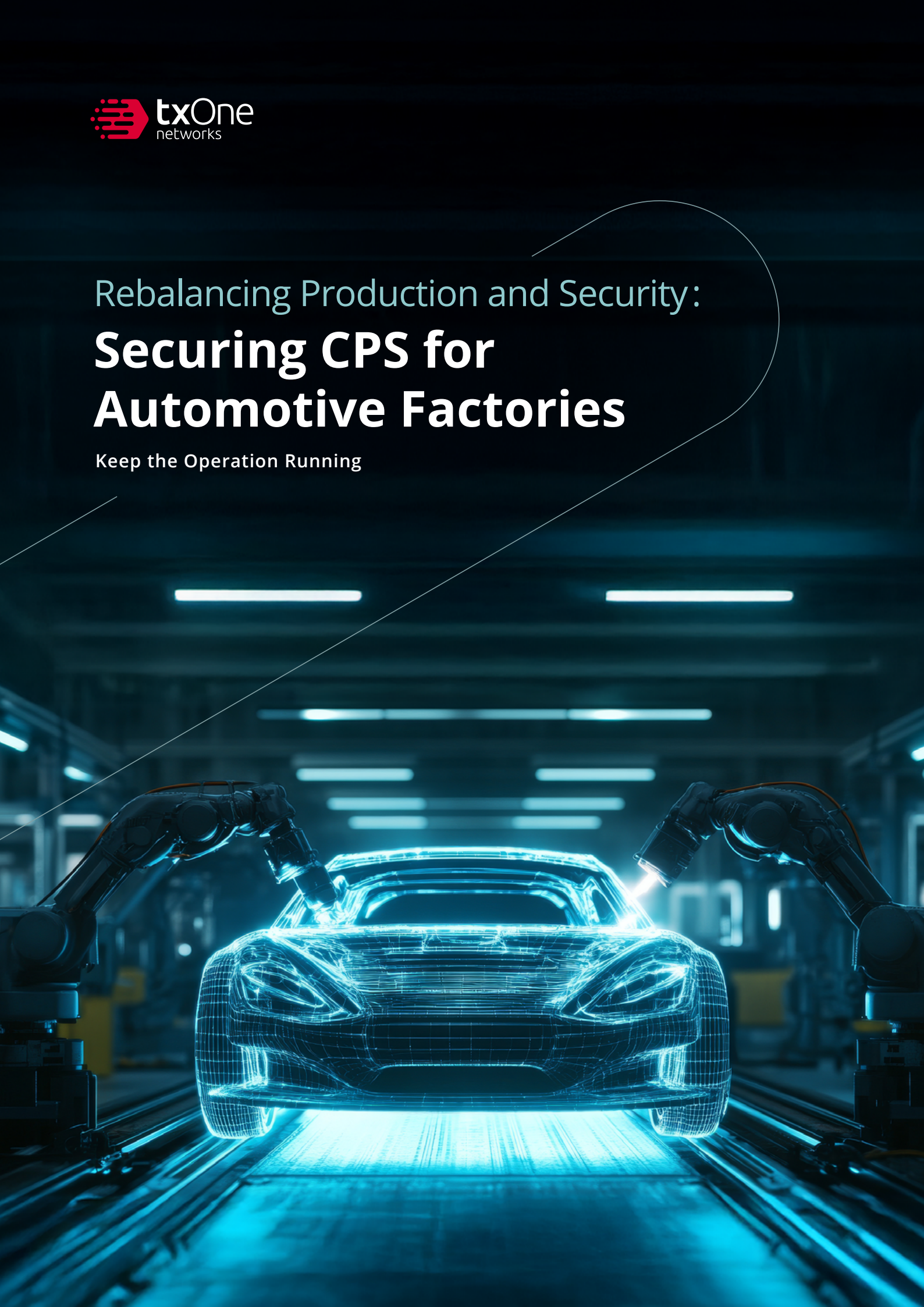
txOne networks

Rebalancing Production and Security:

Securing CPS for Automotive Factories

Keep the Operation Running



Contents

Introduction

The automotive industry is undergoing a rapid digital transformation driven by the integration of advanced technologies into its manufacturing processes.

This article will explore the risks faced by the automotive industry and its supply chain, track the development of regulations, and recommend best practices for cybersecurity in automotive manufacturing.

The automotive industry is undergoing a rapid digital transformation driven by the integration of advanced technologies into its manufacturing processes. According to Rockwell's 2024 report "State of Smart Manufacturing: Automotive Edition,"[1] at least 81% of respondents have adopted or plan to adopt network hardware, industrial computers, and connected devices such as sensors and actuators.

