International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

A Comparative Review of Cybersecurity Frameworks for Industrial Control and SCADA Systems

Sami Ahmad
Department of Information Technology Noida Institute of Engineering & Technology Greater Noida, India
Email: samiahmad2023@gmail.com

https://doi.org/10.55041/ijsmt.v2i5.359

Cite this Article: Ahmad, S. (2026). A Comparative Review of Cybersecurity Frameworks for Industrial Control and SCADA Systems. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.359

License: This article is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting use, distribution, and reproduction in any medium, provided the original author(s) and source are properly credited.

***Abstract*—**Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems form the backbone of critical national infrastructure, including power grids, water treatment facilities, oil and gas pipelines, and manufacturing plants. The convergence of Information Technology (IT) and Operational Technology (OT) networks, accelerated by Industry4.0 and the Industrial Internet of Things (IIoT), has dramatically expanded the attack surface of these systems. This paper presents a comprehensive review of cybersecurity frameworks specifically designed for ICS and SCADA environments, including NIST SP 800-82, IEC 62443, NERC CIP, and the MITRE ATT&CK for ICSframework. We analyze their structural components, applicability, strengths, and limitations, and propose an integrated, defense-in- depth security model that addresses the unique operational, safety, and real-time constraints inherent to industrial environments. Case studies from recent cyberattacks—including Ukraine power grid incidents and the Oldsmar water treatment plant breach—are examined to evaluate real-world framework efficacy. Findings indicate that no single framework is universally sufficient; a hybrid approach combining complementary standards yields the strongest protection posture. Future directions including AI-driven anomaly detection, zero-trust architectures, and quantum-safe cryptography in OT contexts are also discussed.

Index Terms—SCADA security, ICS cybersecurity, NIST SP 800- 82, IEC 62443, NERC CIP, MITRE ATT&CK ICS, OT security, defense-in-depth, critical infrastructure protection, zero-trust.

I. Introduction

Industrial Control Systems (ICS) and SCADA systems were originally conceived as isolated, air-gapped networks operating proprietary protocols over dedicated serial links. Their primary design imperatives were availability and real-time determinism, not confidentiality or integrity in the information-security sense. Consequently, security was largely an afterthought during the foundational decades of industrial automation.

The seismic shift began with the adoption of commercial off-the-shelf (COTS) hardware, TCP/IP networking, and remote monitoring technologies in the 1990s and 2000s. Today, with the advent of Industry 4.0, IIoT sensors, and cloud-connected historians, operational technology (OT) networks are deeply interconnected with enterprise IT networks and, in many cases, with the public internet. This connectivity, while delivering enormous economic and operational benefits, has introduced a landscape of cyber threats that were entirely unknown to earlier generations of control-system engineers [1].

The consequences of a successful cyberattack on ICS/SCADA infrastructure extend far beyond data theft. Physical damage, process disruption, environmental hazards, and loss of human life are all plausible outcomes, as demonstrated by events such as the Stuxnet worm (2010), the Ukrainian power-grid attacks (2015–2016), and the Triton/TRISIS malware campaign targeting Safety Instrumented Systems (SIS) in 2017. The Oldsmar, Florida water-treatment plant intrusion in 2021—where an attacker momentarily increased sodium hydroxide concentration to dangerous levels—underscored that even small utilities operating legacy SCADA platforms face nation-state-calibre threats [2].

Against this backdrop, several standards bodies, governments, and industry consortia have developed cybersecurity frame- works tailored to the operational realities of ICS/SCADA environments. This paper systematically surveys these frameworks, evaluates their alignment with threat realities, and proposes a composite security architecture. The remainder of the paper is structured as follows: Section II reviews related work; Section III describes the ICS/SCADA threat landscape; Section IV analyses the principal frameworks; Section V presents comparative evaluation; Section VI proposes an integrated security model; Section VII discusses implementation challenges and case studies; Section VIII outlines future research directions; and Section IX concludes the paper.

II. Related Work

Research into ICS/SCADA cybersecurity has grown substantially over the past fifteen years. Stouffer et al. [3] provided the first authoritative government treatment of ICS security in NIST SP 800-82, establishing a taxonomy of system components and control-system-specific security concerns. Zhu et al. [4] offered an early taxonomy of SCADA-specific attacks, categorising threats according to their target (field device, communication, or control server) and the attacker's objective.

