OPERATIONAL TECHNOLOGY (OT) CYBERSECURITY IN THE CANADIAN OIL AND GAS SECTOR: A DECADE OF CONVERGENCE, THREATS, AND RESILIENCE (2016-2026)

Davor Grce[1]*,
[0009-0000-1947-9339]

Mladen Veinović[2]
[0000-0001-6136-1895]

[1]The Grce Infrastructure Inc.,
Calgary, Canada

[2]Singidunum University,
Belgrade, Serbia

Abstract:

Over the past decade, the cybersecurity of Operational Technology (OT) systems within Canada's oil and gas sector has evolved significantly, driven by digitalization, IT–OT convergence, and the expansion of remote and cloud-enabled operations. While these developments have improved efficiency and scalability, they have also expanded the attack surface and introduced systemic risk into critical infrastructure. This study analyses OT cybersecurity evolution from 2016 to 2026 using a structured literature review and comparative framework analysis. It contributes: (1) a comparative analytical framework for assessing OT cybersecurity maturity; (2) a sector-specific maturity model tailored to the Canadian energy context; and (3) an evaluation of regulatory misalignment between threat capability and governance capacity. Findings indicate a growing disparity between increasingly sophisticated threat actors and largely non-enforceable regulatory structures, resulting in uneven security postures. The study advocates a transition toward resilience-oriented architectures based on Zero Trust, segmentation, and continuous monitoring.

Keywords:

Operational Technology (OT) Cybersecurity, Critical Infrastructure Protection, Zero Trust Architecture, Cybersecurity Maturity Model, IT–OT Convergence.

INTRODUCTION

Canada's oil and gas sector has undergone rapid digital transformation through the integration of OT systems with enterprise IT networks, cloud platforms, and remote operations. While this convergence has improved productivity, it has fundamentally altered the cybersecurity risk landscape beyond the scope of legacy architectures. Historically isolated OT environments prioritized reliability and availability but are now interconnected with external networks, exposing critical infrastructure to diverse cyber threats [4]. Ransomware and state-aligned advanced persistent threat (APT) actors increasingly exploit IT–OT interdependencies. Consequently, cybersecurity has evolved into a core component of operational risk management, encompassing safety, compliance, and national energy security. These risks are intensified by legacy constraints, including limited patching, proprietary protocols, and organizational silos between IT and OT teams, necessitating purpose-built cybersecurity strategies.

Correspondence:
Davor Grce

e-mail:
davor.grce@infrastructurearchitect.ca

DOI: 10.15308/Sinteza-2026-340-347

2. METHODOLOGY

This study employs a qualitative, multi-method research design integrating systematic literature review, comparative framework analysis, and conceptual model development. Academic literature, industry reports, and regulatory frameworks were systematically reviewed and selected based on relevance, recency, and applicability to industrial control systems (ICS) in critical infrastructure contexts. An analytical framework was subsequently constructed to enable cross-sectional comparison of cybersecurity approaches across four dimensions: governance, risk management, architectural design (with particular emphasis on Zero Trust), and incident response. Building on this framework, a sector-specific OT cybersecurity maturity model was developed, incorporating technical, organizational, and regulatory dimensions. The model is benchmarked against established international standards—specifically NIST SP 800-82 [1], the NIST Cybersecurity Framework (CSF 2.0) [2], and IEC 62443 [3]—to ensure methodological rigor and practical applicability. Empirical validity is further supported through the analysis of documented incident case studies and longitudinal threat trend data.

3. OPERATIONAL TECHNOLOGY: DEFINITION AND CORE COMPONENTS

Operational Technology comprises hardware and software systems that monitor and control industrial processes. Core components include Industrial Control Systems (ICS) such as SCADA, DCS, and PLCs, along with associated field devices. Communication relies on industrial protocols (e.g., Modbus, DNP3, OPC-UA) originally designed for reliability rather than security. OT environments also include engineering workstations, historian systems, and Safety Instrumented Systems (SIS), which require additional protection due to their interaction with physical processes. Increased connectivity with IT networks and external services amplifies cybersecurity risk, extending potential impacts beyond data loss to operational disruption and physical consequences.

