x2026 · Toronto · CSC | CSChE

Closing the Loop

From LOPA to Proof Test — and Back Again

Process Safety Management Division · CSChE

Carsten Acker, P.L.(Eng.), CFSE, CSP

Principal | Director of Operations, Watchmen Industrial Safety Experts

May 2026

Watchmen
INDUSTRIAL SAFETY EXPERTS

WATCHMEN OVERVIEW

- PHA — HAZOP, LOPA, What-If, HAZID and CHAZOP facilitation.
- SIS / SIL Consulting — SIL verification, SRS, proof test procedures, FSAs and full lifecycle support per IEC 61511 / 61508.
- Fire & Gas Engineering — philosophy development, 2D/3D detector mapping and coverage assessment per ISA TR84.00.07.
- Alarm Management — philosophy, rationalization and bad-actor resolution per ISA 18.2 / EEMUA 191.
- Process safety training
- PHA FieldSync (3D walk-throughs and drone-supported field verification).
- Vendor-neutral by design. We don't sell logic solvers, PSVs or DCS platforms — we tell you where your facility can be improved.

Calgary-based. Serving Canadian and international operators in oil & gas, petrochemical, power generation, specialty gases and renewables.

Watchmen
INDUSTRIAL SAFETY EXPERTS

WATCHMEN PRESENTER

CARSTEN ACKER

P.L.(Eng.) · CFSE

Principal & Director of Operations

Watchmen Industrial Safety Experts

20+ years across the safety lifecycle — from the plant floor to the SIL verification.

Watchmen
INDUSTRIAL SAFETY EXPERTS

PROFILE

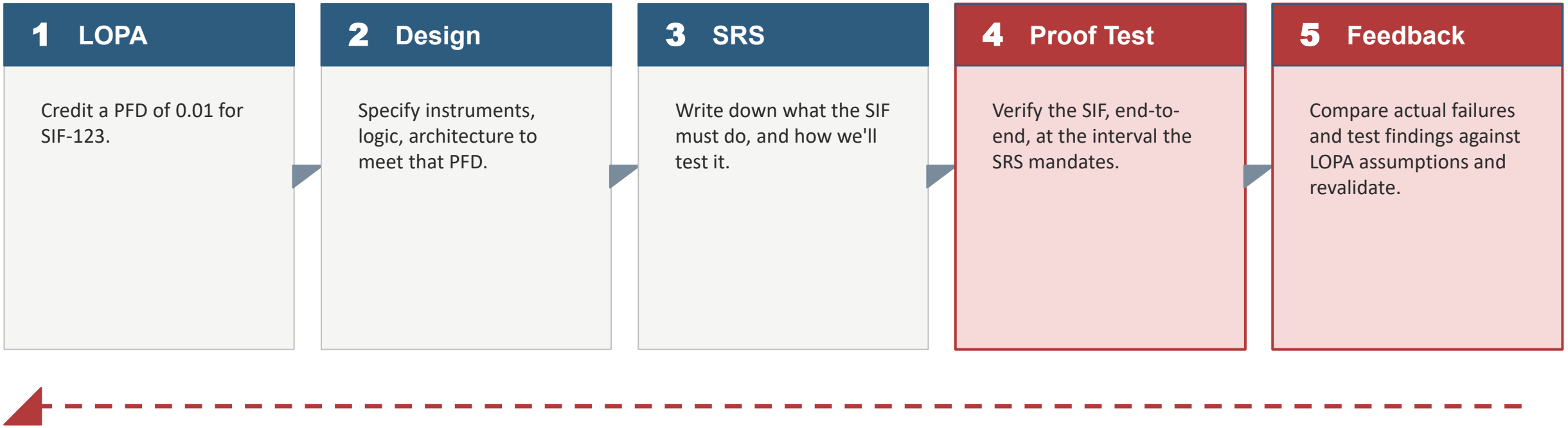
Process & Functional Safety Engineering

CORE PRACTICE

- HAZOP / LOPA facilitation
- SIS lifecycle — SIL determination, verification, SRS, proof test procedures, FSAs (IEC 61511 / 61508)
- Alarm rationalization & lifecycle (ISA 18.2 / EEMUA 191)

THE LIFECYCLE NO ONE FINISHES

LOPA credits a risk reduction. Something out in the field is supposed to deliver it. Between those two moments sits a loop that — in most plants — is never actually closed.



Steps 1 through 3 are expected. Steps 4 and 5 are where most programs go quiet.

Watchmen
INDUSTRIAL SAFETY EXPERTS

WHERE THE LOOP BREAKS

Five places we consistently find the loop broken, in roughly the order you hit them:

1	**PFDs assumed, never verified**	The LOPA team picks a PFD from a table. Nobody ever goes back to check whether the installed equipment — sensors, logic, final elements — actually delivers it.
2	**Proof tests that don't prove much**	Written to tick a box. Limited end-to-end coverage. Dangerous-undetected failures stay undetected.
3	**Repair-and-retest until it passes**	A SIF fails its proof test. The maintainer greases the valve, retests, gets a pass, and closes the work order. The failure data is gone. So is the LOPA's basis.
4	**Modifiers and IEFs go stale**	Initiating event frequencies and LOPA modifiers — occupancy, ignition, enabling conditions — are set once and rarely revisited. They drift with the plant, often upward.
5	**MOC blindness to LOPA**	A process change touches an initiating-event frequency or an IPL assumption. MOC closes. LOPA never reopens.

