
Cybersecurity & Functional Safety Guideline

How ISA TR84.00.09 Defines and Supports the Interplay

Revision 1.0

Product: Guideline / Reference Document
Project name: ISA TR84.00.09 — Safety & Security Integration
Customer: Internal / Reference Distribution
Project no.: SSS-REF-2026-001

Status: Released

	Role	Name / Org. Unit
Author/Responsible	Security Services	Markus Steinmetz / SSS
Verification/Review		
Verification/Review		
Approval		

Template Change History

Version	Date	Author	Change description
1.0	08.04.2026	Markus Steinmetz	Document created

Table of Contents

Template Change History.....	2
Table of Contents.....	2
1. Overview	3
1.1 Change History	3
1.2 Purpose.....	3
1.3 Definitions.....	3
1.4 Abbreviations.....	3
1.5 References.....	4
2. Why This Guideline Exists.....	5
2.1 Document status and editions	5
3. The Core Concepts in Plain Language	5
3.1 What ISA TR84.00.09 actually addresses.....	5
3.2 The key insight: cyber attacks behave like common-cause failures	6
3.3 Two lifecycles, one project	6
4. How the Two Lifecycles Interact.....	6
5. The Cybersecurity Requirements Specification (CRS)	7
6. Roles, Competencies and Responsibilities	8
7. Practical Guidance for Product Development.....	9
7.1 Build the two cases together	9
7.2 Document your security context assumptions	9
7.3 Treat security updates as a safety-relevant change.....	9
7.4 Avoid security controls that create new safety hazards	10
8. Common Pitfalls and How to Avoid Them.....	10
9. Summary	10
ANNEX.....	11

1. Overview

1.1 Change History

Version	Date	Author	Change description
1.0	08.04.2026	Markus Steinmetz	Initial release

1.2 Purpose

This guideline summarizes ISA TR84.00.09 — the technical report issued by the ISA84 committee to bridge functional safety (IEC 61511) and industrial cybersecurity (ISA/IEC 62443). It explains, in language accessible to both specialists and laypeople, how the two disciplines are intended to work in parallel along the safety lifecycle, what artefacts they exchange, and how product developers, integrators, asset owners and engineers can apply the guidance in practice.

The document is intended as an internal reference for SSC consulting engagements that touch process safety, safety instrumented systems and operational technology cybersecurity. It is not a substitute for the original technical report or the underlying standards.

1.3 Definitions

Definition	Description
PSCAI	Process Safety Controls, Alarms and Interlocks — instrumented systems whose function is to keep a process safe; includes the SIS as the most rigorously engineered subset.
SIS	Safety Instrumented System — a system composed of sensors, logic solver and final elements that performs one or more safety instrumented functions.
Common-cause failure	A failure mechanism that simultaneously defeats multiple protection layers because they share an element (in this context, a shared digital asset exploited by an attacker).
Zone / Conduit	Per IEC 62443-3-2, a logical or physical grouping of assets sharing common security requirements (zone), connected by controlled communication paths (conduits).
CRS	Cybersecurity Requirements Specification — the document that translates risk assessment conclusions into verifiable security requirements for the system under consideration.

1.4 Abbreviations

Abbreviation	Description
BPCS	Basic Process Control System
CRS	Cybersecurity Requirements Specification
CSA	Cybersecurity Assessment

Abbreviation	Description
FAT / SAT	Factory Acceptance Test / Site Acceptance Test
FSA	Functional Safety Assessment
HAZOP	Hazard and Operability Study
IACS	Industrial Automation and Control Systems
LOPA	Layer of Protection Analysis
MoC	Management of Change
OT / IT	Operational Technology / Information Technology
PFD / PFH	Probability of Failure on Demand / per Hour
PHA	Process Hazard Analysis
PSCAI	Process Safety Controls, Alarms and Interlocks
SCAI	Safety Controls, Alarms and Interlocks (legacy term)
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SL-T / SL-C	Target Security Level / Capability Security Level
SRS	Safety Requirements Specification