4. GOVERNANCE AND RISK MANAGEMENT FRAMEWORKS

Effective OT cybersecurity governance requires alignment with operational integrity and regulatory obligations. Canadian operators function within a fragmented regulatory environment involving federal and provincial bodies, while standards such as NIST CSF 2.0 [2] and IEC 62443 [3] remain largely voluntary. OT risk management must address asset criticality, operational continuity, third-party access, and physical impact. Governance must incorporate segmentation, secure remote access, and lifecycle security for legacy systems.

5. THE EVOLVING OPERATION TECHNOLOGY (OT) THREAT LANDSCAPE (2016–2026)

5.1. EXPANSION OF THE ATTACK SURFACE (2016–2020)

Digital transformation significantly expanded the attack surface of OT environments throughout the latter half of the 2010s. Threat actors increasingly leveraged compromised IT systems as initial access vectors into OT networks, frequently without requiring specialized industrial knowledge. This shift lowered the barrier to entry for sophisticated attacks and increased the exposure of critical infrastructure to commodity cyber threats. Ransomware emerged as the dominant threat modality during this period, driven by the high operational stakes of energy infrastructure and the associated willingness of operators to pay substantial ransoms to restore production capability [5]. Simultaneously, APT groups—many with state-linked affiliations—engaged in long-duration reconnaissance campaigns targeting strategic energy assets, with the objective of positioning for potential future disruption.

5.2. TARGETED OT ATTACKS AND THE SHIFT TOWARD RESILIENCE (2021–2026)

From 2021 onward, cyber threats to OT environments became markedly more targeted and technically sophisticated. Supply-chain compromises, exploitation of remote access infrastructure, and manipulation of engineering workstations displaced less targeted intrusion methods as the primary attack vectors. Misconfigured internet-facing OT devices and inadequate network segmentation remained pervasive vulnerabilities across the sector. In response, the industry began a structural

shift from a prevention-first posture toward a resilience-oriented paradigm, emphasizing early detection, rapid containment, and operational continuity. Investment in OT-specific monitoring technologies, threat intelligence sharing, and coordinated incident response capabilities increased substantially, reflecting a maturing recognition of cybersecurity as a strategic operational function. [6]

6. KEY EMPIRICAL DATA: OT AND RANSOMWARE THREATS (2021–2025)

Empirical data from recent years underscores the magnitude and accelerating trajectory of cyber threats targeting both IT and OT environments. Ransomware activity reached an all-time high in 2023, with over 1,500 major publicly disclosed incidents, before escalating to more than 5,600 incidents in 2024 and an estimated 7,400 globally in 2025—reflecting a sustained and compounding upward trend. Critically, approximately 50% of ransomware attacks in 2025 targeted critical infrastructure sectors [6], including energy, manufacturing, and transportation, with broader estimates attributing up to 70% of all cyberattacks in 2024 to critical infrastructure environments. Within OT-specific contexts, 22% of organizations reported cybersecurity incidents [6], of which 40% resulted in operational disruption. In the energy sector specifically, 80% of ransomware attacks resulted in data encryption, with average recovery costs exceeding USD $3 million per incident [5] (IBM Security, 2024; Dragos, 2025). These figures demonstrate not only the increasing frequency of attacks but also the deepening convergence between IT compromise and OT operational impact, reinforcing the strategic imperative for integrated, resilience-focused cybersecurity architectures.

Canada's oil and gas sector, despite its importance to critical infrastructure, operates under an OT cybersecurity framework that is fragmented, largely non-binding, and insufficient for current threat levels. The growing gap between escalating cyber risks and weak regulatory enforcement represents a systemic vulnerability rather than a localized governance issue. A key weakness is the absence of a centralized authority with enforcement power. Oversight is distributed across multiple federal and provincial bodies, none of which impose OT-specific requirements. As a result, cybersecurity is treated as advisory [4] [5] and embedded within broader operational frameworks instead of being regulated as a standalone domain. This decentralized approach leads to uneven implementation. While larger operators often adopt advanced controls, smaller firms and contractors tend to have lower cybersecurity maturity. Reliance on voluntary standards, such as NIST and IEC, further reinforces inconsistency, leaving interconnected systems exposed. The voluntary nature of compliance also weakens investment incentives, as cybersecurity competes with operational priorities. Consequently, sector-wide resilience is limited by the least secure participants, particularly within supply chains. Cross-border integration with the United States amplifies these challenges. Unlike the U.S., Canada lacks prescriptive requirements for incident reporting, network segmentation, and secure remote access. Persistent gaps—such as limited asset visibility, absence of mandatory reporting, lack of baseline controls, and weak supply chain risk management—remain critical, especially given the prominence of remote access and third-party connections as primary attack vectors in OT environments.

