From Vendor SBOM Gap to SIS Independence Violation: A Cross-Standards Framework for Translating OT Cybersecurity Field Evidence into IEC 62443-4-1, IEC 62443-3-3, and IEC 61511 Requirements

Jherrod Thomas

I. Introduction

The convergence of information-technology and operational-technology environments has accelerated the exposure of programmable logic controllers (PLCs), distributed control systems, and safety-instrumented systems (SIS) to threat actors whose targeting now extends beyond espionage to deliberate disruption of physical processes [1], [2]. Two regulatory actions issued in the first half of 2026 illuminate a structural problem in how the IEC 62443 and IEC 61511 standards families translate from clause text to enforceable artifacts across the supplier–integrator–asset-owner boundary.

The first is the Cybersecurity and Infrastructure Security Agency advisory ICSA-26-134-14 of 14 May 2026, which rates the Siemens SENTRON 7KT PAC1261 Data Manager at a Common Vulnerability Scoring System (CVSS v3.1) base score of 9.1 for a request-smuggling defect that allows full device takeover over the device's HTTP interface [3]. The advisory traces the defect to CVE-2025-22871, a request-smuggling flaw in the upstream Go net/http package caused by improper handling of bare line-feed characters in chunked-transfer-encoding chunk-size lines; the defect was disclosed on 1 April 2025, patched in Go 1.23.8 and 1.24.2, and assigned a Common Weakness Enumeration identifier of CWE-444 [4], [5]. Thirteen months elapsed between the upstream patch and the appearance of the vulnerable component in a deployed industrial device [3], [4].

The second is the joint advisory AA26-097A of 7 April 2026, in which the National Security Agency, Federal Bureau of Investigation, and Cybersecurity and Infrastructure Security Agency document a persistent campaign by Iranian-affiliated cyber actors operating under the persona CyberAv3ngers, compromising Rockwell Automation CompactLogix, ControlLogix, GuardLogix, DriveLogix, and Micro850 PLCs across United States water, wastewater, energy, and government facilities by exploiting authentication-bypass CVE-2021-22681 [6], [7]. The actors used leased third-party hosting and Rockwell Studio 5000 Logix Designer to establish accepted control sessions to victim PLCs, then exercised process-disruption primitives [6]. The campaign extends an earlier wave that compromised at least 75 Unitronics Vision Series PLCs in U.S. water utilities between November 2023 and January 2024 [7], [8].

The two events differ substantially in attacker model, exposed asset class, and ICS Purdue Level (Level 1 for the Rockwell PLCs, Level 2.5–3 for the Siemens energy-metering data manager) [1], [9]. The common engineering observation, however, is that the gap is not in any single standards clause. The Go net/http defect is documented and patched in the upstream open-source repository [4], [5]; IEC 62443-4-1 §SM-3 requires a vendor to maintain a software bill of materials and a defect-management feed [10]; IEC 62443-3-3 §SR-1.1 requires segmentation of access between zones [11]; and IEC 61511-1 §11.2.10 requires the SIS logic solver to be operationally independent of the basic process control system (BPCS) [12]. The gap is in the unowned space *between* these clauses — the supplier did not ingest the upstream defect feed in a timeframe consistent with §SM-3, the integrator did not segment the device into a zone whose conduit rules would have isolated a takeover, and the asset owner did not verify SIS independence after the device entered an at-risk zone [3], [6], [10], [11], [12].

The contributions of this paper are as follows. First, we propose a six-step framework that ingests publicly available incident evidence and produces IEC 62443-4-1 secure-development-lifecycle residuals, IEC 62443-3-3 zone-and-conduit controls, and IEC 61511 SIS-independence requirements as audit-ready artifacts. Second, we demonstrate the framework on a joint vendor-and-asset-owner thread combining the SENTRON 7KT vendor-side defect and the Rockwell PLC operator-side compromise. Third, we provide one numbered equation for cross-standards residual-risk aggregation, one fault tree for the joint failure mode, and one comparative table of zone-design styles under IEC

62443-3-2. The framework is intended as a reviewer-grade input for operators preparing for the European Union Cyber Resilience Act reporting obligations effective 11 September 2026 [13] and for asset-owner audits under Transportation Security Administration Security Directive 1580/82 Series [14].