Kriaa et al. [5] conducted a survey of safety and security modelling approaches for ICS, highlighting the tension between safety-oriented methods (e.g., HAZOP, FMEA) and security-oriented methods (e.g., attack trees, STRIDE). They argued for integrated safety-security co-analysis, a recommendation that has since informed the IEC 62443-3-2 risk-assessment methodology. Samtani et al. [6] applied machine learning to SCADA vulnerability intelligence gathered from dark-web forums, demonstrating that threat intelligence pipelines can be partly automated even for OT-specific vulnerabilities.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

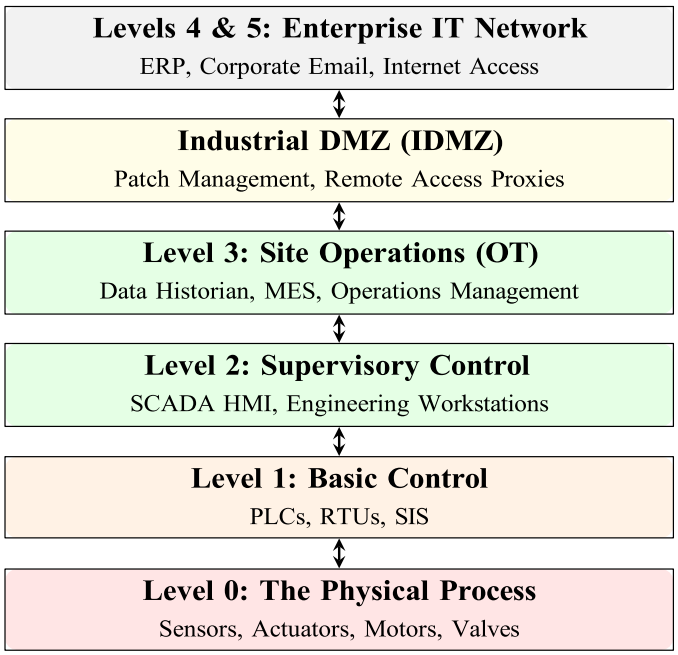

Fig. 1. The Purdue Enterprise Reference Architecture (PERA) highlighting the critical IT/OT boundary and industrial DMZ.

Hemsley and Fisher [7] reviewed the history of ICS cyber-attacks from 1982 to 2018 and identified recurring patterns: attacker persistence, insider knowledge, and exploitation of vendor support channels. Nazir et al. [8] performed a systematic literature review of ICS security frameworks, concluding that most implementations remain compliance-driven rather than risk-driven, and that small-to-medium operators lack resources to implement comprehensive controls. The present paper extends this body of work by incorporating the MITRE ATT&CK for ICS matrix—released publicly in 2020—and by proposing a composite framework validated against post-2020 incidents.

III. ICS/SCADA Threat Landscape

A. System Architecture Overview

A generic ICS/SCADA architecture is commonly modelled using the Purdue Enterprise Reference Architecture (PERA), which stratifies the system into five levels: Level 0 (field devices—sensors and actuators), Level 1 (basic control—PLCs, RTUs, DCS), Level 2 (supervisory control—SCADA HMI, engineering workstations), Level 3 (operations management—data historians, MES), and Levels 4–5 (enterprise and internet). Each boundary between levels represents a potential attack pathway if not adequately protected with network segmentation and monitoring [9].

B. Threat Actor Categories

Threat actors targeting ICS/SCADA systems span a wide capability spectrum. Nation-state actors possess the resources and expertise to develop bespoke ICS malware and conduct multi-year intrusion campaigns. Furthermore, cybercriminal groups increasingly deploy ransomware against OT networks, successfully monetizing systemic vulnerabilities as evidenced by recent pipeline and manufacturing disruptions [10]. Hacktivist groups mount opportunistic attacks on publicly accessible SCADA interfaces (e.g., exposed Modbus/TCP services). Insiders—whether malicious or negligent—represent a persistent threat, particularly in environments with inadequate access controls and audit logging [11].

