

Functional Safety and OT Cybersecurity Aren't Analogous. They Meet Inside the Same Controller.

How asset owners can operationalise ISA/IEC 61511 and ISA/IEC 62443 as one lifecycle, interface by interface.

By Rafael Barreto Jijón, Managing Director, OT-Knight (an RBJCS brand)

In many process plants, functional safety and OT cybersecurity still live in separate worlds: different teams, standards, risk registers and budgets. When they talk, it is in analogies: a SIL is “a bit like” a Security Level.

The analogies are comfortable. They are also where the problem starts.

“Functional safety and OT cybersecurity aren't analogous — they literally meet inside the same controller.”

The Safety Instrumented System (SIS) is both one of the last layers of protection between an abnormal process and a major accident, and a cyber-physical attack target: same logic solver, same I/O, same engineering workstation. TRITON/TRISIS proved it in 2017. When malware reaches for the layer that keeps people alive, “safety incident or cyber incident?” has one honest answer: both.

So stop running two parallel programmes, and start operationalising one lifecycle.

The mandate already runs both ways

The standards already require it.

- **ISA/IEC 61511-1:2016** requires a security risk assessment to identify the security vulnerabilities of the SIS (8.2.4), and an SIS design that provides the necessary resilience against the identified security risks (11.2.12). It also requires access security for bypasses, the maintenance/engineering interface and I/O forcing (11.7.2.3, 11.7.3.2, 11.7.3.4, 11.8.6) and, where the SRS calls for it, documentation of how communications are made secure (12.4.2 k).
- **ISA/IEC 62443-2-1:2024** requires the asset owner to have policies and procedures to protect the safety system from interference by non-safety networks and their devices (NET 1.3), to operate the IACS as designed when disconnected from external networks, for example through fail-safe operation or safe shutdown (NET 1.4), and to change safety-system configuration only when configuration mode is enabled (DATA 1.3).
- **ISA/IEC 62443-3-2:2020** requires safety-related assets to be grouped into zones separated from non-safety assets, or the whole zone to be treated as safety-related (ZCR 3.3), each threat scenario's consequences to be evaluated and documented,

including the worst-case impact on personnel safety (ZCR 5.3, ZCR 5.13), and the management accountable for the safety, integrity and reliability of the process to review and approve the risk-assessment results (ZCR 7.1).

- **ISA/IEC 62443-3-3:2013** requires, at SL 3 and 4, the capability for zone boundaries to fail close when boundary protection fails, designed not to interfere with the operation of an SIS or other safety-related functions (SR 5.2 RE 3).

One SIS, two obligations.

One picture: the Parallel Lifecycle

Figure 1 builds on Table 1 of ISA-TR84.00.09-2024 and adds the governance and assurance layers asset owners actually run.