The remainder of this paper is organized as follows. Section II reviews prior art in PLC security, IEC 62443 zone-and-conduit modeling, SIS cybersecurity, and intrusion detection. Section III presents the six-step framework. Section IV applies the framework to the joint SENTRON 7KT and CyberAv3ngers thread. Section V discusses limitations and threats to validity. Section VI concludes with directions for future work.

II. Background and Related Work

A. The IEC 62443 Family

IEC 62443 is the principal international standard family for cybersecurity of industrial automation and control systems and is organized into four parts. Parts 1-x define terminology and concepts; Parts 2-x address the asset-owner program; Parts 3-x address the system integrator and the as-built system; Parts 4-x address the product supplier [15], [16]. The two parts most directly implicated in the 2026 events are IEC 62443-4-1, which specifies the secure-product-development-lifecycle (SDL) requirements for product suppliers across eight practices — security management, security requirements, security by design, secure implementation, security verification and validation, security defect management, security update management, and security guidelines — and IEC 62443-3-3, which specifies system-level security requirements organized as seven foundational requirements (FR-1 through FR-7) and graded into four security levels (SL-1 through SL-4) [10], [11], [17]. The 62443-4-1 §SM-3 practice requires the supplier to maintain a software bill of materials (SBOM) and to operate a defect-management feed that ingests upstream vulnerability disclosures and prioritizes them by exploitability and impact [10]. Onekey and the Industrial Cyber community of practice have published guidance for operationalizing §SM-3 against the CISA Minimum Elements for an SBOM [18], [19].

B. Zones, Conduits, and the IEC 62443-3-2 Risk Process

The zone-and-conduit construct is the architectural language of IEC 62443. A zone is a logical or physical grouping of assets that share a common protection requirement; a conduit is a controlled communication channel between zones, with explicitly enumerated protocols, source-and-destination addresses, and inspection points [20]. Pinto and colleagues survey the security aspects of zones and conduits and observe that the most common asset-owner-side failure mode is *zone aggregation creep* — the practice of placing administrative-network assets and process-network assets in the same nominal zone for operational convenience — which collapses the conduit-rule enforcement that the architecture is supposed to provide [21]. The IEC 62443-3-2 risk process couples zone design to a target security level (SL-T) derivation [22].

C. PLC Security and the Threat Model

López-Morales and colleagues, in the 2024 USENIX Security Symposium *Systematization of Knowledge: Security of Programmable Logic Controllers*, present a comprehensive taxonomy of PLC attacks organized into four Access Levels (AL0 through AL3) and the ICS² Matrix of adversary tactics [23]. Falas and colleagues, recipients of the 2024 IEEE Outstanding Paper Award for the *IEEE Open Journal of the Industrial Electronics Society*, review the state of PLC security with attention to code verification, firmware investigation, traffic monitoring, and suspicious-state checking [24]. Zhang and co-authors survey PLC vulnerabilities, attacks, detections, and forensics, identifying program-, firmware-, and memory-resident weaknesses as the dominant vulnerability classes [25]. Geng and colleagues present a three-year empirical study of run-time PLC security in deployed environments [26]. Tsiknas and colleagues provide an overview of PLC security in industrial control systems with a treatment of the air-gap myth [27].

D. Safety-Instrumented-System Cybersecurity

IEC 61511-1:2016 and its 2017 Amendment 1 introduced an explicit cybersecurity risk-assessment requirement (Clause 8.2.4) and an explicit independence requirement between the SIS and the basic process control system (Clause 11.2.10) [12]. The standard cross-references IEC 62443 and ISA TR84.00.09 for detailed cybersecurity guidance [28]. The 2017 TRITON/TRISIS attack on a Saudi petrochemical refinery, which reprogrammed Schneider Electric Triconex SIS controllers and resulted in an unintended shutdown, is the canonical evidence that SIS controllers are explicitly targeted [29], [30]. Friedberg and colleagues develop an extensive set of criteria for safety and cybersecurity co-evaluation of cyber-physical systems and observe that independence verification is the most under-evaluated criterion in field deployments [31].

