International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-15 Issue-5, June 2026

Cybersecurity Risk Frameworks for Mission-Critical Process Automation: From IT/OT Convergence to Zero-Trust Architectures

Mohammed Hazique Shaikh

Abstract: ***There is a gap in industrial cybersecurity. Above all, the frameworks that govern OT security, IEC 62443 for short, were built for a time when the air gap existed, and the threat model was physical. That era came to an end quietly, between the first remote vendor access agreement and the first cloud-connected historian. By 2024, more than 12,000 ICS-oriented cybersecurity incidents had occurred in one year, with dual IT/OT breaches averaging USD 4.56 million per event. Zero Trust Architecture, as specified in NIST SP 800-207, is the correct conceptual response: No longer should you trust your network location; verify everything at every step. The caveat is that NIST SP 800-207 is IT-oriented, and its accompanying implementation manual specifically excludes OT. No Zero Trust standard is specifically designed for OT. This paper examines the top-level cybersecurity governance platforms and their relevance to five dimensions of OT, presents a scenario of 2024-2026 industrially harmful environments, and introduces the Adaptive Zero Trust Framework for Industrial Control Systems (AZTF-ICS). AZTF-ICS is an innovative five-pillar model that uses Zero Trust principles to address the unique operational constraints of mission-critical process automation, with real-time requirements, high availability, and safety tasks that are not susceptible to interruption, irrespective of any security control policy.***

Keywords: IT/OT Convergence, Zero Trust Architecture, ICS Cybersecurity, IEC 62443, AZTF-ICS, Process Automation, Industrial Control Systems, NIST SP 800-207, ISAGCA, Operational Technology Security.

Nomenclature:
AZTF-ICS: Adaptive Zero Trust Framework for Industrial Control Systems

I. INTRODUCTION

The February 2021 water treatment plant incident in Oldsmar, Florida, was not sophisticated. Someone used a remote desktop tool to access the plant's HMI and attempted to raise the sodium hydroxide level in the water supply to 111 times the normal concentration. The attempt was caught by a vigilant operator who noticed the cursor moving on their screen. What was disturbing wasn't about the attack itself, but what it showed in practice, with respect to what the attacks highlighted about industrial cybersecurity practice: a key infrastructure facility connected remotely and opened via unsecured remote links (running Windows 7), using the same credentials that a handful of users share. This is not an outside phenomenon. It is characteristic of the IT/OT security stance of several thousand facilities worldwide.

It's hard to argue with the 2024 numbers. Industrial cyberattacks led to 146% year-on-year increases in operational impairments. Attacks on energy, transport, and water infrastructure by the state rose by 49%. Ransomware incidents in industrial organizations surged 87%, with manufacturing alone hosting 56% of the world's ransomware [8]. One hour of unplanned downtime costs more than USD 2.3 million for a large process facility. The average cyber-attack by a dual IT/OT breach now adds up to the total costs of USD 4.56 million [13].

The governance response has been piecemeal. IEC 62443 is the most complete OT security standard and good, but it does not explicitly cover Zero Trust. NIST SP 800-207 presents Zero Trust Architecture, but the OT exclusion is clear and unresolved. While the ISAGCA August 2024 whitepaper serves as a conceptual bridge between the two frameworks, it is guidance rather than a standard. There is no existing Zero Trust model, OT-specific, implementable in real-world OT environments within the community.

This paper fills that gap. It draws a map of the threat landscape and compares the leading frameworks; it introduces a new framework, AZTF-ICS, an original five-pillar framework aimed at operationalising Zero Trust in process automation environments, avoiding the safety and availability problems that make OT environments fundamentally distinct from IT.

II. IT/OT CONVERGENCE AND SECURITY CONSEQUENCES

A. Why the Air Gap Disappeared

OT environments were developed for reliability, not security. The CIA triad here works a little differently: Availability & safety are the key. Integrity is secondary. Confidentiality is often the last thing one needs in process control, but it's increasingly relevant when using plant data in enterprise analytics. From these priorities emerged a hierarchical and isolated architecture. This was

Manuscript received on 30 April 2026 | First Revised Manuscript received on 06 May 2026 | Second Revised Manuscript received on 18 May 2026 | Manuscript Accepted on 15 June 2026 | Manuscript published on 30 June 2026.
*Correspondence Author(s)
Mohammed Hazique Shaikh*, Department of Industrial Automation & Engineering, 161 Mechanic Street, Bellingham (MA), United States of America (USA). Email ID: haziqueshaikh@gmail.com, ORCID ID: 0009-0009-7991-6073

formalised in a five-level model based on the Purdue Reference Architecture, with field devices at the bottom and enterprise systems at the top (with deliberate network boundaries separating them [12]).

