Trustwave SpiderLabs

Manufacturing Sector **Deep Dive**

Convergence of IT/OT

Contents

Executive Summary

The convergence of Information Technology (IT) and Operational Technology (OT) is a growing trend in the manufacturing sector, driven by the need for improved efficiency, cost reduction, and automation. Historically, these two domains have been kept separate due to differing priorities—IT focusing on data, systems, and security, and OT concentrating on the physical processes of production and safety. However, with the advent of Industry 4.0, the Internet of Things (IoT), and data analytics, there is a clear move toward integration.

While this convergence promises operational benefits, it also significantly increases the attack surface and cybersecurity risks. IT and OT networks were designed with different security priorities and operational demands and merging them introduces vulnerabilities that were not previously present. Often overlooked, is the profound impact cybersecurity can have on production loss. The risk becomes even more complex as cybersecurity concerns are often not fully addressed until production or safety is impacted on the shop floor.

Breaches in OT environments can lead to production downtime, safety incidents, and reputational damage, as the traditional separation between IT and OT made it easier to isolate vulnerabilities. From user-based attacks like phishing to third-party supplier attacks, the consequences of a breach can range from financial losses to irreversible damage to property and human life. As organizations strive to integrate IT and OT, the need to balance security, safety, and operational efficiency becomes critical. This challenge requires not just technology, but also a cultural shift, where communication and collaboration between IT and OT teams are prioritized.

This report explores the evolving threat landscape, the unique challenges posed by converged IT/OT environments, and offers actionable recommendations for practitioners, managers, and Chief Information Security Officers (CISOs) to secure their organizations. Emphasizing the need for a comprehensive approach that includes continuous monitoring, specialized training, and collaboration across teams, the goal is to ensure that organizations can address cybersecurity risks effectively while maintaining operational integrity and safety.

This report is supplemental to the of the 2025 Trustwave Risk Radar Report: Manufacturing Sector, a broader and more comprehensive report that analyzes the manufacturing sector's major threats and trends.

Introduction: The Convergence of Worlds

Defining IT and OT

Information Technology refers to systems used to manage data, networks, and information flows across an organization. IT systems include workstations, servers, storage, cloud services, and enterprise applications that focus on data management, communication, and processing.

Operational Technology refers to hardware and software used to monitor, control, and automate physical processes within industries such as manufacturing. OT includes devices like Programmable Logic Controllers (PLCs), Human-Machine Interfaces (HMIs), Supervisory Control and Data Acquisition (SCADA) systems, Remote Terminal Units (RTUs), and various IoT sensors that monitor and control physical production systems.

The Historical Separation and Drivers for Convergence

Historically, IT and OT have been kept separate for practical reasons. OT systems are typically purpose-built and do not require the same level of connectivity or interaction with the broader corporate network as IT systems. OT environments also tend to be more stable, with limited need for updates and minimal or slower changes over time. Meanwhile, IT networks are more dynamic and regularly updated to address security threats.

However, several factors have driven the convergence of these two systems:

- **Industry 4.0:** The move toward smarter manufacturing, characterized by IoT, data analytics, and automation, requires greater integration between IT and OT.
- **IoT and Data Analytics:** The proliferation of connected devices and sensors provides real-time data from OT systems, which can be analyzed and used to optimize production and reduce downtime.
- **Efficiency Improvements:** Converging IT and OT systems allows manufacturers to automate processes, improve maintenance schedules, and optimize resource allocation.

IoT and its Role in the IT/OT Landscape

IoT has become a key enabler in the convergence of IT and OT. IoT devices, such as smart sensors, temperature monitors, and cameras, can gather and transmit data to the cloud or other IT systems, offering valuable insights without the need for traditional OT devices like PLCs. These IoT devices are typically more cost-effective and provide higher flexibility than traditional OT systems. However, they also introduce new vulnerabilities into the ecosystem.