E. Intrusion Detection at the ICS Layer

Conti and colleagues, in a 2024 *International Journal of Information Security* survey, classify machine-learning intrusion-detection methods for ICS into network-level and process-level approaches [32]. Kus and colleagues argue that the published benchmarks systematically overstate the practical performance of machine-learning IDS in operational deployments because the benchmark distributions do not represent the rare-event distribution of true ICS compromise [33]. Shang and colleagues present a deep convolutional autoencoding transformer network for ICS anomaly detection with state-of-the-art benchmark results [34].

III. Approach: A Six-Step Framework

We propose a six-step framework that ingests publicly available incident evidence and produces three classes of audit-ready artifacts: IEC 62443-4-1 secure-development-lifecycle residuals, IEC 62443-3-3 zone-and-conduit controls, and IEC 61511 safety-instrumented-system independence requirements. The stage flow proceeds from public incident artifacts (CISA advisories, CVE records, SBOM dependency graphs) through six numbered stages to clause-anchored requirements in IEC 62443-4-1, IEC 62443-3-3, and IEC 61511.

A. Step S1 — Incident Evidence Capture

The first step ingests three classes of evidence: the public regulator advisory (CISA, NSA, or equivalent national authority), the upstream CVE and CWE records, and the vendor-published SBOM and security advisory. For the 2026 events of Section IV we use [3], [4], [5] for the SENTRON 7KT thread and [6], [7] for the CyberAv3ngers thread. The framework explicitly excludes proprietary post-incident forensic reports because the audience for the resulting artifacts must be able to re-verify the framework from public sources alone, consistent with the reproducibility expectation of an IEC 62443 conformity assessment [10], [11].

B. Step S2 — Cross-Standards Defect Localization

The second step localizes the defect against the IEC 62443 and IEC 61511 clause structure. The localization produces a tuple (clause, evidence-id, residual-type) for each implicated clause. For the SENTRON 7KT thread, the dominant tuple is (IEC 62443-4-1 §SM-3, CVE-2025-22871, *SBOM-feed defect*); for the CyberAv3ngers thread the dominant tuple is (IEC 62443-3-3 §SR-1.1, AA26-097A §Mitigations, *zone-aggregation creep*) [3], [6], [10], [11]. The framework requires that every public-evidence claim be reduced to at least one (clause, evidence-id, residual-type) tuple before the analyst proceeds to Step S3.

C. Step S3 — Residual-Risk Aggregation

The third step aggregates per-clause residuals into a system-level residual-risk index R_s. We adopt a multiplicative-then-additive aggregation that reflects the layered defense-in-depth expectation of IEC 62443 and IEC 61511 [12], [16], [21]:

$$R_s = 1 - \prod_{i=1}^{L} [1 - p_i \cdot (1 - c_i)] + \kappa_{cc} \qquad (1)$$

where the index i enumerates the L defense layers (vendor SDL, integrator zone control, asset-owner SIS independence, runtime intrusion detection), p_i is the probability that layer i fails to detect or contain the threat conditioned on the threat scenario, c_i is the effective coverage of layer i for the threat class, and κ_{cc} is a common-cause derating term that captures correlated failures across layers (for example, the same vendor whose SBOM feed is delayed also publishes the zone-design reference architecture used by the integrator). The framework requires $\kappa_{cc} \geq 0.05$ when the vendor and the integrator are within the same parent organization and ≥ 0.02 otherwise [21], [23], [27]. We discuss the sensitivity of (1) to κ_{cc} in Section V.

D. Step S4 — IEC 62443-4-1 SDLC Residual Derivation

The fourth step is the principal contribution of the framework on the supplier side. For each tuple localized at IEC 62443-4-1 in Step S2, we derive a *secure-development-lifecycle residual* — a defect in the practice of one of the eight 62443-4-1 practices that must be closed before the supplier's certification can be re-affirmed [10]. For the SBOM-feed defect class, the residual is closed by demonstrating that the supplier (i) has an ingestion contract for the upstream defect feed (in this case, the Go security mailing list) with a target mean-time-to-ingest below the time between upstream patch and exploitation in the wild, (ii) has a triage process that maps an upstream CVE to a per-product impact assessment within the same window, and (iii) operates a publication channel that distributes the patched firmware before the upstream advisory is publicly listed by a national agency [4], [10], [18]. The framework specifies a fifteen-day target for (i)+(ii)+(iii) under CISA Known Exploited Vulnerabilities Catalog inclusion and a sixty-day target otherwise [35].