C. Attack Vectors and Techniques

The MITRE ATT&CK for ICS matrix catalogues tactics and techniques observed in real ICS intrusions. Common initial access vectors include spear-phishing targeting engineering workstation operators, exploitation of remote access services (VPNs, RDP, vendor jump servers), supply-chain compromise of firmware or software updates, and watering-hole attacks against industry-specific websites. Lateral movement typically exploits weak segmentation between IT and OT zones. Impact- phase techniques include manipulation of control logic, denial of control, and damage to physical infrastructure by manipu- lating process setpoints beyond safe operating ranges [12].

IV. Principal Cybersecurity Frameworks for ICS/SCADA

A. NIST SP 800-82 Rev. 2 (Guide to ICS Security)

Published by the National Institute of Standards and Technology, NIST SP 800-82 is the US federal government's primary reference for ICS security. Revision 2 (2015) significantly expanded coverage to include DCS, PLCs, and IIoT devices. The document provides: (i) an overview of ICS components and architectures; (ii) a mapping of the NIST Cybersecurity Framework (CSF) functions—Identify, Protect, Detect, Respond, Recover—to ICS contexts; (iii) a tailoring guide for applying NIST SP 800-53 security controls to OT environments; and (iv) detailed network architecture recommendations, including DMZ design for IT/OT boundaries [13].

A key contribution of SP 800-82 is its explicit acknowledgement that availability supersedes confidentiality in OT environments—a fundamental departure from the CIA triad ordering prevailing in IT security. Security controls that introduce latency or require frequent patching are flagged as potentially incompatible with real-time control requirements. Revision 3 (draft, 2022) further addresses cloud connectivity, software-defined networking in OT, and supply-chain risk management.

B. IEC 62443 (Industrial Automation and Control Systems Security)

The IEC 62443 series, developed jointly by IEC Techni- cal Committee 65 and ISA99, is the most comprehensive international standard for IACS security. Organised into four series—General (62443-1-x), Policies and Procedures (62443- 2-x), System (62443-3-x), and Component (62443-4-x)—it addresses the full lifecycle of industrial security from risk assessment through component certification [14].

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

TABLE I
NOTABLE ICS/SCADA CYBERATTACKS (2010–2021)

Incident	Year	Sector	Technique	Impact
Stuxnet	2010	Nuclear	PLC logic modification	~1,000 centrifuges destroyed
Ukraine Grid Attack	2015–16	Energy	Spear-phishing + BlackEnergy	225,000 customers without power
TRITON/TRISIS	2017	Petrochemical	SIS firmware manipulation	Emergency shutdown triggered
Colonial Pipeline	2021	Oil & Gas	Ransomware (DarkSide)	6-day pipeline shutdown, $4.4M ransom
Oldsmar Water Plant	2021	Water	Remote HMI access (TeamViewer)	NaOH setpoint altered 111×

Central to IEC 62443 is the concept of Security Level (SL), defined on a scale of SL 1 (protection against casual/unintentional violation) to SL 4 (protection against state-sponsored attackers with sophisticated resources). The standard introduces the Security Level Target (SL-T), Security Level Capability (SL-C), and Security Level Achieved (SL-A) distinction, enabling gap analysis between desired and actual security posture. The Zone and Conduit model (62443-3-2) provides a systematic method for partitioning industrial networks into security zones and defining conduits—the communication channels between zones—with appropriate controls at each conduit boundary.

C. NERC CIP (Critical Infrastructure Protection)

The North American Electric Reliability Corporation's CIP standards are mandatory, enforceable regulations applicable to entities in the bulk electric system (BES) in North America. The current suite (CIP-002 through CIP-014) covers asset identification and classification, security management controls, personnel and training, physical security, electronic security perimeters, systems security management, incident reporting, recovery planning, configuration change management, vulnerability management, and supply chain risk management [15].

NERC CIP's enforcement mechanism—financial penalties up to $1 million per violation per day—makes it one of the few ICS security frameworks with genuine regulatory teeth. However, its scope is limited to high-impact and medium-impact BES Cyber Systems, leaving distribution-level SCADA systems and other sectors without equivalent mandatory standards. Critics also note that the compliance-oriented nature of NERC CIP can lead to a checkbox mentality that does not necessarily reflect actual security improvement.