For purely practical reasons, this isolation eroded. Cloud-centric process historians require plant data. AI-Predictive Maintenance models require sensor streams, and remote vendor support requires access to controller diagnostics. Every single one of those legitimate businesses needs to punch a hole in the architecture intended to provide security via separation. By the end of 2025, about 41.6 billion devices were connected to global networks, which include a growing share of industrial and operational technology applications [15]. That connectivity is standard, no exception.

B. Three Vulnerabilities that Represent the Converged Attack Surface

The first is legacy. OT hardware operates for between 15 and 30 years. A lot of what we have in service today runs on operating systems that reached the end of their lifespans many years ago, with firmware that doesn't support updates. Typically, installing a security agent on a twenty-year-old PLC may be beyond the technical capabilities. Deep packet inspection can add latency, impacting millisecond-level control loops. Security procedures that work well in IT environments often disrupt OT processes.

The second is organizational. IT teams and OT teams can be viewed as structurally distinct: different reporting lines, different risk tolerances, different vocabularies. Patching decisions, remote access controls, and any network architecture changes that demand coordination between IT and OT are often left in a governance vacuum between the two organisations. Unmanaged remote access was reported in the DoD Zero Trust for OT report to be one of the most consistently exploited entry points in industrial breach investigations [6].

This third one is governance maturity. By 2025, 52% of organizations had moved OT security to the CISO, up from only 16% for 2022 [11]. But being in an org chart doesn't mean operation-level integration, at least not as well as these organizations did: of those organizations, only 35% reported a genuinely integrated IT/OT security operations model [14]. If operational capability doesn't exist, then CISO ownership is restructuring the theatre. The attacks don't care about the org chart.

III. CYBERSECURITY FRAMEWORK COMPARATIVE ANALYSIS

No one-size-fits-all model governs industrial cybersecurity. Table I compares the six most relevant frameworks along four dimensions: OT relevance, Zero Trust alignment, implementation maturity, and primary limitation.

Table I: Cybersecurity Framework Comparison with ICS

Framework	Primary Focus	OT Rel.	ZT Align.	Key Limitation
IEC 62443 SL2/SL3	Zones, conduits, and IACS security levels	High	High	No explicit ZT guidance
NIST SP 800-82 Rev.3	OT Security Architecture/ICS Controls	High	Moderate	IT-centric control derivation
NIST SP 800-207	Zero Trust Architecture principles	Low	High	Explicitly excludes OT scope
ISAGCA ZT Whitepaper	ZT mapped to IEC 62443 for OT	High	High	Guidance only, not a certifiable standard
MITRE ATT&CK ICS	Adversary TTPs for ICS environments	High	Moderate	Detection only, no governance model
Purdue Model (PERA)	ICS network segmentation hierarchy	Moderate	Low	Engineering reference, not a security framework

Source: Author synthesis [1], [2], [3], [4], [5], [12], [16]

A. IEC 62443: OT Security Baseline

IEC 62443 is the most advanced, operational approach for IACS cybersecurity. Its zone-and-conduit model, Security Levels SL1 to SL4, and clear requirement that security controls should not impact critical process functions are all very appropriate for an OT environment. SL2 and SL3 have proved to be practical objectives for mission-critical applications [1]. The ISAGCA whitepaper from August 2024 does important bridging work: it depicts—concretely—just how IEC 62443 zones, conduits, and least-privilege access controls map directly to Zero Trust principles [5]. But the standard itself was not designed as a Zero Trust framework, and that gap matters operationally.

B. NIST SP 800-207: The OT Exclusion Problem

The concept for the converged IT/OT threat environment describes Zero Trust Architecture defined by NIST SP 800-207 [3]. Eliminate implicit trust. Verify everything continuously. Enforce least privilege at every transaction. These principles directly address the attack trends that have permeated industrial environments, especially those that leverage legitimate credentials and protocols to minimise detection. The issue is structural: The implementation companion NIST SP 1800-35 explicitly claims not to include OT and marks this as a separate treatment issue [4]. That discrete treatment has not been delivered. There is no OT-specific ZTA standard. AZTF-ICS is a reaction to this lack.

