyond the Audit: Different Questions, Different Blind Spots

A good PSM audit may confirm that systems exist. An FSA tests whether SIS risk reduction continues to work as assumed throughout the lifecycle.

A PSM audit often confirms...

- Required elements, procedures, and records are present
- PHA / revalidation cadence is being maintained
- MI, MOC, and training programs exist on paper and in governance
- Testing is being performed and deficiencies are being tracked

An FSA probes deeper for...

- Consistency between hazard basis, SIL assumptions, SRS, logic, and field implementation
- Evidence that proof testing, bypass management, and procedures support the claimed risk reduction
- Lifecycle drift caused by modifications, workarounds, documentation gaps, or weak ownership
- Whether the implemented SIS still matches the intent of the risk assessment

The hidden exposure

- “We thought that safeguard was still protecting us.”
- “We had a procedure, but it no longer matched the installed system.”
- “We tested something—but not what the SIL assumption relied on.”
- “We caught the gap only when a startup or an incident forced the issue.”

“What do you mean we are missing a SIF?”

What an FSA is—and is not

Keeping it simple: an FSA is a structured, independent checkpoint on whether SIS lifecycle work is adequate for the phase you are in.

What an FSA is

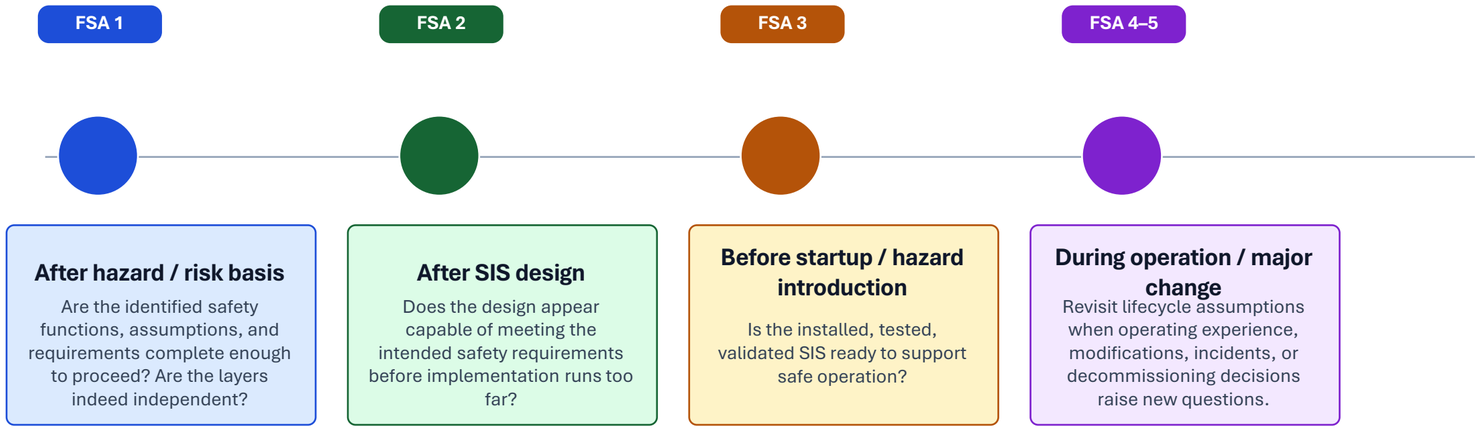
- An evidence-based assessment of lifecycle adequacy at a defined stage of that lifecycle
- A way to test alignment between the hazard basis, requirements, design, implementation, and operating reality
- A mechanism to surface latent gaps before they become startup delays, impairments, or incident findings
- A strong complement to PSM by translating risk-reduction assumptions into verifiable lifecycle evidence

What an FSA is not

- Not just a documentation tidy-up exercise
- Not the same as a general PSM audit or compliance walk-through
- Not only for greenfield projects
- Not too late to do simply because the unit has been operating for years

Where FSAs Fit in the Lifecycle

Focus on the first three stages for projects, then briefly connect later-lifecycle triggers for operating sites.