Additionally, in recent years, the industry has faced major challenges such as supply chain disruptions, chip shortages, and an increase in cyberattacks. However, the automotive sector had already been struggling to balance quality with profitability long before these issues arose. Today, manufacturers have found a solution in smart manufacturing. This integrated approach combines production monitoring, quality management, and Manufacturing Execution Systems (MES) to create a highly efficient, seamlessly operating system. Smart manufacturing technologies utilize real-time data to guide production and resolve quality issues before they disrupt operations. Leading manufacturers are adopting this pragmatic approach to optimize costs and improve profitability without sacrificing quality or customer data integrity.

While digital transformation is undoubtedly essential, the convergence of Information Technology (IT) and Operational Technology (OT) systems has expanded the attack surface for cybercriminals. Therefore, cybersecurity is a critical concern for the global automotive industry. This article will explore the risks faced by the automotive industry and its supply chain, track the development of regulations, and recommend best practices for cybersecurity in automotive manufacturing.

01 Cybersecurity Challenges in Automotive Manufacturing

The Rise of Cyber Risks from IT and OT Systems Integration

In today's smart manufacturing environment, the integration of industrial automation, Cyber-Physical Systems (CPS), and advanced communication networks has transformed automotive production. While this transformation brings unprecedented efficiency, it also significantly expands the attack surface for cyber threats, posing considerable risks to production continuity and product integrity. While these advancements enhance productivity and quality, they also create a highly interconnected system that is vulnerable to sophisticated cyberattacks.

Legacy Systems and Protocols: Struggling with Real-Time Security

The inherent complexity of these systems—from Programmable Logic Controllers (PLCs) and MES to cloud-based data analytics platforms—makes them ideal targets for skilled hackers. These attackers often employ multi-stage penetration strategies, starting with seemingly harmless components. For example, in 2024, a malware named FrostyGoop[2] was discovered. This malware exploited the lack of authentication in the Modbus TCP protocol used by factories, allowing attackers to commandeer Modbus communications and impact OT. Traditional security tools struggle to detect this type of attack because it operates with legitimate commands. Once attackers are inside the network and gain access to PLCs, RTUs, controllers, or other devices running unauthenticated control protocols, they can easily move laterally within the industrial environment, potentially leading to critical data encryption or direct manipulation of production processes.

Internal Threats: Accidental or Intentional Privilege Abuse

Deploying integrated production monitoring and Quality Management Systems (QMS) is an urgent concern for manufacturers; 84% surveyed are already implementing or planning to implement these systems. While these systems are designed to optimize workflows and ensure product consistency, they can become critical points of failure if compromised. For example, internal employee accounts could accidentally or intentionally abuse their privileges to manipulate the MES or PLC, leading to production disruptions or equipment failures. Internal employees may also unintentionally or intentionally use their privileges to make unauthorized system configuration changes or transfer malware via USB devices. If attacks on these platforms occur, they could cause widespread disruptions across the entire production lifecycle, affecting everything from real-time adjustments on robotic welding lines to the final assembly of vehicle components.

VPN and Remote Protocol Vulnerabilities in OT Systems

The challenge of securing these environments is compounded by legacy security paradigms that historically classified sensors and basic instruments as low risk. Modern attack vectors, particularly ransomware and remote management protocol exploits (e.g., RDP or VPN), can easily compromise these "simple" devices. Once breached, these devices become entry points for larger attacks that exploit weaknesses in network segmentation to spread across the OT

environment. Ransomware attacks, for example, are capable of directly targeting industrial systems, bypassing traditional IT-centric security measures. These attacks often exploit vulnerabilities in OT/ICS, such as legacy operating systems or poor patch management practices common in many manufacturing plants. The infamous WannaCry ransomware attack[3], which completely halted production at major manufacturers like Honda, exemplifies how ransomware can cascade into OT environments by exploiting IT vulnerabilities.

The increasing reliance on wireless connectivity and remote access solutions further amplifies these risks. Technologies like 5G and edge computing promise faster communication and lower latency for industrial applications but also introduce new opportunities for network intrusion. Poorly secured remote access gateways, such as unpatched VPNs[4] or unsecured RDP[5] connections, can be exploited by attackers to gain control over critical production systems.

Supply Chain Vulnerabilities in Automotive Manufacturing

Moreover, supply chain vulnerabilities remain a significant issue. Introducing unverified third-party devices or software updates into the production process presents a critical risk, as attackers can exploit these points of contact to infiltrate the manufacturing environment. The interconnected nature of the modern automotive supply chain—where parts suppliers, software developers, and service providers interact within a global ecosystem—further exacerbates the problem. A compromised supplier could introduce malicious code or hardware backdoors into critical systems, potentially disrupting production across multiple facilities.

