

ISA Webinar

All things automation and industrial cybersecurity

Operationalising Functional Safety & OT Cybersecurity

A practical integration for asset owners

Where Safety Meets Security — ISA/IEC 62443 · ACSSA framework · ISA/IEC 61511 · ISA-TR84.00.09-2024



International Society of Automation
Setting the Standard for Automation™

Rafael Barreto Jijón · 2026-10-28

ISA is the leading professional society for automation



Developer of 120+ consensus **standards** used around the world, including ISA/IEC 62443 for OT cybersecurity, ISA-95, ISA-18, ISA-112 and ISA-5



Globally recognized **training and certification** for OT cybersecurity, safety and automation professionals



Publications and **technical content** on ISA's media arm, Automation.com



Industry consortia and conformity assessment offerings for OT cybersecurity and wireless connectivity: ISA Global Cybersecurity Alliance, ISASecure and ISA100 Wireless



Conferences, exhibits and career development



Mimo®: the world's first LLM trained exclusively on automation content

Presenter



ISASecure®
Member



Rafael Barreto

OT Cybersecurity · Functional Safety ·
ISA/IEC 62443 / ISA/IEC 61511
integration

Managing Director — OT-Knight

Dual-discipline practitioner

19+ years across OT cybersecurity, Functional Safety,
SCADA, PLC, DCS and SIS lifecycle

OT Cybersecurity & Functional Safety Manager for multi-
billion € projects

OT CS / FS management as a service

Oil & Gas, Petrochemicals, Power systems, Renewables,
Nuclear medical devices

ISA EMEA 62443 Qualified Trainer; PECB Certified Instructor

Member of the ISASecure technical committee



*"In OT and Critical Infrastructure, Cybersecurity becomes a
Safety Function"*

Selected credentials



ISA/IEC 62443 Cybersecurity
Expert



ISA Qualified Instructor
(62443)



ISASecure ACSSA Evaluator
Specialist



ISO/IEC 27001 Senior Lead
Implementer/Auditor



NIS 2 Directive Senior Lead
Implementer



Certified Functional Safety Master
Expert / Professional



Cybersecurity can affect the safety function

1



Same object

SIS / BPCS / engineering workstations share digital dependencies.

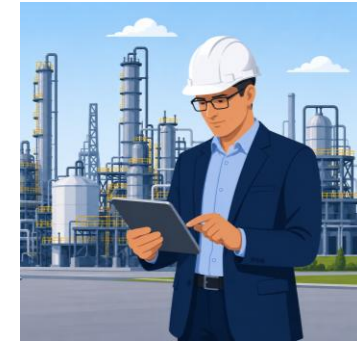
2



Same consequence

Cyber compromise may initiate or worsen a hazardous event.

3



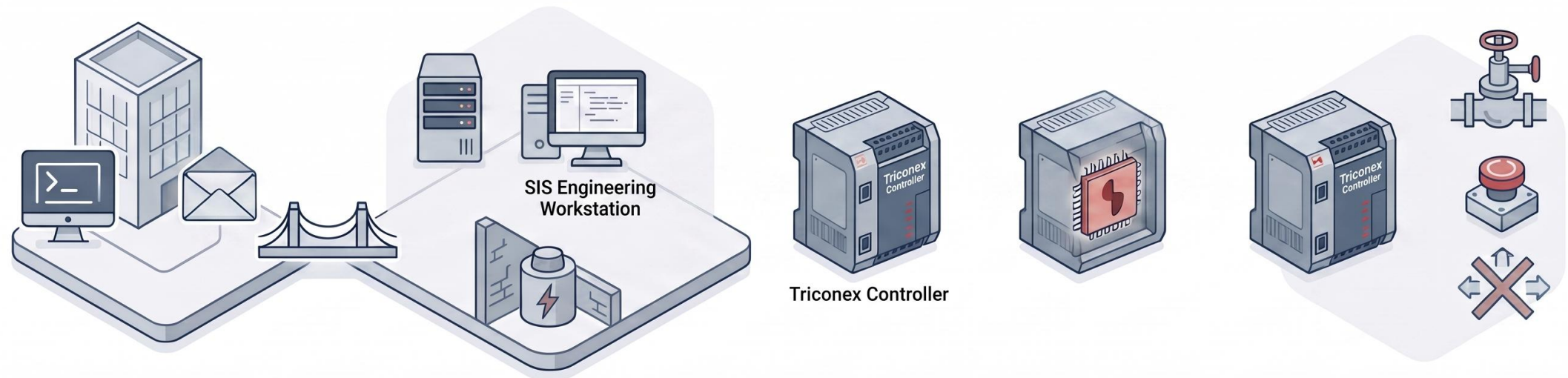
Same accountability

The asset owner must prove both safety integrity and cyber resilience.

"FS and CS aren't analogous — they literally meet inside the same controller."

ISA/IEC 61511 establishes the safety obligation to address SIS security risk; ISA/IEC 62443 and ISA-TR84.00.09 provide practical implementation and assurance structures.

The Hook: TRITON / TRISIS



1. INITIAL IT NETWORK PENETRATION

Attackers gain entry to business systems using routine methods like phishing.

2. LATERAL MOVEMENT TO OT NETWORK

The threat actors pivot through shared systems to reach the SIS engineering workstation.

3. PROPRIETARY PROTOCOL REPROGRAMMING

The unauthenticated TriStation protocol is used to communicate directly with Triconex controllers.

4. IN-MEMORY FIRMWARE MODIFICATION

Malicious binary code is injected into the controller's memory to establish a backdoor.

5. NEUTRALISING FAILSAFE LOGIC

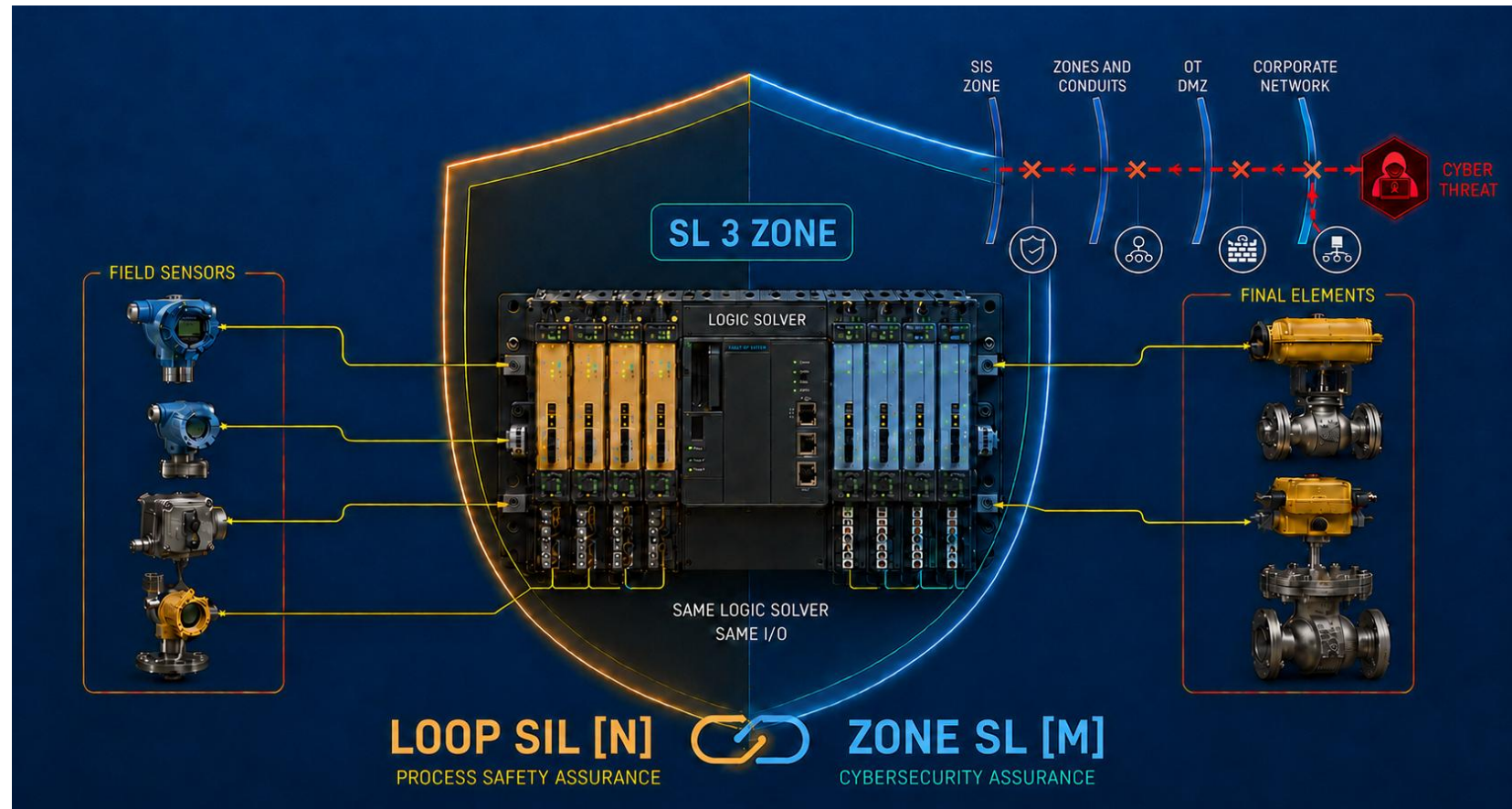
Safety limits are bypassed to prevent the system from shutting down during emergencies.