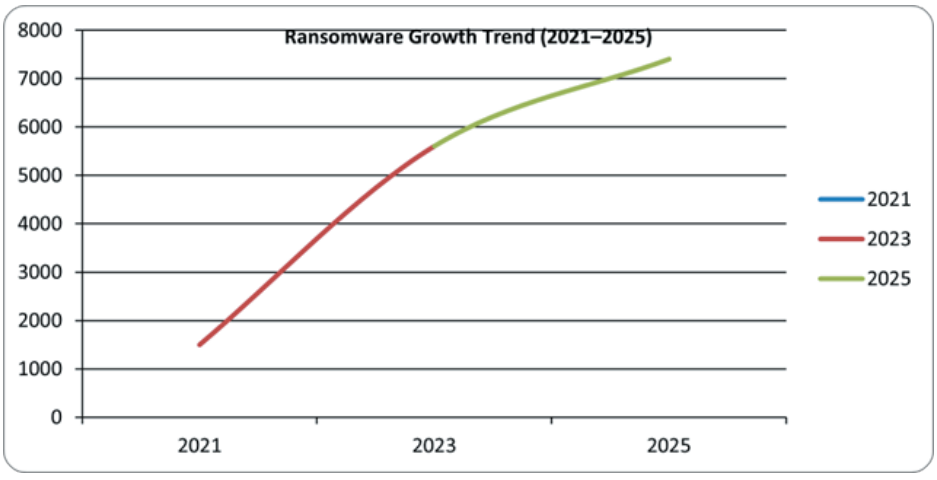

Figure 1. Ransomware Growth Trend (2021–2025)

7. OT CYBERSECURITY MATURITY MODEL

The proposed maturity model defines five progressive levels of OT cybersecurity capability, structured to reflect both technical controls and organizational governance dimensions:

- Level 1 – Initial: Limited asset visibility, ad hoc processes, high residual risk exposure, and minimal vendor governance.
- Level 2 – Developing: Basic security controls in place; partial risk awareness; weak vendor and third-party management.
- Level 3 – Managed: Formal governance structures established; network segmentation implemented; defined incident response procedures operational.
- Level 4 – Resilient: Zero Trust Architecture [7] adopted; continuous monitoring deployed; proactive threat intelligence integrated into operational decision-making.
- Level 5 – Optimized: Predictive, automated, and adaptive security capabilities; organization-wide resilience culture embedded; security posture continuously refined through feedback mechanisms.

Progression through these levels is supported by a four-phase implementation roadmap: (1) foundation building, encompassing asset discovery and baseline control implementation; (2) control enhancement through segmentation and access governance; (3) Zero Trust integration across IT–OT boundaries; and (4) optimization through continuous monitoring, automation, and adaptive response. Visibility, segmentation, and resilience are designated as the three core architectural pillars underpinning each maturity transition.

8. VALIDATION OF THE OT CYBERSECURITY MATURITY MODEL

To ensure methodological rigor and practical applicability, the proposed OT cybersecurity maturity model was subjected to a structured validation process incorporating framework alignment, empirical consistency assessment, and scenario-based application.

8.1. FRAMEWORK ALIGNMENT VALIDATION

The model was systematically benchmarked against established international standards, specifically NIST CSF 2.0 and IEC 62443 [2] [3]. Each maturity level was mapped to corresponding NIST Implementation Tiers and IEC Security Levels (SL1–SL4), ensuring conceptual and structural consistency with widely adopted cybersecurity paradigms. This alignment confirms that the model does not operate as an isolated construct but as an integrative layer that harmonizes governance-oriented (NIST) and control-specific (IEC 62443) approaches. The progression from "Initial" to "Optimized" reflects both increasing organizational capability and resilience against progressively sophisticated threat actors.