Threat Scenario	Attack Method
IT or External Network Intrusion	• Attackers exploit unpatched network vulnerabilities or exposed ports to launch attacks, gain control, or extort manufacturing systems. • Phishing emails or brute force attacks are used to infiltrate the internal network, followed by lateral movement through RDP or VPN to further penetrate OT systems.
Legacy OT Devices	• Software vulnerabilities in industrial equipment like PLCs or robots can be exploited by attackers, leading to malicious command execution or system failure. • Known vulnerability attacks or the exploitation of unpatched systems (e.g., outdated controller firmware) can result in ransomware attacks.[6]
Accidental or Intentional Privilege Abuse by Internal Employees	• Internal employees may unintentionally or deliberately misuse their privileges to operate Manufacturing Execution Systems (MES) or PLCs, causing production disruptions or equipment failure. • Employees may carry out unauthorized system configuration changes with elevated privileges or use USB devices to transfer malware.[7]
VPN and Remote Protocol Vulnerabilities	• Traditional VPN or RDP used for remote control can become an entry point for attackers, who may steal login credentials to gain control over production systems. • Inadequate security measures for internal wireless communication allow hackers to exploit wireless vulnerabilities to infiltrate factory systems.
Supply Chain Attacks	• Attackers infiltrate the factory's OT system through third-party equipment or software in the supply chain by preloading malicious programs before deployment in the facility. • Attackers tamper with hardware devices or software update packages from suppliers, injecting malware into the production environment.[8]

TABLE 1. Common Threat Scenarios and Attack Methods

02

Cybersecurity Regulations in the Automotive Industry

The future of automobiles will likely be defined by software. With automobile OEMs becoming one of the largest software suppliers, there will be significant cybersecurity risk. Hackers will try to gain access to the system through this software, thereby threatening security functionality or consumer privacy. However, we believe the severity of the threat will change soon.[9] The World Forum for Harmonization of Vehicle Regulations (WP.29) under the United Nations Economic Commission for Europe (UNECE) released two important cybersecurity regulations, R155 Cyber Security[10] and R156 Over-The-Air Software Update (OTA)[11] on June 24, 2020. These regulations subsequently took effect in early 2021.

- **UNECE WP.29 R155: Cyber Security Management System (CSMS)**
- **UNECE WP.29 R156: Software Update Management System (SUMS)**

These two security regulations are mandatory for ensuring market access and vehicle type approval in UNECE WP.29 member states and contain binding requirements for car manufacturers (and Tier 1 and Tier 2 suppliers). From July 2022, the requirements within UNECE Member States (derived from the 1958 Agreement) apply to type approval of all new car models, and from July 2024 on, they will apply to all vehicles. It is at this point that we believe the severity of the threat will decrease significantly. Compared to UNECE WP.29 R156, we have studied UNECE WP.29 R155 more carefully because UNECE WP.29 R155 is closely related to the field of automobile manufacturing. At the same time, we also found that many companies have begun to realize that UN R155 not only covers products but also product development and organizations.

UNECE WP.29 R155: Cybersecurity Management System Overview

UN R155 came into force in early 2021 and is binding in 64 UNECE member countries. Two critical dates mark its application: from July 2022, UN R155 requirements apply to all new vehicle types for type approval, and from July 2024, they will apply to all vehicles. This puts enormous pressure on OEMs and their supply chains, as certification is required to launch a car on UNECE's market. For type approval, OEMs must meet three main requirements:

- **Implement a Cyber Security Management System (CSMS)**
- **Provide evidence that vehicle design, risk assessment procedures, and cybersecurity controls implementation are properly executed for each specific vehicle type**
- **Comply with regulations, including Annex 5 chapters**

A certified CSMS is essential for connected vehicle approval, setting new standards for managing cybersecurity risks throughout a vehicle's lifecycle—covering security by design, vulnerability mitigation, supply chain risk management, and incident management. OEMs are responsible for maintaining CSMS compliance across the automotive value chain, with suppliers also adhering to CSMS principles. CSMS certification, a prerequisite for vehicle type approval, must be renewed every three years.

Although UN R155 does not provide specific guidelines for implementation, the ISO/SAE 21434 standard offers clear organizational, procedural, and technical requirements for cybersecurity throughout the vehicle lifecycle.

ISO/SAE 21434: Guiding the Automotive Industry Toward Cybersecurity Compliance

The International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE) have released ISO/SAE 21434, a standard designed by industry experts and considered to be the most advanced in the automotive industry. These standards provide cybersecurity guidance, and compliance with ISO/SAE 21434 enables automakers to adopt common frameworks and processes that align with industry practices to enhance product safety. To standardize the implementation of UN R155, ISO/SAE 21434 offers guidance on cybersecurity verification, including clauses related to cybersecurity management, project-dependent management, continuous activities, threat and risk assessment methods, and cybersecurity measures throughout the concept, development, and post-development stages of road vehicles.