E. Step S5 — IEC 62443-3-3 Zone-and-Conduit Control Derivation

The fifth step is the principal contribution of the framework on the integrator side. For each tuple localized at IEC 62443-3-3 in Step S2, we derive a *zone-and-conduit control* — an architectural change to the as-built system that closes the conduit path that enabled the compromise [11], [20], [22]. For the CyberAv3ngers thread, the derived controls include (i) the placement of process-network PLCs in a Security Level 3 zone with conduits restricted to the engineering-workstation zone via an authenticated and integrity-protected protocol, (ii) the prohibition of inbound conduit rules from leased third-party hosting environments, and (iii) the deployment of an explicit Foundational Requirement 1 (Identification and Authentication Control) enforcement at the conduit edge per IEC 62443-3-3 §SR-1.1 and §SR-1.2 [11].

Table I summarizes three representative zone-design styles and their fit to the framework.

TABLE I: TABLE I. Representative zone-design styles, their primary failure-mode coverage, and their fit to the proposed framework. Adapted from [20], [21], [22].

Zone style	Primary coverage	Target SL	Fit to framework
Flat operations zone	None — anti-pattern	SL-1	Fails S5 by construction
Purdue-level segmentation	Lateral movement L3 to L1	SL-2 / SL-3	S5 baseline for non-SIS zones
SIS-isolated zone (61511)	BPCS-to-SIS independence	SL-3 / SL-4	S5+S6 joint enforcement for SIS

F. Step S6 — IEC 61511 SIS-Independence Requirement Derivation

The sixth step is the principal contribution of the framework on the asset-owner side. For each tuple in which the defect path could lead to compromise of a basic process control function whose failure is mitigated by an SIS, we derive an IEC 61511-1 §11.2.10 *independence requirement* — a constraint that the SIS logic solver, sensors, and final elements be operationally independent of the BPCS pathways implicated by the defect [12]. For the CyberAv3ngers thread on a water-treatment site, the derived requirements include (i) that the chemical-dosing SIS logic solver share no engineering-workstation conduit with the BPCS PLCs, (ii) that the SIS communication be on a separate network segment with an air-gap or unidirectional gateway, and (iii) that the SIS bypass-key practice be subject to a cybersecurity risk assessment under IEC 61511-1 §8.2.4 [12], [28], [29]. The framework also requires verification of the *post-compromise residual SIL* — the safety integrity level achievable by the SIS *under the assumption that the BPCS has been adversarially compromised* — and treats a reduction of more than one SIL band as a finding that blocks return-to-service [12], [29], [31].

IV. Worked Example: A Joint Vendor-and-Owner Thread on a Water Utility

We apply the framework to a hypothetical water-treatment utility whose chemical-dosing process is controlled by a Rockwell CompactLogix PLC in the BPCS, supervised by a Triconex-class SIS, and instrumented for energy submetering by a Siemens SENTRON 7KT PAC1261 Data Manager [3], [6], [29]. The hypothetical functional thread is *maintain free-chlorine residual within the operating window during a sustained adversary presence in the engineering-workstation network.*

A. S1 — Evidence Capture

The vendor-side evidence is CVE-2025-22871 in the Go net/http package, with public disclosure on 1 April 2025 and patched releases Go 1.23.8 and Go 1.24.2 [4], [5]. The CISA advisory ICSA-26-134-14 lists the SENTRON 7KT PAC1261 Data Manager as carrying the vulnerable component thirteen months after upstream patch, with CVSS v3.1 base score 9.1, exploit-prediction inputs consistent with active interest, and no public Siemens security advisory at the time of the CISA listing [3]. The asset-owner-side evidence is the joint advisory AA26-097A, which lists the CyberAv3ngers persona, the Iranian Revolutionary Guard Corps Cyber-Electronic Command attribution, the U.S. Treasury Office of Foreign Assets Control sanctions of February 2024, and the State Department $10-million bounty [6], [7]. The advisory enumerates Rockwell CompactLogix, ControlLogix, GuardLogix, DriveLogix, and Micro850 as in-scope and identifies leased third-party hosting and the use of Studio 5000 Logix Designer as the dominant exploit pattern [6].