IV. THE INDUSTRIAL THREAT LANDSCAPE

Table II outlines the primary threat vectors to converged IT/OT environments, based on reports from Dragos, ENISA, Honeywell, and CISA for 2024-2026.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Table II: Key Threat Vectors in Converged IT/OT Environments

Threat Vector	Attack Type	OT Impact	Priority
IT-to-OT Lateral Movement	Ransomware pivot	Production halt, safety risk	Critical
Remote Access Exploitation	Credential theft, VPN abuse	Unauthorized control access	Critical
Supply Chain Compromise	Trojanised firmware	Persistent backdoor	High
Nation-State APT	Long-dwell intelligence	Critical infrastructure disruption	High
IIoT Device Exploitation	Default credentials, unpatched FW	Network foothold, lateral spread	High

Sources: [8], [9], [10], [19]. FW = firmware.

A. Ransomware: from Data to Operations

Ransomware targeting industrial targets has evolved. Early campaigns encrypted data and threatened to pay for decryption keys. The current generation attacks operational continuity head-on, acknowledging that a factory or refinery will pay more to restore production than to recover the data. Honeywell has reported over 2,400 ransomware attacks in Q1 2025 only, compared to 6,130 in all of 2024 (annualized run rate suggesting the trend remains accelerating and not stabilizing [10]). Manufacturing bore 56% of the worldwide increase [8]. The economics of ransomware payments are structurally different from those in IT environments, where downtime costs USD 2.3 million per hour.

B. Targeting Critical Infrastructure in State-Sponsored Attacks

Industrial control systems are now bona fide strategic targets of nation-state actors [17]. A 49% increase in attacks (in line with state interests) on energy, transport, and water infrastructure in 2024 [8]. CISA verified a range of compromises by pro-Russian hacktivist groups targeting industrial equipment using commodity tools, including legacy VNC programs and limited or shared credentials. During the same period, IRGC-affiliated actors attacked programmable logic controllers and HMIs targeting adversarial areas. In December 2025, CISA issued specific guidance on risks related to AI integration in OT environments, with model drift and safety process bypass as new attack vectors [19] a glimpse into how the terrain of threat would change as AI integrates with industrial control.

V. ADAPTIVE ZERO TRUST FRAMEWORK FOR INDUSTRIAL CONTROL SYSTEMS (AZTF-ICS)

AZTF-ICS is a legitimate solution since a direct port of NIST SP 800-207 into OT environments would break them. The never-trust, always-verify principle in theory works. In practice, it is not much of a configuration challenge to make it operational for a safety instrumented system that should execute the shutdown logic within 500 milliseconds, without relying on any network-based authentication service. It constitutes architectural incompatibility. AZTF-ICS addresses this incompatibility through a tiered exception management system, where Zero Trust can be enforced with zero tolerance and clear exceptions when the operational autonomy of safety functions must outweigh the enforcement policy. The framework combines the zone-and-conduit paradigm of IEC 62443 with the identity-centric, continuous-verification philosophies of NIST SP 800-207 across five functional pillars.

A. Pillar 1: Classification of Assets with Risk Strata

With AZTF-ICS, nothing begins until we make a judgment of the class, four layers based on the operational relevance. Tier 1 is safety-critical systems: Safety Instrumented Systems, Emergency Shutdown Devices, and protection functions. Zero Trust controls only apply along zone boundaries. Within the zone, communication among safety components remains independent and uninterruptible. No authentication service, no policy engine, and no network monitoring tool touches any part of the SIS execution path. This is not a security gap. It is indeed the implementation of the ISAGCA constraint: Zero Trust must not prevent critical safety functions from working [5].

Tier 2 includes process-critical assets: DCS controllers, PLCs, SCADA servers, HMIs. ZT for only human access: Conditional. Rather than continuous authentication, which would introduce unacceptable latency in time-critical control loops, allowlisted behavioural baselines govern device-to-device communication. Tier 3 is for operational infrastructure, including process historians, engineering workstations, and OT data aggregators. Full ZTA with micro-segmentation and least-privilege apply here. Tier 4 includes enterprise interfaces: IT/OT integration gateways, remote-access infrastructure, and business intelligence feeds. This is the intersection of the IT and OT domains, making it the highest-density area for ZT controls.