TRITON'S UNIQUE IMPACT VS. HISTORICAL ICS MALWARE

MALWARE	PRIMARY TARGET	ULTIMATE INTENT
 Stuxnet	Enrichment Centrifuges	Equipment Sabotage
 Industroyer	Electrical Grids	Operational Disruption
 Triton	Safety Systems (SIS)	Physical Catastrophe

Was that a cyber incident, or a safety incident?

Why integrate



The Safety Instrumented System is simultaneously the last line of process-safety defense — and a cyber-physical attack target. Same logic solver, same I/O.

“E.g., an SIL-2 loop runs in a controller in an SL-3 zone — protect one without the other and you’ve not protected the plant.”

The Mandate Runs Both Ways

Same SIS, two directions: 61511 requires the cyber risk assessment; 62443 requires protecting the safety system in return.

ISA/IEC 61511-1:2016 — REQUIRES CYBERSECURITY

A security risk assessment shall identify the security vulnerabilities of the SIS (§8.2.4)

The SIS design shall provide resilience against the identified security risks (§11.2.12)

Bypasses, engineering interfaces and I/O forcing shall be access-secured (§11.7.2.3, 11.7.3.2, 11.7.3.4, 11.8.6)

ISA/IEC 62443-2-1:2024 & 62443-3-2:2020 — PROTECT THE SAFETY SYSTEM

Policies shall protect the safety system from interference by non-safety networks (2-1, NET 1.3)

Policies shall ensure the IACS can fail-safe and operate when disconnected externally (2-1, NET 1.4)

Safety system configuration shall change only in an enabled, authorized mode (2-1, DATA 1.3)

Safety-related assets shall be grouped into their own zone, separated from the rest (3-2, ZCR 3.3)

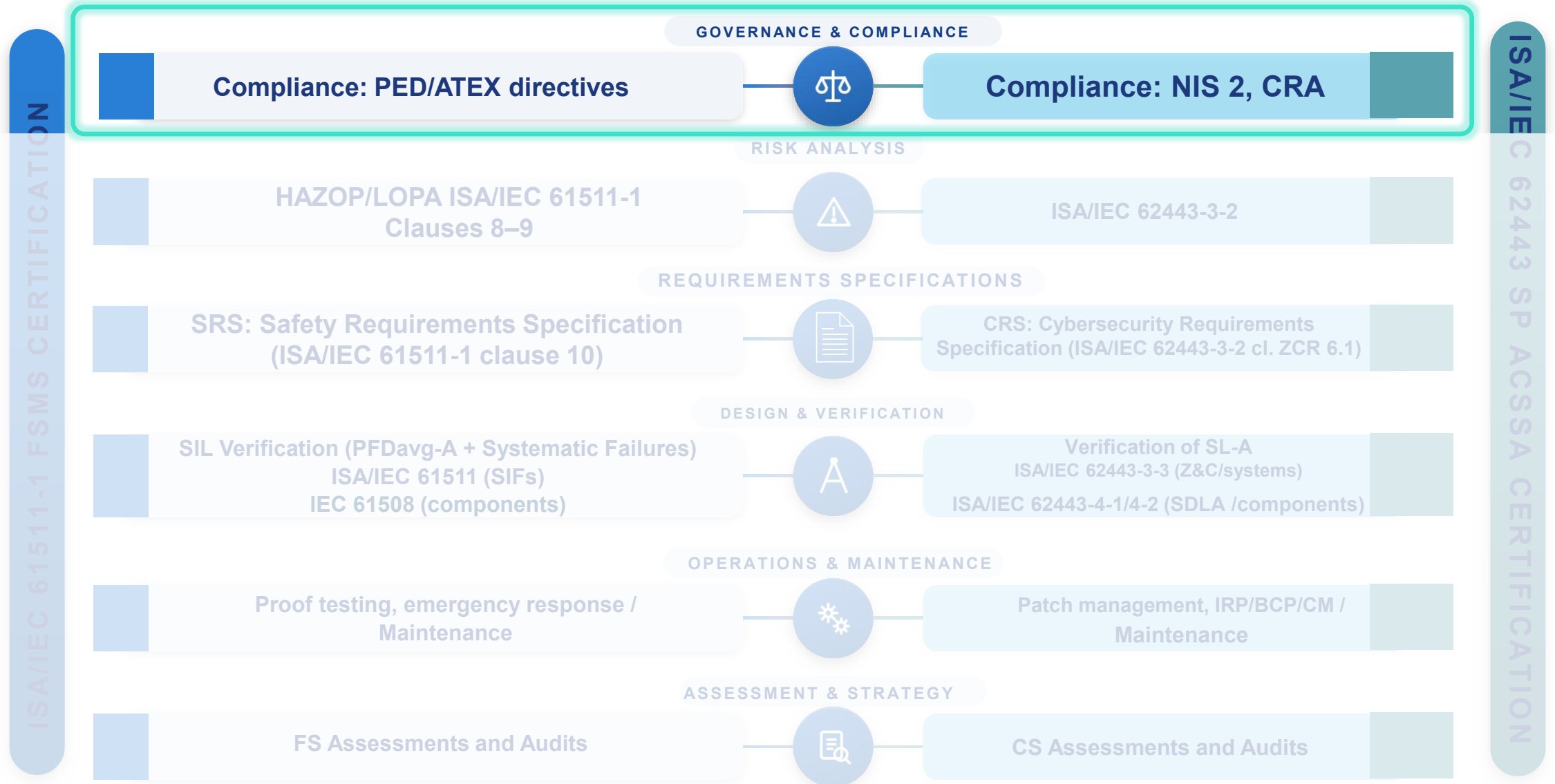
Management accountable for process safety shall approve the risk assessment results (3-2, ZCR 7.1)

Same SIS, both directions — 61511 mandates the risk assessment; 62443 mandates the protection.