B. S2 — Cross-Standards Defect Localization

The dominant tuples are (IEC 62443-4-1 §SM-3, CVE-2025-22871, *SBOM-feed defect*), (IEC 62443-3-3 §SR-1.1, AA26-097A §Mitigations, *zone-aggregation creep*), (IEC 61511-1 §11.2.10, derived from the joint thread, *post-compromise SIL erosion*) [3], [6], [10], [11], [12]. Two further tuples appear in the worked example: (IEC 62443-4-1 §SVV-3, CWE-444, *verification gap*) and (IEC 62443-3-3 §SR-3.4, AA26-097A §Mitigations, *software-and-information-integrity gap*) [4], [5], [11].

C. S3 — Residual-Risk Aggregation

We instantiate (1) with $L = 4$ layers (vendor SDL, integrator zone control, asset-owner SIS independence, runtime IDS) and threat-conditioned values $p_{\mathrm{SDL}} = 0.90$ (the upstream patch was not ingested), $c_{\mathrm{SDL}} = 0.10$; $p_{\mathrm{zone}} = 0.70$, $c_{\mathrm{zone}} = 0.40$ (Purdue segmentation present but with cross-vendor engineering-workstation conduits); $p_{\mathrm{SIS}} = 0.40$, $c_{\mathrm{SIS}} = 0.50$ (Triconex on a separate network segment, but BPCS-to-SIS bypass key in a shared cabinet); $p_{\mathrm{IDS}} = 0.60$, $c_{\mathrm{IDS}} = 0.30$ (process-level anomaly detection on chlorine residual; no network-level IDS on the leased-hosting conduit) [11], [12], [32], [33]. With $\kappa_{cc} = 0.05$ — appropriate because Rockwell and Siemens are independent organizations but share a common engineering-workstation tool ecosystem [21] — (1) yields $R_s \approx 0.55$. A reduction below 0.10 requires $p_{\mathrm{SDL}} \cdot (1 - c_{\mathrm{SDL}}) \leq 0.20$ (closure of the SBOM-feed defect) *and* $p_{\mathrm{zone}} \cdot (1 - c_{\mathrm{zone}}) \leq 0.20$ (closure of zone-aggregation creep) *and* an unchanged SIS independence layer; closing only one is insufficient.

D. S4 — IEC 62443-4-1 SDLC Residuals

We derive the vendor-side residuals as follows. *Residual SDL-1:* the supplier shall publish a Software Bill of Materials in CycloneDX or SPDX format that lists the Go

runtime version and all transitive Go-module dependencies, refreshed on each firmware release per CISA Minimum Elements [18]. *Residual SDL-2:* the supplier shall operate an ingestion contract for the upstream golang/go security feed with mean-time-to-ingest no greater than fifteen days for KEV-listed CVEs and no greater than sixty days otherwise [4], [35]. *Residual SDL-3:* the supplier shall maintain a per-product impact assessment that maps each upstream CVE to a determination of *applies / does not apply / mitigated by control / requires patch* and shall publish the determination on the vendor PSIRT channel within the same window. *Residual SDL-4:* the supplier shall verify that the firmware build pipeline emits a reproducible build artifact and that the binary attestation chains to the SBOM. *Residual SDL-5:* the supplier shall add a verification test that exercises the chunked-transfer-encoding code path with non-conforming line terminators per CWE-444 against every supported configuration of the embedded HTTP server [5], [11], [25].

E. S5 — IEC 62443-3-3 Zone-and-Conduit Controls

We derive the integrator-side controls as follows. *Control ZC-1:* the SENTRON 7KT and the Rockwell CompactLogix shall be placed in distinct zones, with the SENTRON in a metering/data zone and the CompactLogix in a process-control zone. *Control ZC-2:* the conduit between the metering/data zone and the process-control zone shall be restricted to a unidirectional gateway with explicit protocol allow-listing (Modbus/TCP read-only or OPC UA pub/sub read-only). *Control ZC-3:* inbound conduit rules from the corporate network and from the leased third-party hosting environment shall be blocked at the conduit edge, with allow-listed VPN-and-MFA paths only for explicitly authorized engineering workstations per IEC 62443-3-3 §SR-1.1 and §SR-1.2 [11]. *Control ZC-4:* the engineering-workstation conduit shall enforce role-based access control with separation of *engineer* and *integrator* roles, and the integrator role shall be restricted to scheduled change-control windows. *Control ZC-5:* the process-control zone shall implement network-flow anomaly detection on conduit traffic with explicit alarms on out-of-window engineering-workstation sessions [11], [32], [33], [34].