1.5 References

Reference abbreviation	Name / Issue
ISA-TR84.00.09-2024	ISA-TR84.00.09-2024 Part 1, Cybersecurity Related to the Safety Lifecycle. International Society of Automation, 2024.
IEC 61511	ANSI/ISA-84.00.01 / IEC 61511 (all parts), Functional safety — Safety instrumented systems for the process industry sector.
ISA/IEC 62443	ANSI/ISA-62443 / IEC 62443 series, Security for industrial automation and control systems — in particular Parts 2-1, 2-4, 3-2, 3-3, 4-1 and 4-2.
IEC 61508	IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems.
IEC 62443-3-2:2020	Security risk assessment for system design — references ISA-TR84.00.09 for guidance on the Cybersecurity Requirements Specification (CRS).

2. Why This Guideline Exists

Industrial automation systems used to be safe because they were isolated. A safety instrumented system (SIS) sat behind locked cabinet doors, communicated over proprietary buses, and was assessed only against random hardware failures and systematic design faults. That world no longer exists. Modern safety controls share networks, operating systems, engineering tools and even hardware platforms with the basic process control system, the historian and, indirectly, the corporate IT environment. A successful cyber-attack can therefore do something that classical functional safety analysis never anticipated: it can simultaneously create a hazardous demand and disable the protection layer that is supposed to respond to it.

This is not a theoretical concern. The 2017 TRITON / TRISIS attack on a petrochemical facility in Saudi Arabia targeted Triconex safety controllers directly, with the apparent intent of forcing the plant into an unsafe state while bypassing its safety functions. That single incident made it impossible to keep treating cybersecurity and functional safety as separate disciplines that meet only in the project handover meeting.

ISA TR84.00.09 is the technical report that the ISA84 committee — responsible for the ANSI/ISA 84 / IEC 61511 family of functional safety standards — wrote precisely to bridge this gap. It explains, step by step, how to weave cybersecurity considerations into every phase of the functional safety lifecycle, and how to do so in a way that is consistent with the ANSI/ISA 62443 (IEC 62443) cybersecurity standards. This guideline summarizes what the technical report says, what it means in practice, and how laypeople and specialists alike can use it.

2.1 Document status and editions

The original ISA TR84.00.09 was published in 2013 and revised in 2017. A substantially redrafted edition, ISA-TR84.00.09-2024 Part 1 “Cybersecurity Related to the Safety Lifecycle,” was issued in 2024 and is the current reference. The 2024 edition modernizes terminology — notably moving from “Safety Controls, Alarms and Interlocks / SCAI” toward “Process Safety Controls, Alarms and Interlocks / PSCAI” — aligns more tightly with the current ISA/IEC 62443 series, and incorporates lessons learned from real-world incidents. The conceptual framework, however, has been stable across editions: integrate cybersecurity into the safety lifecycle, treat cyber threats as a potential common-cause failure mechanism, and assign clear responsibilities across the OT/IT boundary.

3. The Core Concepts in Plain Language

3.1 What ISA TR84.00.09 actually addresses

The technical report has a deliberately narrow scope: the cybersecurity of instrumented systems whose job is to keep a process safe. In current terminology these are PSCAI — Process Safety Controls, Alarms and Interlocks — and they include the SIS as the most rigorously engineered subset. The report does not try to redefine functional safety, and it does not try to be a complete cybersecurity standard. It sits in the overlap between IEC 61511 (functional safety for the process

industries) and the ISA/IEC 62443 series (cybersecurity for industrial automation and control systems), and it tells the reader how to apply both at the same time without contradictions, gaps or duplicated effort.

3.2 The key insight: cyber-attacks behave like common-cause failures

Functional safety analysis is built on the assumption that protection layers are independent. Layer of Protection Analysis (LOPA), for example, only credits an independent protection layer if it cannot be defeated by the same event that caused the initial demand. A cyber-attack breaks this assumption in a way that classical failure modes cannot. A single attacker, exploiting a single shared vulnerability — a common engineering workstation, a shared Windows domain, a common protocol stack, a shared maintenance laptop — can simultaneously initiate a hazardous condition in the basic process control system and prevent the SIS from responding to it. From a hazard analysis point of view, this is a common-cause failure with a very high consequence and a probability that is hard to estimate but is certainly not negligible. ISA TR84.00.09 makes this explicit and tells the reader to address it during the hazard and risk assessment, not after the fact.