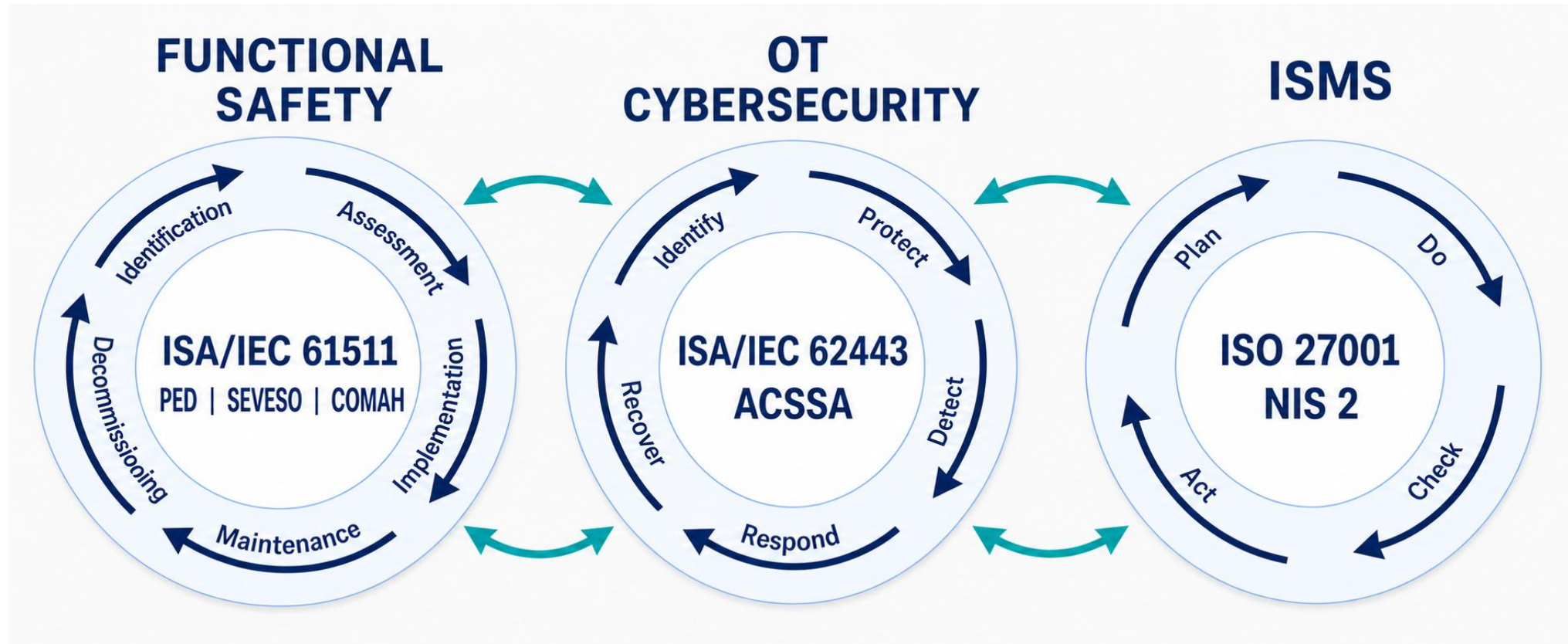
The Parallel Lifecycle



The Parallel Lifecycle



GOVERNANCE AND COMPLIANCE



Bridging the management systems

ISO 27001 ↔ 62443-2-1 ORG 1.1 ↔ ISA/IEC 61511

ISO 27001 management clause	ISA/IEC 62443-2-1 bridge	ISA/IEC 61511 FSMS section
5 Leadership policy · roles · commitment	ORG 1.1: Security Program coordinates with ISMS	5.2.1 / 5.2.2 management responsibility · FS policy · resources
6 Planning objectives · change planning	SP applies OT-specific planning	Clause 6 + 5.2.4 safety lifecycle structure & planning
7 Support resources · competence · documented information	Security Program competence / responsibilities	5.2.2 resources + 5.2.2.3 competence + Clause 19
6.1 / 8.2–8.3 risk assessment & treatment	62443 SP + 3-2 cyber risk logic	5.2.3 + Clause 8 + Clause 9 risk evaluation, H&RA, allocation
9 + 10 monitoring · audit · review · improvement	Program audits + maturity improvement	5.2.5 + 5.2.6 + Clause 7 monitoring, FSA/audit/revisions, verification

People: the cross-competency requirement

Interfacing is a people problem before it is a technical one.

OT cybersecurity practitioner
must understand FS

SIS / SIF basics
SIL · PFDavg
61511 lifecycle
consequence of failing a SIF

One competence
framework

single training matrix
periodic assessment
documented evidence

Functional safety practitioner
must understand cyber

threats / vulnerabilities
zones / conduits
SL
cyber as common cause

“You can’t secure an SIS if your security team doesn’t know what an SIF is.”

“You can’t see cyber as a common cause if your safety team doesn’t know zones and conduits.”

Two cultures, one mindset

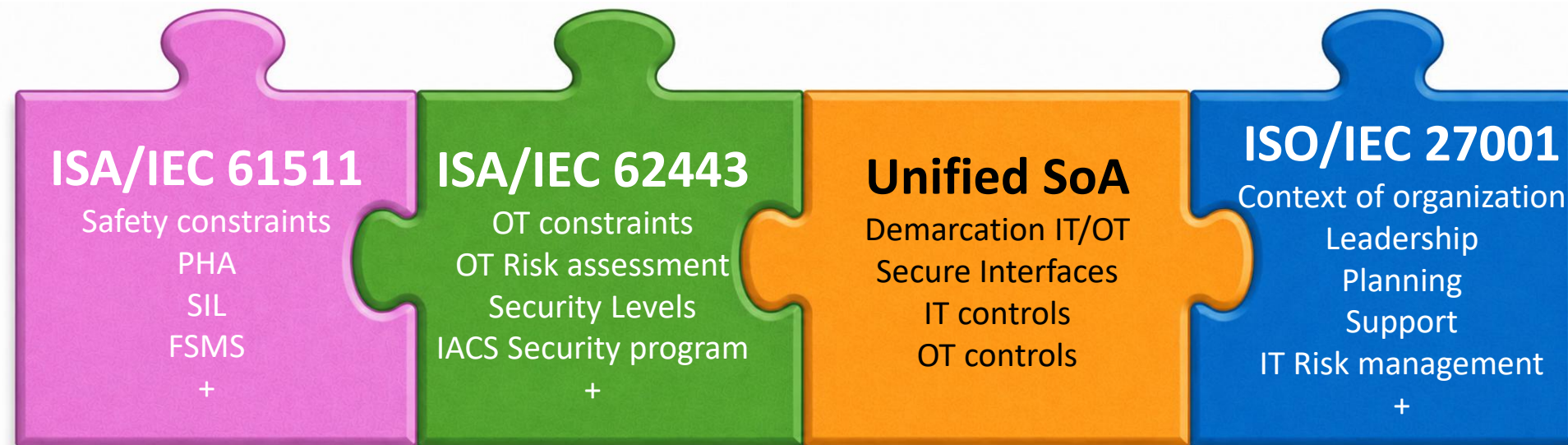
Extend the safety-culture machinery to cybersecurity — do not build a separate culture from zero.



Culture is not a single training event: it is refreshed through lessons learned, incident reviews, exercises and practical demonstrations.

Bridging IT and OT: Coordinating with the ISMS (ORG 1.1)

Operationalising: use management elements from ISO/IEC 27001, write a unified Statement of Applicability demarcating IT/OT and including IT/OT controls, and apply the ISA/IEC 62443 security program integrated with the ISA/IEC 61511 FSMS



RECOMMENDED READING: Refer to ISAGCA Whitepaper — *Securing Operational Technology: Understanding the ISA/IEC 62443 Series of Standards from an ISO/IEC 27001 and ISO/IEC 27002 Perspective.*

► OPERATIONALISE IT

Make The Case, Map The Obligations

- 1 Make the case once, jointly**

Single combined FS+CS risk briefing to leadership — not two competing budget pitches.
- 2 Map obligations to assets**

One-page regulatory map: NIS2 / CRA / PED-ATEX / Seveso-COMAH, with one accountable owner per asset.
- 3 Make safety explicit in OT risk**

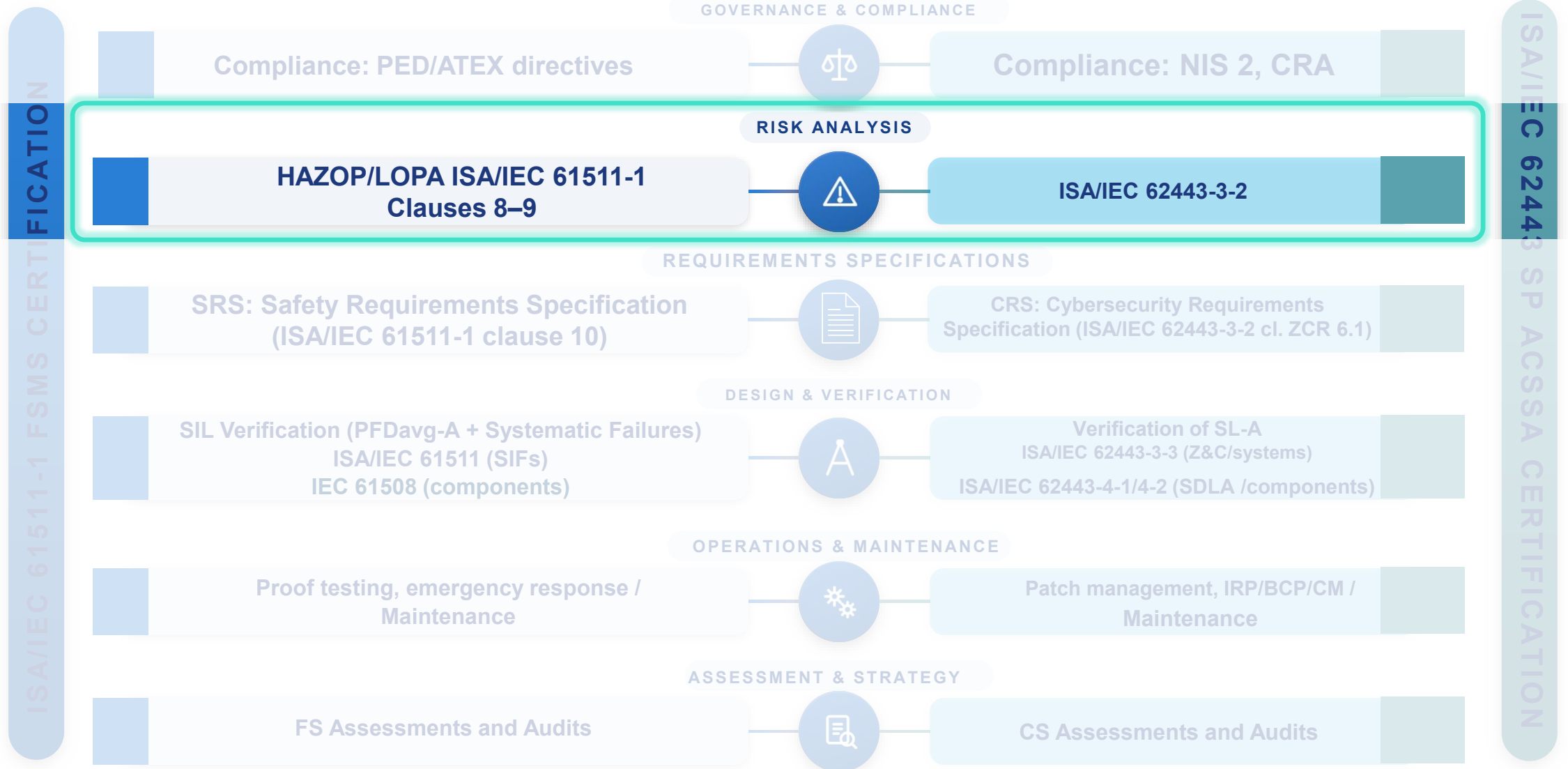
List “safety” as a separate objective and reference the SIS security risk assessment from safety documentation.
- 4 Integrate the management systems**

One governance policy, one SoA demarcating IT/OT/safety, one combined internal audit + management review.
- 5 Use one competence framework**

Single training matrix and periodic documented competence assessment spanning safety and security roles.
- 6 Use TR84 Table 1 as a worksheet**

List existing 61511 deliverables, tag where cyber tasks / CRS insert, assign an owner.