F. S6 — IEC 61511 SIS-Independence Requirements

We derive the asset-owner-side requirements as follows. *Requirement SIS-1:* the chemical-dosing SIS logic solver shall be operationally independent of the BPCS PLCs per IEC 61511-1 §11.2.10, with no shared engineering-workstation conduit [12]. *Requirement SIS-2:* the SIS communication shall be on a separate network segment, with the conduit to the BPCS network mediated by a unidirectional gateway or an air-gap with documented data-diode behavior. *Requirement SIS-3:* the SIS bypass-key practice shall be subject to a documented cybersecurity risk assessment per IEC 61511-1 §8.2.4 and shall require dual-authorization for activation. *Requirement SIS-4:* a post-compromise SIL verification shall demonstrate that the SIS achieves the demand-mode SIL target assuming the BPCS PLCs are adversarially compromised, with no reduction in achieved SIL by more than one band; the verification shall be reviewed by an assessor independent of the integrator [12], [29], [31]. *Requirement SIS-5:* the SIS proof-test schedule shall include a cybersecurity-event proof test triggered on detection of an out-of-window engineering-workstation session in the BPCS zone.

A joint fault tree for the *process-disruption* top event places the basic events SDL-1 (vendor SBOM feed defect), ZC-3 (integrator conduit rule), and SIS-1 (asset-owner SIS independence) beneath an OR gate that captures any single-layer failure, with an AND gate beneath the joint vendor-and-integrator basic events to capture the dependent-failure path of (1).

V. Discussion

A. Threats to Validity

The most material threat to validity is the dependence of (1) on the conditional probabilities p_i and effective coverages c_i, which are estimated from a small set of public incident records. Conti and colleagues observe that the population of public ICS incidents is biased toward water, wastewater, and energy because those operators are subject to mandatory reporting under sector-specific directives [32]. Kus and colleagues warn that ML-IDS benchmark distributions over-represent dense-attack windows and under-represent the rare-event distribution of true compromise [33]. The framework therefore treats the (1) instantiation in Section IV-C as illustrative of the cross-layer aggregation behavior rather than as a defensible point estimate.

A second threat is the assumption of independence among layers, encoded by the $\kappa_{cc} \geq 0.05$ lower bound for cross-vendor configurations. Pinto and colleagues observe that the most common asset-owner-side failure is precisely the practice that violates this independence assumption — zone-aggregation creep across vendor families that share a common engineering-workstation tool [21]. The framework requires the analyst to widen κ_{cc} when the integrator and the SIS operator share personnel.

A third threat is the absence of a formal mapping from IEC 62443-3-3 Security Levels (SL-1 through SL-4) to IEC 61511 Safety Integrity Levels (SIL 1 through SIL 4). The two scales are not commensurable in any formal sense; the framework treats the SL-T derivation per IEC 62443-3-2 [22] as a *constraint* on the residual-SIL verification of Step S6 rather than as a quantitative input.

B. Limitations

The framework treats only the supplier–integrator–asset-owner triple and explicitly excludes the *sector regulator* and the *national agency* layers. The EU Cyber Resilience Act will, after 11 September 2026, impose reporting obligations on suppliers that interact with the framework's Step S4

residuals but are not directly modeled [13]. The U.S. Transportation Security Administration Security Directives for pipeline and rail systems impose owner-side obligations that interact with Steps S5 and S6 but are sector-specific [14]. The framework also treats AI-resident PLC ladder logic, model-based control, and other non-classical control software as out of scope; an extension to ISO/PAS 8800-adjacent industrial safety-and-AI artifacts is a direction for future work.

C. Reproducibility

Every numerical claim, every clause reference, and every standards designation used in the worked example of Section IV is sourced from public records, vendor advisories, regulator advisories, or open standards. The framework is therefore reproducible by a reviewer with access only to public documents.

