PHA/LOPA to SIL: Translating Risk Analysis into SIL Selection & Verification

Tuesday, May 12, 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).

Today’s Agenda

- How This Completes the Series
- The Biggest Misconception
- What Each Step is Really Doing
- The Correct Chain of Logic
- When LOPA Should Lead to a SIF, and When It Doesn’t
- Where Programs Commonly Get Misaligned
- Why This Matters to PSM Leaders
- What SIL Verification Does and Does Not Prove
- Red Flags for PSM Managers
- What PSM Leaders Should Ask For
- Key Takeaways

How This Completes the Series

The third webinar moves upstream to where many FSA findings begin.

1. Functional safety belongs inside PSM
2. FSAs reveal hidden SIS risks
3. Risk analysis must connect to SIL selection and verification

Many lifecycle gaps are symptoms. The upstream cause is often a weak or poorly traced risk basis.

The Biggest Misconception

Risk Ranking ≠ **SIL**

Risk ranking
Screens and prioritizes scenario risk based on severity and likelihood.

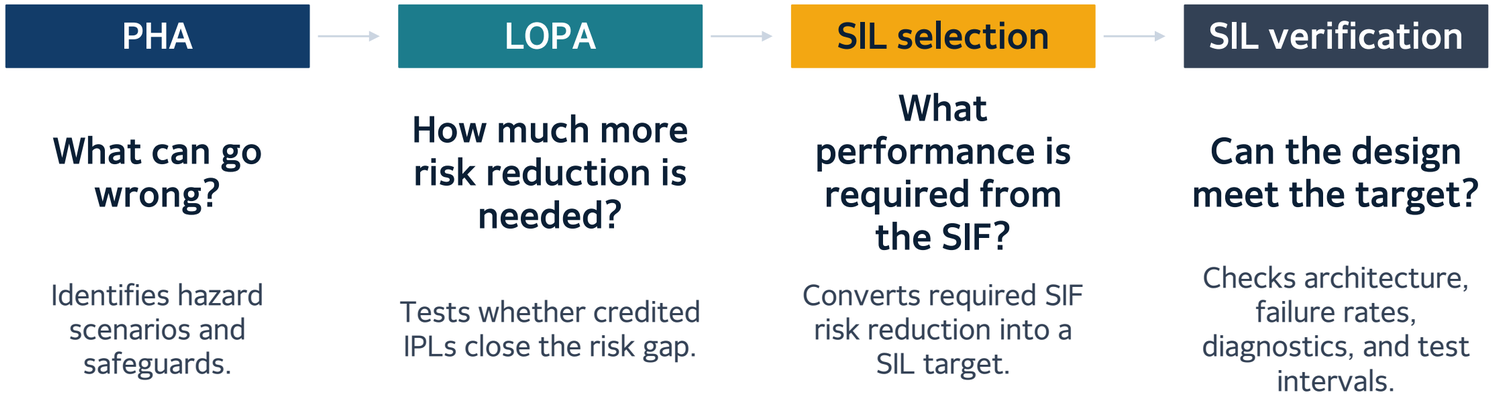
SIL target
Represents the performance needed from a SIF to achieve required risk reduction.

A high PHA risk ranking does not automatically mean a high SIL.

The missing question is not “What risk box are we in?”
It is “What risk reduction is still needed after credible protection layers?”

What Each Step is Really Doing

Each activity answers a different question, and confusion begins when those questions blur.



Good functional safety management preserves the logic across all four steps.

The Correct Chain of Logic

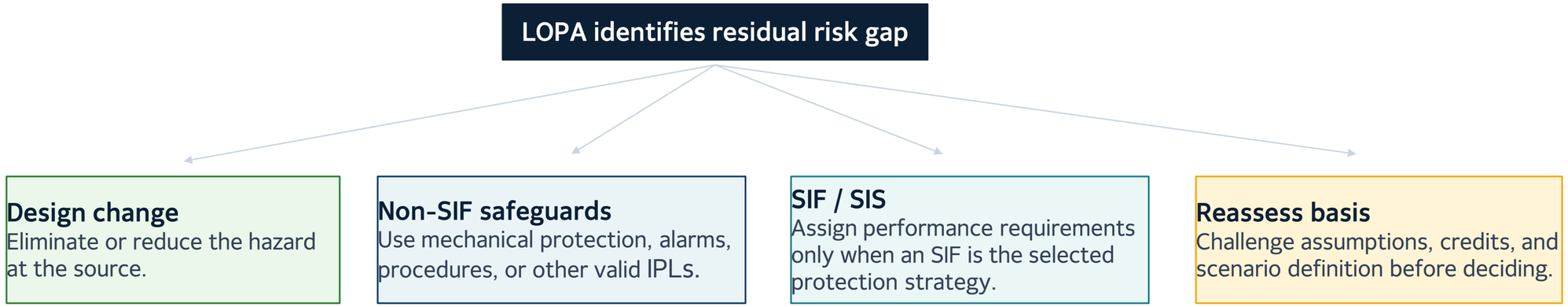
The goal is traceability from the hazard scenario to the field performance expectation.