Examples of Converged Systems

- **SCADA Integrated with ERP:** Manufacturers are integrating their SCADA systems with Enterprise Resource Planning (ERP) solutions to improve operational efficiency. This integration allows real-time data from production to feed directly into supply chain management, inventory systems, and workforce scheduling.
- **Smart Sensors and Cloud Platforms:** Automated systems, such as backup diesel generators with embedded sensors, collect data about engine health, fuel consumption, and maintenance needs. Collecting this data in the cloud and including data from other makes and models, allows analytics and AI to forecast maintenance, engine life, warehousing of parts, and the size of a human workforce needed.

Increased Cyber Risk

The more OT systems integrate with IT infrastructure and cloud services, the greater the risk. As manufacturing becomes more automated and connected, OT systems are exposed to a broader range of cyber threats. This increased connectivity opens doors for cybercriminals to exploit vulnerabilities in both IT and OT environments.

Cybersecurity is a common daily practice among IT professionals, such as System Administrators and Network Engineers. However, the same cannot be said for OT personnel, such as OT Engineers, Operators, and even Shop Floor Supervisors.

With the convergence of IT and OT, many practices on the shop floor have yet to fully consider the cybersecurity implications of their actions. Decisions affecting productivity often prioritize human safety and production uptime.

As a result, these decisions frequently overlook cybersecurity risks, leaving the organization vulnerable to breaches that can impact production, safety, and reputation.

According to the NIST 2024 Annual Report on the U.S. Manufacturing Economy, manufacturers lost between $8.3 billion and $36.3 billion due to cybercrime. These incidents often take weeks or even months to recover from, with full recovery to pre-incident operational norms sometimes taking over a year.

The Evolving Threat Landscape

Traditional OT Threats

OT systems have historically been less secure than IT systems, often due to:

- **OT devices come with inherent risks, often including built-in vulnerabilities.**
  - Vulnerabilities may range from non-secure protocols to poorly developed firmware/software with critical flaws.
- **Lack of Patching:** OT devices rarely receive regular updates, and those that do are often not focused on cybersecurity. Many OT systems continue to run outdated firmware that is vulnerable to exploitation.
- **The release of patches and updates for OT devices is limited and inconsistent.**
  - Updates are typically infrequent and often focus on functional improvements rather than cybersecurity.
  - Unlike IT systems, OT devices do not follow a structured lifecycle, and many organizations adopt a “no break, no fix” approach, meaning OT systems often have no formal lifecycle.
- **Legacy Systems:** Older OT systems are particularly susceptible to attacks, as they were not designed with modern security threats in mind.
- **Limited Security Controls:** OT systems were initially designed for operational functionality rather than security. This can lead to:
  - Poor password practices
  - Unsecured communication protocols
  - Other vulnerabilities

Emerging Threats from Convergence

The convergence of IT and OT introduces new attack vectors, including:

Ransomware targeting control systems:

- Cybercriminals are increasingly targeting OT systems with ransomware, encrypting critical production data and halting manufacturing operations.

Lateral movement from IT to OT:

  - Once attackers compromise an IT system, they can move laterally into OT networks, exploiting the lack of segmentation between the two environments.

Supply chain attacks:

- Attackers can target suppliers of both IT and OT components to gain access to manufacturing systems, exploiting vulnerabilities introduced by third-party vendors.

Cybercriminals leverage any available weaknesses to move between IT and OT environments, extending their dwell time within the network.

Threats Surrounding IoT

Many risks in IoT mirror those in OT but are often magnified due to the greater capabilities of IoT devices. With more complex firmware and better connectivity, IoT devices can become attractive targets for cybercriminals. If compromised, they could potentially give attackers full access to both IT and OT systems.

OT devices (e.g., PLCs) have limited processing power, handling basic tasks like network communication and control input/outputs. IoT devices, however, often feature dual or quad-core processors, gigabytes of RAM, and storage capacity ranging from hundreds of gigabytes to a terabyte, with simplified versions of Linux running on them.