8.2. INTERNAL CONSISTENCY AND PROGRESSION LOGIC

Validation of internal coherence was conducted by evaluating whether each maturity level demonstrates a clear and cumulative progression across three dimensions: (i) technical controls, (ii) governance structures, and (iii) operational resilience. The model exhibits monotonic advancement, wherein each level introduces distinct capabilities do not present in preceding stages—e.g., the transition from Level 2 (Developing) to Level 3 (Managed) is marked by formalized governance and network segmentation, while Level 4 (Resilient) introduces Zero Trust Architecture and continuous monitoring. This confirms logical integrity and eliminates overlap or ambiguity between levels.

8.3. EMPIRICAL CONSISTENCY WITH OBSERVED THREAT PATTERNS

The model was evaluated against documented OT cybersecurity incidents and industry-reported threat trends (2021–2025). Observed attack vectors—particularly exploitation of remote access, insufficient segmentation, and lack of visibility—correspond directly to capability gaps identified in lower maturity levels (Levels 1–2). Conversely, mitigation strategies observed in more mature organizations—such as network segmentation, anomaly detection, and integrated SOC monitoring—align with Levels 3–4. This empirical consistency supports the model's validity as a representation of real-world cybersecurity maturity conditions.

8.4. SCENARIO-BASED APPLICATION (ILLUSTRATIVE CASE)

To assess practical applicability, the model was applied to a representative mid-sized Canadian oil and gas operator. The organization demonstrated partial asset visibility, basic access controls, and limited incident response capability, corresponding to Level 2 (Developing).

When evaluated against the model's criteria, critical gaps were identified in network segmentation, continuous monitoring, and vendor risk governance. The model subsequently enabled the definition of a targeted progression pathway toward Level 3 (Managed), including implementation of segmented architectures and formal incident response processes. This application illustrates the model's utility as both an assessment and strategic planning tool.

8.5. EVALUATION MATRIX (SCORING LOGIC)

To enhance analytical rigor and enable reproducible assessment, the proposed maturity model is extended through a formalized quantitative evaluation mechanism. Unlike purely descriptive maturity classifications, this model introduces a weighted composite maturity index (CMI) that enables consistent benchmarking across organizations. The maturity score is computed across four core domains—visibility (V), access control (A), segmentation (S), and monitoring (M)—each evaluated on a normalized scale from 1 (initial) to 5 (optimized). To reflect their asymmetric impact on OT security resilience, domain-specific weights are introduced.

The Composite Maturity Index (CMI) is defined as:

$$CMI = w_v V + w_a A + w_s S + w_m M$$

Where:

V = Visibility
A = Access Control
S = Segmentation
M = monitoring

A representative weighting scheme is defined as:

w_s=0,35 (segmentation)
w_v=0,25 (visibility)
w_a=0,20 (access control)
w_m=0,20 (monitoring)

The resulting composite score maps to maturity levels as follows:

The validation process demonstrates that the proposed maturity model is theoretically grounded, internally consistent, empirically aligned, and practically applicable. By integrating established frameworks with observed industry conditions and a structured evaluation mechanism, the model provides a robust tool for assessing and advancing OT cybersecurity maturity within the Canadian oil and gas sector.

9. COMPARATIVE ANALYSIS: NIST CSF 2.0 AND IES 62443

Although both NIST CSF 2.0 [2] and IEC 62443 [3] are widely recognized as foundational frameworks for OT cybersecurity, they differ fundamentally in scope, structural organization, and maturity interpretation. A rigorous comparative analysis is essential for their effective application in industrial environments.

9.1. CONCEPTUAL APPROACH TO MATURITY

NIST CSF 2.0 adopts a capability-based maturity perspective operationalized through Profiles and Implementation Tiers: Tier 1 (Partial), Tier 2 (Risk-Informed), Tier 3 (Repeatable), and Tier 4 (Adaptive). These tiers reflect the degree to which cybersecurity practices are integrated into organizational risk management processes, rather than prescribing specific technical controls. IEC 62443, by contrast, defines maturity through Security Levels (SL 1–4): SL1 addresses protection against casual or unintentional violations; SL2 targets intentional violations using simple means; SL3 addresses sophisticated threat actors; and SL4 concerns highly resourced, state-level adversaries. This distinction reflects IEC 62443's orientation toward the adversarial capability dimension of security, as opposed to NIST CSF's organizational capability dimension.