VI. Conclusion and Future Work

We have proposed a six-step framework that ingests publicly available operational-technology cybersecurity incident evidence and produces three classes of audit-ready artifacts — IEC 62443-4-1 secure-development-lifecycle residuals, IEC 62443-3-3 zone-and-conduit controls, and IEC 61511 safety-instrumented-system independence requirements — and we have demonstrated the framework on a joint vendor-and-owner thread combining the 2026 SENTRON 7KT request-smuggling defect and the 2026 CyberAv3ngers PLC compromise campaign. The framework reveals that the engineering gap exposed by these events is not in any single clause of any single standard but in the unowned space between the supplier, integrator, and asset-owner artifacts that the IEC 62443 and IEC 61511 families together require.

Three directions for future work are immediate. The first is a sector-specific instantiation of the framework for water utilities under EPA Public Water System cybersecurity guidance and for chemical facilities under the Chemical Facility Anti-Terrorism Standards successor regime. The second is the construction of a public benchmark of paired incident-evidence and clause-anchored residual tuples that can support quantitative calibration of (1). The third is a formal mapping from IEC 62443-3-3 Security Levels to the post-compromise residual SIL of an IEC 61511 SIS, which would close the most prominent absence in the present framework.

References

[1] Joint Cybersecurity Advisory NSA/FBI/CISA/DC3, "Iran-Linked Threat Actors Conduct Cyber Activity Against U.S. Critical Infrastructure," advisory AA25-159A, Cybersecurity and Infrastructure Security Agency, Jun. 2025.

[2] NIST, "Guide to Operational Technology (OT) Security," NIST Special Publication 800-82r3, Sep. 2023, doi: 10.6028/NIST.SP.800-82r3.

[3] Cybersecurity and Infrastructure Security Agency, "Siemens SENTRON 7KT PAC1261 Data Manager," ICS Advisory ICSA-26-134-14, May 2026.

[4] Go Security Team, "CVE-2025-22871: net/http: request smuggling through invalid chunked data," oss-security mailing list, Apr. 2025.

[5] MITRE Corporation, "CWE-444: Inconsistent Interpretation of HTTP Requests (HTTP Request/Response Smuggling)," Common Weakness Enumeration, 2024.

[6] Joint Cybersecurity Advisory NSA/FBI/CISA, "Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across U.S. Critical Infrastructure," advisory AA26-097A, Cybersecurity and Infrastructure Security Agency, Apr. 2026.

[7] Joint Cybersecurity Advisory CISA/FBI/NSA/EPA/INCD, "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors," advisory AA23-335A, Dec. 2023.

[8] K. Goyal, B. Cusack, and J. Goh, "Compromise of Internet-Exposed Unitronics PLCs in U.S. Water Utilities: A Forensic Reconstruction," in *Proc. IEEE Int. Conf. on Critical Infrastructure Protection*, Mar. 2024, pp. 142–155, doi: 10.1109/CIP.2024.0142.

[9] T. J. Williams, "The Purdue enterprise reference architecture," *Computers in Industry*, vol. 24, no. 2–3, pp. 141–158, Sep. 1994, doi: 10.1016/0166-3615(94)90017-5.

[10] International Electrotechnical Commission, "Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements," IEC 62443-4-1:2018, Jan. 2018.

[11] International Electrotechnical Commission, "Security for industrial automation and control systems — Part 3-3: System security requirements and security levels," IEC 62443-3-3:2013, Aug. 2013.

[12] International Electrotechnical Commission, "Functional safety — Safety instrumented systems for the process industry sector — Part 1," IEC 61511-1:2016 + Amd. 1:2017.

[13] European Parliament and Council, "Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)," Official Journal of the European Union, L 2024/2847, Dec. 2024.

[14] Transportation Security Administration, "Security Directive Pipeline-2021-02D and SD-1580/82-2022-01E," U.S. Department of Homeland Security, 2024.

[15] ISA/IEC, "Security for industrial automation and control systems — Part 1-1: Terminology, concepts and models," ISA/IEC 62443-1-1, 2009/2024.

[16] P. Ackerman, *Industrial Cybersecurity*, 2nd ed. Birmingham, U.K.: Packt Publishing, 2021.

[17] International Electrotechnical Commission, "IEC 62443-4-2: Technical security requirements for IACS components," Feb. 2019.

[18] CISA, "Minimum Elements for a Software Bill of Materials (SBOM): Updated Guidance (Draft)," Jun. 2025.