Additionally, these standards require OEMs, Tier 1 suppliers, and other critical suppliers to comply with network security engineering requirements. They primarily focus on the following phases:

- **Development**
- **Production**
- **Post-production**

02 Production Control Plan Requirements (ISO/SAE 21434 Clause 12)

ISO/SAE 21434 provides a framework for automotive manufacturers and their supply chains to implement specific security practices for a Cybersecurity Management System (CSMS) during vehicle development and manufacturing.[12] These practices also enable the assessment and verification of cybersecurity compliance for third parties such as automotive Tier 1 and Tier 2 suppliers, thus improving security throughout the entire supply chain; for example, by establishing reliable security testing processes between OEMs and suppliers.

Previous research has primarily focused on the risk analysis methodology (Clause 8) and the concept phase of development (Clause 9) within ISO/SAE 21434. However, less attention has been given to production security, particularly Clause 12. The questions that arise are: How should a CSMS be implemented in post-development and how can vulnerabilities be kept out of the production process? This paper briefly discusses the necessary measures and tools that should be integrated into an organization's processes to ensure compliance. Article 12.2 of the ISO/SAE 21434 standard stipulates that automobile manufacturers must "apply cybersecurity requirements in the post-development stage (including production)" and "prevent the introduction of vulnerabilities in the production process".

Specific requirements include:

- [RQ-12-01] A production control plan that applies cybersecurity requirements for post-development must be created. This should cover both the production phase and post-production phase.

- [RQ-12-02] The production control plan must include:
  a. A sequence of steps that apply cybersecurity requirements for post-development
  b. Production tools and equipment
  c. Cybersecurity controls to prevent unauthorized alteration during production
  d. Methods to confirm that cybersecurity requirements for post-development are met

- [RQ-12-03] The production control plan must be fully implemented.

03

Best Practices for Protecting Cyber-Physical Systems

In the automotive sector, rapid technological advancements have introduced new cybersecurity challenges, pushing leading enterprises to rethink their security strategies. This section reviews innovative best practices in addressing cyber threats within the automotive industry and its supply chain, and how these practices can inspire other sectors.

Conducting Security Inspections on Supplier Equipment

Before critical assets enter a factory or facility, asset owners should perform thorough scans to ensure there are no potential malicious programs or severe security vulnerabilities within the assets. This step must align with CSMS policies while establishing a health record for the assets to facilitate future maintenance and management. For equipment providers, addressing all security vulnerabilities may not always be easy. Regardless, even if these known vulnerabilities cannot be completely resolved, there should be mitigation measures in place to ensure they don't pose a potential risk during production.

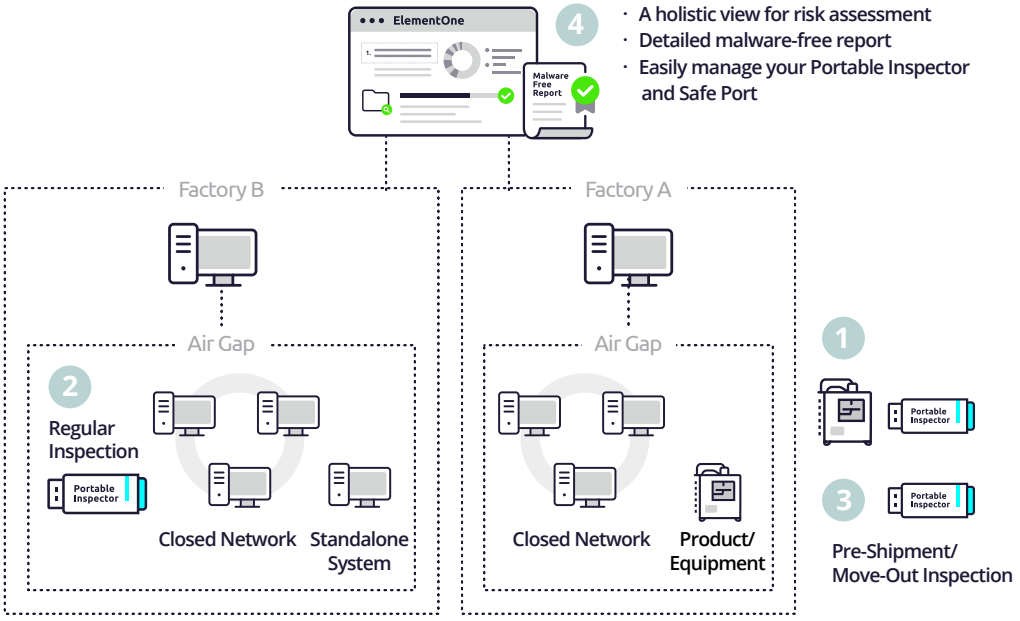


Figure 1. Use Portable Inspection Tools to Secure Supply Chain Equipment

TXOne Networks' Portable Inspector solution enables automotive manufacturers to follow best practices for conducting asset security inspections without the need for software installation. Using a portable scanning tool, automatic scans can be performed without a network connection, ensuring supply chain security before critical assets enter the production facility.

