# **The New Industrial Threat Paradigm: Exploits in Manufacturing and Strategic Cybersecurity Countermeasures**

## **Executive Summary**

The manufacturing sector is at a critical juncture. The cyber threat landscape has undergone a significant transformation, shifting from a focus on data theft to a new paradigm of physical disruption. While the overall number of documented attacks saw only a minor increase in 2024, their impact escalated dramatically, with the number of sites experiencing physical consequences surging by a remarkable 146%.1 This escalation is not primarily the result of direct assaults on operational technology (OT) systems but is driven by a new and highly effective tactic: exploiting the vulnerabilities in interconnected IT systems to pivot into and manipulate industrial environments. This report provides a detailed analysis of this trend, deconstructing the common attack vectors targeting core equipment such as SCADA, Distributed Control Systems (DCS), and Human-Machine Interfaces (HMIs). It also examines the strategic, research-backed countermeasures being developed to combat these threats, from new hardware-based detection methods to the adoption of sophisticated frameworks like NIST and ISA/IEC 62443. The central finding is that a critical chasm exists between the priorities and expertise of IT and OT teams, a gap that adversaries are systematically exploiting. Bridging this intellectual and architectural divide is no longer a technical consideration but a strategic imperative for operational and financial resilience.

## **1. The Evolving Threat Landscape: Trends and Strategic Implications for Manufacturing**

### **1.1. A New Paradigm of Escalation: The Rise of Physically Disruptive Attacks**

The most profound trend in the industrial cyber threat landscape is the growing chasm between attack frequency and attack impact. Data from a 2025 OT Cyber Threat Report indicates that while the number of attacks rose only slightly from 72 in 2023 to 76 in 2024, the scale of their impact expanded dramatically.1 The number of sites that experienced physical disruption increased by 146%, from 412 in 2023 to 1,015 in 2024.1 This disproportionate increase in consequences, relative to the number of incidents, signals a fundamental shift in attacker methodology. Adversaries have refined their tactics to exploit a systemic, widespread vulnerability that leads to a much greater impact per attack.

The evidence points to the proliferation of indirect attacks as the primary catalyst for this escalation. Approximately 90% of attacks that led to physical outcomes did not directly compromise OT systems.1 Instead, they originated from compromised IT systems or dependencies on cloud-based services, which attackers leveraged to gain a foothold before moving laterally into the operational environment.1 This method is highly effective because it capitalizes on the widespread adoption of "flat networks" with poor IT-OT segmentation, which has become a hallmark of the modern manufacturing environment.1 The push for greater efficiency and connectivity, embodied by the "smart factory" model, has expanded the attack surface faster than security controls have been able to adapt, creating a highly effective bridge for adversaries.4

This trend has also exposed a critical defensive blind spot, often referred to as the "Level 0" security gap. Traditional OT security models rely on monitoring network traffic or logs to detect threats. However, these methods are often insufficient because they cannot detect silent failures or subtle process manipulation at the physical level.1 "Level 0" refers to the raw, unfiltered electrical measurements—such as pressure, flow, voltage, and actuation signals—that are the "only source of truth" for what is physically occurring. If an organization's security architecture lacks direct visibility into this process-level data, it is relying on inference, which is a key vulnerability that attackers are now exploiting with devastating results.1

### **1.2. The Faces of the Threat: From Cybercrime to State-Sponsored Sabotage**

The motivations behind these attacks are becoming more diverse and dangerous, requiring a nuanced threat model. The landscape is dominated by two primary categories of threat actors: financially motivated cybercriminals and politically motivated state-sponsored actors.1

Ransomware remains the most frequent threat, accounting for 87% of attacks with physical consequences.1 The manufacturing sector is a prime target for these actors due to its low tolerance for work disruptions, which translates to a high likelihood of a swift ransom payment.5 This has fueled a surge in "Ransomware-as-a-Service" (RaaS) groups, such as RansomHub, Akira, LockBit, Play, and Clop, which have commoditized attack tools and lowered the barrier to entry.4 This commoditization has made the threat more decentralized and pervasive, increasing the overall volume of attacks even if per-incident sophistication is lower than that of a nation-state.