BREAK #1 — THE ASSUMED PFD

Where it bites hardest: complex architectures

- Simple loops are forgiving. A 1oo1 sensor / 1oo1 valve hides its sins openly — and field data eventually shows them.
- Complex basic protection layers are where the assumed PFD goes invisible. 3oo3 final elements, sensor pairs on a shared process connection. The assumed RRF is 10 while the actual installation often warrants less. This can result in a large difference of initial event frequency for the SIF when using BPCS protection layers that are not as reliable as initially assumed. In this case an RRF of 200 should actually be 526.

Architecture	PFD assumed	PFD as-built (real)	Effective change
1oo1 sensor + 1oo1 final element (typical assumption)	1.0E-1	~1.1E-1 (reduced PTC)	**~10% performance drop vs. expected**
2oo2 sensor + 3oo3 final element (medium complexity loop)	1.0E-1	**~2.67E-1 (impact of voting architecture)**	**~62% performance drop vs. expected**

A PFD that assumes a simple and independent application is often just fiction.

Watchmen
INDUSTRIAL SAFETY EXPERTS

BREAK #2 — TESTS THAT DON'T TEST

WRITTEN TO PASS

- "Stroke the valve from the DCS graphic."
- "Confirm the solenoid de-energizes and watch the HMI for proof."
- "Pump up the transmitter and apply a lamacoid tag."
- No end-to-end trip. No process-side verification.

TESTS THAT BITE

- Reference the paperwork from the last proof test — trend the as-found data, not just the pass/fail.
- Start at the sensor. Induce a real process-side upset or use a documented simulation.
- Measure the valve's closure time and look for seat leakage.
- Record the as-found state before you touch anything. That's your failure data.
- Close out against the SRS and proof test procedure.

If a proof test can't fail, it isn't a proof test. It's a function check.

Watchmen
INDUSTRIAL SAFETY EXPERTS

BREAK #3 — REPAIR AND RETEST

A SIF fails its proof test. What happens next — and what should happen — are very different things.

WHAT USUALLY HAPPENS

- Test reveals a sticky valve, slow trip, or sensor out of spec.
- Maintainer greases the actuator, cycles it, retests. Passes the second time.
- Work order closes as "completed — proof test passed."
- As-found state never captured. No failure record. PM Program reports 100% test pass rate.
- The only evidence the LOPA's PFD assumption is wrong — is gone.

WHAT SHOULD HAPPEN

- Record the as-found state BEFORE any intervention and testing.
- Log the failure against the SRS requirement. "Failed criteria 3.2.1" — not "sticky valve."
- Classify: dangerous-detected, dangerous-undetected, safe-detected, safe-undetected.
- Repair, then RE-PROOF-TEST. The pass-after-repair is a different data point from the original failure.
- Re-proof test after a short period of time to validate the repairs will lead to long lasting results, not just a band-aid
- Feed the failure data back to the LOPA or SIS design team.

When a SIF fails its proof test, the as-found state IS the data. Lose it, and you've erased the LOPA's basis along with the failure.

Watchmen
INDUSTRIAL SAFETY EXPERTS

BREAK #4 — MODIFIERS & IEFs GO STALE

LOPA's RRF math is only as good as the IEF and the modifiers underneath it. Both drift with the plant — usually upward, usually unseen.

- Initiating Event Frequencies (IEF) — pump trip, control loop failure, operator error — are typically set once at LOPA, citing generic data tables.
- After a few years, your facility has its OWN data: trip counts in the historian, near-miss logs, abnormal-shutdown trend. Almost no one feeds it back.
- Modifiers — Time at Risk, Occupancy, Ignition, Enabling Condition — are even more invisible. "Occupancy 0.1" set in 2018 when the unit was unmanned. Now there's a permanent operator round through it twice a shift.
- Most LOPA revalidations don't recheck IEFs at all — they accept the original frequency and rework the IPLs. Wrong direction.

If your IEF drifted from

1E-1

to

2E-1 / yr

your required RRF doubles. Your installed IPLs didn't.

An IEF set in 2015 is a hypothesis about 2015. Validate it against your own data, every revalidation.

Watchmen
INDUSTRIAL SAFETY EXPERTS

BREAK #5 — MOC DOESN'T READ LOPA

LOPA makes quiet assumptions. A change that breaks one is often a change no one thought required a LOPA revisit.