Case Studies

1. **NotPetya Ransomware Attack (2017):** Initially aimed at Ukrainian organizations, NotPetya spread globally and impacted several multinational manufacturers. The attack caused significant disruption to operations, highlighting the vulnerability of interconnected IT/OT environments.
2. **Triton Malware (2017):** Targeting a critical infrastructure facility, Triton malware specifically aimed at the safety systems of OT devices. This attack demonstrated the potential for cybercriminals to directly endanger human lives by targeting OT systems.
3. **Nuclear Power Plant Attack in Asia (2019):** Bad actors used malware to compromise a nuclear power plant's domain controller, gaining control of OT devices in pressurized water reactors for over six months before detection. Proper OT monitoring could have identified unusual traffic and access attempts earlier.
4. **Food Processing Plant (2021):** Disrupted operations internationally and resulted in the company paying an $11 million ransom to the Russian hacker group REvil.
5. **Colonial Pipeline Attack (2021):** This attack disrupted the U.S. East Coast's fuel supply, highlighting the impact of ransomware on critical OT systems.
6. **Water Treatment Plant Attack in Western PA (2023):** The Iran-backed group "Cyber Av3ngers" claimed responsibility for the hack of the Municipal Water Authority of Aliquippa. While the attack did not affect the drinking water supply, it served as a wake-up call about the potential for cyberattacks to disrupt essential services.

Threat Actor Motivations

Cyberattacks targeting manufacturing environments can stem from a variety of motivations, including:

- **Monetary Gain:** Cybercriminals often target manufacturers for financial gain, especially when ransom payments are involved.
- **Nation-State Attacks:** Political or geopolitical motives, as seen with cyberattacks aimed at critical infrastructure, can drive nation-state actors to target OT systems.
- **Intellectual Property Theft:** Competitors or cybercriminals may seek to steal sensitive production data, designs, or processes.

Key Security Challenges in Converged Environments

Visibility and Asset Inventory

Lack of Comprehensive Asset Inventory:

- The biggest challenge in large, complex, and distributed OT environments is the absence of a full asset inventory.
- Outside of OT Engineers, organizations often don't know or fully understand the function of their OT assets.
- OT Engineers usually only understand the specific line they are assigned to, and this knowledge is often limited to institutional knowledge shared among OT Engineers.

The Role of OT Engineers:

- OT Engineers' primary focus is to keep the production line operational, not to manage or track OT assets.
- Unlike IT, where daily administrative tasks (e.g., asset inventory software, GPO controls) are routine, OT administration occurs infrequently, often on an ad-hoc basis.
- The responsibility for applying patches to OT devices, like PLCs, is not part of the daily duties of OT Engineers.

Impact on Asset Inventory and Documentation:

- The focus on production has led to poor asset inventory management and inadequate documentation of the OT environment.

Unmanaged devices: It's common to find unmanaged switches or SOHO Wi-Fi routers scattered throughout the environment.

Role overlap: OT Engineers often assume network engineering responsibilities due to the breakdown between IT and OT, timing constraints, and the complexity or safety requirements of the production environment.

Network Segmentation and Micro-Segmentation for IT/OT Environments

Historical Context and the IT/OT Divide: The traditional divide between IT (Information Technology) and OT (Operational Technology) has resulted in the segmentation of the two networks. This separation serves several critical purposes:

- **Downtime Management:** Minimizes the impact of downtime between IT and OT systems.
- **Patching and Vulnerability Management:** Ensures OT systems remain unaffected by routine IT patches and updates.
- **Cybersecurity:** Reduces the risk of cyber threats spreading between IT and OT networks, protecting sensitive OT systems.
- **Cyber Insurance Requirements:** Helps organizations meet specific insurance policy requirements by maintaining distinct IT and OT networks.