Concurrently, a more alarming trend is the tripling of nation-state attacks with physical consequences in 2024.1 These actors, often from countries like China, Russia, and Iran, are well-funded and persistent, with motivations that extend beyond financial gain.1 The goal of these attacks is typically ideological, competitive, or strategic, involving cyber espionage and sabotage to cause operational paralysis or geopolitical disruption.8 Historical examples, such as the Shamoon virus that wiped data from 30,000 computers at Saudi Aramco, and the 2021 Colonial Pipeline attack, underscore the devastating potential of such actors and highlight a clear historical trendline of attacks evolving from espionage to outright physical or operational sabotage.10 This necessitates a defense strategy that is not only prepared for opportunistic criminals but also resilient against sophisticated and persistent state-sponsored campaigns. The threat of insiders, whether disgruntled former employees or malicious actors, also remains a constant concern, as they can cause major disruptions with existing access.8

### **1.3. The Manufacturing Sector's Unique Vulnerability Profile**

The manufacturing sector is uniquely vulnerable due to a combination of technical debt and the modern push for connectivity. A significant portion of industrial control systems (ICS) and equipment, including SCADA components, were installed decades ago, long before modern cybersecurity was a concern.6 These legacy systems often operate on outdated software, use proprietary communication protocols without encryption, and lack robust authentication mechanisms, creating a vast array of attack vectors for modern adversaries.13 The challenge of patching or replacing this equipment is a major operational and financial hurdle, creating a perpetual window of opportunity for attackers.

The paradox of the "smart factory" model is that while it drives efficiency and productivity, it has exponentially expanded the attack surface by integrating IT, OT, and Industrial Internet of Things (IIoT) devices.4 The abuse of external remote services, a key enabler of this model, is a growing problem, with alerts for their exploitation surging by 130% in the manufacturing sector.4 The supply chain also presents a critical weakness. Attackers are increasingly targeting large manufacturers by first compromising smaller, less-secure third-party vendors, as exemplified by the Colonial Pipeline attack, where a compromised third-party VPN was the initial entry point.6

## **2. Deconstructing the Attack Chain: Common Vulnerabilities and Exploits in Detail**

### **2.1. The SCADA/DCS Core: Legacy Vulnerabilities and Modern Exploits**

SCADA and DCS are the foundational control systems of industrial operations, and their inherent vulnerabilities make them a primary focus for adversaries. The persistence of legacy flaws in these systems is a systemic failure of the industrial security model. Many SCADA systems lack robust authentication, rely on proprietary protocols without encryption, and contain unpatched vulnerabilities in their legacy components.3 The historical Stuxnet malware, for example, demonstrated a highly sophisticated capability by targeting specific SCADA systems and their associated PLCs, proving that these systems could be manipulated to cause physical damage.15 This event serves as a historical precedent for the motivations and capabilities of today's nation-state actors who are increasingly focused on physical sabotage.

The threat is not theoretical; CISA regularly releases advisories detailing vulnerabilities in products from major vendors.16 For example, a single release in August 2025 listed 32 advisories for products from Siemens and Rockwell Automation, covering a wide range of components from engineering platforms and control systems to specific HMIs.16 Another set of advisories released just two days earlier targeted products from Johnson Controls, Schneider Electric, and AVEVA.17 These alerts cover everything from vulnerabilities in control logic platforms to flaws in specific controllers, demonstrating that the attack surface is vast and continuously being targeted. This constant stream of vulnerabilities highlights a fundamental challenge: the industrial environment's emphasis on uptime and long operational lifecycles makes a consistent patching schedule unfeasible, creating a perpetual window of opportunity for attackers and underscoring the need for alternative mitigation strategies like virtual patching.13