Change on the plant floor	LOPA assumption it invalidates
Operating mode shifts from batching to consistent production	*TAR assumption invalid; demand rate changes*
Feed change pushes the unit into more severe service (more H_2S, temperature, pressure)	*IEF for loss-of-containment rises*
A valve swap upstream changes the trip response time	*SIF response window assumption violated*
PSV inspection interval pushed from 1 to 5 years	*IPL PFD drifts quietly upward*
Operator staffing reduced on night shift	*Operator-action IPL becomes untenable*

An MOC checklist that asks "does this affect the SIS?" doesn't catch any of these.

Watchmen
INDUSTRIAL SAFETY EXPERTS

THE FEEDBACK PROBLEM

Even when individual breaks are spotted, the information almost never makes it back to the LOPA.

Proof test records

Sit in the preventative maintenance program. Pass/fail. Rarely analyzed as failure data.

→ *LOPA*

Override logs

Live in the DCS historian. Read once a quarter, if that.

→ *LOPA*

Incident reports

Tracked in a separate system. Tagged by location, not by LOPA scenario.

→ *LOPA*

Three silos. Zero feedback into the original risk calculation. This is the loop nobody closes.

Three datasets that should be one conversation. The LOPA is the room nobody walks back to.

Watchmen
INDUSTRIAL SAFETY EXPERTS

WHAT GOOD LOOKS LIKE

A closed-loop functional safety program doesn't need new tools. It needs a handful of connections that most programs are missing.

SRS in plain English

Every SIF has a Safety Requirement Specification that a maintainer can read, and that a proof test procedure can be traced to.

Procedures that can fail

Proof tests that induce or simulate a real process demand — and that document an as-found state before anyone intervenes.

Bypass metrics as a KPI

Bypass hours per SIF reported monthly alongside reliability KPIs. Anything over 2% gets a conversation.

A LOPA that ages with the plant

LOPA revalidation triggered by MOC, by proof test failures, and near misses — not just by the 5-year clock.

Site failure data feeds PFD

Once enough proof tests accumulate, site data replaces generic PFDs in the SIL verification. Your numbers, not OREDA's.

One report, one audience

A quarterly functional-safety report that reads proof tests, overrides and incidents through the lens of the LOPA scenarios they touch.

WRITING PROOF TESTS THAT BITE

A checklist I keep on my laptop, that has saved more SIFs than any piece of software:

- ☐ Does the test cover the sensor, the logic solver, and the final element — in one continuous procedure?
- ☐ Is there a process-side demand (actual or documented simulation), or are we just cycling the DCS graphic?
- ☐ Do we record as-found state before we touch the device?
- ☐ Do we measure — not infer — closure time, leakage, and response?
- ☐ Does the close-out reference the SRS requirement, by paragraph number?
- ☐ Does a dangerous-undetected failure have a path to show up in this procedure?
- ☐ Is the test interval the one the SIL verification assumed, or the standard preventative maintenance interval?

If you answer no to any of these, the SIL on paper isn't the SIL in the pipe rack.

Watchmen
INDUSTRIAL SAFETY EXPERTS

A LOPA THAT AGES WITH THE PLANT

Revalidation on a five-year clock isn't wrong — it's just too slow. These are the triggers that should reopen a LOPA before the clock says to:

Any proof test failure on a credited IPL	Not a retest. The original failure. The PFD assumption is on the line — and the as-found state is the data.
IEF drift: trip counts and near-misses in the historian	Compare actual demand frequency against the IEF in the LOPA every revalidation. Drift up by >2× is a revisit, not a footnote.
Modifier review on operational change	Occupancy, ignition, enabling conditions, time-at-risk — re-check whenever staffing, layout, schedule or operating mode changes.
MOC that touches process conditions and safety protection complexity	Not just "does this affect the SIS." Each of these changes touches LOPA inputs directly.
Site failure data available	Once you have roughly ten years of run-time, switch your PFD from generic to site-specific.

Watchmen
INDUSTRIAL SAFETY EXPERTS

WHAT THIS COSTS — AND DOESN'T

DOES COST

- Rewriting proof test procedures for every SIF — once — typically 2–4 hours per SIF.
- Giving the reliability engineer an extra half-day per month to look at overrides and proof test trends.
- A PM program tweak to capture as-found data — not a new system.
- One internal champion who owns the LOPA–PT feedback loop.

DOESN'T COST

- A new safety system. The one you have is probably fine — the problem is the assumptions around it.
- A seven-figure software platform. Most of this runs on the PM Program and historian you already own.
- Re-doing every LOPA from scratch. Most only need the assumptions flagged and the data plugged in.
- A cultural revolution. It's a small set of connections, done consistently.

A closed loop is cheaper than an open one. The open one just hides the bill until something happens.

Watchmen
INDUSTRIAL SAFETY EXPERTS

Thank you.

Questions are genuinely welcome — especially the ones that start with "but at our site…"

CONTACT US

Carsten Acker

Principal · Director of Operations

587-777-3055

cacker@watchmenise.com

Business inquiries: Dave Summers — dsummers@watchmenise.com

www.watchmenise.com

Watchmen
INDUSTRIAL SAFETY EXPERTS