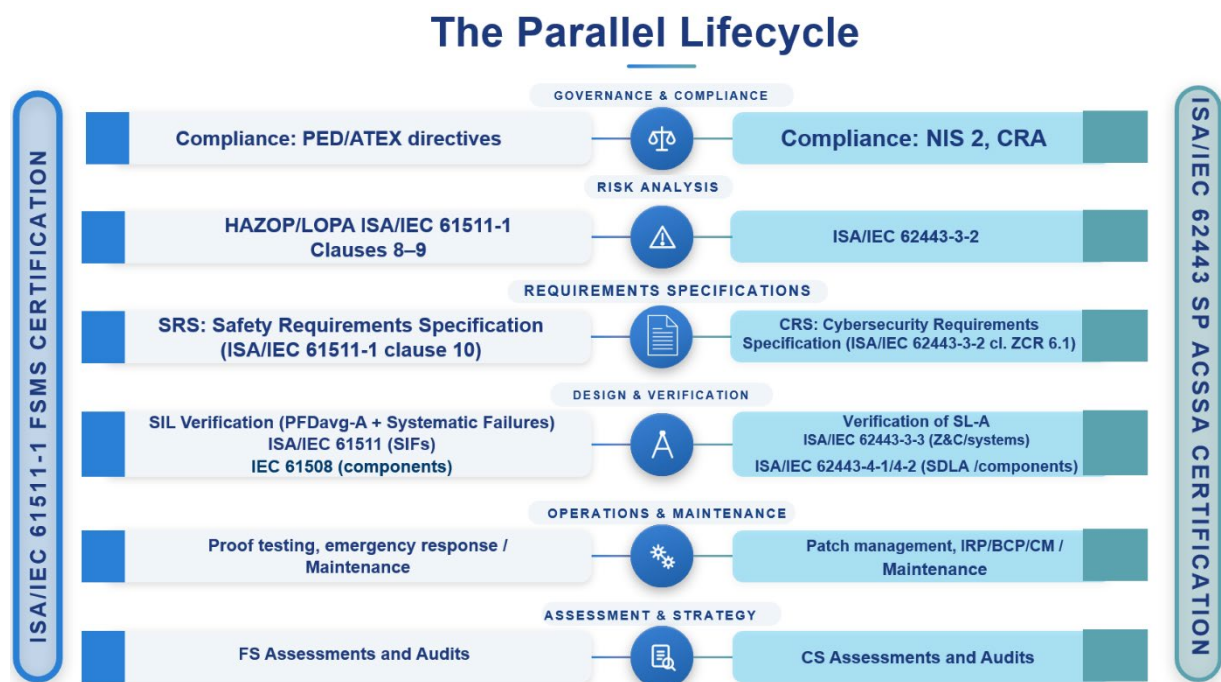


Figure 1 – The Parallel Lifecycle. Based on ISA-TR84.00.09-2024, Table 1.

The value is in the circles between the columns. **Every row is an interface:** one discipline's output must become the other's input. If those hand-offs are not designed, they do not happen.

Governance: one management spine, not three

ISA/IEC 62443-2-1 is explicit: where the asset owner has an ISMS, the IACS security program shall be coordinated with it (ORG 1.1). Most process operators also run functional safety management under ISA/IEC 61511-1 Clause 5. Three management systems, one governance logic.

Run them on one spine: one governance policy, one Statement of Applicability that demarcates IT, OT and safety, including the IT/OT secure interface, and one combined internal audit and management review.

And use one competence framework. **You can't secure an SIS if your security team doesn't know what an SIF is** — and a *safety engineer who has never worked with zones and conduits will not see cyber as a common cause.*

Risk analysis: one consequence basis

Classical LOPA credits a protection layer only if it is independent of the others (ISA/IEC 61511-3, Annex F). A cyberattack breaks that assumption where the BPCS and the SIS share a network without segregation, a common-cause path ISA/IEC 61511-1 itself flags (9.4.2): one compromise can defeat two layers credited as independent, and even create the demand while disabling the SIF that should respond. As ISA-TR84.00.09 notes, cyberattacks are not random and can cause hazards “in an orchestrated sequence that can result in consequences not recognized if not considered in the analysis.”

Interface HAZOP / LOPA and cyber risk assessment

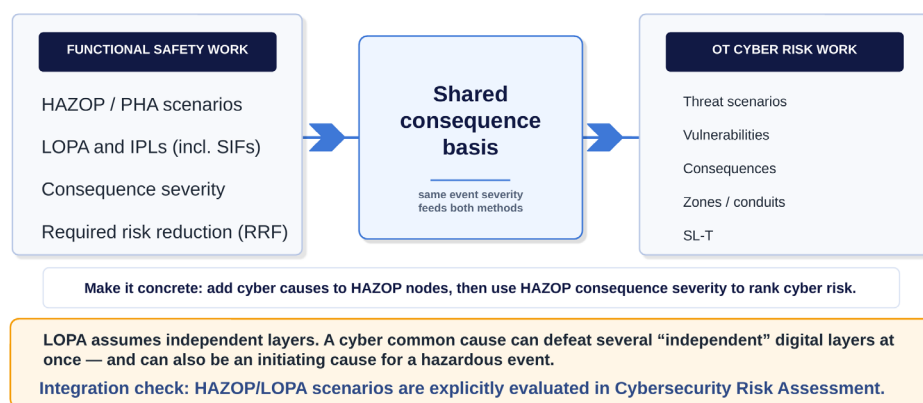


Figure 2 – One consequence basis for safety and cyber risk.

The guidance to ISA/IEC 62443-3-2 ZCR 5.3 already points the way: review existing PHA and other risk assessments, including functional safety, when determining consequence and impact. In practice:

- **Cross-staff the workshops.** A functional safety engineer in the cyber risk assessment; a cyber-informed engineer in the HAZOP/LOPA.
- **Share the consequences.** Add cyber causes to HAZOP nodes and use HAZOP severity to rank cyber risk. But HAZOP considers one cause–consequence pair at a time (TR84.00.09), so also look for multi-cause scenarios it missed.
- **Ask two standing questions.** Could cyber initiate or worsen this scenario? Is there a non-digital safeguard that designs the risk out?

A relief valve cannot be hacked, but TR84.00.09 warns that a cyberattack can create a demand it was never designed for. Credit non-digital safeguards after checking their design basis against the cyber scenario.

Requirements: reconcile the SRS and the CRS

TR84.00.09 puts it simply: “Documentation of a CRS is a requirement of ISA-62443-3-2, just as a safety requirements specification is a requirement of ISA-61511 Part 1.” The Safety Requirements Specification (SRS, ISA/IEC 61511-1 Clause 10) and the Cybersecurity Requirements Specification (CRS, ISA/IEC 62443-3-2 ZCR 6.1) turn risk into design.

