International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1(s) (2026)

www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

Need of Cyber Security in Operational Technologies (OT) (Electronics) When Connected to the Internet of Things (IoT)

Prof. Ambarish Nandkumar Kulkarni,

Abhinav Education Society's College of Computer Science and Management, Ambegaon Bk, Pune-411046

E-Mail: Ambarish.n.kulkarni@gmail.com

Abstract

The convergence of Operational Technology (OT) and the Internet of Things (IoT) under Industry 4.0 has created highly integrated cyber-physical systems with significantly expanded attack surfaces. While OT environments historically prioritized reliability and safety over connectivity, integration with IP networks, cloud services, and 5G-enabled edge devices exposes critical infrastructure to threats such as ransomware, supply-chain compromises, and OT-specific malware. This paper examines cybersecurity risks at the intersection of OT and IoT, characterizes key threat vectors and real-world incidents, and maps a defense-in-depth strategy to established standards including IEC 62443 and NIST SP 800-82. We further highlight tools, regulatory developments, and future trends such as AI-driven autonomous defense, quantum-resistant cryptography, and blockchain-based integrity mechanisms that are reshaping OT/IoT security architectures. The results underscore that OT security, when coupled with IoT, must be addressed as a strategic, cross-disciplinary concern rather than an isolated technical task.

Index Terms— Internet of Things (IoT), Operational Technology (OT), industrial control systems (ICS), cyber-physical systems, IEC 62443, NIST SP 800-82, ransomware, defense-in-depth.

I. INTRODUCTION

Digital transformation across manufacturing, energy, water, transport, and smart city domains is accelerating adoption of IoT and convergence of OT with traditional IT. IoT devices with embedded sensing, processing, and communication capabilities now monitor and control physical processes that were previously confined to isolated industrial control systems (ICS), enabling advanced analytics, predictive maintenance, and remote operations. However, these benefits come at the cost of a larger attack surface, heterogeneous device ecosystems, and complex multi-domain risk profiles that challenge traditional perimeter-based security paradigms.

Historically, OT networks were "air-gapped" and relied on proprietary protocols, with security assumptions rooted in physical isolation. The introduction of IP-based connectivity, remote access, and cloud integration has eroded these assumptions and enabled attackers to bridge IT and OT domains. High-impact incidents such as ransomware in energy pipelines, attacks on water treatment facilities, and tailored OT malware demonstrate that cyber threats can produce direct physical consequences.

This paper addresses the following research question: **Why is cyber security essential for OT when tightly integrated with IoT, and how can organizations systematically mitigate the resulting cyber-physical risk?** We pursue four objectives:

1. Define and distinguish IoT and OT in the context of cyber-physical systems.
2. Analyze IT–OT convergence and its security implications.
3. Characterize key challenges, threat vectors, and representative incidents.
4. Propose a defense-in-depth approach aligned with IEC 62443 and NIST SP 800-82 and outline future research directions.

The remainder of this paper is organized as follows: Section II presents background on IoT and OT; Section III describes IT–OT convergence; Section IV discusses key challenges; Section V analyzes threats; Section VI summarizes case studies; Section VII outlines defensive strategies and standards; Section VIII discusses future trends; and Section IX concludes.

II. BACKGROUND: IoT AND OPERATIONAL TECHNOLOGY

A. Internet of Things (IoT)

The Internet of Things is an ecosystem of networked devices embedded with sensors, software, and connectivity enabling data exchange and autonomous interaction. Typical IoT deployments span consumer wearables and smart home devices to industrial sensors, connected vehicles, and environmental monitoring nodes in critical infrastructure. Projections indicate tens of billions of IoT devices in operation in the mid-2020s, driven by decreasing hardware costs, cloud services, and high-bandwidth wireless technologies such as 5G.

Despite rapid growth, security in many IoT devices remains limited. Common weaknesses include default or hard-coded credentials, unencrypted communication channels, minimal logging, and lack of secure over-the-air (OTA) update mechanisms. Resource constraints on microcontrollers (CPU, memory, battery) further restrict adoption of strong cryptographic algorithms and conventional endpoint protection agents.