03 Integrating Production Equipment into Secured Factory Networks

To secure factory networks, they are isolated from the enterprise network and the internet, with a firewall enforcing a default-deny rule. This security approach is crucial for OT environments, enabling organizations to create a secure zone to protect sensitive devices, data, and applications. For automation and system integration, firewall rules allowing necessary connections to the datacenter must be carefully reviewed and approved under a strict allowlist policy.

In addition, micro-segmentation of factory networks and systems is essential. Traditional OT network segmentation, which primarily uses VLANs on network switches to limit the impact of compromised assets, fails to provide effective monitoring, inspection, or segmentation of east-west traffic. It also lacks visibility into OT network traffic from layer 2 to layer 7. Organizations should implement next-generation OT Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS) to achieve deep visibility and control. OT decision-makers should consider deploying protective industrial IPS at the front end of core industrial control systems. These industrial IPS perform deep analysis and filtering of major industrial control system protocols such as Modbus, S7, Ethernet/IP, and OPC, detecting data packets that don't conform to protocol standards or operational requirements.

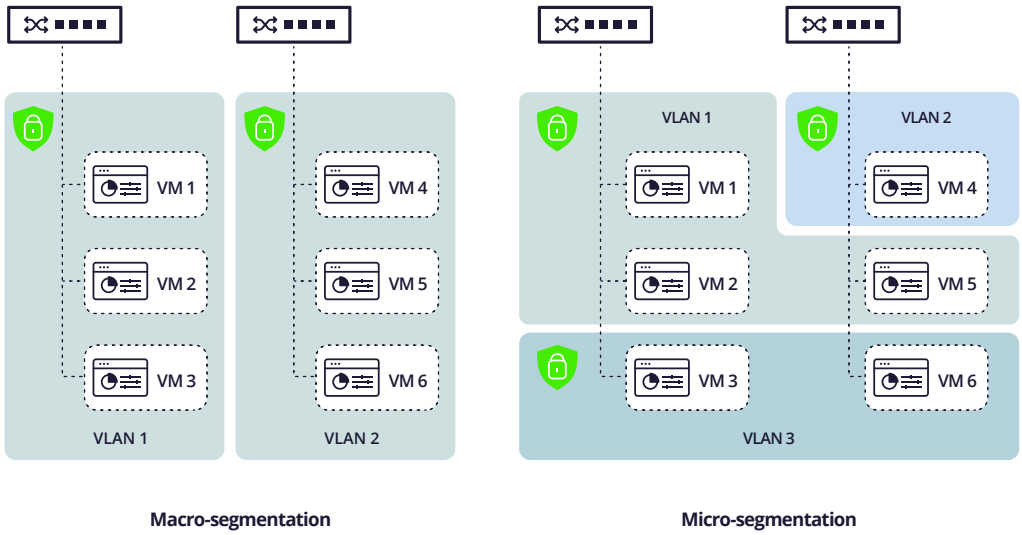


Figure 2. Micro-segmentation[13]

This practical OT security approach enhances security by enabling segmentation of zones based on specific security needs and applying Access Control Lists (ACLs) to regulate east-west traffic. Additionally, it helps detect and mitigate network-level threats from adversarial malware, such as abnormal SMB transmissions, preventing the lateral movement of viruses and malware. As factory networks expand, their topology becomes increasingly complex and traditional network micro-segmentation and ACLs face challenges in achieving optimal security. Different departments, devices, and applications have varying requirements, making it difficult to apply a one-size-fits-all segmentation strategy. Strict ACL settings may disrupt system operations and business processes, particularly in industrial environments reliant on real-time communication.

Clearly, finding the balance between security and operational needs is a significant challenge. TXOne Edge network solution leverages baseline auto-rule learning technology, which automatically learns from the organization's daily network traffic and converts it into robust access policies, enabling efficient network strategy deployment. This technology strengthens control over OT/ICS networks and boosts network defense capabilities.

When designing an OT network architecture, the primary objective is to ensure the secure, stable, and real-time operation of OT systems. Additionally, due to the unique nature of industrial environments, the hardware used in OT networks must possess characteristics like high-temperature tolerance to withstand harsh working conditions. The TXOne Edge network solution offers advanced network defense capabilities tailored to the specific requirements and operational contexts of each vertical. This ensures that every industry can deploy an optimal solution for its unique environment, including a variety of OT protocols, micro-segmentation, asset-centric auto-rule learning technology, ultimate operational continuity, anomaly detection and prevention, and malware landing prevention.