### **2.2. The Human-Machine Interface (HMI) as a Critical Entry Point**

Human-Machine Interfaces (HMIs) serve as the digital control panel for industrial operations, providing a direct pathway to critical systems and making them a significant attack vector. HMIs are a primary target for ransomware and phishing attacks, as they grant access to production systems and sensitive data.5 Attackers who gain unauthorized access can manipulate operational settings, jeopardize product quality, or create hazardous working conditions, which in turn can lead to costly downtime and safety risks for workers.5

The vulnerabilities in HMIs stem from both technical flaws and human factors. Manual entry of passwords or PINs is a major source of breaches, as it is susceptible to being compromised and is a common attack vector for phishing campaigns.5 Securing HMIs, therefore, requires a multi-pronged approach that moves beyond traditional password security. Mitigation strategies include implementing multifactor authentication (MFA) and passwordless single sign-on readers to eliminate manual credential entry and improve workflow efficiency.5 Furthermore, role-based access control (RBAC) and time-limited credentials can be used to limit access to critical system components, reducing the window of opportunity for a malicious actor.14 The importance of HMI security is also a matter of regulatory compliance, as solutions that verify credentials and training records ensure that only qualified individuals can operate equipment, which is a requirement for standards like OSHA.5

### **2.3. The IT-OT Confluence: A Bridge for Adversaries**

The confluence of IT and OT networks is no longer just a vulnerability but is a new attack paradigm that adversaries are weaponizing. The majority of successful attacks do not begin with a zero-day exploit in a PLC but with a well-known vulnerability in a poorly segmented IT network. The "Win-DDoS" technique, a novel attack discovered in 2025, is a perfect case study of this evolving threat model.19

The Win-DDoS exploit weaponizes thousands of public Windows Domain Controllers (DCs) to form a botnet for Distributed Denial-of-Service (DDoS) attacks.19 The attack leverages a zero-click, no-credentials flaw in Windows' Lightweight Directory Access Protocol (LDAP) client, which can be hijacked via a crafted Remote Procedure Call (RPC) to point DCs at a victim server through endless LDAP referrals.19 This attack challenges traditional security assumptions because it does not rely on malware or credential theft and turns a core enterprise asset (the DC) into a weapon.19 Its ability to bypass traditional endpoint detection systems and challenge the assumption that DoS is an "Internet-edge problem" makes it a significant threat to poorly segmented manufacturing networks.

The success of these indirect attacks exposes a critical organizational and cultural problem: the misaligned priorities and siloed expertise of IT and OT teams. While IT teams typically prioritize Confidentiality, Integrity, and Availability (CIA), OT teams are primarily focused on Safety, Reliability, and Availability (SRA).13 This divergence in priorities can lead to delayed responses, inconsistent security standards, and insufficient funding for OT-specific initiatives, as OT cyber is often buried within IT or engineering hierarchies without direct access to decision-makers.21 This intellectual and organizational silo is the underlying vulnerability that attackers are systematically exploiting.

## **3. The State of the Cyber-Defense: Research, Frameworks, and Strategic Countermeasures**

### **3.1. Shifting Defensive Paradigms: The Push for Physics-Based Security**

The limitations of traditional network-centric security have spurred a new wave of research and resources focused on more robust, process-oriented defenses. The Department of Energy's Industrial Control Systems (ICS) Cybersecurity Initiative and the 2025 OT Cyber Threat Report both emphasize the critical need for "physics-based" and "Level 0" security.1 This approach involves moving beyond network traffic analysis to directly monitor unfiltered, electrical measurements of physical processes like pressure, flow, and voltage.1 This real-world process data cannot be spoofed, rerouted, or suppressed by an attacker, making it a reliable source for detecting unauthorized changes even when network-level defenses fail.1 This represents a fundamental shift in defensive philosophy, moving from a model of "detecting the attack" to "detecting the outcome of the attack."