3.3 Two lifecycles, one project

The functional safety lifecycle in IEC 61511 and the cybersecurity lifecycle in ISA/IEC 62443 look superficially similar. Both start with hazard or risk analysis, both define requirements, both implement and verify, both operate and maintain, and both eventually decommission. ISA TR84.00.09 maps these lifecycles phase-by-phase and identifies, at each phase, what needs to flow between them. The result is not a merged lifecycle but two lifecycles that exchange information at well-defined points. This matters because the people, the competencies and the verification methods are different on each side and forcing them into a single process tends to dilute both.

4. How the Two Lifecycles Interact

The heart of ISA TR84.00.09 is a phase-by-phase mapping that shows where functional safety and cybersecurity activities meet, what artefacts they exchange, and which discipline owns the result. The table below summarizes this mapping in a form that can be used as a project checklist.

Lifecycle phase	Functional safety activity (IEC 61511)	Linked cybersecurity activity (ISA/IEC 62443) per TR84.00.09
Hazard & risk analysis	PHA / HAZOP / LOPA identifies process hazards, initiating events and required risk reduction.	Add cyber-initiating events as a credible cause; treat compromise of shared digital assets as a potential common-cause failure between BPCS and SIS.
Allocation of safety functions	Assign required risk reduction to protection layers; determine SIL targets for each safety instrumented function.	Define zones and conduits per IEC 62443-3-2; assign target Security Levels (SL-T) to the zone(s) containing PSCAI; ensure independence between the BPCS zone and the SIS zone.

Lifecycle phase	Functional safety activity (IEC 61511)	Linked cybersecurity activity (ISA/IEC 62443) per TR84.00.09
Safety / cybersecurity requirements	Produce the Safety Requirements Specification (SRS) describing each SIF, its SIL, response time, fail-safe state and proof-test interval.	Produce a Cybersecurity Requirements Specification (CRS) for the same scope. ISA TR84.00.09 explicitly defines the recommended elements of the CRS; IEC 62443-3-2 references this guidance.
Design & engineering	Select certified devices, design the SIS architecture, perform PFD/PFH calculations, design proof testing.	Select components meeting the required SL-C (IEC 62443-4-2); verify that countermeasures (firewalls, data diodes, authentication, hardening) do not impair the safety function or its response time.
Integration & FAT/SAT	Factory and site acceptance testing of the safety functions; validation against the SRS.	Cybersecurity verification: vulnerability scans, configuration review, penetration testing of the safety zone, validation against the CRS. Tests must not invalidate safety certifications.
Operation & maintenance	Proof tests, demand records, bypass management, management of change, periodic functional safety assessment.	Patch management, vulnerability monitoring, account and access management, security event logging, periodic cybersecurity assessment. Any change is reviewed by both disciplines under one MoC process.
Decommissioning	Safe shutdown, removal and archival of safety documentation.	Secure data wipe of devices, revocation of credentials and certificates, controlled disposal to prevent information leakage.

The single most important takeaway from this mapping is the second row: the assignment of zones and conduits. ISA TR84.00.09 strongly recommends that the SIS reside in its own security zone, separated from the BPCS zone by a controlled conduit. This is the cyber equivalent of the long-standing IEC 61511 principle of separation between the BPCS and the SIS, and it preserves the independence that LOPA depends on. Where this separation is not feasible — for example in older integrated platforms — the technical report requires that the loss of independence be analyzed explicitly and compensated by other measures.