B. Pillar 2: Identity-Centric Access Governance

Each entity that comes into contact with the OT environment requires a verifiable identity. This is true whether this entity is a human operator, a vendor engineer connecting remotely, an automated process, or a hardware device. In this new era of capable platforms, hardware-rooted identity is the standard, enabled by TPM 2.0. Legacy devices that cannot provide hardware identity necessitate proxied attestation to a security gateway at the zone boundary.

Human access in Tier 2 and higher is governed by role-based, limited-time credentials provided through privileged access management systems, and multi-factor authentication is mandatory for all remote session access. Vendor/Contractor access is subject to the strictest controls: just-in-time access grants, mandatory session recording, and automatic expiration. The underlying reason is simple: remote third-party access has been the gateway to a disproportionate share of reported ICS breaches. Oldsmar is an example of this.

C. Pillar 3: Dynamic Micro Segmentation

Zones and conduits of IEC 62443 serve as the conceptual model. AZTF-ICS applies it at the software layer through policy-driven micro-segmentation without the need for physical network redesign. The implementation needs to be sequenced carefully. Before you enforce any allowlist

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

policy, establish 60 to 90 days of behavioural baselines for device communications. In more complex process environments, such as seasonal or batch production cycles, 90 to 120 days may be necessary to capture the full operational envelope. Enforcing the allowlist before the baseline is complete triggers an alert volume that OT operations teams cannot digest, leading to false positives and prompting operators to disable monitoring rather than investigate.

The order: behavioural baseline first, allowlist enforcement at Tier 1 and Tier 2 second, dynamic policy enforcement in Tier 3 and Tier 4 third. This is progressive, not big bang.

D. Pillar 4: Continuous Monitoring and Threat Intelligence

Zero Trust is not an accomplishment; it is a commitment. It is an operational discipline that demands ongoing data collection, data analysis, and action. AZTF-ICS mandates a unified monitoring posture on IT and OT events for a uniform security operations function and MITRE ATT&CK taxonomy for ICS classification [16]. Practical experience here has revealed a recurring issue: IT SOC tools used without knowledge of OT protocols result in false-positive rates that are simply unacceptable in operational environments. Operators who get false alarms learn to ignore every single one again. It's not optional to invest in OT-specific detection logic, parsers for protocols like Modbus, DNP3, PROFINET, and similar protocols, and OT-context-aware analysts. In addition to adversarial techniques to poison training data of AI-driven OT security tools, which degrade detection ability over time, the 2025 Threat Landscape from ENISA raises another point of concern [9]. Adversarial robustness should be baked into decision engines that design detection models.

E. Pillar 5: Lifecycle Security Governance

The longest-lived assets in OT environments are not the hardest to secure when new. They are the hardest to secure over decades of operation. AZTF-ICS makes lifecycle security a foundational governance issue: secure procurement through supply chain risk assessment; verified firmware integrity—critical during commissioning and every update; cryptographic key rotation on pre-defined schedules; and cybersecurity requirements baked into engineering change management instead of tacked on as an afterthought [18]. Auditing trails must be tamper-resistant, and event logs stored in a read-only format must be sent to centralized monitoring systems that track assets from Tier 1 through Tier 3. These logs enable IEC 62443 SL2/SL3 compliance, forensic investigation within the event scenario, and the continuous evolution of the monitoring models outlined in Pillar 4.

VI. RESULT AND DISCUSSION

A. What AZTF-ICS adds that Existing Frameworks don't

AZTF-ICS is not a substitute for IEC 62443 or NIST SP 800-207. Let me be upfront about that. Both are better-resourced, better-validated frameworks built by consensus bodies with substantial industry input. What AZTF-ICS does is serve as the translation layer between them. IEC 62443 does not mention Zero Trust. OT is not included in NIST SP 800-207. The ISAGCA whitepaper connects them conceptually, not explicitly, how. AZTF-ICS shows how: through the tiered exception model that makes Zero Trust enforcement safe at Tier 1, practical at Tier 2, and fully rigorous at Tiers 3 and 4.

The architectural innovation is the tier exception model. It's the mechanism that resolves the fundamental conflict between ZTA's never-trust principle and the ISAGCA restriction that Zero Trust must absolutely keep vital safety functions from running. By limiting ZT to zone boundaries at Tier 1 and enforcing progressively more strictly upward through the tiers, AZTF-ICS makes Zero Trust feasible in environments where blanket implementation could not be tolerated, as it would cause unacceptable safety risks.