The most practical message is simple: the earlier the lifecycle checkpoint, the cheaper the correction.

Misconceptions that keep sites exposed

These are common reasons organizations postpone functional safety work—often due to budgetary and schedule constraints — until an event forces it. (e.g., owner operator requirements, insurance company requirements, or a near miss investigation)

Myth	Better framing
“We already do PSM audits, so we are covered.”	Audits and FSAs are complementary; they test different failure modes.
“It is too late to do an FSA now.” or “I’d rather not know.” *(Yikes!)*	Late is still better than blind. Operating sites often gain the most by finding lifecycle drift.
“FSAs are only for new projects.”	Projects need staged assessments, but brownfield units also need lifecycle reality checks.
“This is an engineering detail, not a PSM management issue.”	SIS risk lives inside PHA, LOPA, MI, MOC, procedures, impairment control, and incident defensibility. *(Imagine your day in court)*

What Hidden SIS Risks FSAs Expose at Operating Sites

Most meaningful findings are not dramatic single failures; they are layered weaknesses that slowly erode claimed risk reduction.

(Think onion layer and Swiss cheese model; and learn the differences between Random and Systematic Failures)

Basis risk

- Trip setpoints, cause/consequence logic, or operator actions no longer reflect the current hazard basis
- LOPA credits remain in spreadsheets, but traceability to the installed SIS is weak

Integrity risk

- Proof-test assumptions, diagnostic assumptions, or failure-rate assumptions are not supported by field practice
- Bypasses, impairments, or partial tests are accepted without strong visibility *(Think of a skipped FAT or SAT)*

Change risk

- Brownfield modifications quietly alter independence, voting, procedures, or final element behavior *(Do we go back and retroactively generate missed MOCs or PSSRs?)*
- SIS documentation drifts after turnarounds and incremental changes

Capability risk

- Roles, competency, procedures, and alarm/operator interfaces are not aligned with the intended protection strategy
- The organization cannot quickly demonstrate why the current SIS should still be trusted *(Are you familiar enough or have enough trust in your SIS to defend its compliance to RAGAGEP in an audit?)*

Representative Operating-Site Findings

Here are a few examples we've encountered; these are not scare tactics. Can you relate to any of these situations?

1. A credited SIF could not be cleanly traced from LOPA assumption to current field implementation and testing evidence.
2. The proof-test interval used in SIL verification did not match the interval actually sustained in the maintenance program.
3. Partial-stroke or diagnostic coverage was assumed in calculations, but execution and documentation were inconsistent in practice.
4. Logic changes were made during turnaround work, yet the SRS, cause-and-effect matrix, and procedures were not fully reconciled.
5. Bypass procedures existed, but prolonged impairments lacked strong escalation, visibility, or management review.
6. Operator actions credited in the risk basis were not fully supported by alarm presentation, timing, or procedure detail.

Mini Case Pattern: “We thought it was too late.”

A common brownfield reality: the unit has run for years, small changes accumulated, and nobody is confident that a staged FSA history really exists.

What the site looked like

- Legacy unit with credited SIS protection from prior PHAs / LOPAs
- Multiple incremental changes through turnarounds and operations
- Testing was happening, but assumptions and evidence were fragmented
- No one wanted to ask the question because “if we never did the FSAs, maybe it is too late now.”