The Parallel Lifecycle



The Trap: Common-Cause Via Cyber



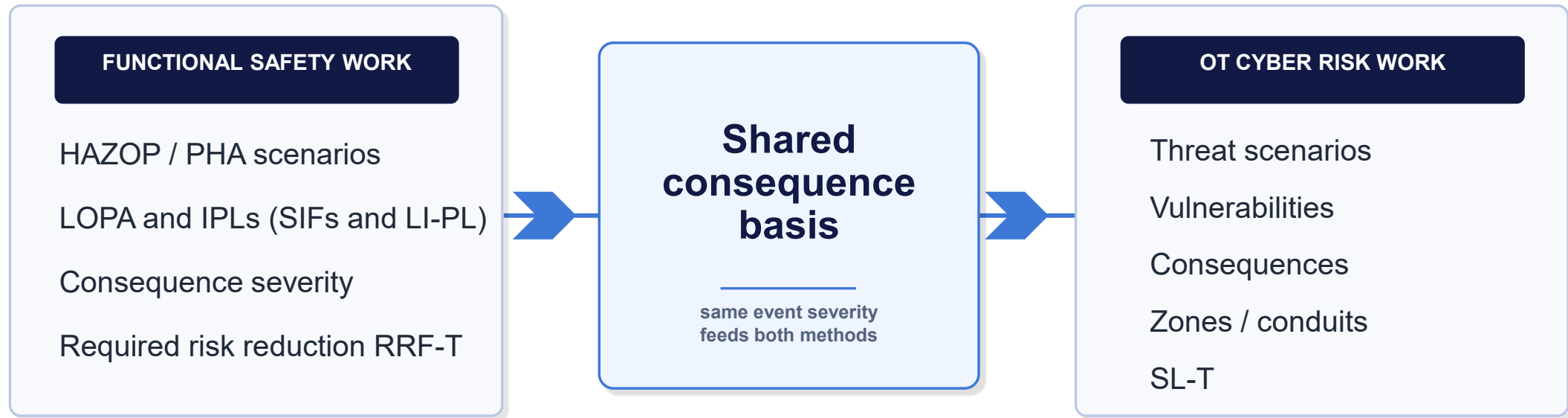
THE TRAP

Classical LOPA assumes layers fail *independently*. A cyberattack can defeat multiple layers at once through a shared compromised digital common cause — the several controllers, shared network, or common engineering workstation.

Cyber is a credible common-cause / common-mode contributor to process-safety risk.

↳ TRITON, again.

Interface HAZOP / LOPA and cyber risk assessment



Make it concrete: add cyber causes to HAZOP nodes, then use HAZOP consequence severity to rank cyber risk.

LOPA assumes independent layers. A cyber common cause can defeat several “independent” digital layers at once — and can also be an initiating cause for a hazardous event.

Integration check: HAZOP/LOPA scenarios are explicitly evaluated in Cybersecurity Risk Assessment.

HINT: The strongest answer to a cyber common-cause is sometimes **not** a cyber control. A non-digital safeguard — a *PSV or check valve, physically immune to cyberattack* — can be credited as an IPL in both risk registers.

► OPERATIONALISE IT

Integrate the Risk Work

1 **Cross-staff the workshops**

Put a process-safety / functional-safety expert on the 62443-3-2 cyber assessment and a cyber-informed engineer in the HAZOP/LOPA.

2 **Use one consequence basis**

Run or refresh HAZOP/PHA first or alongside the cyber assessment so cyber inherits the safety consequences.

3 **Add two standing prompts**

Could cyber initiate/worsen this scenario? Is there a non-digital safeguard that designs the risk out?

4 **One combined risk register**

Cross-train facilitators and schedule workshops merged or back-to-back — not months apart.

The Parallel Lifecycle



SRS ↔ CRS reconciliation

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

61511-1 Clause 10

62443-3-2 req. ZCR 6.1



A cyber requirement must not undermine a safety requirement — and vice versa.

Example: patching cannot bypass the SIF change-validation basis; safety bypass rules cannot weaken access control.

Reconciliation Has An Order

TR84.00.09 defines the sequence: draft the SRS first, use it in detailed cyber risk assessment, record the CRS, then reconcile both specifications.

- 1 Initial SRS drafted after the safety H&RA — already scoped to include the initial cyber risk assessment (TR84.00.09, Initial SRS)
- 2 That initial SRS is carried forward as an input to the detailed cybersecurity risk assessment (TR84.00.09, Initial SRS)
- 3 The detailed cyber risk assessment output is recorded in the CRS, reflecting the design basis (TR84.00.09, Requirements specification)
- 4 SRS and CRS are reconciled — contradictions between safety and cybersecurity requirements resolved (TR84.00.09, Requirements specification)

**“Documentation of a CRS is a requirement of ISA-62443-3-2, just as a SRS is a requirement of ISA-61511 Part 1.”
— ISA-TR84.00.09**

Format is flexible. Reconciliation is not.

What Reconciliation Actually Looks Like

Three real **conflicts** between SRS and CRS, and the specific control that resolves each one — never a blanket safety override, never a blanket security bypass.

PATCHING A LOCKED-DOWN SIS

SRS: No unvalidated change to the SIF logic or configuration.

CRS: Patch the SIS engineering workstation within 30 days of release.

✓ Test the patch offline, apply it in a scheduled MOC window, then proof-test the SIF before returning to service.

REMOTE VENDOR SUPPORT

SRS: The SIS shall be isolated — no external system may alter its logic.

CRS: Enable secure remote engineering access for vendor support.

✓ Time-bound, operator-authorized sessions through a jump host — only while the SIS is in an enabled configuration mode.

SOC VISIBILITY

SRS: Nothing may degrade the SIS logic solver's real-time, deterministic performance.

CRS: Log and monitor all SIS engineering workstation activity in real time.

✓ Monitor passively through a SPAN port feeding the SOC — never an inline device on the safety loop.

Same pattern every time: a real conflict, a specific control that resolves it — documented in the CRS, traceable back to the SRS.



Consideration: What if remote access drops while you are working on a live SIS?