D. MITRE ATT&CK for ICS

Released publicly in 2020, the MITRE ATT&CK for ICS matrix catalogues adversary tactics and techniques observed in real-world ICS intrusion campaigns. Unlike prescriptive frameworks such as IEC 62443, ATT&CK for ICS is descriptive—it documents what attackers do, not what defenders should implement. Its value lies in threat modelling, red-team exercise scoping, detection-rule development, and assessing the coverage of defensive controls against known adversary behaviours [12]. The matrix is organised across eleven tactics: Initial Access, Execution, Persistence, Privilege Escalation, Evasion, Discovery, Lateral Movement, Collection, Command and Control, Inhibit Response Function, and Impair Process Control. Each tactic contains multiple techniques with sub-techniques, real-world procedure examples, and suggested mitigations. Integration with the enterprise ATT&CK matrix enables end- to-end kill-chain modelling for attacks that traverse the IT/OT boundary.

E. ICS-CERT Recommended Practices and CISA Advisories

The US Cybersecurity and Infrastructure Security Agency (CISA), through its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), publishes recommended practice documents, alerts, and advisories addressing specific ICS vulnerabilities. Key publications, alongside recent Cross-Sector Cybersecurity Performance Goals (CPGs), provide actionable guidance aligned with NIST and IEC 62443 principles, serving as accessible entry points for smaller operators lacking dedicated OT security teams [16].

V. COMPARATIVE EVALUATION OF FRAMEWORKS

Table II presents a structured comparison of the four principal frameworks across seven evaluation dimensions derived from the security requirements unique to ICS/SCADA environments. The evaluation reveals complementary strengths but also exposes significant analytical trade-offs. While IEC 62443 provides deep structural and lifecycle coverage, its high implementation cost and procedural complexity present substantial adoption barriers, particularly for small-to-medium enterprises (SMEs) managing legacy infrastructure. Conversely, NIST SP 800-82 provides an accessible bridge between IT and OT cultures but lacks the strict compliance mechanisms seen in NERC CIP.

However, NERC CIP suffers from regulatory fragmentation, applying only to bulk electric systems and leaving critical sectors like water treatment heavily exposed. Furthermore, all prescriptive frameworks struggle with legacy-device incompatibility, as standards dictating modern encryption or access controls cannot be retrofitted onto aging PLCs. Ultimately, no single framework is universally sufficient, motivating the synthesized approach proposed in Section VI.

VI. PROPOSED INTEGRATED DEFENCE-IN-DEPTH SECURITY MODEL

Rather than proposing a fundamentally novel architecture, we propose an integrated framework synthesizing existing best

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

TABLE II
COMPARATIVE FRAMEWORK EVALUATION

Criterion	NIST SP 800-82	IEC 62443	NERC CIP	ATT&CK ICS
Scope	All ICS/SCADA	All IACS	BES only	All ICS
Enforceability	Voluntary (US Federal)	Voluntary / Contractual	Mandatory (N. America)	Voluntary
Risk-based Approach	Moderate	High	Low–Moderate	High
OT/RT Awareness	High	High	Moderate	High
Threat Intelligence	Low	Low	Low	Very High
Implementation Complexity	Moderate	High	High	Low–Moderate
Supply Chain Coverage	Moderate (Rev. 3 draft)	High (62443-2-4)	High (CIP-013)	Moderate

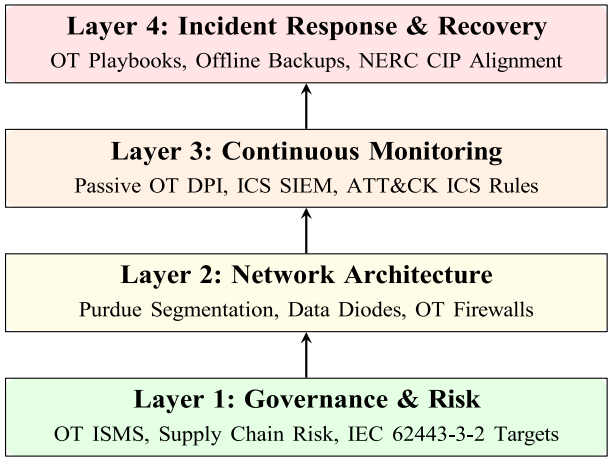

Fig. 2. The proposed Integrated ICS Security Model (IISM) synthesizing complementary strengths from existing frameworks.

practices into a four-layer Integrated ICS Security Model (IISM). This model synthesises the strongest elements of the evaluated frameworks while structurally respecting the operational constraints of industrial environments (Figure 2).