What the assessment uncovered

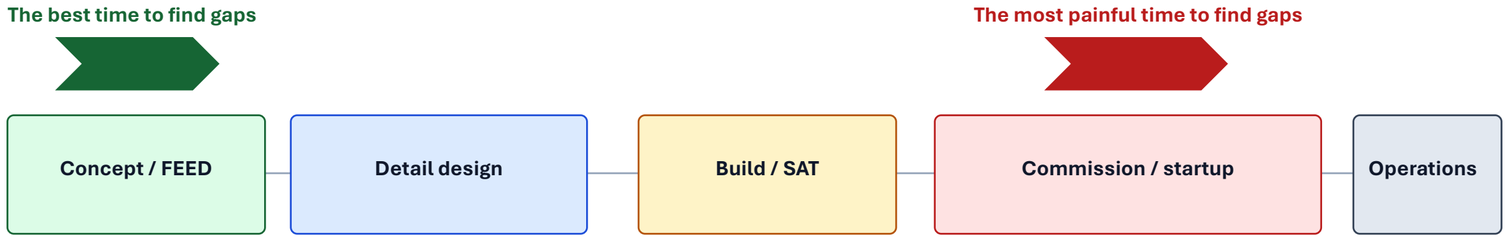
- Traceability breaks between hazard basis, SRS content, logic, and maintenance evidence
- Testing practices that did not fully support the credited integrity assumptions
- Procedural and bypass-management weaknesses that were tolerated as routine
- A few high-priority remediation items that mattered far more than the many cosmetic gaps

Why it mattered

- The late assessment did not create the risk—it revealed it.
- The site gained a prioritized path forward instead of continuing blind.
- Management could finally distinguish urgent gaps from cleanup work.

Capital Projects: Why is late FSA discovery expensive?

Project teams rarely regret doing lifecycle checks too early. They often regret discovering missing evidence only when startup pressure is highest.



Early lifecycle benefit

- Requirements and design gaps are cheaper to fix before procurement and implementation harden.