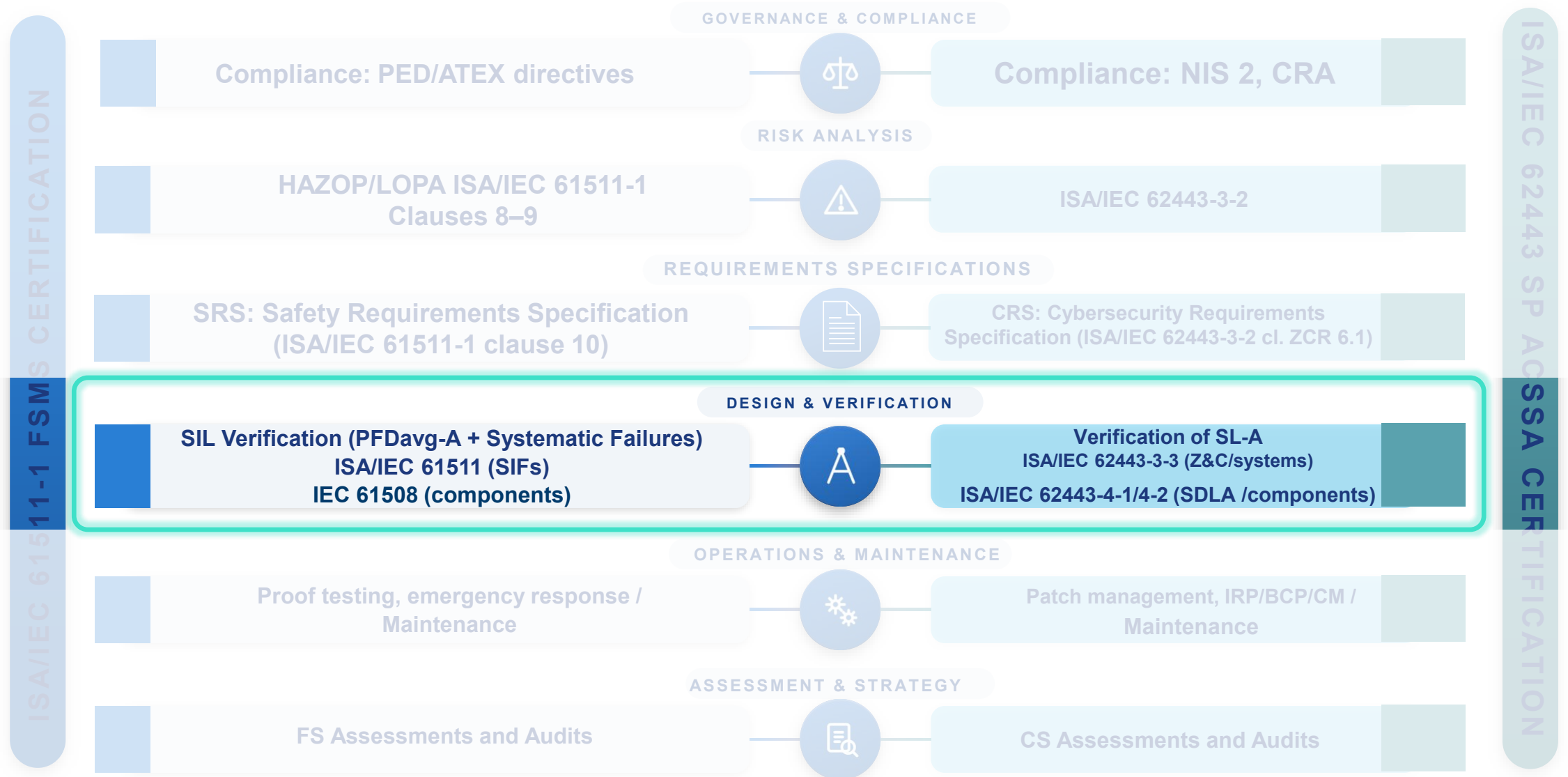
Never work on a SIS when you cannot see the process and operators are nearby — even with secure remote access and an approved MOC or work order.

► OPERATIONALISE IT

Reconcile Cyber and safety requirements specifications

- 1 Write SRS and CRS together** Hold one reconciliation review that explicitly resolves safety/security conflicts.
- 2 Consider operational constraints** Operational constraint, schedules and resources should be considered for proof-test turnarounds, patch update and maintenance/MOC procedures.

The Parallel Lifecycle



SIL verification ↔ SL verification

WHAT FUNCTIONAL SAFETY DOES

SIL VERIFICATION

Quantitative confirmation that achieved PFDavg / RRF and systematic capability meet or exceed the SIL target.

Also confirms architectural constraints and lifecycle controls for systematic failures.

ACHIEVED $\geq$ TARGET

WHAT CYBERSECURITY DOES

SL VERIFICATION

Capability and coverage confirmation that installed ISA/IEC 62443-3-3 measures achieve SL-A $\geq$ SL-T for each Foundational Requirement.

Gaps require additional or compensating countermeasures.

ACHIEVED $\geq$ TARGET

SIL verification produces probabilities and systematic capability evidence. SL verification produces a per-FR capability vector — not one probability or one aggregate number.

► OPERATIONALISE IT

Combine and interface the security and safety targets and verifications

- 1 Treat SL verification as an assurance activity**

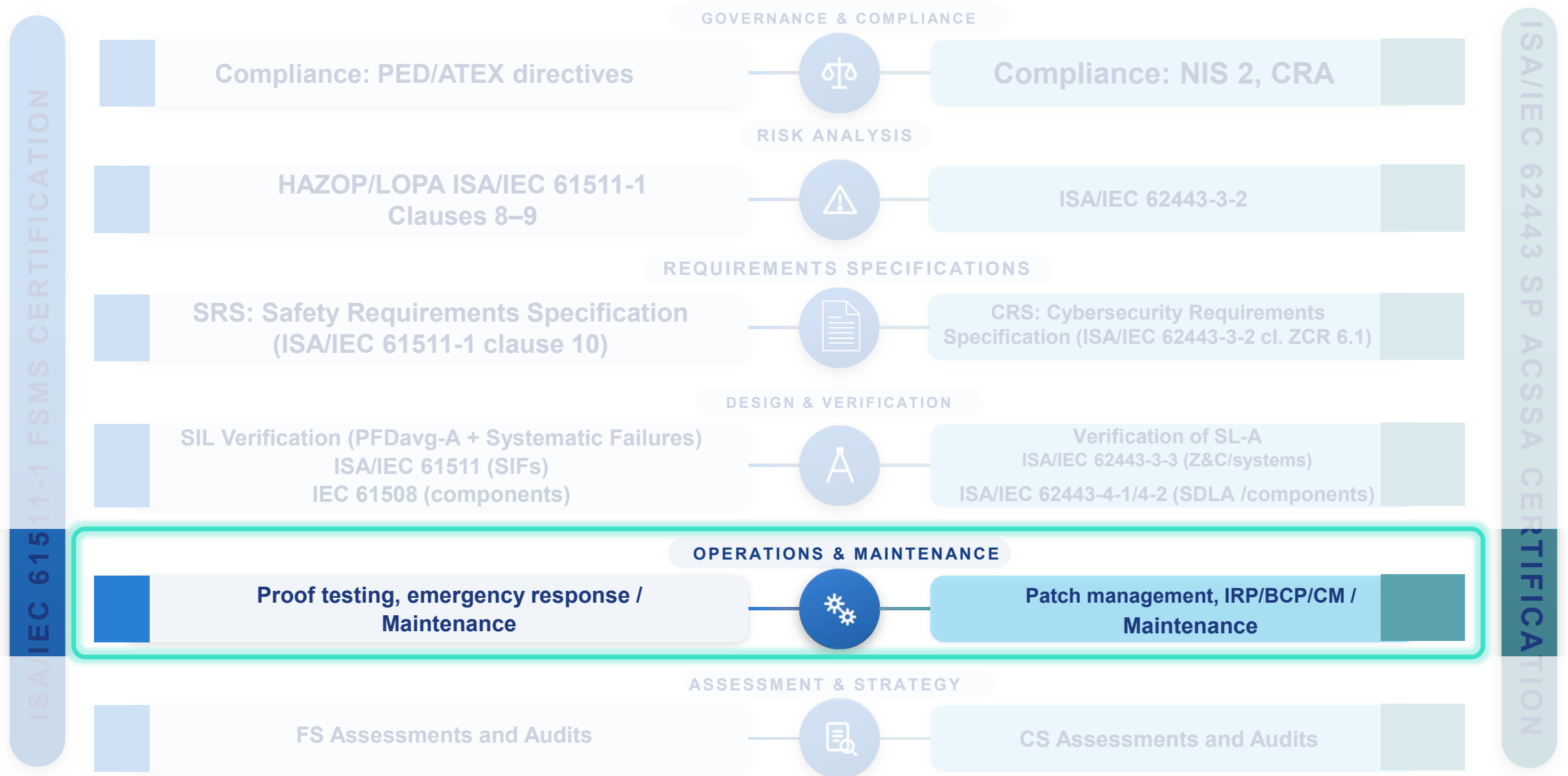
Don't reduce SL verification to a tick-box. Define scope, method, evidence and acceptance criteria — as formally as SIL.
- 2 Assign competent, independent reviewers**

SIL needs reliability and architecture skills. SL needs 62443-3-3, zones/conduits and control skills.
- 3 Verify achieved $\geq$ target**

SIL verification closes PFDavg, RRF and architectural gaps. SL closes SL-A vs SL-T gaps per Foundational Requirement.
- 4 Make the evidence auditable**

Record assumptions, deviations and residual gaps. Re-verify with the same discipline as safety evidence.

The Parallel Lifecycle



Proof testing ↔ security testing / pen-testing

WHAT FUNCTIONAL SAFETY DOES

PROOF TESTING

Scheduled testing reveals dangerous failures that remain hidden until demand.

A failed proof test triggers repair, revalidation and lifecycle learning.

HIDDEN DEGRADATION REVEALED



WHAT CYBERSECURITY DOES

SECURITY / PEN-TESTING

Periodic vulnerability assessment and (OT) penetration testing reveal weaknesses before an attacker exploits them.

Patch and vulnerability management provide the remediation pathway.