If you cannot trace the reasoning, the SIL may look valid on paper but be weakly supported.

Alignment is not matching labels — it is preserving the basis for risk reduction.

When LOPA Should Lead to a SIF — and When It Should Not

A SIF is one possible risk-reduction response, not the default answer for every gap.



Management takeaway: The quality of SIL selection depends on the quality of the protection strategy decision.

Where Programs Commonly Get Misaligned

Many gaps are not due to calculation errors; they are due to decision-quality errors.

Matrix severity drives SIL
SIL chosen from consequence alone, not required risk reduction.

Optimistic IPL crediting
Credits assumed without independence, reliability, auditability, or field evidence.

Vague SRS linkage
SIF requirements do not clearly trace back to the scenario.

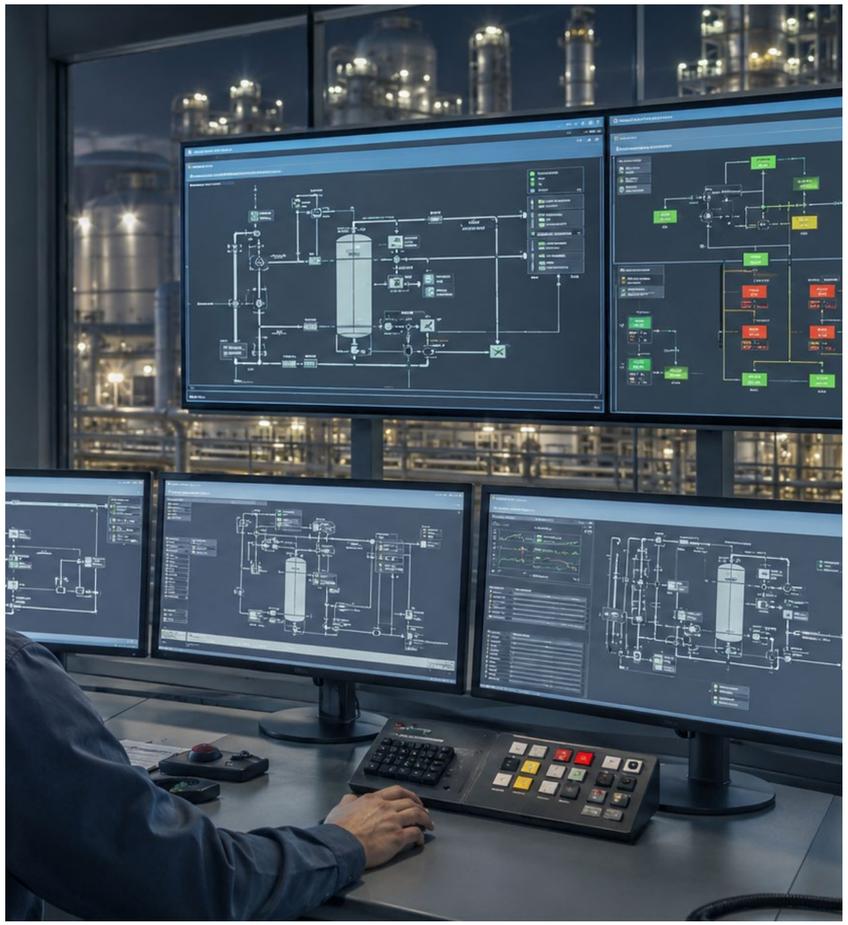
Box-check verification
The calculation passes, but the underlying assumptions no longer reflect reality.

Verification cannot rescue a weak risk basis.

Why This Matters to PSM Leaders

This is not just an engineering detail; it affects the integrity of the PSM program.

- PHA / LOPA basis
- MOC triggers
- MI / proof testing
- Audit defensibility
- Operating discipline



PSM leaders do not need to run the calculation. They need to govern the process that makes it defensible.

Mini Case: When the SIL Was Right — But the Basis Was Weak

A technically passing verification can still rest on assumptions that are not defensible.