B. Operational Technology (OT)

Operational Technology encompasses hardware and software systems used to monitor and control physical processes in industrial environments. Key components include programmable

logic controllers (PLCs), supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and human–machine interfaces (HMIs). These systems are pervasive in power generation and distribution, oil and gas pipelines, water treatment plants, manufacturing lines, transportation systems, and building automation.

OT systems are designed with priorities markedly different from IT: availability, determinism, and safety are paramount, and unplanned downtime can lead to equipment damage, environmental impact, or loss of life. Many OT installations run for decades using proprietary protocols and obsolete operating systems that were never intended for exposure to the public internet.

III. IT–OT CONVERGENCE

In pursuit of operational efficiency, real-time analytics, and remote management, organizations are increasingly connecting OT systems to IT networks and cloud platforms. Typical use cases include centralized monitoring, predictive maintenance, remote diagnostics, and integration of shop-floor data into enterprise resource planning (ERP) systems. This convergence introduces Ethernet, Wi-Fi, and IP-based protocols into environments that previously relied on isolated fieldbuses and serial communications.

The security implications of IT–OT convergence are profound:

- Attack paths from IT to OT: Compromise of corporate IT assets can enable lateral movement into OT networks, impacting safety-critical control systems.
- Exposure of insecure protocols: Legacy OT protocols without authentication or encryption become accessible over routable networks.
- Expanded supply-chain dependencies: Cloud services, remote vendors, and integrators introduce additional trust relationships and potential attack vectors.

As a result, OT can no longer rely on isolation as a primary security control. Instead, it must adopt structured architectures that integrate cyber security principles across both IT and OT layers.

IV. CHALLENGES IN OT/IoT CYBER SECURITY

A. Legacy Systems and Technical Debt

A large proportion of OT assets operate on outdated operating systems (e.g., unsupported versions of Windows) that cannot easily be patched or upgraded without significant downtime or certification challenges. These legacy systems often lack basic hardening features and host software that is no longer supported, resulting in persistent vulnerabilities.

B. Resource-Constrained, Heterogeneous Devices

IoT devices are frequently constrained in CPU, memory, and energy, limiting the feasibility of computationally expensive cryptography and continuous security monitoring. Furthermore, the ecosystem is highly heterogeneous, comprising many vendors, proprietary stacks, and varying update mechanisms, complicating centralized asset and vulnerability management.

C. Limited Visibility and Scalability

Organizations may lack a comprehensive inventory of OT and IoT assets, their firmware versions, network paths, and communication patterns, which hampers risk assessment and incident response. Manually managing security policies for thousands or millions of devices is impractical, making automation and standardized telemetry essential.

D. Physical–Digital Coupling and Safety Risk

In OT/IoT environments, cyber incidents can directly impact physical processes, for example by altering chemical dosing, changing set-points, or disabling protection systems. This physical–digital nexus elevates the impact of security failures and requires safety-aware incident response procedures that differ from conventional IT playbooks.

V. THREAT LANDSCAPE AND ATTACK VECTORS

A. IoT-Focused Threats

1. **Botnets and Distributed Denial of Service (DDoS):** Insecure IoT devices have repeatedly been conscripted into large botnets used to launch DDoS attacks against critical services and internet infrastructure. Weak default credentials and open management interfaces contribute to mass compromise.
2. **Man-in-the-Middle (MitM) Attacks:** Use of unencrypted or weakly authenticated protocols enables adversaries to intercept and modify telemetry or commands, undermining integrity and potentially enabling stealthy manipulation of processes.
3. **Firmware and Supply-Chain Compromise:** Attackers may reverse-engineer firmware to discover vulnerabilities or introduce malicious code into update channels, affecting large fleets of devices simultaneously.

B. OT-Specific Threats

1. **Ransomware in Industrial Environments:** Recent ransomware attacks against pipeline operators and manufacturing firms have triggered operational shutdowns, regional fuel shortages, and large financial losses. Sensitive OT networks are often indirectly impacted by IT-focused ransomware due to shared infrastructure and poor segmentation.
2. **Tailored OT Malware:** Stuxnet demonstrated the feasibility of malware specifically designed to alter PLC logic while falsifying telemetry to operators, enabling covert

sabotage of physical equipment. Subsequent malware families have continued to target ICS components and protocols.

