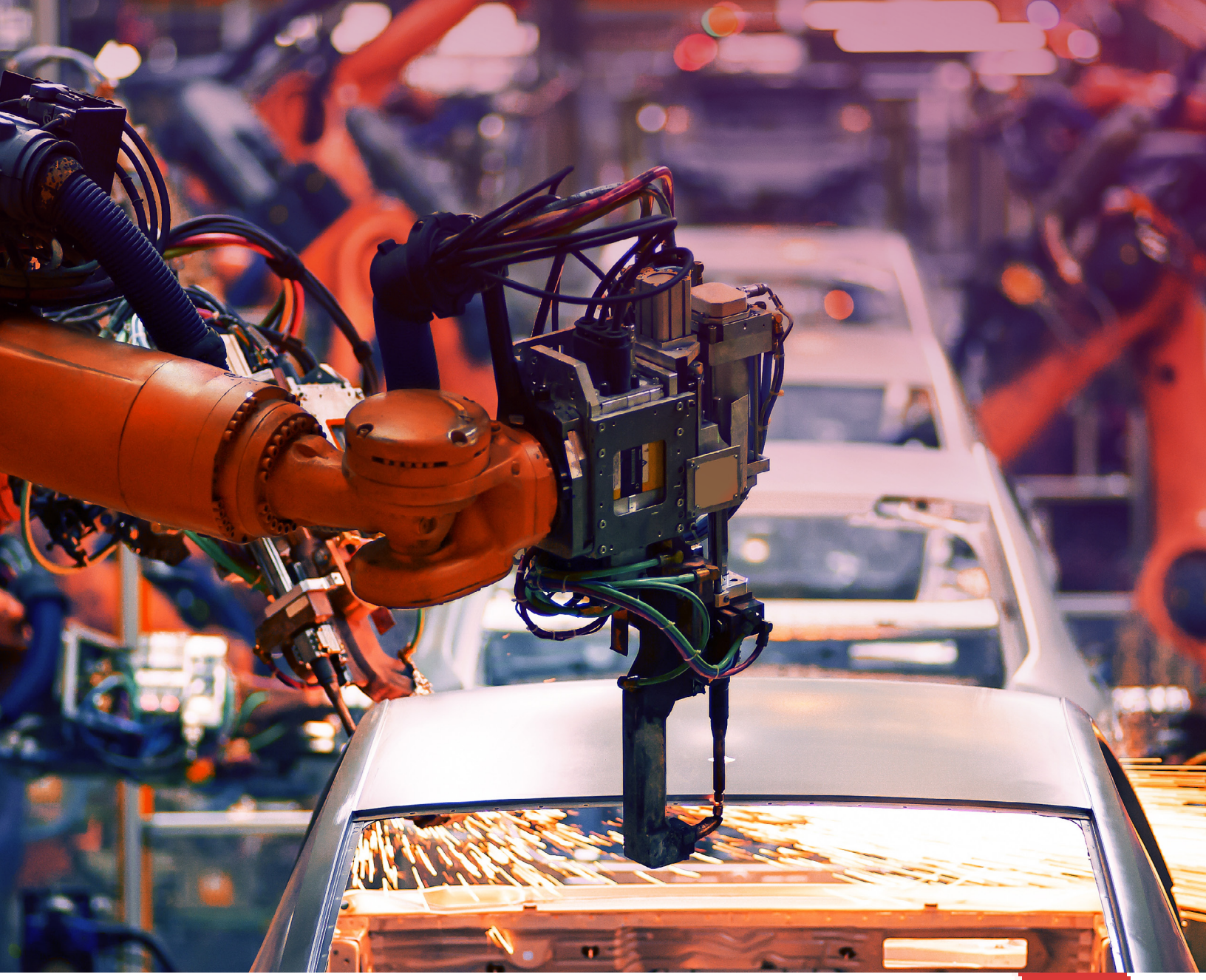

Rockwell Automation

UNDERSTANDING AUTOMOTIVE CYBERSECURITY:

# Common Threats, Proactive Prevention

## Executive Summary

Malicious actors are targeting automotive companies with successful cyberattacks. Recent high-profile incidents indicate current automotive industry cybersecurity protections clearly aren't robust enough:

- **February 2021.** One leading automobile manufacturer in South Korea suffered a ransomware attack that resulted in outages to payment services, their mobile apps, and dealerships' internal systems.
- **June 2020.** Japan's leading automotive manufacturer fell victim to a cyberattack that led to operational disruptions at plants in the U.K., North America, and Italy.
- **April 2020.** One automotive publication's investigation found serious security flaws in two best-selling car models.

Several factors contribute to an expanded attack surface at automotive companies, including:

- Increased data flow, communication, connectivity and integration of operational technology and information technology (OT/IT) infrastructure.
- Lack of skilled resources to manage risks involving Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and other OT systems.
- Poor visibility into the number and types of assets connected to automotive networks.
- The ongoing pandemic has strained supply chain operations making the risk and cost of manufacturing downtime even higher, at a time when inventory is tightly constrained. Unfortunately, this situation is unlikely to subside anytime soon.
- The advent of electric vehicle infrastructure generates new threats to connected vehicles, public charging stations, even the electric grid. And a lack of security standards to safeguard charging stations only further complicates their protection.

Adversaries target vulnerabilities across the installed base of network assets, including machines and devices on plant floors. Because almost half of today's top 100 automotive manufacturers are considered highly susceptible to ransomware incidents[1], it's clear: risk management in the automotive industry is still too reactive to address the increasing speed and sophistication of attacks.

[1] Black Kite

## Costs and Consequences

Vulnerabilities exploited by malicious actors can lead to multiple negative operational outcomes that include but also extend beyond typical IT-centric concerns, such as data breaches.