Three observations based on the practitioner deployment experience. In energy, chemical, water treatment, and manufacturing deployments, three results are constant across deployments and findings consistent with each application:

First: Behavioural baselines take longer than anticipated. In climates with seasonal demand dynamics, monthly or quarterly batch cycles, or production schedules that vary according to feedstock availability, setting a reliable baseline for allowlist enforcement may take four to six months. 30-day plans don't work. Baseline is not administrative overhead; it is the tech base on which it all rests in Pillar 3.

Second, IT SOC integration is more complicated than it appears on paper. Generic IT security information and event management tools lack awareness of OT protocols, leading to false-positive rates that OT operations teams cannot sustain. OT-specific detection logic should be a must-have, not a nicety, but is continually poorly budgeted in organizations at least approaching this for the first time.

Third: Tier 1 exception governance should be the most politically challenging part of the implementation. Agreement on what measures constitute an essential element of safety, and, as such, what it considers a ZT exception boundary, rests on a shared definition among process safety engineers, cybersecurity professionals, and operations leadership. This sort of cross-functional decision is almost impossible for these groups to navigate effectively within the organisation. The biggest source of delays in deploying the AZTF-ICS pillar structure is the governance bottleneck, rather than any technical failings.

B. Limitations and Future Development

AZTF-ICS is a practice-informed conceptualization. The next step is formal empirical validation across a plethora of industrial sectors, on a deployment scale. The framework does not yet extend to AI-driven control systems: the integrity of ML model inference on edge control nodes is a new frontier. It requires treatment beyond the five-pillar model. The regulatory environment is maturing too: DoD DTM 25-003, issued in July 2024, imposes Zero Trust on all classified and unclassified systems, ultimately establishing compliance requirements for industrial systems. found in defence-adjacent sectors [7], [20]. These evolving mandates will need to be adopted in future AZTF-ICS revisions alongside the

voluntary standards currently defining the field.

VII. CONCLUSION

The governance of industrial cybersecurity is long overdue for a fundamental redesign. Data from 2024-2025:>12,000 ICS incidents on hand, a +49% increase in state-aligned infrastructure attacks, and ransomware rates accelerating at nearly double the rate in industries demonstrate just what frontline practitioners already knew: the perimeter model has vanished, and frameworks built for it were not good enough. IT and OT have converged for years, and the trend has been irreversible. Security architecture, however, has not kept up.

You are right that Zero Trust is the ideal conceptual response. But by no means should Zero Trust, as defined in IT environments, be transplanted directly into OT without introducing new risks. Safety functions should stay independent. Authentication latency cannot be absorbed through control loops. Security agents cannot run in legacy systems. These are not objections to Zero Trust. They are the constraints a whole OT Zero Trust framework must work around.

AZTF-ICS addresses these by building in the hierarchical exception model as follows: strict ZT enforcement for enterprise interfaces and operational infrastructure, conditional ZT for process-critical assets and zone-boundary-only ZT for safety-critical systems. The five pillars, risk-stratified classification, identity-centric access governance, dynamic micro-segmentation, continuous monitoring, and lifecycle security governance, offer an operational architecture that makes the principles operative, not dream-like.

For practitioners in real manufacturers, energy and chemical, and water treatment companies with security decisions made in real production environments, AZTF-ICS offers something that is lacking in the literature: a structured roadmap to zero trust from perimeter dependency that respects and validates the limitations of implementation that characterise process automation.