A. Layer 1 – Governance and Risk Management (IEC 62443-2-1 / NIST CSF)

The foundation layer establishes the policy, risk management, and organisational structures necessary to sustain a security programme. This includes: an OT-specific Information Security Management System (ISMS) aligned with ISO/IEC 27001; a documented risk assessment methodology employing the IEC 62443-3-2 zone-and-conduit model; roles and responsibilities clearly delineating IT and OT security ownership; and a cybersecurity-aware supply-chain procurement programme aligned with CIP-013.

B. Layer 2 – Network Architecture and Segmentation (IEC 62443-3-3 / NIST SP 800-82)

The architecture layer operationalises the zone-and-conduit model. Key controls include: (i) strict implementation of the Purdue Model segmentation with dedicated data diodes or unidirectional security gateways at Level 3/Level 2 boundaries for high-consequence processes; (ii) industrial-grade firewalls with application-layer inspection of OT protocols (Modbus, DNP3, IEC 61850, OPC-UA) at all conduit boundaries; (iii) out-of-band management networks for remote access and patching, eliminating dual-homed workstations; and (iv) network access control (NAC) enforcing device identity at the port level to prevent rogue device connection [17].

C. Layer 3 – Continuous Monitoring and Detection (ATT&CK ICS / NIST SP 800-82)

Given the difficulty of patching legacy OT devices, compensating detective controls are essential. This layer encompasses: (i) passive OT network monitoring (e.g., Claroty, Dragos Platform, Nozomi Networks) with protocol-aware deep packet inspection to establish process baselines and detect anomalous command sequences; (ii) a Security Information and Event Management (SIEM) ingesting logs from OT and IT networks with ATT&CK ICS-aligned detection rules; (iii) Security Orchestration, Automation, and Response (SOAR) playbooks adapted for OT incident response, ensuring that automated actions cannot inadvertently disrupt live processes; and (iv) ICS-specific threat intelligence feeds integrated into the detection pipeline [18].

D. Layer 4 – Incident Response and Recovery (NERC CIP / NIST SP 800-82)

The uppermost layer ensures operational resilience. Components include: (i) an OT Incident Response Plan (IRP) developed in conformance with CIP-008 and NIST SP 800-61r2, with runbooks specific to ransomware, logic manipulation, and denial-of-control scenarios; (ii) regular tabletop and red-team exercises using ATT&CK ICS techniques as adversary emulation playbooks; (iii) secure, offline backups of PLC/DCS logic, historian data, and configuration files, tested for restoration integrity at least annually; and (iv) post-incident forensic capabilities including network packet capture retention and tamper-evident audit logs.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

VII. Implementation Challenges and Case Study Analysis

A. Implementation Challenges

Legacy device constraints represent the most pervasive challenge. Many PLCs and RTUs in operational service were designed in previous decades with minimal memory and no cryptographic capability. Retrofitting modern authentication or encrypted communication protocols is often infeasible without replacing the device entirely. Compensating controls—network segmentation, anomaly detection, physical access restrictions—must substitute for host-based security that cannot be installed [19].

Patch management in OT environments is fundamentally different from IT. Vendor qualification of patches, process downtime windows, and the risk of patch-induced regression in safety-critical logic mean that OT assets frequently run software versions years or decades behind supported release levels. A structured vulnerability management programme that prioritises compensating controls for unpatched vulnerabilities is essential.

Cultural and organisational barriers heavily persist between IT and OT domains. OT engineers prioritise availability and safety; IT security practitioners prioritise confidentiality and integrity. Bridging this divide requires joint training, shared incident response exercises, and governance structures that give both communities a voice in security decisions.

B. Case Study: Ukraine Power Grid (2015–2016)

The BlackEnergy/Industroyer attacks on Ukraine's electricity distribution infrastructure are a benchmark for sophisticated ICS cyberattacks. In December 2015, attackers compromised corporate workstations at three distribution companies via spear-phishing, conducted months of reconnaissance, and eventually opened circuit breakers remotely, resulting in a massive power outage for 225,000 customers [11].

Analyzed through the proposed framework, this incident underscores catastrophic failures in network segmentation (IISM Layer 2) and continuous monitoring (IISM Layer 3). The corporate network was insufficiently isolated from SCADA systems, enabling lateral movement. Furthermore, the absence of OT-network behavioural monitoring meant that reconnaissance activity went undetected for months. The defensive lesson is clear: establishing segmented industrial DMZs and deploying protocol-aware DPI monitoring are critical baseline defenses for critical infrastructure.