3. **Insecure Industrial Protocols:** Protocols such as Modbus and DNP3 lack built-in authentication and encryption, making them susceptible to replay, spoofing, and command-injection attacks when accessible beyond tightly controlled networks.

C. Emerging Vectors

Emerging threats include malicious tampering in hardware supply chains, insider-enabled attacks leveraging stolen credentials, and exploitation of edge and 5G architectures that connect cloud services directly to field devices. These developments demand continuous reassessment of trust boundaries and monitoring coverage.

VI. CASE STUDIES

A. Colonial Pipeline Ransomware Incident

In 2021, ransomware actors exploited a compromised VPN account lacking multi-factor authentication to infiltrate an energy pipeline operator, leading to a shutdown of fuel delivery on the U.S. East Coast. The incident highlighted the interdependence of IT and OT networks, the importance of strong identity controls, and the need for segmentation between enterprise and control environments.

B. Oldsmar Water Treatment Facility

Attackers obtained remote access credentials for a water treatment plant's remote desktop software and attempted to alter sodium hydroxide levels to unsafe values. An attentive operator observed the change and manually reverted it, preventing harm and demonstrating the continued importance of human oversight in OT operations.

C. Stuxnet

The Stuxnet worm targeted Siemens Step7 software and PLCs at an Iranian nuclear facility, spreading via USB drives and exploiting multiple zero-day vulnerabilities. By subtly altering centrifuge speeds while falsifying sensor readings, it destroyed equipment and delayed operations, proving that cyber-physical sabotage is technically feasible and challenging to detect.

D. OT Monitoring Deployments

Recent deployments of passive, agentless OT monitoring solutions in sectors such as pharmaceuticals and water utilities have demonstrated rapid asset discovery, detection of misconfigurations (e.g., open shares, rogue devices), and generation of remediation playbooks without disrupting production. These deployments exemplify practical steps toward improving OT/IoT situational awareness.

VII. DEFENSIVE STRATEGIES AND STANDARDS

A. Defense-in-Depth Architecture

A multi-layered architecture is essential to limit the blast radius of compromises and provide overlapping protections.

1. **Zero Trust and Segmentation:** Zero Trust principles advocate continuous verification of users and devices, least-privilege access, and micro-segmentation to constrain lateral movement. Applying Purdue-style zoning with demilitarized zones (DMZs) between IT and OT aligns with IEC 62443 concepts of zones and conduits.
2. **Industrial DMZs:** Proxy-based industrial DMZs mediate communication between enterprise systems and control networks, preventing direct inbound connectivity to control devices and reducing exposure of industrial protocols.

B. Technical Hardening

1. **Secure Device Configuration:** Enforcing secure boot, hardware roots of trust (e.g., TPM), and certificate-based authentication mitigates device spoofing and unauthorized firmware modification.
2. **Encryption:** Adoption of contemporary cryptographic protocols for data in transit and at rest, with lightweight variants for constrained devices, protects confidentiality and integrity over untrusted networks.
3. **Patch and Vulnerability Management:** Automated OTA updates for IoT devices and carefully staged patching for OT—supported by comprehensive testing—are critical to address known vulnerabilities without jeopardizing availability.

C. Monitoring and Incident Response

1. **Security Monitoring and Anomaly Detection:** SIEM platforms and OT-aware network detection tools build baselines of normal behavior and employ AI/ML to detect anomalies such as unusual PLC command patterns or unauthorized protocol use.
2. **Deception Technologies:** Honeypots and decoy assets deployed in industrial networks provide high-fidelity alerts with minimal operational risk and can slow or mislead attackers.
3. **OT-Specific Incident Response:** Response plans must prioritize human safety and process integrity, including safe shutdown procedures, validated recovery sequences, and coordination with engineering teams.