HIDDEN VULNERABILITY / MISCONFIGURATION REVEALED

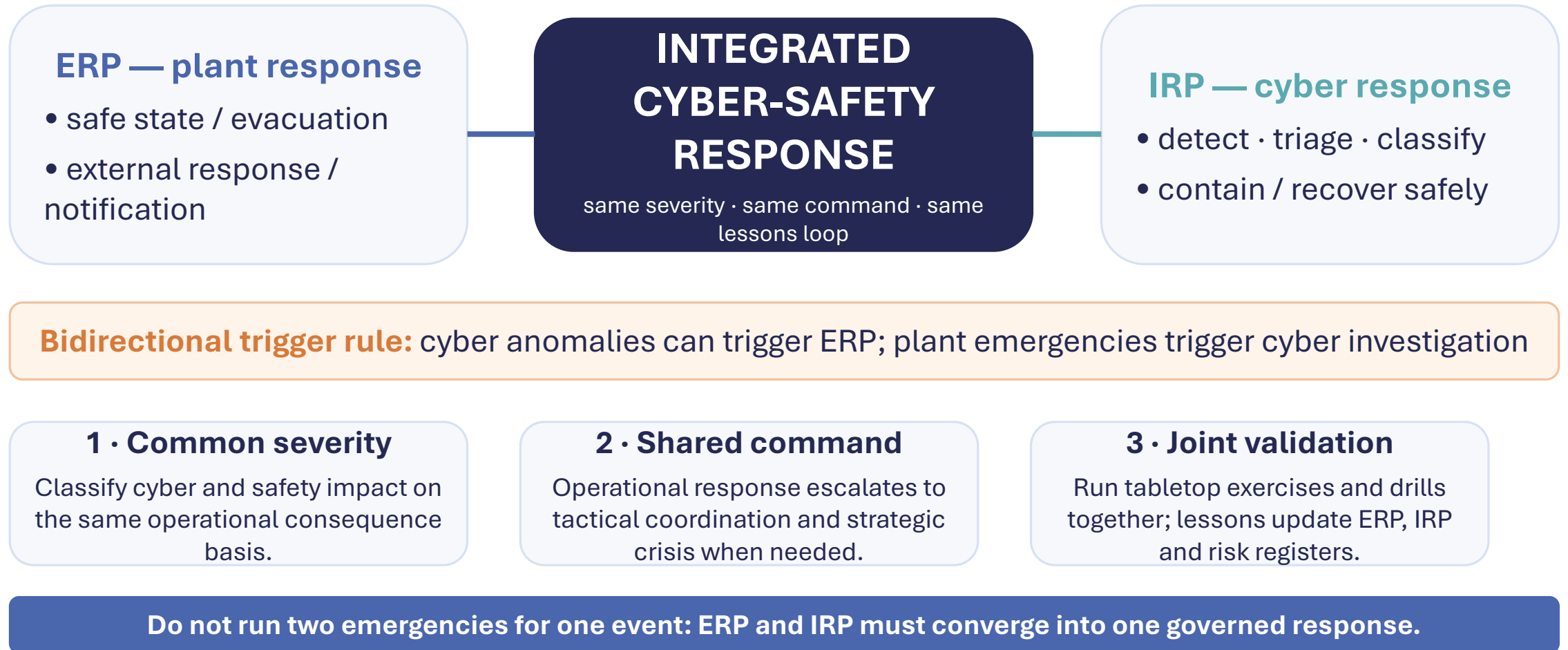
Proof Testing detects degradation; security testing detects vulnerabilities and misconfigurations.

Maintenance, MOC & Permits: One Regime

FUNCTIONAL SAFETY	OT CYBERSECURITY
Preventive & corrective (breakdown) maintenance per the SIS maintenance plan (61511 §16.2.1)	Preventive patching & corrective fixes tracked in plant CMMS — not the IT ticketing system
MOC initiates, documents, reviews, approves any SIS change (61511 §5.2.6.2.4–5)	Cyber MOC (patch, config, firewall rule) feeds the SAME platform-floor MOC register — one log, the same system, not two
Bypasses need authorization & a log (61511 §16.2.7) — the model for permit-to-work	Any patch/update needs a work permit opened by the lead operator or authorized person at the platform
Emergency Response is the outermost plant level protection layer (61511 Fig 9)	Cyber IRP integrated into that same platform Emergency Plan — joint tabletop exercises & drills

One maintenance regime, one MOC register, one permit gate, one emergency plan — safety and security share the same operational backbone.

ERP + IRP: one integrated response



► OPERATIONALISE IT

Embed cyber operations into plant operations

1 Maintenance = controlled work

Preventive and corrective safety/security maintenance shall be planned, risk-assessed, evidenced and closed in an OT CMMS — not handled as an IT ticket queue.

2 Cyber MOC belongs at plant floor

Patches, updates, rule changes and configuration changes shall enter the plant MOC process and require a work permit opened/authorized by the lead operator or authorized plant-floor person.

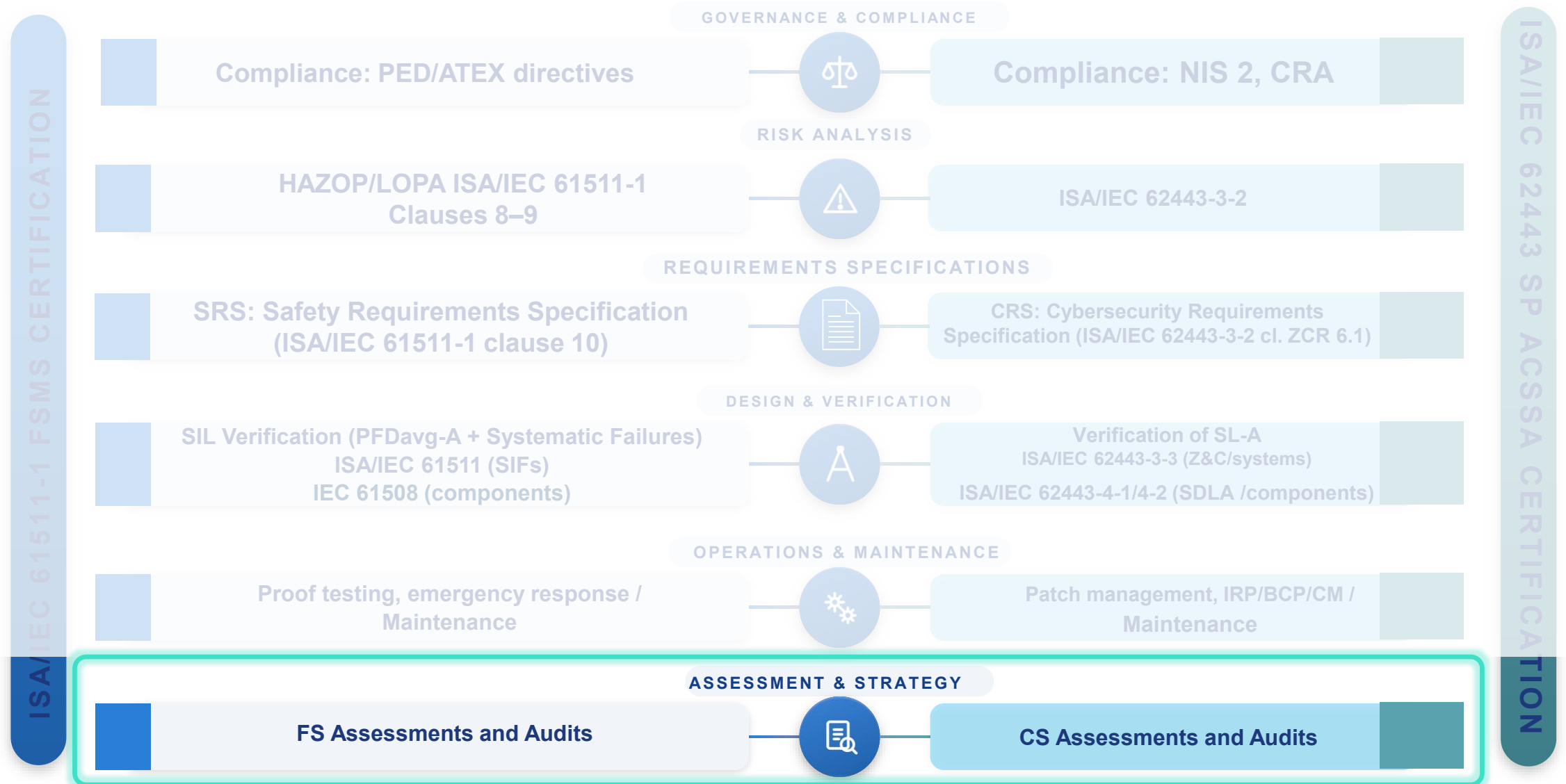
3 One emergency playbook

Integrate the cyber IRP with the plant Emergency Plan; run joint tabletop exercises and drills, then feed lessons back into MOC, risk registers and maintenance plans.

4 Run joint cyber-safety tabletops

At least annually; cyber-induced loss-of-containment scenario; lessons feed both risk registers.