DECLARATION STATEMENT

As the article's author, I must verify the accuracy of the following information after aggregating input from all authors.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted objectively and without external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. ISA/IEC, "ANSI/ISA 62443: Security for Industrial Automation and Control Systems," International Society of Automation, 2018. [Online]. Available: https://www.isa.org/standards-and-publications/isa-iec-62443-series-of-standards
2. National Institute of Standards and Technology, "Guide to Operational Technology (OT) Security," NIST Special Publication 800-82, Revision 3, 2023. DOI: https://doi.org/10.6028/NIST.SP.800-82r3
3. National Institute of Standards and Technology, "Zero Trust Architecture," NIST Special Publication 800-207, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207
4. National Cybersecurity Centre of Excellence (NCCoE), "Implementing a Zero Trust Architecture," NIST SP 1800-35 (Fourth Draft), 2024. [Online]. Available: https://www.nccoe.nist.gov/zero-trust-architecture
5. ISA Global Cybersecurity Alliance (ISAGCA), "Zero Trust Outcomes Using ISA/IEC 62443 Standards," ISAGCA Whitepaper, August 2024. [Online]. Available: https://www.isagca.org/zero-trust-outcomes-using-isa-iec-62443-standards
6. U.S. Department of Defence, "Zero Trust for Operational Technology Activities and Outcomes, Version 2," DoD CIO, November 2025. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-OT-v2.pdf
7. U.S. Department of Defence, "DTM 25-003: Implementing the DoD Zero Trust Strategy," July 2025. [Online]. Available: https://www.defense.gov/News/Releases/Release/Article/dtm-25-003-zero-trust
8. Dragos, Inc., "OT Cybersecurity Year in Review 2025," Dragos, Inc., 2025. [Online]. Available: https://www.dragos.com/year-in-review/
9. European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2025," ENISA, 2025. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
10. Honeywell International, "Ransomware in Q1 2025: OT Threat Analysis," Honeywell International, 2025. [Online]. Available: https://www.honeywell.com/us/en/press/2025/q1-ot-ransomware-analysis
11. PwC, "Emerging OT Threats and Cybersecurity Strategies 2026," PricewaterhouseCoopers, 2025. [Online]. Available: https://www.pwc.com/gx/en/issues/cybersecurity/emerging-ot-threats
12. SANS Institute, "Introduction to ICS Security Part 2: The Purdue Model," SANS ICS, July 2021. [Online]. Available: https://www.sans.org/white-papers/ics-security-purdue-model-introduction/
13. IBM Security, "Cost of a Data Breach Report 2024," IBM Corporation, 2024. [Online]. Available: https://www.ibm.com/reports/data-breach
14. Claroty, "Five Important Considerations for Implementing Zero Trust in OT Environments," Claroty, 2024. [Online]. Available: https://claroty.com/resources/whitepapers/zero-trust-ot
15. IoT Analytics, "OT Cybersecurity Insights Report 2026," IoT Analytics, December 2025. [Online]. Available: https://iot-analytics.com/ot-cybersecurity-insights
16. The MITRE Corporation, "ATT&CK for ICS Framework," The MITRE Corporation, 2024. [Online]. Available: https://attack.mitre.org/matrices/ics/
17. Industrial Cyber, "Bridging the Gap: Integrating Zero Trust Strategies in IT and OT Environments," Industrial Cyber, November 2024. [Online]. Available: https://industrialcyber.co/zero-trust/bridging-it-ot-zero-trust
18. North American Electric Reliability Corporation (NERC), "Zero Trust Security for Electric Operating Technology," NERC, June 2023. [Online]. Available: https://www.nerc.com/pa/CI/Documents/ZeroTrust_OT.pdf
19. Cybersecurity and Infrastructure Security Agency (CISA), "Guidance on Secure Integration of AI in Operational Technology," CISA, December 2025. [Online]. Available: https://www.cisa.gov/resources-tools/resources/guidance-secure-integration-ai-operational-technology
20. DoD CIO, "Zero Trust Capability Execution Roadmap for Operational Technology," DoD Chief Information Officer, 2024. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-OT-Roadmap.pdf

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

AUTHOR'S PROFILE

Mohammed Hazique Shaikh is a Senior Future Offer Manager in the Industrial Automation division at Schneider Electric, where he leads new product introduction strategy and execution for next-generation software-defined industrial controllers. His professional work focuses on developing open automation platforms, edge computing architectures, and product value proposition frameworks for mission-critical process automation environments across the energy, chemical, water treatment, and manufacturing sectors. He holds a Master of Science in Engineering Management from Northeastern University, Boston, MA, and a Bachelor of Technology in Mechanical Engineering from the Vellore Institute of Technology, India. Before his current role, he held engineering and product management positions at Tata Consultancy Services, where he led cross-functional teams delivering technology products for Ford Motor Company and Mitsubishi Motors across automotive electronics, battery management systems, and ADAS domains. His research interests include software-defined industrial automation, open process automation standards, edge computing for process control, cybersecurity in IT/OT converged environments, and product strategy in engineering-intensive B2B technology markets.