SRS ↔ CRS reconciliation

The SRS and CRS are key factors in achieving risk reduction.

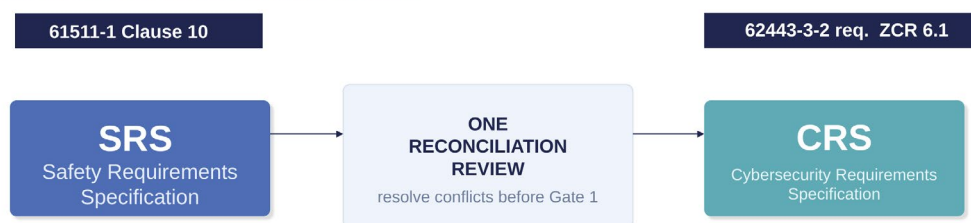


Figure 3 – SRS/CRS reconciliation before the first assessment gate.

TR84.00.09 also sets the order: an initial SRS after the hazard and risk analysis and allocation to protection layers, already informed by the initial cyber risk assessment; then the detailed cyber risk assessment, recorded in the CRS; then reconciliation of any contradictions.

The rule: **a cyber requirement must not undermine a safety requirement, and vice versa**. If the CRS demands timely patches on the SIS platform and the SRS forbids unvalidated changes, neither wins by default. Test the patch for compatibility and approve it (ISA/IEC 62443-2-1 COMP 3.2), install it through MOC, and re-verify the affected SIFs before return to service (ISA/IEC 61511-1 Clause 17). The CRS may be separate or part of the SRS. **Format is flexible. Reconciliation is not.**

Verification: achieved must meet target

SIL verification ↔ SL verification

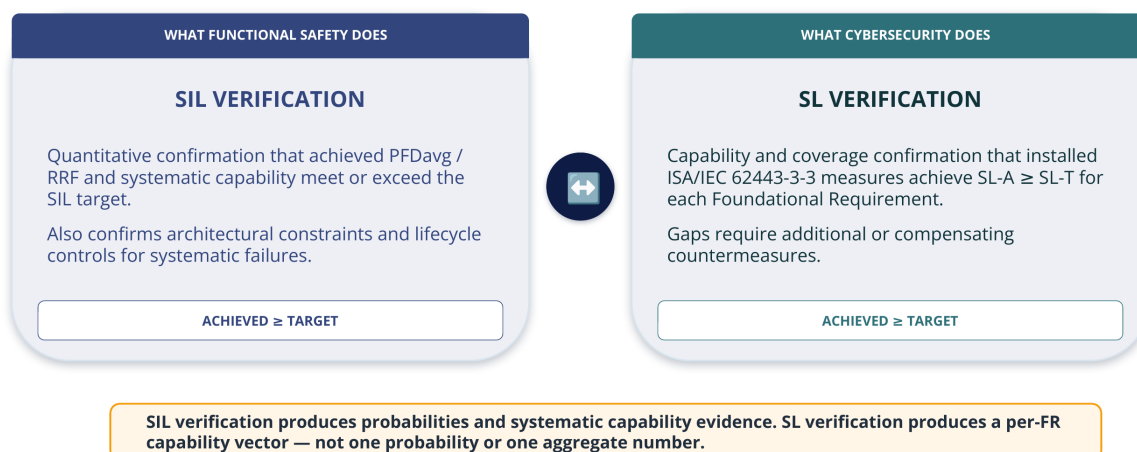


Figure 4 – Same loop, different measures.

Both close the same loop: achieved must meet or exceed target, and gaps are fixed and re-verified. TR84.00.09 Table 1 pairs quantitative SIL verification of each SIF with verification of each zone's capability against the foundational requirements.

SIL verification produces a calculated failure measure (PFDavg or RRF in low-demand mode, PFH in high-demand or continuous mode) plus evidence of architectural constraints and systematic capability. SL verification produces a vector: the achieved Security Level (SL-A) per Foundational Requirement against the target (SL-T) set for each zone or conduit (ISA/IEC 62443-3-2 ZCR 5.6). Where SL-A falls short, add or compensate countermeasures.