5. The Cybersecurity Requirements Specification (CRS)

If a single artefact captures the spirit of ISA TR84.00.09, it is the Cybersecurity Requirements Specification. The CRS is to cybersecurity what the SRS is to functional safety: a document that translates the conclusions of the risk assessment into concrete, verifiable requirements that the design must meet and that operations must maintain. ISA TR84.00.09 lists the recommended contents of the CRS, and IEC 62443-3-2 explicitly points to TR84.00.09 for this guidance.

A well-formed CRS for a PSCAI/SIS scope typically contains the following elements:

- A description of the system under consideration, its boundaries, and the zones and conduits that contain it.
- The target Security Level (SL-T) for each zone, derived from the cyber risk assessment and consistent with the SIL targets of the safety functions in that zone.
- Functional cybersecurity requirements: identification and authentication, use control, data integrity, confidentiality, restricted data flow, timely response to events and resource availability — the seven foundational requirements of the IEC 62443 series.
- Constraints arising from functional safety: requirements that cybersecurity measures must not increase the response time of safety functions, must not introduce single points of failure, and must not interfere with proof testing or bypass procedures.
- Assumptions about the operating environment: physical security, trusted personnel, network architecture, expected threat actors and their capabilities.
- Verification and validation requirements, including the methods and acceptance criteria for demonstrating that the implementation meets the CRS.
- Maintenance and operational requirements, including patching, account management, logging, monitoring, incident response, and the cybersecurity aspects of management of change.

The CRS is not a separate document living in a different folder from the SRS. ISA TR84.00.09 explicitly accepts that the CRS may be a section of an existing safety document, provided that its content is complete and traceable. What matters is that every cybersecurity requirement can be traced back to a risk and forward to a verification.

6. Roles, Competencies and Responsibilities

One of the practical reasons functional safety and cybersecurity tend to be poorly integrated is that the people involved come from different organizational silos with different cultures. Functional safety engineers report to engineering or operations and think in terms of hazards, demands and proof tests. Cybersecurity engineers often report to IT and think in terms of vulnerabilities, threat actors and patch cycles. ISA TR84.00.09 does not prescribe an organizational chart, but it does insist that responsibilities be assigned explicitly and that the relevant competencies be available across the lifecycle.

Role	Primary responsibility	Interface with the other discipline
Asset owner / operator	Defines tolerable risk, owns the integrated risk picture, approves SL-T and SIL targets, owns the management of change process.	Ensures that the safety case and the security case are reviewed together, not in isolation.
Functional safety engineer	Hazard and risk analysis, SIL determination, SRS, design verification, proof testing, periodic FSA.	Provides the list of safety functions and their criticality to the cybersecurity team; reviews proposed cyber controls for safety impact.

Role	Primary responsibility	Interface with the other discipline
Cybersecurity engineer	Threat and risk assessment, zone and conduit design, CRS, component selection per SL-C, hardening, verification, periodic CSA.	Translates safety constraints into cyber requirements; advises on common-cause analysis where shared digital assets exist.
Product supplier	Develops devices and software per IEC 62443-4-1 (secure development) and IEC 62443-4-2 (component capabilities), and per IEC 61508 / 61511 for functional safety.	Provides clear documentation of security capabilities, security context assumptions, and any constraints relevant to functional safety certification.
Integrator / service provider	Implements the system per the SRS and CRS, performs FAT/SAT, supports operation per IEC 62443-2-4.	Single point of accountability for the integrated system meeting both safety and security acceptance criteria.

7. Practical Guidance for Product Development

For organizations developing components that may end up inside a PSCAI — sensors, logic solvers, final elements, gateways, engineering tools — ISA TR84.00.09 has indirect but important consequences. Even if your product is not itself a SIS, if it can be used in or near one, your customers will increasingly expect you to support their integrated safety-and-security lifecycle. The following practical points usually make the largest difference.

7.1 Build the two cases together

Functional safety certification (typically against IEC 61508) and cybersecurity certification (typically against IEC 62443-4-1 for the development process and IEC 62443-4-2 for the product capabilities) should be planned as a single program, not as two sequential audits. The artefacts overlap: hazard analysis informs threat analysis, the safety manual informs the security guidelines, the verification plan covers both. Organizations that try to bolt cybersecurity on after a completed safety certification usually pay for it twice.