The Parallel Lifecycle



Layered Assurance

LAYER	FUNCTIONAL SAFETY	CYBERSECURITY
1 · Audits	FS audit (61511 §5.2.6.2)	ORG 2.4 SP reviews (62443) - ISMS internal audit (27001)
2 · Assessments	FSA (5 stages)	CSSA as per ISA TR84.00.09
3 · Design reviews	SIS design review	Secure-by-design review
4 · Verification	SIL verification (Cl.7)	SL-Verification: SL-A vs SL-T; 62443-3-3
5 · Validation	SIS safety validation (Cl.15)	Security validation testing
6 · Procurement	Specify Systematic Capability (SC) and provider competencies	Specify requirements based on ISA/IEC 62443-2-4/4-1/4-2
7 · Compliance	Check legal compliance (PED / SEVESO / COMAH)	Check legal compliance (NIS 2 / CRA)

SL verification confirms the required controls are implemented per ISA/IEC 62443-3-3.
SL validation goes further, reviewing the SL verification results and the CRS design requirements, and confirming the risk-assessment assumptions still hold.

No single check is sufficient — assurance has its own defense in depth.

► OPERATIONALISE IT

Review cybersecurity with the same rigor as safety reviews

1 Plan reviews jointly

Plan FS and CS reviews with the same rigor.

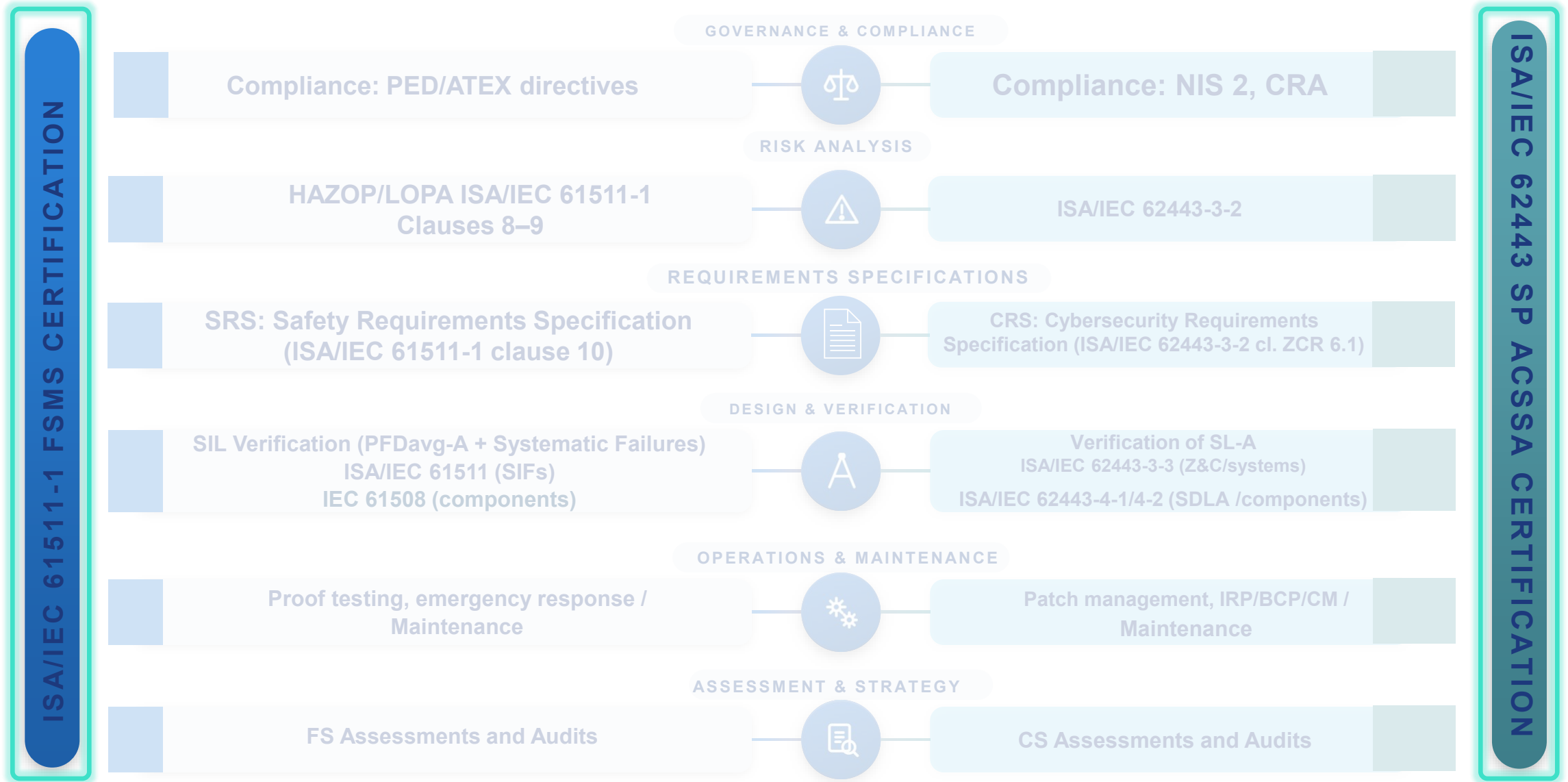
2 Procurement & contracts

Specify 62443-certified components (ISASecure CSA) and FSM-certified suppliers (exida / TÜV); write 4-1/4-2 + 61508 requirements into contracts and the CRS.

3 One evidence pack

Answers NIS2/CRA and the FS audit from the same artifacts — not duplicate binders.

The Parallel Lifecycle



ACSSA: securing the operating site

Filling the critical gap in OT cybersecurity assurance — assessing the deployed operating site itself.



Conformity assessment

Based on ISA/IEC 62443 assurance requirements for the asset owner's deployed IACS.

ISA/IEC 62443

2-1 · 2-4 · 3-2 · 3-3



Critical infrastructure

Designed to scale across automation and control systems in high-consequence sectors.

- Oil & gas
- Chemicals
- Electrical power
- Other industrial sectors



Strategic & boardroom value

Independent verification:

structured check of 62443 security practices.

Regulatory compliance:

tangible due diligence evidence for regulators and insurers.

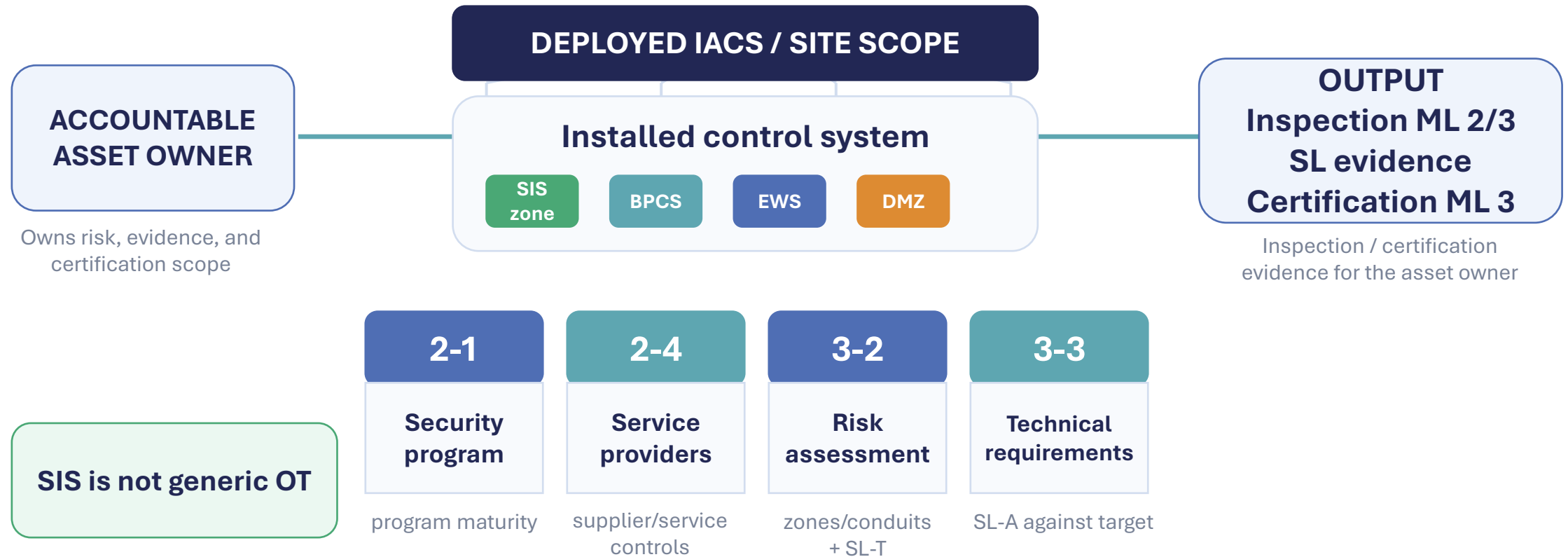
Increased confidence:

gaps and operational risk are visible, owned and tracked.