Treat SL verification with the same discipline as SIL verification: defined scope, method and acceptance criteria, competent reviewers, auditable records. **Not a tick-box.**

Operations and maintenance: one regime, one response

Most programmes fail quietly in operation. Proof testing detects dangerous hidden faults; security testing reveals hidden vulnerabilities. Run both on one operational backbone:

- **One maintenance regime** in the plant CMMS, not an IT ticket queue.
- **One MOC register.** Patches, firewall rules and configuration changes go through the plant MOC process ISA/IEC 61511-1 already requires for the SIS (5.2.6.2.4).
- **One permit gate.** No intrusive cyber work on a live system without a plant-floor work permit.
- **One emergency playbook.**

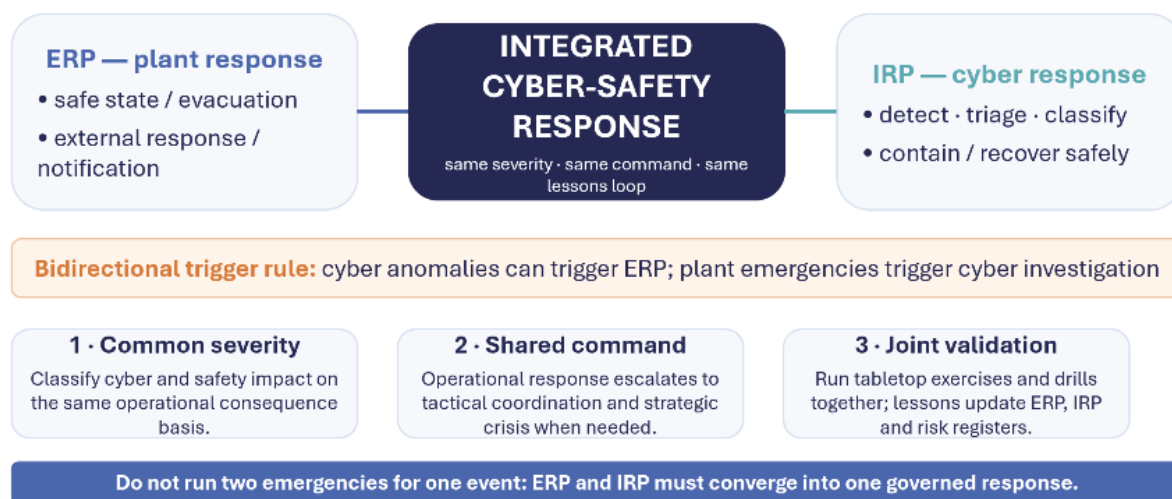


Figure 5 – One integrated cyber-safety response.

TR84.00.09 recommends reconciling or integrating cyber incident response procedures with the site emergency response plan, confirmed at the pre-startup safety review. Cyber anomalies can trigger the Emergency Response Plan (ERP); plant emergencies should trigger a cyber investigation. **Do not run two emergencies for one event.**

Assessment: prove it together

ISA/IEC 61511-1 identifies five stages for functional safety assessment (FSA); an FSA before hazards are present and periodic FSAs in operation are mandatory. TR84.00.09 mirrors them with five cybersecurity stage assessments (CSSA), run as part of the FSA or separately. One assessment plan, one calendar, overlapping teams.

For the operating site, ISASecure ACSSA assesses the deployed IACS against ISA/IEC 62443-2-1, 2-4, 3-2 and 3-3 together. It does not treat the SIS as generic OT: ACSSA-101 lists the SIF first among the essential functions and, building on ISA/IEC 62443-3-3, states that a denial-of-service event on the control system or SIS network shall not prevent SIFs from acting.

Five actions for Monday

1. **Create the joint team:** process safety, functional safety, automation, OT cybersecurity, operations and suppliers.
2. **Integrate the risk work:** cyber prompts in the HAZOP; HAZOP consequences in the cyber risk assessment.
3. **Reconcile the requirements:** one SRS/CRS conflict review before design freeze.
4. **Align the assurance gates:** one FSA/CSSA calendar; cyber items in PSSR and MOC.
5. **Build evidence continuously:** ACSSA-ready evidence from daily operations, not last-minute binders.

Success means one integrated risk register, one integrated action register, and evidence that survives assessment.

Final thought

In OT and critical infrastructure, cybersecurity becomes a safety function — when it preserves the ability of the process to remain in, or return to, a safe state. Safety engineers know how to protect that ability; security engineers know how an adversary will try to take it away. Neither can protect the plant alone.

The asset owners who get this right will not be the ones with the thickest binders. They will be the ones whose two teams work from one lifecycle.

About the author

Rafael Barreto Jijón is Managing Director of OT-Knight, an RBJCS brand, and an OT cybersecurity and functional safety practitioner with more than 19 years' experience in oil and gas, petrochemicals, power and critical infrastructure. He is an ISA/IEC 62443 Cybersecurity Expert, a Certified Functional Safety Master/Expert, an ISASecure ACSSA Evaluator Specialist, a certified ISO/IEC 27001 Senior Lead Implementer/Auditor, a NIS 2 Senior Lead Implementer, an ISO 31000 Senior Risk Manager and an ISA Qualified Instructor. Contact: information@ot-knight.com

Initially published on ISASecure.org.