[19] ONEKEY GmbH, "Tackling Software Supply Chain Risks with IEC 62443 and SBOM," white paper, 2024.

[20] M. G. Jaatun, S. O. Johnsen, S. Frøystad, and P. H. Meland, "Implementation of Zones and Conduits in Industrial Control and Automation Systems," in *Proc. ESREL 2024*, Krakow, Poland, Jun. 2024.

[21] R. Pinto, T. Cruz, and P. Simoes, "Security Aspects of Zones and Conduits in IEC 62443: A Survey," *Journal of Cybersecurity and Privacy*, vol. 6, no. 2, pp. 52–78, Apr. 2026, doi: 10.3390/jcp6020052.

[22] International Electrotechnical Commission, "IEC 62443-3-2: Security risk assessment for system design," Jun. 2020.

[23] E. López-Morales, U. Ozmen, M. Rocchetto, S. Etigowni, S. Zonouz, and A. A. Cárdenas, "SoK: Security of Programmable Logic Controllers," in *Proc. 33rd USENIX Security Symposium*, Aug. 2024, pp. 1421–1438, doi: 10.48550/arXiv.2403.00280.

[24] D. Falas, A. Tsiknas, K. Demertzis, C. Skianis, K. Rantos, and M. Mavrouli, "Security of Programmable Logic Controllers and Related Systems: Today and Tomorrow," *IEEE Open Journal of the Industrial Electronics Society*, vol. 4, pp. 462–481, Nov. 2023, doi: 10.1109/OJIES.2023.3331271.

[25] M. Zhang, G. Zhao, X. Xu, J. Cheng, X. Wei, and J. Xie, "A Survey on Programmable Logic Controller Vulnerabilities, Attacks, Detections, and Forensics," *Processes*, vol. 11, no. 3, art. 918, Mar. 2023, doi: 10.3390/pr11030918.

[26] R. Geng, Y. Zhang, S. Etigowni, A. A. Cárdenas, and Z. B. Celik, "Towards Comprehensively Understanding the Run-time Security of Programmable Logic Controllers," arXiv:2212.14296, Dec. 2022.

[27] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "An Overview of the Security of Programmable Logic Controllers in Industrial Control Systems," *Encyclopedia*, vol. 4, no. 2, pp. 874–887, May 2024, doi: 10.3390/encyclopedia4020056.

[28] ISA, "Security countermeasures related to safety instrumented systems (SIS)," ISA Technical Report ISA-TR84.00.09, 2017.

[29] A. Di Pinto, Y. Dragoni, and A. Carcano, "TRITON: The First ICS Cyber Attack on Safety Instrumented Systems," Nozomi Networks / Black Hat USA, Aug. 2018.

[30] R. M. Lee, B. Allen, A. Bohne, and K. Lee, "TRISIS Malware: Analysis of Safety System Targeted Malware," Dragos Inc., Jan. 2018.

[31] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, "STPA-SafeSec: Safety and security analysis for cyber-physical systems," *J. Information Security and Applications*, vol. 34, pp. 183–196, Jun. 2017, doi: 10.1016/j.jisa.2016.05.008.

[32] M. Conti, D. Donadel, and F. Turrin, "Using machine learning to detect network intrusions in industrial control systems: a survey," *Int. J. Information Security*, vol. 23, pp. 4393–4421, Nov. 2024, doi: 10.1007/s10207-024-00916-x.

[33] D. Kus, E. Wagner, J. Pennekamp, K. Wehrle, and M. Henze, "A False Sense of Security? Revisiting the State of Machine Learning-Based Industrial Intrusion Detection," in *Proc. 8th ACM Cyber-Physical System Security Workshop*, May 2022, pp. 73–84, doi: 10.1145/3494107.3522773.

[34] C. Shang, D. Gao, Z. Yu, X. Liu, X. Zheng, and Y. Sun, "An Efficient Anomaly Detection Method for Industrial Control Systems: Deep Convolutional Autoencoding Transformer Network," *Int. J. Intelligent Systems*, vol. 2024, art. 5459452, May 2024, doi: 10.1155/2024/5459452.

[35] CISA, "Known Exploited Vulnerabilities Catalog," accessed Jun. 2026.