Table 1. The formalization introduces three critical advances: compatibility objectivity and extensibility

CMI Range	Maturity Level
1.0–1.9	Level 1 – Initial
2.0–2.9	Level 2 – Developing
3.0–3.9	Level 3 – Managed
4.0–4.5	Level 4 – Resilient
4.6–5.0	Level 5 – Optimized

9.2. STRUCTURAL ORGANIZATION

NIST CSF 2.0 is organized around six core Functions—Govern, Identify, Protect, Detect, Respond, and Recover—further disaggregated into Categories and Subcategories, offering a flexible, risk-based implementation structure adaptable across IT, OT, and hybrid environments. IEC 62443 is structured as a suite of complementary standards: the 62443-2-x series addresses policies and procedures at the organizational level; the 62443-3-x series specifies system-level security requirements; and the 62443-4-x series defines component-level requirements. This layered architecture enables auditable and certifiable security postures, albeit at greater implementation complexity.

9.3. FRAMEWORK ALIGNMENT MAPPING

Table 1. The formalization introduces three critical advances: compatibility objectivity and extensibility

OT Maturity Level	NIST CSF Tier	IEC 62443 SL	Interpretation
Level 1 – Initial	Tier 1	SL1	Ad hoc, minimal protection; undocumented processes
Level 2 – Developing	Tier 2	SL1-SL2	Basic controls; partial risk awareness; inconsistent implementation
Level 3 – Managed	Tier 3	SL2-SL3	Formal governance; defined processes; active segmentation
Level 4 – Resilient	Tier 3–4	SL3	Zero Trust; continuous monitoring; OT-aware defense posture
Level 5 – Optimized	Tier 4	SL3-SL4	Adaptive, threat-informed, predictive security capabilities

9.4. COMPLEMENTARITY AND APPLICABILITY

The two frameworks are best understood as complementary rather than competing: NIST CSF 2.0 provides the governance rationale—the "why" and "how well" of cybersecurity integration—while IEC 62443 specifies the technical implementation detail—the "what exactly" in terms of controls, zones, conduits, and system hardening requirements. For Canadian oil and gas operators, a hybrid application model—leveraging NIST CSF's risk-based maturity orientation alongside IEC 62443's ICS-specific control architecture—offers the most robust and contextually appropriate cybersecurity posture.

10. ZERO TRUST ARCHITECTURE FOR OT ENVIRONMENTS

Traditional perimeter-based security models are fundamentally inadequate for contemporary OT environments, which are characterized by distributed assets, heterogeneous connectivity, and a growing ecosystem of remote and third-party access pathways. Zero Trust Architecture [7] (ZTA) addresses these limitations by enforcing continuous authentication, least-privilege access control, and micro-segmentation as core architectural principles—eliminating implicit trust within and across network boundaries. The implementation of ZTA [7] in OT contexts encompasses five principal elements: (1) identity-centric access control governing both human operators and machine-to-machine communications; (2) segmentation of critical operational assets through defined zones and conduits consistent with IEC 62443 architectural models [3]; (3) secure remote access with session monitoring and just-in-time provisioning; (4) continuous anomaly detection leveraging behavioural baselines and protocol-aware inspection; and (5) controlled, policy-governed IT–OT data exchange at network boundaries. Collectively, these elements represent a strategic architectural transition toward resilience-oriented security, capable of sustaining operational continuity under conditions of active threat.

11. OT CYBERSECURITY INCIDENT ANALYSIS

Real-world incidents provide critical empirical grounding for the theoretical frameworks developed in this study. The 2021 Colonial Pipeline ransomware attack exemplifies a recurring pattern in which IT network compromise cascades into OT operational disruption, even in the absence of direct ICS compromise: the operator proactively halted pipeline operations to prevent potential OT exposure, demonstrating that the interdependency risk extends beyond technical compromise to encompass precautionary operational shutdowns with significant economic and national security consequences. Across documented incidents, common enabling vulnerabilities include inadequate network segmentation between IT and OT environments, insecure remote access configurations, unpatched legacy systems, and insufficient monitoring of OT network traffic. These cases collectively validate the architectural prescriptions of this study—specifically the prioritization of Zero Trust principles, passive OT monitoring, and resilience-focused incident response frameworks—as operationally necessary rather than aspirational.