7.2 Document your security context assumptions

IEC 62443-4-2 requires every product to declare its assumed security environment: which threats it protects against, which it does not, and what compensating controls the integrator must provide. ISA TR84.00.09 expects these assumptions to be visible to the safety engineer of the receiving system, because they directly affect whether the device is usable in a given safety zone. Make these assumptions explicit, machine-readable where possible, and easy to compare against a target SL-T.

7.3 Treat security updates as a safety-relevant change

A firmware update that fixes a vulnerability is, from the point of view of IEC 61511 management of change, a modification of a safety-related component. ISA TR84.00.09 makes the point that update procedures must be designed so that they can be applied without invalidating the safety certification — which means, in practice, that updates must be cryptographically signed, that

rollback must be controlled, that the device must be able to demonstrate its post-update integrity, and that the update process itself must be auditable. The product features that support this are the same ones that EMB3D and IEC 62443-4-2 list under “secure update” and “integrity of the boot process.”

7.4 Avoid security controls that create new safety hazards

This is the failure mode that ISA TR84.00.09 warns about most consistently. A well-meaning cybersecurity measure — forcing reauthentication during an alarm condition, blocking a diagnostic port that engineering needs for emergency troubleshooting, encrypting a communication channel in a way that adds latency to a fast safety loop — can defeat the safety function it is supposed to protect. The technical report’s answer is not “don’t apply security controls” but “validate every security control against the safety requirements before you ship it.” This is also why the CRS contains an explicit section on safety constraints.

8. Common Pitfalls and How to Avoid Them

- **Treating cybersecurity as a post-design add-on.** By the time the safety design is frozen, the cheap opportunities to influence zone boundaries, network topology and component selection are gone. Bring cybersecurity into the hazard analysis, not into the FAT.
- **Confusing SIL with SL.** Safety Integrity Level and Security Level are not the same thing and there is no fixed mapping between them. A SIL 3 function may sit in a zone with an SL-T of 2 or 3 depending on the threat environment. Each is determined by its own risk assessment.
- **Assuming the SIS is air-gapped.** Almost no modern SIS is truly air-gapped; engineering workstations, USB drives, vendor maintenance laptops and shared historians create paths that need to be analyzed and controlled.
- **Letting IT and OT run separate change processes.** A single management of change process covering both safety and cybersecurity changes is one of the most effective controls the technical report recommends.
- **Neglecting the operate-and-maintain phase.** Most cyber risk to a PSCAI accumulates after handover: unpatched vulnerabilities, drifted configurations, expired certificates, departed personnel with active accounts. The lifecycle does not end at SAT.

9. Summary

ISA TR84.00.09 exists because functional safety and cybersecurity can no longer be managed as independent disciplines for any digital safety system. Its central messages are simple, even if the implementation is not: cyber-attacks can act as common-cause failures and must be considered during hazard analysis; the safety lifecycle and the cybersecurity lifecycle should be run in parallel with explicit information exchange at each phase; the Cybersecurity Requirements

Specification is the bridging artefact that ties cyber risk to verifiable design requirements; cybersecurity controls must be validated against safety constraints before they are applied; and responsibilities must be assigned explicitly across the asset owner, the safety engineer, the cybersecurity engineer, the product supplier and the integrator.

For laypeople, the key insight is that safety in a digitally connected plant is no longer only about random hardware failures and software bugs; it now includes deliberate attackers, and the same engineering rigor that has long been applied to safety must now be applied to security in parallel. For experts, ISA TR84.00.09 provides the structural framework that lets the two well-developed disciplines of functional safety and industrial cybersecurity work together without contradiction, double effort or gaps.

Read together with IEC 61511 (functional safety for the process industries) and the ISA/IEC 62443 series (industrial automation and control system security), ISA TR84.00.09 is the document that turns “safety and security” from a slogan into a workable engineering practice.

ANNEX

— *No annex content for this revision* —

===== END OF DOCUMENT =====