1	**Scenario**	High-pressure event with severe consequences identified in PHA.
2	**Decision**	LOPA assigns credits and selects SIL 2 SIF.
3	**Review**	Verification passes, but assumptions on IPL credit and initiating event rate are weak.

Lesson: The problem was not only the SIL. It was the weak chain of reasoning.

What SIL Verification Does — and Does Not — Prove

Verification DOES confirm
The calculated SIF design can meet the target SIL based on the stated architecture, failure data, diagnostic coverage, proof-test interval, and assumptions.

Verification DOES NOT confirm
The original scenario basis was correct, IPL credits were valid, the SRS was complete, field testing matches the assumptions, or MOC triggers are being managed.

A correct calculation can still be attached to a weak basis.

Red Flags for PSM Managers

If several of these are true, your PHA/LOPA-to-SIL chain may need to be reviewed.

- ! SILs assigned without clear scenario traceability
- ! Verification is performed late or after design freeze
- ! LOPA assumptions vary by unit, facilitator, or project
- ! MOC does not trigger review of SIL basis or IPL assumptions
- ! SRS does not clearly link to the analyzed hazard scenario
- ! Proof test intervals in verification do not match MI reality

The issue is not whether paperwork exists. The question is whether the logic still holds.

What PSM Leaders Should Ask For

Questions that improve consistency, traceability, and defensibility.

1. Can we trace each SIF back to a specific analyzed scenario?
2. Are IPL credits consistent, independent, reliable, and auditable?
3. Does the SRS state the action, response time, process limits, and proof test assumptions?
4. Does verification use assumptions that reflect real field conditions?
5. Do MOC and MI programs trigger review when assumptions change?

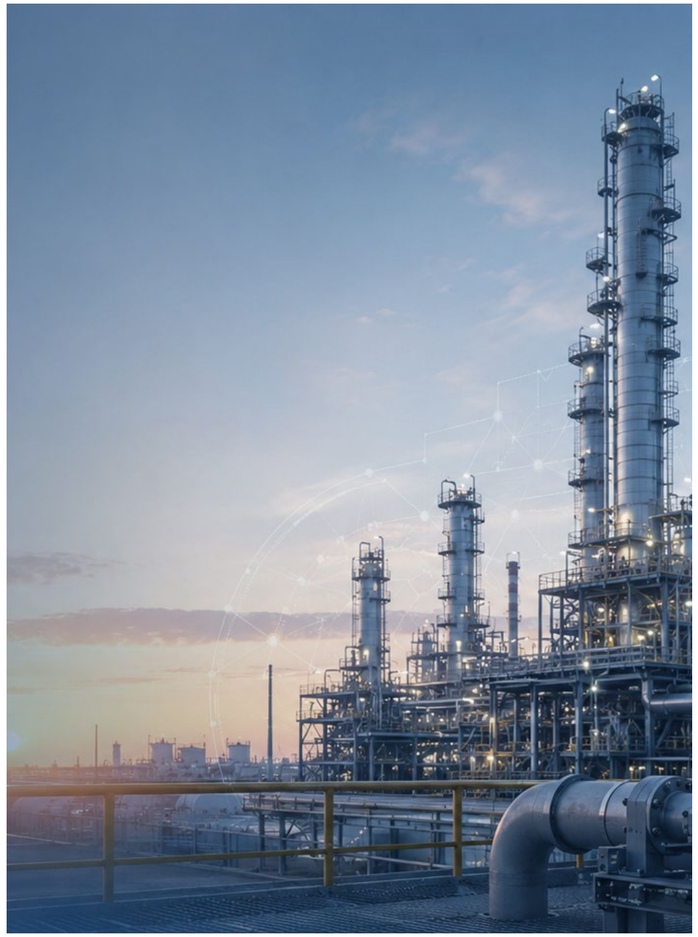
If these questions are hard to answer, the program may be carrying hidden SIS risk.

Key Takeaways

Aligned programs make better, more defensible risk decisions.

1. SIL is not a direct translation of a risk ranking.
2. PHA/LOPA should establish a traceable risk basis.
3. Verification confirms performance only against stated assumptions.
4. PSM leaders govern the integrity of the decision chain.

Better alignment helps avoid overdesign, underdesign, and false confidence.



Questions?

Submit questions using the Q&A box.

THANK YOU

Webinar Recordings Now Available

www.youtube.com/@acutechconsultinggroup

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

AcuTech
PROCESS RISK MANAGEMENT

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