This new defensive paradigm is driving innovative research and technological development tailored to the unique constraints of the OT environment. For example, a novel, lightweight hardware device has been developed to detect and mitigate ARP spoofing attacks in Modbus TCP/IP networks without relying on conventional computer-based infrastructure.23 Similarly, a "Lightweight Industrial IoT Authentication (LI2A)" method has been introduced to secure resource-constrained IIoT devices, ensuring the integrity and reliability of communication in interconnected systems.23 These solutions are designed to be implemented on devices with long lifecycles and limited computing power, acknowledging that traditional IT solutions are often impractical in industrial settings.

### **3.2. Strategic Frameworks and Standards: NIST and ISA/IEC 62443**

Navigating the complex OT threat landscape requires a structured, strategic approach, and two major frameworks provide the necessary guidance.

The **NIST Cybersecurity Framework (CSF)** is a flexible, risk-based approach that helps organizations of all sizes understand and improve their cybersecurity risk management.24 It is structured around five core functions:

**Identify, Protect, Detect, Respond, and Recover**.24 The development of a voluntary

**NIST Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile** illustrates how the framework is being tailored to address the unique and complex risks of specific industrial sectors.26 This customization is crucial because a one-size-fits-all approach is insufficient to address the varied and highly specific challenges faced by different industries.

The **ISA/IEC 62443 series of standards** is a comprehensive, international framework specifically designed for cybersecurity in industrial automation and control systems (IACS).27 It provides a systematic, lifecycle-based methodology for implementing security and defining the "shared responsibility" among all stakeholders, from product developers to end-users.28 The standard defines four security levels (SL 1-4) that provide a clear maturity roadmap for organizations, allowing them to assess and improve their security posture against a defined scale of threats.27 The coexistence and complementary nature of the high-level NIST CSF and the granular ISA/IEC 62443 standards provide a robust, dual-tiered approach to industrial cybersecurity. The NIST framework provides the strategic "why" and "what to do," while IEC 62443 provides the technical "how-to," making them a powerful combination for both leadership and technical practitioners.

### **3.3. Hardening the Environment: A Multi-Layered Approach**

A robust defense requires a layered approach that combines strategic frameworks with proven, foundational best practices.

* **Network Segmentation:** A cornerstone of industrial cybersecurity, network segmentation involves dividing the network into isolated zones based on function and sensitivity. This limits an attacker's lateral movement once a foothold is gained, containing potential damage.3 Implementing micro-segmentation further subdivides networks within critical areas to enhance this isolation.14 This practice is a central principle of the ISA/IEC 62443 standard.27
* **Access Control:** Robust authentication is paramount. This includes implementing multifactor authentication (MFA) for critical systems, enforcing the principle of least privilege through role-based access control (RBAC), and using time-limited credentials for third-party or temporary access.3
* **Patch Management & Virtual Patching:** The challenge of patching decades-old legacy systems is a major weakness.13 Organizations must establish a structured patch management process that aligns with operational needs. Where traditional patching is impractical or risky, virtual patching—using network-based controls like firewalls to shield vulnerabilities—can serve as a crucial compensating control.14
* **Continuous Monitoring & Threat Hunting:** Passive, ICS-focused monitoring technologies that baseline normal operations and detect deviations are essential for identifying threats that evade traditional defenses.22 These technologies should be capable of detecting unauthorized IT-to-OT movement and actions consistent with the MITRE ATT&CK for ICS framework.22 Organizations should also move beyond automated alerts and establish a continuous threat hunting program to proactively search for potential threats and vulnerabilities.14

## **4. Forward-Looking Recommendations for Resilient Industrial Operations**

### **4.1. Strategic Imperatives for Leadership: Bridging the IT-OT Divide**

The analysis indicates that the most critical vulnerability in the manufacturing sector is not a technical one, but an organizational one: the chasm between IT and OT. Leadership must address this challenge with strategic imperatives that foster a unified approach.