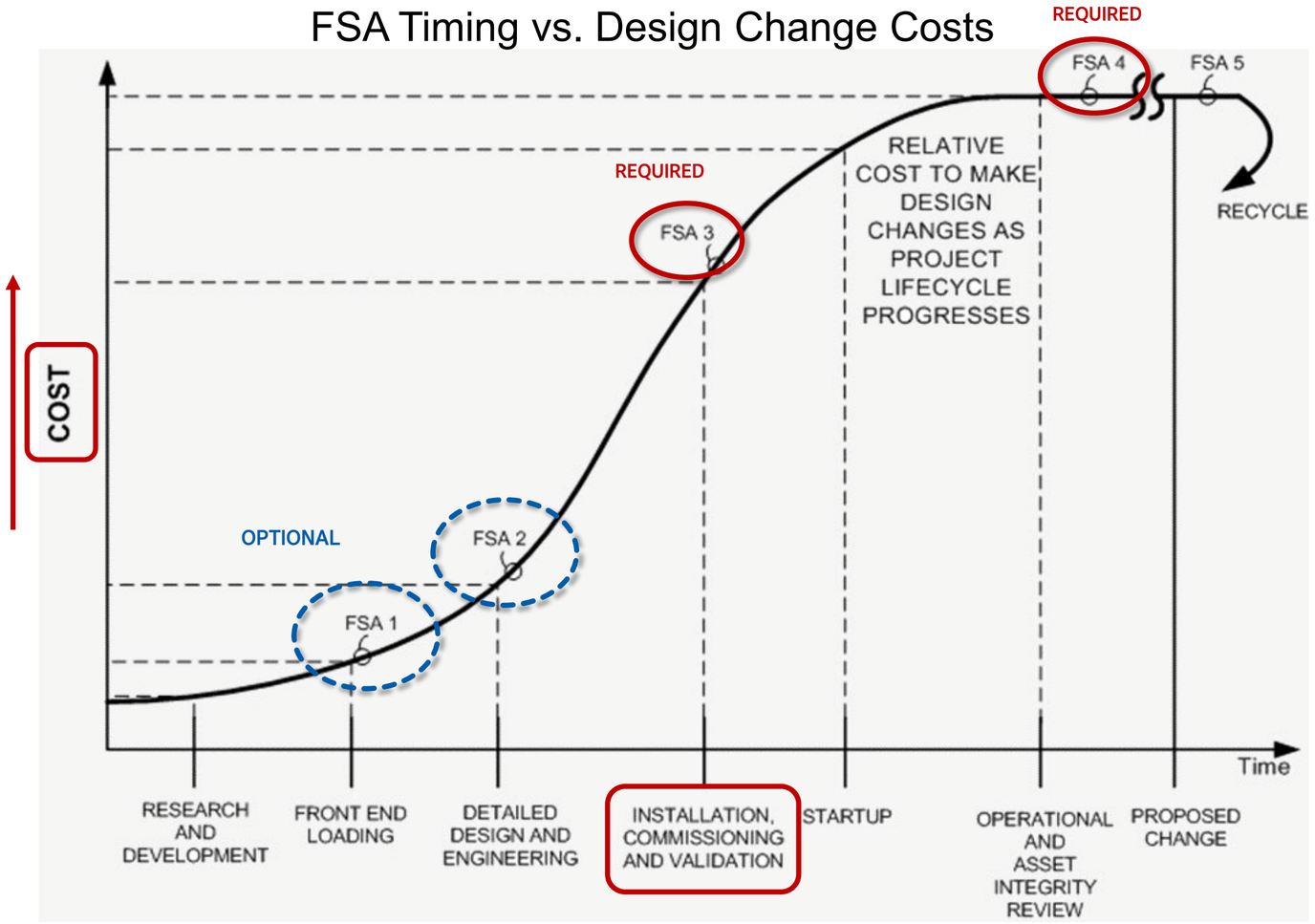
Late lifecycle pain

- Missing evidence forces rework of SRS, logic, procedures, test plans, and closure packages under schedule pressure.

Commercial consequence

- Unbudgeted remediation, startup delay, strained owner-contractor relationships, and a weaker defensible position.

IEC 61511 Functional Safety Assessments



Source: ISA-TR84.00.04-2020

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

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

FSA Team Independence 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.

(*) Common Question: Can I Use Internal Resources?
In larger companies, internal teams may be utilized if the assessor is independent from the project or facility.
This means that the assessor should not report to the same chain of command, be employed at that facility, or be part of the project team.
Additionally, the project's size and complexity should also permit the use of internal resources. Large or complex projects often require external consultants.

Source: ANSI/ISA-61511-1:2018

Mini Case Pattern: The startup scramble nobody budgeted for

This pattern is familiar: SIS hardware and SAT are planned, but staged FSA effort, closure time, and evidence readiness are not.

What was planned

- Design package, procurement, SAT, and commissioning activities
- Risk studies and SIL work completed earlier in the project
- A belief that startup readiness would mostly be a documentation exercise

What surfaced late

- Requirements gaps and inconsistencies between narratives, cause-and-effect, and logic
- Procedures and proof-test packages not ready to support lifecycle claims
- Open items that should have been discovered earlier in design, not at the edge of startup

Lesson for PSM leaders

- Budget staged FSAs and closure effort from the start
- Demand evidence readiness—not just hardware readiness
- The cheapest corrective action is the one caught before installation or before startup pressure takes over

Self-Diagnostic: Does your site likely need a gap assessment?

If several of these sound familiar, there is a strong case for a targeted FSA gap assessment or SIS health check.

Common red flags

- No clear history of staged FSAs, or uncertainty about what was actually assessed
- SIF / SIL assumptions are hard to trace to current design, logic, and test evidence
- SRS documentation is incomplete, outdated, or inconsistent across documents
- Proof-test intervals, coverage, or impairment practices do not clearly align with credited assumptions
- Frequent bypasses, overrides, or nuisance trips have become normalized

More red flags

- MOCs rarely receive a deep SIS-specific impact review
- Operator actions credited in the risk basis are weakly supported by procedures, alarms, or timing
- Cause-and-effect, narratives, graphics, and procedures do not fully agree
- Major brownfield changes, turnarounds, or expansions have occurred since the last serious lifecycle review
- Leadership would struggle to defend today why the SIS should still be trusted as assumed

Rule of thumb: if 3 or more are true, start with a scoped FSA gap assessment or SIS health check—not a massive all-at-once program.

What Good Looks Like: Integrating FSA Thinking into PSM

The strongest programs do not treat SIS lifecycle work as a separate island. They connect it to existing PSM ownership points.