Core message: ACSSA moves assurance from paper claims to the operating site — scope, evidence, maturity and technical security together.

ACSSA in one picture

ACSSA is asset-owner assurance for a deployed IACS — program, suppliers, risk and technical controls checked together.



Dedicated safety-system treatment: own zone, essential function, controlled configuration mode.

How ACSSA Treats Safety Systems

It's special, not generic.

- 1** **SIS must be its own zone** (62443-3-2 ZCR 3.3 · ACSSA-101 §4.9)
- 2** **SIF protected as an essential function — DoS must not stop it** (ACSSA-101 §4.8)
- 3** **Essential functions stay up even if the zone firewall fails into close/island mode** (ACSSA-101 §4.8)
- 4** **Every zone's essential functions & target SL are required ACSSA submissions — not optional** (ACSSA-300 §4.2)

Build the ACSSA-ready evidence pack while operating



Boundaries

SuC, IACS scope, ingress/egress



Inventory

Assets, versions, owners, criticality



Risk

62443-3-2 risk assessment + safety consequence links



Architecture

Zones, conduits, SL-T, diagrams



Controls

3-3 requirements, hardening, access, backups



Program

2-1 policies, competence, procedures, audits



Providers

2-4 responsibilities, evidence and interfaces



Operations

testing, monitoring, exceptions, MOC, corrective actions

Operationalisation test: Can you trace every security requirement from risk → design → implementation → operation → evidence?

► OPERATIONALISE IT

Evaluate the Security Program using the ACSSA framework

1 **Treat ACSSA like a formal assessment gate**

Define scope, zones/conduits, accountable owner, evidence boundaries and evaluation criteria before the review starts.

2 **Prepare evidence with FSA-level rigor**

Use a controlled evidence pack mapped to 62443-2-1, 2-4, 3-2 and 3-3; assign competent reviewers and retain records.

3 **Close findings through MOC and re-assessment**

Manage gaps as formal actions with owner, due date and risk acceptance; trigger re-evaluation when site, SIS, supplier or architecture changes.

► ASSET-OWNER PLAYBOOK

Five actions for Monday.

- 1 Create the joint team**
Process safety · FS · automation · OT cyber · operations · suppliers
- 2 Integrate risk work**
Cyber prompts in HAZOP; HAZOP consequences in cyber risk assessment
- 3 Reconcile requirements**
One SRS/CRS conflict review before design freeze
- 4 Align assurance gates**
Coordinated FSA/CSSA calendar; cyber in PSSR and MOC
- 5 Build evidence continuously**
ACSSA-ready evidence from daily operations, not after-the-fact binders

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

In OT and Critical Infrastructure, Cybersecurity becomes a Safety Function

When it preserves the ability of the process to remain — or return — to a safe state.

Thank you!



www.ot-knight.com

Visit the ISA blog of this topic [here](#)

Contact: information@ot-knight.com

Bibliography & References

FUNCTIONAL SAFETY

ISA/IEC 61511-1:2016+AMD1:2017 — Framework, definitions, system, HW & app-programming requirements

ISA/IEC 61511-2:2016 — Application guidelines

ISA/IEC 61511-3:2016 — Determination of required SIL

IEC 61508 (series) — E/E/PE functional safety

THE FS ↔ CS BRIDGE

ISA-TR84.00.09 (2024) Part 1 — Cybersecurity related to the Safety Lifecycle

CRISIS MANAGEMENT

BS EN ISO 22361:2022 — Crisis management guidelines

CASE REFERENCE

TRITON / TRISIS — Triconex SIS attack, public threat-intel 2017: Mandiant/FireEye, Dragos

BOOKS

Marszal, E.M. & McGlone, J. — Security PHA Review for Consequence-Based Cybersecurity, 1st ed. (ISA, 2019, ISBN 978-1-64331-000-8)

OT / IACS CYBERSECURITY (ISA/IEC 62443)

62443-2-1:2024 — Security program (asset owners)

PAS 62443-2-2:2025 — Protection scheme (SPR)

62443-2-4:2023 — Security program requirements for IACS service providers

62443-3-2:2020 — Security risk assessment

62443-3-3:2013 — System requirements & SLs

62443-4-1:2018 — Secure product development

62443-4-2:2019 — Component technical requirements

ASSURANCE (ISASECURE ACSSA)

ACSSA-100 — Schemes

101 — Evaluation planning

102 — Baseline/Errata

200 — CAB operations

204 — Symbols/certs

205 — Cert format

300 — Inspection & cert requirements

303 — Sample report

304–305 — Evaluation planning/plan

311 — Evaluation methods

OT-Knight MATERIALS

“Converging IT-OT Cybersecurity Compliance” (panel slides)

“Operationalising ISA/IEC 62443” (ISA-UK conference)

INFORMATION SECURITY (ISO/IEC)

ISO/IEC 27001:2022 — ISMS requirements

ISO/IEC 27002:2022 — Information security controls

ISO/IEC 27005:2022 — Risk management

ISO/IEC 27035:2023 — Incident management

GUIDANCE PAPERS (ISAGCA)

“Securing Operational Technology: Understanding the ISA/IEC 62443 Series from an ISO/IEC 27001 and 27002 Perspective”

“Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for OT Environments”

SUPPORTING REFERENCES

ANSI/ISA-18.2-2016 — Alarm management

NIST CSF — Identify/Protect/Detect/Respond/Recover

NIST SP 800-207 — Zero Trust (cited by TR84.00.09)

ISA-95 / Purdue Model

REGULATORY CONTEXT

NIS2 (EU 2022/2555) · Cyber Resilience Act (EU 2024/2847) · PED/ATEX · Seveso III / COMAH (UK)

List of acronyms

ACSSA — Automation & Control System Security Assurance (ISASecure site scheme)
ANSI — American National Standards Institute
ATEX — Atmosphères Explosibles (EU explosive-atmospheres directive)
BCP — Business Continuity Plan
BPCS — Basic Process Control System
BS EN — British Standard / European Norm
CAB — Conformity Assessment Body
CM — Crisis Management
CMMS — Computerised Maintenance Management System
COMAH — Control of Major Accident Hazards (UK)
CRA — Cyber Resilience Act (EU)
CRS — Cybersecurity Requirements Specification
CS — Cybersecurity
CSA — Component Security Assurance (ISASecure)
CSF — Cybersecurity Framework (NIST)
CSSA — Cyber Security Site Assessment (cyber counterpart to the FSA)
DCS — Distributed Control System
DMZ — Demilitarised Zone
DoS — Denial of Service
EMEA — Europe, Middle East & Africa
ERP — Emergency Response Plan
EU — European Union
EWS — Engineering Workstation
FR — Foundational Requirement (ISA/IEC 62443)

FS — Functional Safety
FSA — Functional Safety Assessment
FSM — Functional Safety Management
FSMS — Functional Safety Management System
H&RA — Hazard & Risk Assessment
HAZOP — Hazard and Operability study
HW — Hardware
IACS — Industrial Automation and Control System(s)
IEC — International Electrotechnical Commission
IPL — Independent Protection Layer
IRP — Incident Response Plan
ISA — International Society of Automation
ISAGCA — ISA Global Cybersecurity Alliance
ISASecure — ISA Security certification program (ISCI)
ISBN — International Standard Book Number
ISCI — ISA Security Compliance Institute
ISMS — Information Security Management System
ISO — International Organization for Standardization
IT — Information Technology
LI-PL — Low-Integrity Protection Layer (non-SIF IPL)
LOPA — Layer of Protection Analysis
ML — Maturity Level
MOC — Management of Change
NIS2 — Network & Information Security Directive 2 (EU)
NIST — National Institute of Standards and Technology (US)
OT — Operational Technology
PAS — Publicly Available Specification

PECB — Professional Evaluation and Certification Board
PED — Pressure Equipment Directive (EU)
PFDavg — Average Probability of Failure on Demand
PHA — Process Hazard Analysis
PLC — Programmable Logic Controller
PSSR — Pre-Startup Safety Review
PSV — Pressure Safety Valve
RA — Risk Assessment
RBJCS — RBJ Consulting and Services (deck author)
RRF — Risk Reduction Factor (RRF-T = target)
SC — Systematic Capability
SCADA — Supervisory Control and Data Acquisition
SDLA — Security Development Lifecycle Assurance (ISASecure)
SIF — Safety Instrumented Function
SIL — Safety Integrity Level
SIS — Safety Instrumented System
SL — Security Level (SL-T target, SL-A achieved, SL-C capability)
SoA — Statement of Applicability (ISO/IEC 27001)
SOC — Security Operations Centre
SP — Special Publication (NIST)
SPR — Security Protection Rating (ISA/IEC 62443-2-2)
SRS — Safety Requirements Specification
SuC — System under Consideration (ISA/IEC 62443-3-2)
TR — Technical Report
UK — United Kingdom
Z&C — Zones and Conduits
ZCR — Zone and Conduit Requirement (ISA/IEC 62443-3-2)