* **Align Priorities and Forge a Unified Strategy:** The fundamental disconnect between the security priorities of IT and OT teams is a critical vulnerability.13 Leadership must mandate a unified cybersecurity culture and strategy, ensuring that OT cyber is viewed as a business risk and receives adequate funding and influence at the enterprise level.21
* **Invest in OT-Specific Expertise:** Centralized IT-led security teams often lack the deep operational knowledge required to respond effectively to industrial incidents.21 Organizations must either train existing personnel in both automation and cybersecurity or invest in professionals who are fluent in both domains to close this critical skills gap.13
* **Embrace a Collective Defense Model:** The Department of Energy emphasizes the value of a collective-defense capability, where organizations share insights and threat detections with government partners and Information Sharing and Analysis Centers (ISACs).22 This collaborative approach strengthens the entire ecosystem and allows for more rapid and informed responses to threats.

### **4.2. Actionable Roadmap for Implementation**

Based on the trends and countermeasures identified, a phased roadmap can guide organizations toward a more resilient security posture.

* **Phase 1: Foundation (Identify & Protect)**
  + **Comprehensive Asset Inventory:** Conduct a full, real-time inventory of all managed and unmanaged IT, OT, and IIoT devices to eliminate blind spots.29
  + **Risk Assessment:** Use frameworks like the NIST CSF and ISA/IEC 62443 to conduct a risk-based assessment and develop a security roadmap.24
  + **Network Segmentation:** Implement robust logical and physical segmentation between IT and OT networks, using firewalls and access control lists to restrict lateral movement.3
* **Phase 2: Maturation (Detect & Respond)**
  + **Implement OT-Specific Monitoring:** Deploy passive, sensor-based monitoring technologies with deep packet inspection for industrial protocols.22 These technologies should baseline normal operations and detect anomalies.22
  + **Enhance Access Control:** Deploy passwordless MFA solutions for HMIs and critical systems 5, and enforce role-based access control based on the principle of least privilege.3
  + **Establish Incident Response Plans:** Develop and regularly practice OT-specific incident response plans that include clear escalation paths and communication protocols, addressing the unique physical safety impacts of an OT breach.21
* **Phase 3: Optimization (Recover)**
  + **Modernize and Patch:** Plan for system modernization to replace legacy equipment.14 In the meantime, use virtual patching and compensating controls to mitigate vulnerabilities that cannot be immediately addressed.13
  + **Continuous Threat Hunting:** Move beyond automated alerts and establish a continuous threat hunting program to proactively search for threats and vulnerabilities.14
  + **Secure Backup and Recovery:** Implement a secure, encrypted backup strategy for both OT configurations and data to ensure business continuity and recovery from ransomware attacks.12

## **Appendix**

### **Table of Key Distinctions between IT and OT Security**

| Attribute | OT Security | IT Security |
| --- | --- | --- |
| **Primary Objective** | Safety, Reliability, Availability (SRA) | Confidentiality, Integrity, Availability (CIA) |
| **Typical System Lifespan** | 15-20 years (or more) | 3-5 years |
| **Update Cadence** | Infrequent, carefully scheduled | Regular, often automated |
| **Expertise Required** | Automation & Cybersecurity | IT & Cybersecurity |

Source: 13

### **Table of CISA ICS Advisories (August 2025)**

| Vendor | Component | Advisory ID |
| --- | --- | --- |
| **Siemens** | SIMATIC RTLS, SIPROTEC 5, RUGGEDCOM, etc. | ICSA-25-226-xx, ICSA-25-226-10, etc. |
| **Rockwell Automation** | FactoryTalk Viewpoint, ControlLogix Ethernet Modules, etc. | ICSA-25-226-23, ICSA-25-226-28, etc. |
| **Johnson Controls** | iSTAR Ultra, iSTAR Edge G2, etc. | ICSA-25-224-02 |
| **Schneider Electric** | EcoStruxure Power Monitoring Expert | ICSA-25-224-03 |
| **AVEVA** | PI Integrator | ICSA-25-224-04 |