PHA / LOPA	MI / testing	MOC	Procedures & training	Governance
Risk basis, credited safeguards, and assumptions stay traceable and current.	Proof tests, impairment controls, and deficiency resolution support what the risk basis claims.	Changes explicitly assess SIS impacts on requirements, independence, testing, and procedures.	Operator response, bypass handling, and maintenance tasks match the actual protection strategy.	Audits, metrics, and leadership reviews can distinguish cosmetic gaps from genuine risk erosion.

Bottom line: PSM manages the program; FSA assesses whether SIS risk reduction remains real, current, and defensible.

What to do Next: A Practical Starting Point

Keep the first step right-sized. The objective is to surface real risk and prioritize—not to create a huge program overnight.

For operating sites

- Identify where SIS risk reduction is being actively credited in current PHAs / LOPAs
- Gather the basis documents: key risk studies, SRS content, cause-and-effect, logic narratives, test intervals, and impairment practices
- Use a red-flag screen to scope a focused FSA gap assessment or SIS health check
- Prioritize the small set of findings that actually change risk or defensibility

For projects / new installations

- Place stage-appropriate FSA checkpoints into the project schedule—not just at the edge of startup
- Budget time for closure of findings, not merely the assessment meeting itself
- Define evidence expectations early: requirements, design basis, validation, procedures, and readiness records
- Treat lifecycle readiness as a startup prerequisite, not a late paperwork exercise

Questions PSM Managers often Ask:

- How is a gap assessment different from a formal staged FSA?
- Can we do this unit-by-unit rather than site-wide?
- What documents do we need to start?
- How disruptive is this for operations and maintenance?
- What are the fastest “high-value” checks for an operating site?

Questions PSM Managers often Ask:

- How is a gap assessment different from a formal staged FSA?
- Can we do this unit-by-unit rather than site-wide?
- What documents do we need to start?
- How disruptive is this for operations and maintenance?
- What are the fastest “high-value” checks for an operating site?

What documents do we need?

This is a practical list, not a perfect-world list.

Usually enough to start

- Recent PHA / LOPA or other risk-basis material
- Any SRS content, narratives, cause-and-effect, logic, and setpoint basis
- Testing intervals, procedures, and impairment practices
- Relevant MOC history and known problem areas

Helpful but not always available

- Validation records and lifecycle closure packages
- Prior FSA reports or internal review records
- Failure history, bypass data, and proof-test observations
- Vendor / integrator design detail

Key message

- Do not delay because the document set is imperfect.
- An assessment often helps reveal what is missing and what matters most first.

How disruptive is this for operations and maintenance?

When properly done by an experienced team, it shouldn’t be.

What a scoped gap assessment usually targets

- Traceability from hazard basis to implemented SIS
- SRS adequacy and lifecycle documentation quality
- Testing, impairment control, and procedure alignment
- Prioritized findings with practical remediation steps

What it usually does not try to do on day one

- Rebuild the entire SIS program from scratch
- Review every instrumented loop on the site at once
- Create months of disruption for operations
- Replace the need for ongoing PSM ownership

Three takeaways to leave with:

Let’s end on clarity and confidence.

1. Audits and FSAs are complementary

- A strong PSM audit does not automatically prove SIS lifecycle adequacy.
- FSAs expose hidden gaps in assumptions, traceability, implementation, and sustainment.

2. It is not too late

- Operating facilities gain value from late-stage assessments because they surface lifecycle drift and help prioritize remediation.
- The assessment reveals the risk; it does not create it.

3. Timing matters

- For projects, the cheapest finding is the one caught before startup pressure.
- For sites, the most valuable finding is the one that restores confidence in credited protection.

AcuTech supports owner/operators with focused FSA gap assessments, SIS health checks, and lifecycle improvement work.