Arming Production Systems Against Cyber Threats

Hardening involves fortifying assets to eliminate attack vectors by addressing system vulnerabilities and disabling unnecessary services—such as applications, user permissions, accounts, network ports, and other non-essential system functionalities. By hardening assets, IT teams can significantly reduce the likelihood of attackers gaining access to mission-critical computers and prevent the execution of malware.

Many OT assets continue to run on outdated Windows systems, including Windows XP, which was released over 20 years ago. In reality, plant managers face a complex decision-making process, where cybersecurity risks are just one of many factors they must address. The interplay of costs, compatibility, and vendor support creates significant barriers to modernizing OT systems. Moreover, traditional antivirus software is not designed for industrial control environments. It requires constant internet connectivity to update its scanning engine and virus signatures, and file scanning often consumes excessive computing and memory resources, leading to overloaded endpoints and frequent false positives.

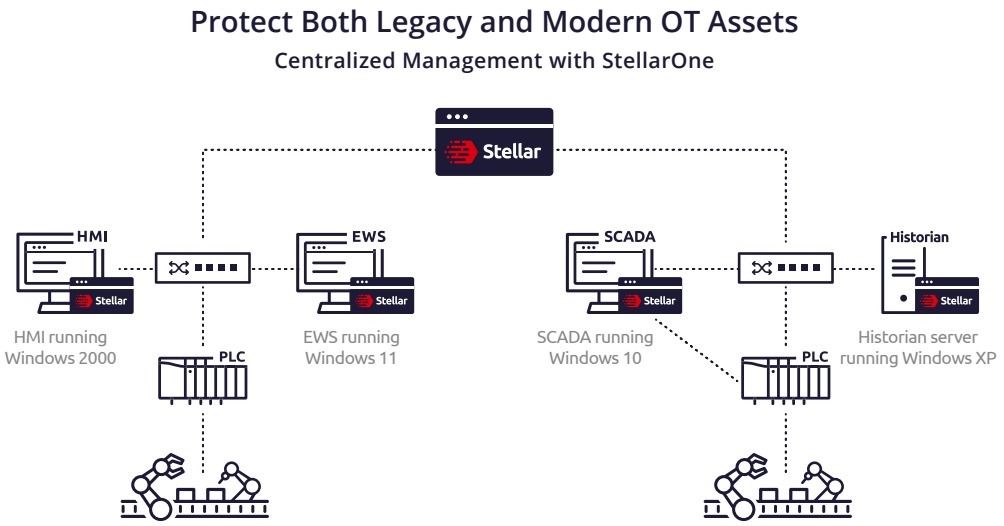


Figure 3. Protect Both Legacy and Modern OT Assets

03

In environments where these systems are critical to operations, TXOne Networks offers Stellar endpoint protection solution, a next-generation CPS security tool tailored for essential OT assets. Specifically designed for OT environments, Stellar prevents any unintended system changes that could disrupt operations. It is the first solution to offer seamless protection and comprehensive oversight for both legacy and modern OT assets operating simultaneously. This includes industrial-grade next-gen malware scanning, abnormal behavior detection, application lockdown, and trusted peripheral control.

Continuous Security Monitoring, Detection, and Response for CPS

Implementing security monitoring, detection, and response is crucial to identify and address cybersecurity incidents in real time, effectively mitigating their impact on manufacturing systems, networks, data, and devices. The process involves monitoring networks and systems for signs of potential security breaches, analyzing the data to determine whether an incident has occurred, and then taking appropriate action to contain and remediate the incident.

In recent OT attacks, hackers increasingly leverage "living off the land" techniques, where malicious programs exploit built-in operating system functions (such as PowerShell, WMIC, and ping commands) instead of targeting critical vulnerabilities.[14] On the network side, attackers often take advantage of legacy OT protocols that lack proper authentication, like Modbus TCP, rather than more secure options like Modbus/TCP Security protocol.

Once strict zero-trust mechanisms, such as network allowlists and endpoint application whitelisting, are deployed in OT environments, the next challenge lies in ensuring that these zero-trust policies remain uncompromised. To uphold zero-trust integrity, we present the CPSDR (Cyber-Physical Systems Detection and Response) solution. CPSDR addresses the risk of hackers executing unauthorized operations with legitimate, well-formatted commands—attacks that can still cause serious damage. The apparent legitimacy of these commands make these attacks harder to detect, but CPSDR identifies any unintended changes to operations and immediately issues an alert, rather than spending time to analyze whether the unintended change is legitimate or not.

TXOne Networks advocates for an operations-centric defense approach in OT/ICS environments to maximize operational uptime. This approach leverages the unique characteristics of each device and implements comprehensive security strategies to prevent unintended changes and their associated risks. The CPSDR framework generates actionable alerts, enabling security teams to respond to emerging threats while allowing operational teams to investigate potential process issues or changes.