C. Case Study: Oldsmar Water Treatment Plant (2021)

The Oldsmar incident illustrates the severe threat posed by unsecured remote access. An attacker gained access to the plant's SCADA HMI via TeamViewer—a remote desktop application being shared across multiple workstations without adequate access controls—and dangerously increased the sodium hydroxide setpoint. Fortunately, an alert operator observed the cursor moving and reversed the change within seconds [2].

This case directly maps to IISM Layer 2 (no network segmentation, no access control) and Layer 1 (no policy governing remote access tools or password management) failures. NIST SP 800-82's recommendation for out-of-band remote access with multi-factor authentication, and IEC 62443's requirement for unique credentials, would have been directly preventive.

VIII. Future Research Directions

A. AI and Machine Learning for OT Anomaly Detection

Passive network monitoring produces high-volume telemetry that overwhelms human analysts. Machine learning models offer the potential to identify subtle process manipulation that rule-based systems cannot detect. However, research challenges must directly address ICS constraints: achieving deterministic latency for real-time alerting, securing formal safety certifications for ML-driven interventions, and enabling OT-safe ML deployment that respects deterministic control loops. Developing explainable AI models that plant operators can trust during critical events remains a primary obstacle [18], [20].

B. Zero-Trust Architecture in OT Environments

Zero-trust principles are increasingly advocated for IT environments but face significant challenges in OT deployment. Legacy PLCs suffer from severe compute constraints and cannot participate in certificate-based mutual authentication. Furthermore, real-time control communications cannot tolerate the real-time authentication latency introduced by policy engines. Research into OT-compatible zero-trust proxies, hardware-rooted trust for embedded devices, and lightweight authentication protocols suitable for resource-constrained controllers is an active and important area [21], [22].

C. Quantum-Safe Cryptography for ICS

The anticipated arrival of cryptographically relevant quantum computers threatens the asymmetric algorithms underpinning VPN tunnels and code-signing schemes used to protect OT firmware integrity. Because industrial hardware lifecycles often span 15 to 20 years, migrating OT environments to post-quantum cryptography (FIPS 203, 204, 205) requires a crypto-agility roadmap developed well in advance. Navigating these narrow OT patching windows and managing industrial protocol cryptography overhead without disrupting continuous availability remains a critical research frontier [23].

D. Digital Twins for Security Validation

High-fidelity digital twins of ICS/SCADA systems offer a safe environment for security testing and the evaluation of new controls without risking live plant shutdowns. Research opportunities include improving twin fidelity for cyber-physical simulation, developing attack injection frameworks natively compliant with ATT&CK ICS, and utilizing twin-generated datasets to safely train ML anomaly detectors on destructive failure scenarios [24].

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

IX. Limitations

This survey and the proposed Integrated ICS Security Model acknowledge several limitations. First, the survey scope is constrained by the rapidly evolving threat landscape; the continuous emergence of novel OT ransomware campaigns means that defensive frameworks must constantly adapt. Second, limited public OT incident data and proprietary industrial deployments restrict empirical validation, as organizations are hesitant to release detailed forensic data regarding critical infrastructure breaches. Third, framework implementation variability and the lack of standardized evaluation metrics significantly hinder the independent verification of advanced security benchmarks across disparate industrial sectors. Finally, stark regional differences in regulatory compliance make standardizing a single, universally applicable framework practically unfeasible.

X. Conclusion

This paper has presented a comprehensive survey of cybersecurity frameworks for Industrial Control and SCADA Systems, analysed their structural components and limitations, and proposed an Integrated ICS Security Model that synthesises their complementary strengths into a coherent defence-in-depth architecture.

The convergence of IT and OT has irreversibly altered the threat landscape facing critical infrastructure operators. The Stuxnet, Ukraine grid, Triton, Colonial Pipeline, and Oldsmar incidents collectively demonstrate that ICS/SCADA cyberattacks are no longer theoretical concerns but regular operational realities with potential for catastrophic physical consequence. No single framework—whether NIST SP 800-82, IEC 62443, NERC CIP, or MITRE ATT&CK for ICS—provides complete protection in isolation; each addresses distinct aspects of the problem.