D. Standards and Regulatory Guidance

IEC 62443 offers a comprehensive, lifecycle-oriented framework for securing industrial automation and control systems, covering product development, system design, and organizational processes. NIST SP 800-82 provides guidance for ICS security, including risk

management, network architecture, and access control recommendations. Emerging regulations, such as the EU Cyber Resilience Act, further promote secure-by-design requirements for network-connected products, including IoT devices.

VIII. FUTURE TRENDS AND RESEARCH DIRECTIONS

Several trends will shape OT/IoT cyber security:

- **AI-Driven Autonomy:** AI-based detection and automated response mechanisms promise self-healing networks capable of isolating compromised segments and adapting defenses dynamically, though adversarial AI remains a concern.
- **Post-Quantum Cryptography:** As quantum computing advances, post-quantum algorithms will be needed to secure long-lived OT and IoT deployments against "harvest-now, decrypt-later" attacks.
- **Blockchain-Based Integrity and Provenance:** Distributed ledgers can support tamper-evident firmware distribution, device identity management, and supply-chain transparency for critical OT assets.
- **6G and Advanced Edge Computing:** Future communication and edge architectures will embed new security primitives but will also introduce novel attack surfaces, requiring updated threat models and controls.
- **Sustainable, Secure IoT:** Designing energy-efficient yet secure IoT solutions is vital to support sustainable industrial operations without compromising resilience.

IX. CONCLUSION

As OT becomes deeply interconnected with IoT and IT infrastructures, security cannot rely on isolation, obscurity, or ad-hoc controls. This paper has shown that legacy assets, heterogeneous and resource-constrained devices, insecure protocols, and the physical consequences of cyber-physical attacks collectively demand a proactive, defense-in-depth approach grounded in standards such as IEC 62443 and NIST SP 800-82. Organizations must integrate robust architecture design, technical hardening, continuous monitoring, and safety-aware incident response into unified strategies that span IT, OT, and IoT domains. Building such resilience is inherently cross-disciplinary, requiring collaboration among engineers, cyber security specialists, and decision-makers to ensure that safety and reliability remain central in increasingly connected industrial environments.

REFERENCES

[1] cases - iOT365: All-in-one AI-Powered Cybersecurity Platform for OT and IoT
https://iot365.io/cases/

[2] cases - Cutting-edge Agent-less Threat Detection System, iot365 https://iot-365.net/cases/

[3] Strengthen Operational Resilience Against Targeted OT Threats https://live.paloaltonetworks.com/t5/community-blogs/strengthen-operational-resilience-against-targeted-ot-threats/ba-p/1248890

[4] OT/IoT Cybersecurity Trends & Insights 2026 - Nozomi Networks https://www.nozominetworks.com/ot-iot-cybersecurity-trends-insights-2026

[5] IoT/OT Security Startup Funding Strategies for 2026 Success https://qubit.capital/blog/funding-iot-ot-security-startups

[6] Internet of Things (IoT) security: A challenge for 2026 - Fabrity https://fabrity.com/blog/internet-of-things-iot-security-a-challenge-for-2026/

[7] Dragos 2026 OT Cybersecurity Report: A Year in Review https://www.dragos.com/ot-cybersecurity-year-in-review

[8] IoT Security: Business Case Studies https://iln.ieee.org/public/contentdetails.aspx?id=7F3386A71BAB48DA8EEA8345515422DA

[9] Uncertainty, undone: A 2026 OT/IoT Cybersecurity Strategy for ... https://www.nozominetworks.com/resources/uncertainty-undone-a-2026-ot-iot-cybersecurity-strategy-for-converged-environments

[10] The Top 8 IT/OT/IoT Security Challenges and How to Solve Them https://www.balbix.com/insights/addressing-iot-security-challenges/

[11] Industrial IoT Security: Top 12 Rules for Improved IIoT Safety https://www.itransition.com/iot/industrial-security

[12] What Is Industrial Internet of Things (IIoT) Security? https://www.paloaltonetworks.in/cyberpedia/what-is-iiot-security

[13] IIoT Cybersecurity Explained https://gca.isa.org/blog/iiot-cybersecurity-explained