The advanced solutions for CPS protection in automotive manufacturing include:

- **CPSDR for Networking**

TXOne's Edge series of networking security appliances integrate cutting-edge CPSDR technology to detect and predict anomalous network behaviors early on. By employing CPSDR, your OT network can proactively mitigate cyber risks, stopping potential threats before they escalate.

- **CPSDR for Endpoints**

TXOne's Stellar solution analyzes each device's unique fingerprint at the agent level and monitors deviations in normal operations. With real-time detection through deviation and behavior analysis, it catches unauthorized access, malware, unintended configuration changes, and malicious process modifications, suppressing these risks before any impact occurs.

03 Safe File Exchange: Securing Data Transfers

The exchange of files and data within and outside manufacturing environments requires robust security controls. For data exported from the manufacturing environment, the primary focus is on safeguarding equipment logs. These logs contain critical information about the manufacturing process, including machine configurations, production data, and quality control metrics. Protecting these logs is essential to maintaining the company's competitive edge and profitability. This defense is not only necessary to protect proprietary information but also to prevent unauthorized access, tampering, or loss of critical data that could affect production quality and efficiency.

OT decision-makers should deploy boundary network defense appliances between different network borders to ensure secure access control and block unauthorized network access. Industrial control networks must never connect to the internet without protection. If remote maintenance is required, organizations should secure remote access channels through authentication and encryption methods, such as using Virtual Private Networks (VPNs). Additionally, each access account should be assigned to a specific individual, with regular audits of account activity to ensure security compliance. TXOne's EdgeFire firewall rules and remote access controls can establish a secure site-to-site VPN with remote access capabilities to protect OT networks from unauthorized access or interception.

Additionally, equipment maintenance often involves both hardware repairs (such as hard drive replacements) and software configuration changes, system upgrades, and security updates. Typically, factories schedule regular maintenance operations. However, any changes introduce potential risks, and OT security decision-makers need to ensure that assets remain synchronized with the latest security policy and intelligence, and that any replaced hardware or software complies with the asset owner's security configuration policies.

It's crucial to avoid introducing new security vulnerabilities through software updates. Thus, during maintenance, we recommend that production equipment managers perform multiple malware and vulnerability scans. Extra security checks, including malware and vulnerability scans, should be conducted when replacing hardware or software components or making software configuration changes. This is especially critical for portable devices or computers brought into the production environment by vendors or maintenance personnel.

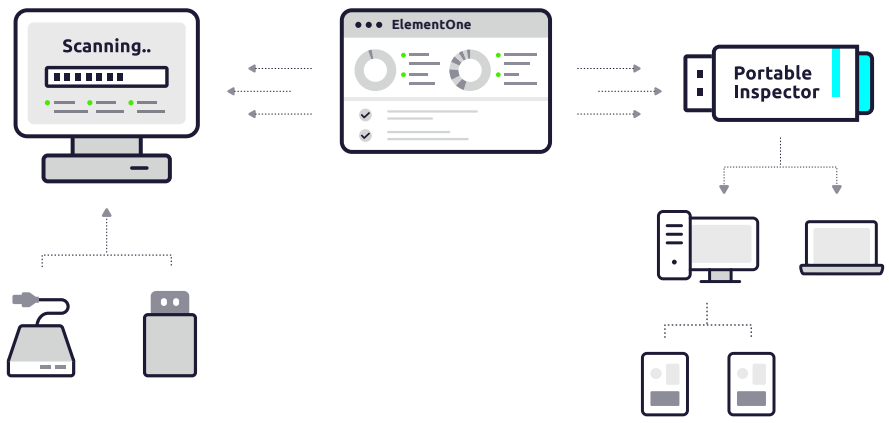


Figure 4. Safe Port Rapidly Secures and Sanitizes Removable Media

Since security checks are often conducted on-site, where the environment is typically offline, TXOne's Safe Port can perform security inspection tasks without relying on a network, preventing potential entry points for malware. Additionally, the Portable Inspector offers a complementary solution by scanning assets using USB storage devices without interfering with software or relying on a network. It ensures that the original equipment software and configuration remain untouched while verifying the cleanliness of the device.

Enhancing CPS Security with Real-Time Situational Awareness and Threat Detection

To achieve robust OT cybersecurity, a deep understanding of operations is essential. Factory security teams require a clear, real-time platform to manage the cybersecurity of numerous devices, enabling swift detection and response to attacks as they occur. It is crucial to maintain situational awareness of all assets, monitor software configuration changes, system upgrades, and security updates.