The four-layer IISM model proposed in this paper—spanning governance, network architecture, continuous monitoring, and incident response—provides a structured approach to integrating framework elements that is both risk-based and operationally viable. Case study analysis of the Ukraine and Oldsmar incidents demonstrates that systematic application of the model's Layer 1 and Layer 2 controls would have been directly preventive in both cases.

Future work should address the specific challenges of quantum-safe cryptography migration, AI-driven anomaly detection in process environments, and the development of OT-compatible zero-trust architectures. As industrial systems continue to evolve toward greater connectivity and autonomy, the cybersecurity community must ensure that security frameworks evolve in parallel, grounded in both theoretical rigour and operational practicality.

References

[1] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 2nd ed. Syngress, 2015.

[2] Cybersecurity and Infrastructure Security Agency (CISA), "ICS-CERT advisories and incident summaries," https://www.cisa.gov/ics, accessed: Apr. 2026.

[3] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security," National Institute of Standards and Technology, Tech. Rep. NIST Special Publication 800-82 Rev. 2, May 2015.

[4] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proceedings of the International Conference on Internet of Things and Cyber, Physical and Social Computing*, 2011, pp. 380–388.

[5] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability Engineering & System Safety*, vol. 139, pp. 156–178, Jul 2015.

[6] S. Samtani, K. Chinn, C. Larson, and H. Chen, "AZSecure hacker assets portal: Cyber threat intelligence and malware analysis," in *IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2016, pp. 19–24.

[7] K. E. Hemsley and R. E. Fisher, "History of industrial control system cyber incidents," Idaho National Laboratory, Tech. Rep. INL/CON-18- 44411, 2018.

[8] S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," *Computers & Security*, vol. 70, pp. 436–454, Sep 2017.

[9] ISA-99 Committee, "Security for industrial automation and control systems," International Society of Automation, Research Triangle Park, NC, Tech. Rep. ANSI/ISA-62443 Series.

[10] S. McLaughlin *et al.*, "The rise of ransomware in operational technology environments," *IEEE Security & Privacy*, vol. 22, no. 1, pp. 45–53, 2024.

[11] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the ukrainian power grid," SANS ICS Defense Use Case, Tech. Rep., Mar 2016.

[12] MITRE Corporation, "ATT&CK for industrial control systems," https://attack.mitre.org/matrices/ics/, accessed: Apr. 2026.

[13] National Institute of Standards and Technology, "Cybersecurity framework v2.0," NIST, Tech. Rep., Feb 2024.

[14] International Electrotechnical Commission, "IEC 62443-3-3:2013, industrial communication networks – network and system security – part 3-3: System security requirements and security levels," IEC, Geneva, Tech. Rep., 2013.

[15] North American Electric Reliability Corporation, "CIP standards," https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx, accessed: Apr. 2026.

[16] Cybersecurity and Infrastructure Security Agency (CISA), "Cross-sector cybersecurity performance goals," CISA, Tech. Rep., 2024.

[17] S. Adepu and A. Mathur, "Distributed detection of single-stage multipoint cyber attacks in a water treatment plant," in *Proceedings of the ACM Asia Conference on Computer and Communications Security (Asia CCS)*, 2016, pp. 449–460.

[18] J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly detection in cyber physical systems using recurrent neural networks," in *Proceedings of the IEEE International Symposium on High Assurance Systems Engineering (HASE)*, 2017, pp. 65–70.

[19] Dragos, Inc., "ICS/OT cybersecurity year in review," Dragos, Tech. Rep., 2023.

[20] S. Ahmed *et al.*, "Artificial intelligence and machine learning for cybersecurity in critical infrastructure: A review," *IEEE Access*, vol. 11, pp. 23 456–23 470, 2023.

[21] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," National Institute of Standards and Technology, Tech. Rep. NIST Special Publication 800-207, Aug 2020.

[22] J. Pacheco *et al.*, "Towards zero trust architecture in industrial IoT environments," *IEEE Internet of Things Journal*, vol. 11, no. 4, pp. 1245–1256, 2023.

[23] National Institute of Standards and Technology, "Post-quantum cryptography standardization," NIST, Tech. Rep. FIPS 203/204/205, 2024.

[24] W. Dietz *et al.*, "Digital twins for cyber-physical systems security: State of the art and open challenges," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1234–1245, 2023.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.