Source: 16

### **Table of Threat Actor Motivations**

| Motivation (MIC-E) | Associated Threat Actors | Example Attacks/Impact |
| --- | --- | --- |
| **Money** | Ransomware-as-a-Service (RaaS) groups, Cybercriminals | Ransomware, data theft, extortion |
| **Ideology** | Nation-states, Hacktivists | Sabotage, operational disruption, IP theft |
| **Compromise** | Insiders (malicious or unintentional) | Data theft, operational disruption, sabotage |
| **Ego** | Individuals, Hacktivists | Embarrassment, reputational harm |

Source: 7

### **Glossary of Technical Terms**

* **SCADA (Supervisory Control and Data Acquisition):** A control system architecture that uses computers, networked data communication, and graphical user interfaces for high-level process supervisory management.
* **DCS (Distributed Control System):** A control system for a process or plant where control elements are not centralized but distributed throughout the system, often with many control loops.
* **HMI (Human-Machine Interface):** A user interface or dashboard that connects a person to a machine, system, or device. In manufacturing, HMIs allow operators to monitor and control industrial processes.
* **IIoT (Industrial Internet of Things):** The use of smart sensors and actuators to enhance manufacturing and industrial processes, often by providing data-driven insights and automation.
* **Level 0:** The lowest level of the Purdue Model, referring to the physical process itself, including sensors, actuators, and mechanical equipment. It is considered the "only source of truth" for what is physically occurring.
* **Purdue Model:** A reference model for Industrial Control System (ICS) networks, which segments the network into hierarchical layers from the enterprise network (Level 5) down to the physical process (Level 0).
* **ISA/IEC 62443:** A series of international standards that define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS).
* **NIST Cybersecurity Framework (CSF):** A voluntary framework that consists of standards, guidelines, and best practices to help organizations manage and reduce cybersecurity risk.