By continuously tracking routine schedules and leveraging TXOne's SageOne platform, organizations can optimize threat detection and response. SageOne centralizes all CPS security solutions into a unified management console, offering comprehensive visibility across OT environments. Integrating TXOne's Stellar, Element, and Edge products, SageOne provides full lifecycle protection, managing the CPS attack surface with advanced AI-powered threat detection. With capabilities like cross-telemetry analysis and behavior-based threat intelligence, SageOne ensures rapid responses to both known and unknown threats, safeguarding critical infrastructure while enhancing cybersecurity governance throughout the asset lifecycle.

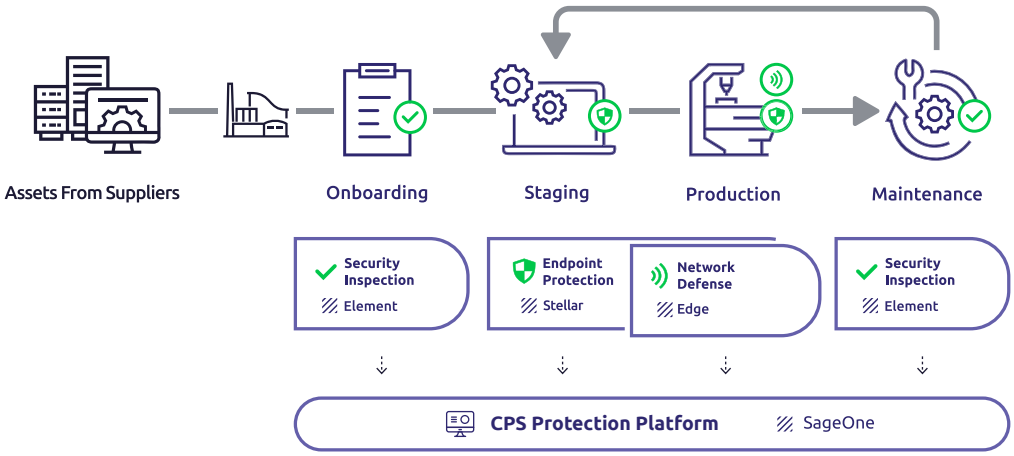


Figure 5. CPS Protection Platform Provides Insights

Conclusion

As the industry continues to embrace digital transformation, the integration of advanced security solutions tailored to industrial contexts will be essential in ensuring long-term operational resilience and protecting the future of smart automotive manufacturing. Ensuring cybersecurity in this environment is no longer an option; it is a critical requirement for maintaining operational integrity and safeguarding sensitive data. By adhering to stringent regulations like UNECE WP.29 R155 and ISO/SAE 21434, and implementing robust cybersecurity practices—including real-time monitoring, network segmentation, and endpoint protection—automotive manufacturers can effectively mitigate risks.

TXOne Networks works with partners in the automotive industry to provide comprehensive solutions from CPS endpoints to the network, and a unified cybersecurity platform for CPS attack surface management. If you would like to learn more about our products, please contact us.

Reference

[1] Rockwell Automation, “State of Smart Manufacturing: Automotive Edition”, June 2024.

[2] Dean Parsons, “What’s the Scoop on FrostyGoop: The Latest ICS Malware and ICS Controls Considerations?”, August 9, 2024.

[3] Catalin Cimpanu, "Top exploits used by Ransomware gangs are VPN bugs, but RDP still reigns supreme", ZDNet, August 23, 2020.

[4] Ravie Lakshmanan, "Warning: DEEPDATA Malware Exploiting Unpatched Fortinet Flaw to Steal VPN Credentials", The Hacker News, November 27, 2024.

[5] Naomi Tajitsu, Richard Pullin, "Honda Halts Japan Car Plant After WannaCry Virus Hits Computer Network", Reuters, June 27, 2017.

[6] Henry Hui, Kieran McLaughlin, Sakir Sezer, "Vulnerability Analysis of S7 PLCs: Manipulating the Security Mechanism", International Journal of Critical Infrastructure Protection, December 2021.

[7] Rommel Joven, Ng Choon Kiat, "The Spies Who Loved You: Infected USB Drives to Steal Secrets", Mandiant, July 11, 2023.

[8] U.S. Department of Defense, "Securing the Software Supply Chain: Recommended Practices for Suppliers", U.S. Department of Defense, October 31, 2022.

[9] TXOne Networks Team, “Mitigating Cyber Risks in Automotive Supply Chain: An Analysis of ISO/SAE 21434 Guidelines”, TXOne Networks, February 7, 2023.

[10] UNECE, “UN Regulation No. 155 - Cyber security and cyber security management system”, UNECE, 2021.

[11] UNECE, “UN Regulation No. 156: Software Update and Software Update”, 2021.

[12] ISO, “ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering”, 2021.

[13] Ramaswamy Chandramouli, “Guide to a Secure Enterprise Network Landscape”, NIST, November 2022.

[14] Health Sector Cybersecurity Coordination Center (HC3), “Living off Land Attacks”, HC3, October 17, 2024.