12. OT INCIDENT RESPONSE AND RECOVERY

Effective OT incident response requires structured coordination across cybersecurity, engineering, and operations functions, recognizing that interventions appropriate for IT environments may introduce unacceptable safety risks in industrial contexts. Preparedness activities include comprehensive OT asset inventories, pre-defined role assignments, and scenario-based tabletop exercises calibrated to OT-specific threat scenarios. Detection capabilities rely on network traffic monitoring, industrial protocol analysis, and behavioural anomaly identification. Containment strategies must prioritize operational safety and system integrity, avoiding disruptive interventions that could compromise physical processes. Recovery procedures require validated system restoration protocols, controlled reactivation sequences, and documented post-incident review processes to support continuous improvement of response capability.

13. OT ASSET VISIBILITY AND CONTINUOUS MONITORING

Asset visibility constitutes the foundational prerequisite for effective OT security governance. Legacy devices, proprietary communication protocols, and the absence of native telemetry capabilities create significant blind spots in OT environments, necessitating the deployment of purpose-built passive monitoring solutions that do not disrupt operational processes. Continuous monitoring enables anomaly detection through protocol-aware traffic analysis and the establishment of behavioural baselines for normal operational patterns. Integration of OT monitoring capabilities with enterprise Security Operations Center (SOC) and Security Information and Event Management (SIEM) platforms ensures unified visibility across IT–OT boundaries, enabling correlated threat detection and coordinated response. This integration is an essential precondition for achieving the higher maturity levels described in the proposed framework, where proactive threat hunting and automated response capabilities are operational.

14. RECOMMENDATIONS FOR CANADIAN OIL AND GAS OPERATORS (2026–2030)

Based on the foregoing analysis, the following strategic priorities are recommended for operators seeking to advance OT cybersecurity maturity within the 2026–2030 planning horizon: Achieve comprehensive OT asset visibility through passive discovery and continuous inventory management. Implement secure remote access architectures with multi-factor authentication, privileged access management, and session recording for all third-party connectivity. Enforce network segmentation consistent with IEC 62443 zone and conduit models, with particular attention to IT–OT boundary controls. Deploy continuous OT network monitoring integrated with enterprise SOC/SIEM capabilities. Establish formalized supply-chain and vendor risk management programs with contractual cybersecurity obligations. Develop and regularly exercise OT-specific incident response plans incorporating safety-first containment protocols. Initiate Zero Trust Architecture [7] adoption, beginning with identity governance and segmentation as foundational elements. Formalize cybersecurity governance structures with board-level accountability and cross-functional leadership engagement. Proactively engage with evolving Canadian regulatory initiatives [4] to position for mandatory compliance requirements. Invest in OT-specific cybersecurity workforce development, including both technical skills and cross-disciplinary IT–OT competencies.

15.CONCLUSION

The convergence of OT with IT and cloud systems has transformed cybersecurity in Canada's energy sector from a technical function into a core element of operational resilience and national security. OT environments are now interconnected and exposed to advanced threats. Key risks stem from increased connectivity, legacy system weaknesses, and fragmented regulation, all of which expand vulnerability to supply-chain and ICS-targeted attacks. As a result, resilience has become central, requiring approaches such as Zero Trust, segmentation, continuous monitoring, and integrated IT–OT security. Addressing these challenges necessitates regulatory alignment, stronger public–private coordination, and sustained investment in technical and human capabilities to ensure secure and reliable energy operations.

REFERENCES

[1] NIST, “Guide to Operational Technology (OT) Security, SP 800-82 Rev. 3,” 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/82/r3/final.

[2] U. D. o. Commmerce, “NIST Cybersecurity Framework 2.0: Cybersecurity, Enterprise Risk Management, and Workforce Management Quick-Start Guide,” 2026. [Online]. Available: https://www.nist.gov/cyberframework.

[3] ISA.org, "ISA/IEC 62443 Series of Standards," [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[4] G. o. Canada, "The cyber threat to Canada’s oil and gas sector," [Online]. Available: https://cyber.gc.ca/en/guidance/cyber-threat-canadas-oil-and-gas-sector.

[5] IBM, "Cost of a Data Breach Report 2025," IBM, 2025. [Online]. Available: https://ibm.com/reports/data-breach.

[6] Dragos, "2026 OT Cybersecurity Year in Review," [Online]. Available: https://isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[7] NIST, "Zero Trust Architecture, SP 800-207," August 2020. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/207/final.