#### Works cited

1. The 2025 OT Cyber Threat Report - SIGA, accessed August 14, 2025, <https://sigasec.com/the-2025-ot-cyber-threat-report/>
2. The 2025 OT Cyber Threat Report | Waterfall Security Solutions, accessed August 14, 2025, <https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2025-threat-report-ot-cyberattacks-with-physical-consequences/>
3. SCADA Security Essentials: Your Need-to-Know Guide, accessed August 14, 2025, <https://www.ssh.com/academy/operational-technology/scada-security-essentials-need-to-know-guide>
4. Threat Landscape Report: Uncovering Critical Cyber Threats to Manufacturing Sector, accessed August 14, 2025, <https://reliaquest.com/blog/threat-landscape-report-uncovering-critical-cyber-threats-to-manufacturing-sector/>
5. The Ultimate Guide to HMI Security: What Manufacturers Need to Know - rf IDEAS, accessed August 14, 2025, <https://www.rfideas.com/about-us/blog/ultimate-guide-hmi-security-what-manufacturers-need-know>
6. Major Cyber Attacks Targeting Manufacturing Industry in 2025 - SOCRadar, accessed August 14, 2025, <https://socradar.io/major-cyber-attacks-manufacturing-industry-in-2025/>
7. Hacktivists, state-sponsored groups step up cyberattacks targeting manufacturing operations and OT systems - Industrial Cyber, accessed August 14, 2025, <https://industrialcyber.co/manufacturing/hacktivists-state-sponsored-groups-step-up-cyberattacks-targeting-manufacturing-operations-and-ot-systems/>
8. What are the motivations for cyber-attacks? - Stratix Systems, accessed August 14, 2025, <https://stratixsystems.com/what-are-the-motivations-for-cyber-attacks/>
9. What is Cyber Espionage? - CrowdStrike, accessed August 14, 2025, <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage/>
10. The ICS Cybersecurity Lifecycle - exida, accessed August 14, 2025, <https://www.exida.com/resources/Whitepapers/The-ICS-Cybersecurity-Lifecycle>
11. Why are Cyberattacks Shifting to ICS? - ISA Global Cybersecurity Alliance, accessed August 14, 2025, <https://gca.isa.org/blog/why-are-cyberattacks-shifting-to-ics>
12. Industry 4.0 and cybersecurity – How to protect your investment | NIST, accessed August 14, 2025, <https://www.nist.gov/blogs/manufacturing-innovation-blog/industry-40-and-cybersecurity-how-protect-your-investment>
13. OT Security: Guide for Critical Infrastructure | Rockwell Automation | US, accessed August 14, 2025, <https://www.rockwellautomation.com/en-us/company/news/blogs/ot-security-guide.html>
14. 9 SCADA System Vulnerabilities and How to Secure Them, accessed August 14, 2025, <https://gca.isa.org/blog/9-scada-system-vulnerabilities-and-how-to-secure-them>
15. 14 Major SCADA Hacks - DPS Telecom, accessed August 14, 2025, <https://www.dpstele.com/blog/major-scada-hacks.php>
16. CISA Releases Thirty-Two Industrial Control Systems Advisories, accessed August 14, 2025, <https://www.cisa.gov/news-events/alerts/2025/08/14/cisa-releases-thirty-two-industrial-control-systems-advisories>
17. CISA Releases Seven Industrial Control Systems Advisories, accessed August 14, 2025, <https://www.cisa.gov/news-events/alerts/2025/08/12/cisa-releases-seven-industrial-control-systems-advisories>
18. The Rising Threat of Ransomware in Manufacturing, accessed August 14, 2025, <https://www.threatintelligence.com/blog/manufacturing-ransomware>
19. New Win-DDoS Flaws Let Attackers Turn Public Domain Controllers ..., accessed August 14, 2025, <https://thehackernews.com/2025/08/new-win-ddos-flaws-let-attackers-turn.html>
20. Win-DoS' Zero-Click Exploit Could Weaponize Windows ..., accessed August 14, 2025, <https://gbhackers.com/win-dos-zero-click-exploit/>
21. OT cybersecurity reporting remains a structural weakness as threats outpace legacy governance models - Industrial Cyber, accessed August 14, 2025, <https://industrialcyber.co/features/ot-cybersecurity-reporting-remains-a-structural-weakness-as-threats-outpace-legacy-governance-models/>
22. Considerations for ICS/OT Cybersecurity Monitoring Technologies ..., accessed August 14, 2025, <https://www.energy.gov/ceser/considerations-icsot-cybersecurity-monitoring-technologies>
23. ASI | Special Issue : Industrial Cybersecurity - MDPI, accessed August 14, 2025, <https://www.mdpi.com/journal/asi/special_issues/7I5F2YX93Q>
24. Understanding NIST for the Manufacturing Industry - CIT | Computer Integration Technologies | Twin Cities MN IT Provider, accessed August 14, 2025, <https://www.cit-net.com/nist-for-manufacturing/>
25. Frameworks | NIST, accessed August 14, 2025, <https://www.nist.gov/frameworks>
26. Cybersecurity Framework Profile for Semiconductor Manufacturing ..., accessed August 14, 2025, <https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-semiconductor-manufacturing>
27. IEC 62443 Standard: Enhancing Cybersecurity for Industrial Automation and Control Systems | Fortinet, accessed August 14, 2025, <https://www.fortinet.com/resources/cyberglossary/iec-62443>
28. ISA/IEC 62443 Series of Standards, accessed August 14, 2025, <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>
29. The Top 8 IT/OT/IoT Security Challenges and How to Solve Them | Balbix, accessed August 14, 2025, <https://www.balbix.com/insights/addressing-iot-security-challenges/>