Segmentation Benefits: Segmentation of OT networks and IoT devices provides a crucial layer of protection. By isolating these systems, breaches can be contained within one segment, minimizing the impact on critical OT systems. For example, micro-segmentation through VLANs (Virtual Local Area Networks) can be implemented, where distinct OT functions (e.g., Shipping and Receiving, Production Line #1) are placed into separate VLANs. This approach ensures that if one system is compromised, the rest of the OT environment remains protected, and the **Return Time to Operations (RTO)** is minimized.

Access Control: Access between segments should be tightly controlled. For example, a **Deny All** firewall rule should be enforced, allowing only specific IP-to-IP communications through defined ports (e.g., x.1 → x.2.1 → Port 80, 443). This prevents unrestricted access and reduces exposure to external threats. Although establishing data flow diagrams for this can be complex, it is essential for protecting OT environments.

Vulnerability Management and Patching

Complexity of Vulnerability Management: Managing vulnerabilities in OT environments presents significant challenges due to:

- Limited downtime for patching
- Irregular patch release schedules
- Aging or End-of-Life (EOL) devices
- A general lack of cybersecurity focus in many patching processes

Limited Downtime and Production Priorities: Due to the operational nature of OT environments, scheduled downtime is often minimal, and production priorities take precedence over patching activities. When downtime is available, it is frequently consumed by other production issues (e.g., electrical or sensor malfunctions). Applying patches in these scenarios requires careful planning, including:

- Time for patch application
- Reprogramming of devices or PLCs
- Conducting safety checks before returning devices to production

Enhanced Security Through Micro-Segmentation and Monitoring:

Critical Resource Segmentation: It's vital to segment critical resources, such as Active Directory (AD), to avoid compromising both IT and OT environments. Sharing the same AD resource between IT and OT poses a significant risk. If the AD server is compromised, attackers could potentially gain access to both environments. To mitigate this risk, usernames should differ between the two environments, and account names should be anonymized (e.g., using a non-attributed, five-digit username).

Network Monitoring and Data Capture: To effectively monitor OT traffic, it's best to send captured data packets through a span port to a completely separate security VLAN. This separation ensures that monitoring does not interfere with either the IT or OT environments. While some organizations currently span OT traffic to IT networks for monitoring purposes, it's essential to keep this one-way traffic flow (from OT to IT) to maintain security.

Inconsistent Patch Releases:

- Manufacturers typically release patches infrequently—sometimes only once or twice a year.
- Patch focus: Patches usually prioritize production functionality over cybersecurity issues, with many patches lacking significant security updates.
- Often, new production releases may have the same or even more vulnerabilities than previous versions.

Challenges with EOL and Aging Products:

- As products reach End-of-Life (EOL), updates become less frequent or unavailable.
- These aging products are rarely replaced due to:
  - The significant downtime required for replacement
  - The high cost of system upgrades

Authentication and Access Control

Firmware Vulnerabilities and Authentication Issues:

- Along with firmware updates that may contain built-in vulnerabilities, there is a critical need for strong authentication and access control.

Legacy System Limitations:

- Older legacy systems often cannot support modern authentication and access control mechanisms due to physical or technical limitations.
- These systems frequently transmit credentials in clear text, leaving them vulnerable to interception.

Security Monitoring and Incident Response

OT monitoring is challenging due to the unique traffic they generate. OT traffic doesn't fit the cookie cutter mold, unlike IT.

OT Traffic Characteristics:

- OT traffic is typically static, with OT devices not generating excessive network chatter.
- OT traffic can be baselined quickly, making it easier to identify anomalies.

Benefits of Monitoring Software:

- Can detect unusual traffic entering or exiting OT devices
- Can detect code changes
- Can detect anomalies within OT devices

Challenges in Security Monitoring:

- Security monitoring remains challenging in the manufacturing industry due to:
  - OT infrastructure switches, originally built for OT environments, often lack modern features or support.
  - Aging OT infrastructure, which limits support for features like Port Spanning.