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

AcuTech
PROCESS RISK MANAGEMENT

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

Upcoming Webinar

From PSM to Performance: Your Functional Safety Deep Dive

Tuesday, May 12, 2026

12:00pm EDT
11:00am CDT

https://meet.zoho.com/iwok -ioc -kmo

Webinar 1 Recording Now Available

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

www.youtube.com/@acutechconsultinggroup

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

Appendix: Visual Aid Slides

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

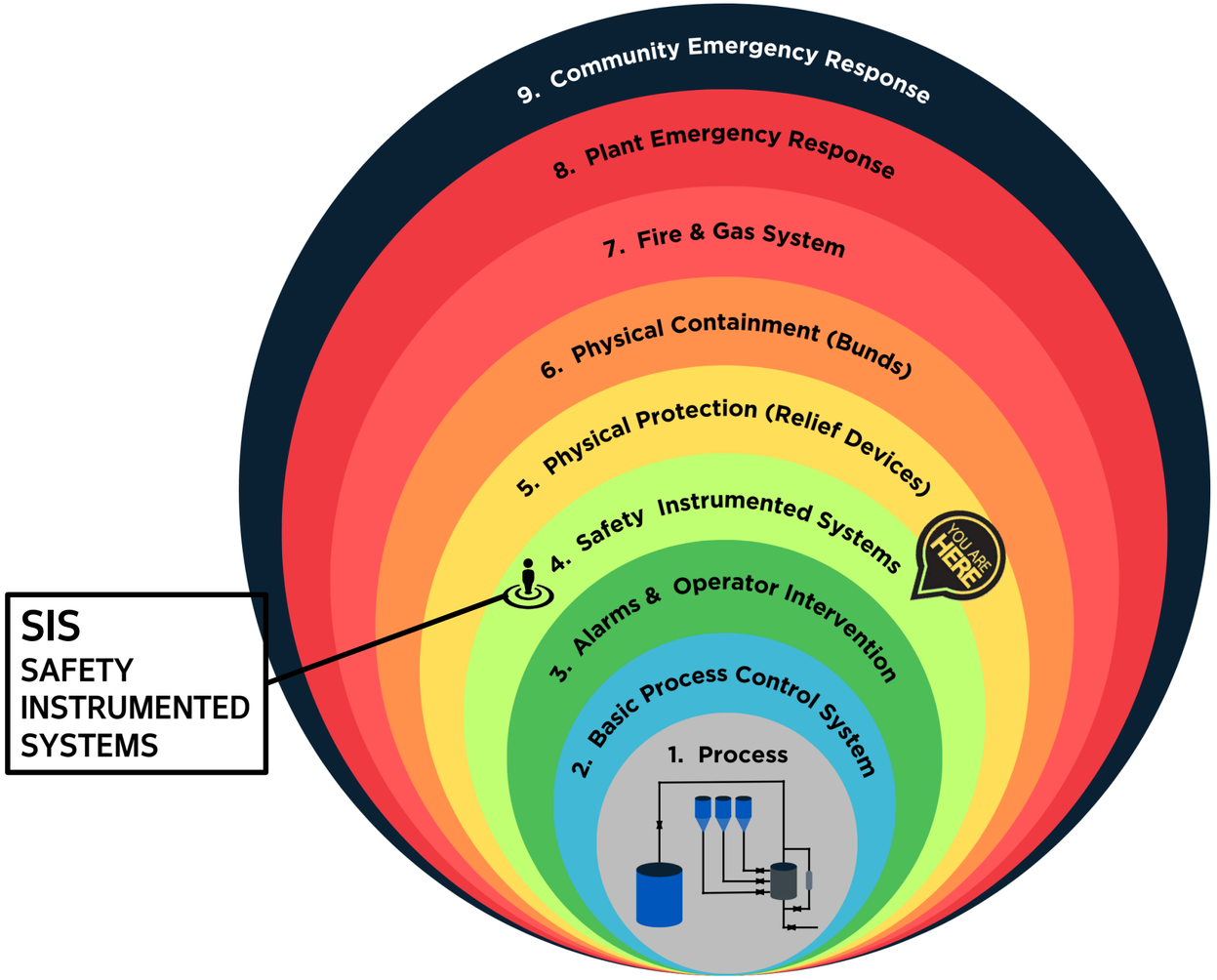
4 **Installation & Commissioning**

- As-built tested per procedures

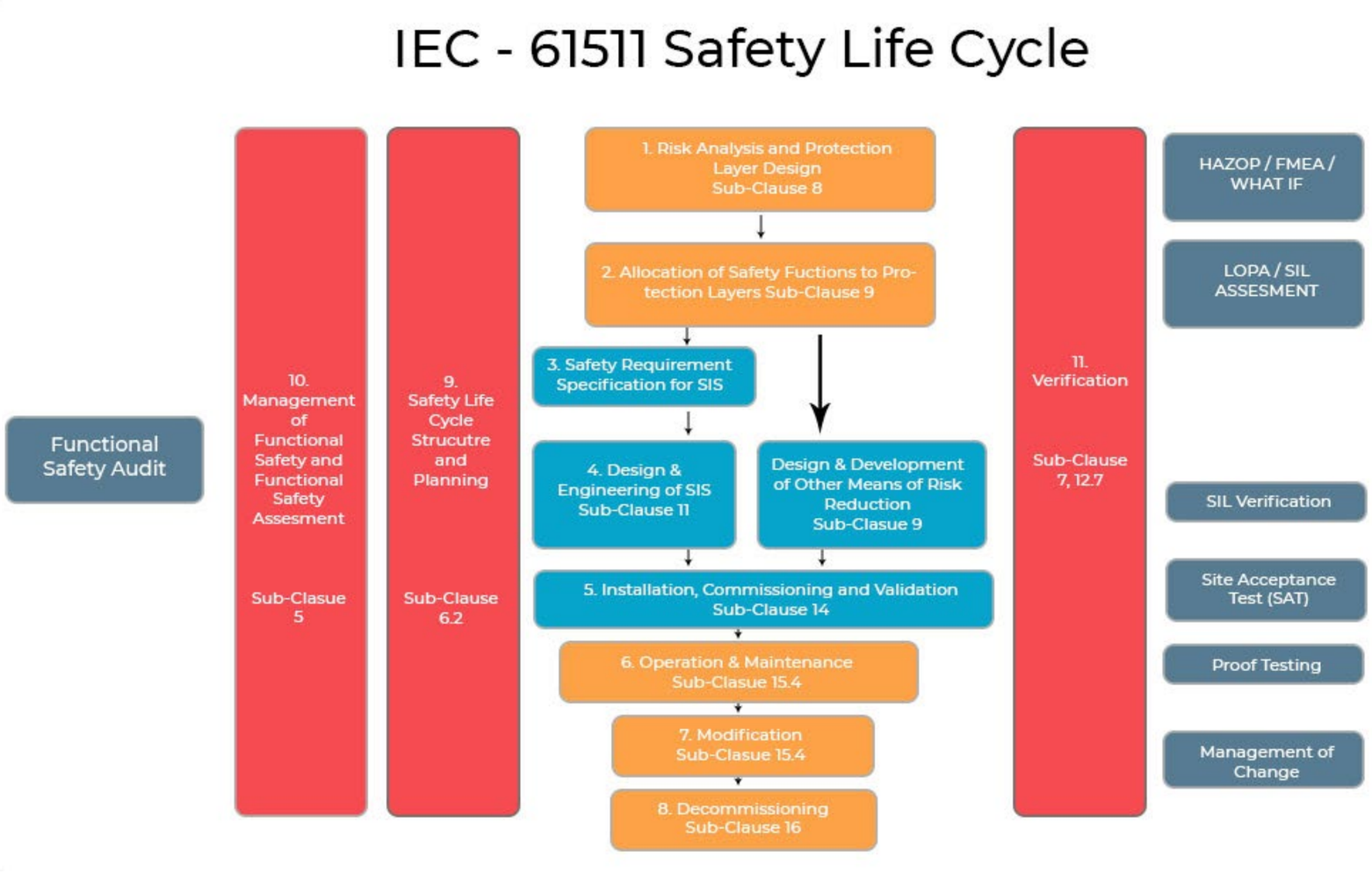
5 **Operational Verification**

- Proof testing & maintenance

Process Safety Onion Diagram



IEC 61511 Functional Safety Lifecycle



Source: NIST Global Pvt. Ltd.