Impact of Limited Monitoring Capabilities:

- Without Port Spanning, monitoring is typically restricted to firewalls or the egress points of the OT network.
- This approach does not capture:
  - Third-party access
  - Insider threat vectors
  - Other malicious activities within the network
- As a result, activity within the OT environment often goes undetected until an incident occurs.

Passive Monitoring as the Best Defense:

- Passively monitoring OT traffic remains the industry's best option for detecting malicious or unwelcome traffic.

Limitations of Endpoint Defense:

- Due to the OS/firmware, storage, RAM, and processing power limitations of many OT devices, endpoint defense software cannot be installed.

Skills Gap

There is a significant shortage of cybersecurity professionals with the specialized skills required to secure OT environments. This gap is compounded by the differing priorities between IT and OT teams, making it difficult to find professionals who understand both domains, for example, the understanding of safety and irreversible damage that can be caused on the production floor.

Actionable Recommendations for Different Roles

For Practitioners (Engineers, Analysts)

- **Human Health and OT Safety Training:** Given the potential for irreversible damage in organizations with OT production equipment, it is recommended that all engineers, analysts, and administrators complete an annual Human Health and OT Safety course.
- **Network Segmentation:** As IT and OT converge, network segmentation should be designed to minimize exposure in the event of a system compromise.
- **Vulnerability Assessments and Penetration Testing:** OT systems are delicate, so vulnerability assessments or penetration testing should be conducted with extreme caution, ideally during off-production hours or scheduled downtime.
- **Security Monitoring in OT Environments:** OT systems are inherently vulnerable, and due to limited resources, EDR solutions may not be feasible. The best defense is to closely monitor security logs and respond promptly to security alerts.
- **OT Security Awareness Training:** OT and IT practitioners should receive specialized training in OT security awareness to better understand the unique risks and needs of these environments.

For Managers (Security Managers, IT/OT Managers)

Bridging the IT/OT Gap:

- OT and IT systems, as well as the people who manage them, have different priorities and it's highly recommended for managers to bridge this gap by facilitating communication and understanding each other's concerns.

Allot for Budget Differences:

- OT security differs significantly from IT security, as OT systems have more limited functions and features.
- As such, managing security budgets and resources for OT requires a distinct approach, with consideration for production deadlines and safety issues.

Building Cross-Functional IT/OT Teams:

- Establishing IT/OT cross-functional teams is essential.
- These teams should understand the technical, legal, regulatory, business, relational, and safety requirements of both IT and OT environments to ensure effective communication and safety for all employees.

Incident Response and Recovery Planning:

- Both IT and OT should have established incident response and recovery plans.
- Recovery Time to Operations (RTO) for production floors will differ from IT, with additional restrictions on what, when, and how systems can be taken offline.
- Since production time is money, a comprehensive recovery plan is just as, if not more, important than the incident response plan.

For CISOs and Senior Leadership

- **Security Policies and Procedures for OT:** Developing and implementing security policies and procedures that include OT requires a tailored approach—one size does not fit all in this case.
- **OT Security Strategy Development:** Develop a comprehensive OT security strategy aligned with production business objectives, but keep in mind aging, End-of-Life (EOL) equipment that is still functional, but limited in capabilities and expensive to replace.
- **Security Governance Framework:** Establish a security governance framework that spans the entire life of the production floor.
- **Communicating Security Risks:** Effectively communicate security risks to executive leadership and the board to ensure alignment and appropriate action.
- **Investment in Security Technologies and Training:** Invest in both security technologies and ongoing training to ensure the workforce is well-equipped to manage OT security risks.
- **Fostering a Security-Conscious Culture:** Foster a culture of security that emphasizes the importance of security from both IT and OT perspectives.
- **Supply Chain Risk Management:** Develop a robust supply chain risk management program to address vulnerabilities introduced by third-party vendors.

Conclusion: Balancing Operational Efficiency with Cybersecurity

OT environments are traditionally slow to evolve due to the constraints of downtime, safety concerns, technology limitations, and costs. However, the threat landscape for OT is rapidly growing, and these environments are increasingly vulnerable. With the average OT environment having a production life of over 30 years, and OT equipment often exceeding 40 or 50 years before replacement, the challenge of modernizing and securing these systems becomes even more pressing.

As we move toward Industry 4.0, OT systems are becoming more interconnected with IT through automation, cloud integration, CRM systems, and AI technologies. This convergence introduces a new set of risks, including external threats from third-party compromises, nation-state actors, and advanced persistent threats. Connectivity, once seen as a necessity to maintain production efficiency, is now increasing exposure for both OT and IT systems.

While OT environments are slow to change and built on tried-and-true processes focused on production outcomes, new technologies—such as IoT sensors, 5G integration, and automated systems—introduce additional vulnerabilities. Without continuous monitoring and proactive threat detection, OT environments become ripe for exploitation, leading to potential loss of intellectual property, production disruptions, and even safety hazards.

OT systems, which are designed primarily for productivity rather than security, make easy targets for cybercriminals. With infrequent patching cycles and outdated or End-of-Life equipment in use, the risk profile for OT environments is high. Managing this risk requires strategies like asset segmentation, which limits exposure and reduces the number of vulnerable systems.

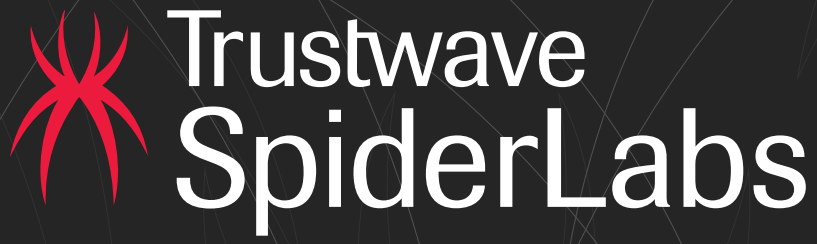
Beyond systems, a critical issue lies in the human factor. IT and OT engineers operate under very different mindsets, with stark differences in priorities and risk perception. IT engineers often focus on data breaches, while OT engineers prioritize safety, environmental impacts, and the risk to human life. This divide complicates integration and requires intentional effort to foster communication, collaboration, and alignment between these two groups. The convergence of IT and OT is not just about merging technical environments, but also about aligning people and processes to effectively manage risk.

To safeguard OT environments, proper monitoring and detection are key. Due to technical limitations, many OT devices cannot run traditional security software like EDR. Therefore, monitoring must occur at strategic points, such as switches and ingress/egress areas, to detect malicious activity. OT traffic tends to be static and low-bandwidth, making it easier to baseline and identify irregularities. However, without proper monitoring, the risk of undetected malicious activity—especially with increasing connectivity to external resources—remains a major concern.

Ultimately, addressing OT security requires continuous improvement, not just in technology but in processes and people. Organizations must be agile and responsive, adapting to new threats by developing and refining OT-specific incident response and recovery plans. Both IT and OT engineers need specialized security training to understand how bad actors could exploit vulnerabilities in each environment. Regular cross-functional exercises, such as OT/IT tabletop simulations, can improve communication and collaboration, strengthening overall security.

OT and IT are fundamentally different, and the convergence of these domains requires more than just physical integration. It demands an understanding of how processes, people, and security practices need to evolve together. OT systems, due to their complex and often outdated nature, require tailored incident response and recovery plans that account for production floor-specific risks. To bridge the communication gap, it's essential to engage both IT and OT teams regularly—at least quarterly—to foster a culture of continuous improvement and ensure alignment in adapting to the ever-changing threat landscape.

For all of Trustwave SpiderLabs' research on the Manufacturing sector, please see the full series here.


Trustwave
SpiderLabs