### PRODUCTION DOWNTIME

Unplanned downtime is one of the greatest risks for automotive companies because factory downtime is so costly. One estimate showed a cost of $22,000 per minute or $1.3 million per hour of downtime. Some estimates show a cost of $50,000 per minute.[2] Often, cyberattacks cause downtime in OT environments and adversaries understand that vehicle production interruptions come with these high costs, making the automotive industry a prime target.

Separate from downtime costs are expenses from operational and physical damages, to response, remediation and recovery costs from cyberattack, which are typically estimated between $1 million+ to $13 million or more per incident.

### SENSITIVE DATA COMPROMISES

The potential for sensitive data compromise extends from IT to OT. Confidential data on the plant floor takes a different form, however. Trade secrets, including formulas, techniques, software, or machine and recipe data, are extremely valuable intellectual property and highly competitive business assets. Automotive manufacturers prize this information because it may provide a competitive advantage in operational efficiency or product features, especially around the shift to electric vehicles and charging stations.

Attackers that manage to infiltrate OT/ICS environments can compromise and exfiltrate vital information, and/or sensitive customer data.

### SUPPLY CHAIN SHORTAGES

Auto makers are not the only ones attackers focus on. Risks extend to suppliers who provide automotive companies with critical manufacturing components, such as air conditioning and heating systems. Severe cyberattacks on suppliers can bring on a ripple effect that can lead to extended supply chain shortages.

Cybercriminals target vulnerabilities at all levels of the automotive supply chain. In October 2021, for example, German automotive parts supplier Eberspächer Group[3], which operates 50 plants, suffered a ransomware attack on its global networks and servers that encrypted data. The company shut down IT systems as a precautionary measure but was forced to contend with significant disruption, sending workers home on paid leave and generating other losses.

### PHYSICAL SAFETY THREATS

Cyberattacks infiltrating automotive OT environments can turn into potential threats to physical safety as well. Malware, worms, and viruses can sabotage industrial devices such as programmable logic controllers (PLCs) and give adversaries control over assembly line machines. Unexpected adjustments to assembly line processes or equipment behavior may also pose safety threats to plant floor workers. In addition, intentional OT damage could harm product integrity and put customer safety at risk.

[2] TPC , [3] Eberspaecher

## Automotive Threat Actors and Common Cyberattacks

To gain an unobstructed view of the automotive cybersecurity landscape, it's important to understand more about the malicious threat actors targeting automotive companies, and the methods commonly used in attacks. It's also important to note that while attack sophistication is growing exponentially, most successful cyberattacks exploit well-known vulnerabilities that can be fixed with available tools and best practices.

### THREAT ACTORS

Malicious cybersecurity operatives, such as ransomware gangs, seek to infiltrate networks for monetary reward. Other threat actors may attack automotive companies with the intention to cause physical harm, or steal valuable intellectual property, personal identifiable information, or other prized information assets.

In addition, the automotive industry is part of the Critical Manufacturing sector identified by the Cybersecurity and Infrastructure Security Agency (CISA)[4] as crucial to U.S. economic prosperity and continuity. The critical economic nature of automotive manufacturing makes businesses in this industry susceptible to nation-state cyberattacks as well. In an attempt to further their own national interests, countries may hire threat actors to gather intelligence or sabotage key industrial targets.

Security researchers also discover and publicize vulnerabilities in automotive companies' cybersecurity postures. One recent incident[5] saw security researchers analyze the computer systems of a large U.S. auto manufacturer's popular model and uncover a set of Wi-Fi credentials for an assembly plant.

While security researchers typically don't set out to maliciously exploit vulnerabilities, they can uncover gaps that create public relations nightmares, impacting credibility among customers.

Now let's turn to common attacks that auto makers and their suppliers frequently experience.

### RANSOMWARE

Ransomware is a fast-growing attack type, creating problems across all industries. Black Kite's 2021 Third Party Breach Report[6] found ransomware is now the number one origin of third-party data breaches, accounting for 27% of attacks in 2021, 53% of CISOs said they were hit by ransomware at least once in the last year.

In a typical ransomware attack, adversaries infiltrate the network and deliver a malicious payload that encrypts multiple files and devices. Many ransomware incidents involve data exfiltration and encryption because threat actors believe extortion is more likely to be successful if they can threaten to publicize stolen sensitive information. As the lines between IT and OT blur, ransomware attacks can lead to dreaded plant floor production disruptions.

[4] CISA , [5] Which.co , [6] Black Kite

## ICS ATTACKS

Integrated connectivity and increasingly open communications across IT, OT, and Internet of Things (IoT) devices have also expanded the attack surface in ICS environments, exposing often decades-old technologies to the Internet and to cloud-based applications for the first time. Organizations that consider themselves sufficiently air gapped are finding the opposite to be true.

Frequent attacks include the exploitation of insecure communications protocols; unpatched software; weak IoT security; and supply chain malware attacks impacting manufacturing devices. And ICS attacks are on the rise, as evidenced by the disclosure of 41% more ICS vulnerabilities[7] in the first half of 2021 than the same period in 2020.

## CONNECTED VEHICLE HACKS

Modern connected motor vehicles have several onboard computer systems that threat actors can target with remote and physical attacks. Vehicles today 'wake up' and become connected before they come off the assembly line, equipped with potentially exploitable systems.

- The Telematic Control Unit (TCU) may be susceptible to hacks. In one incident[8], researchers took a telematics unit from a vehicle, pulled the subscriber identity module (SIM) card from it, and managed to use the SIM's access to gain full control of the original equipment manufacturer (OEM's) corporate network using admin credentials.
- The Controller Area Network (CAN) bus enables communication between different microcontrollers and sensors on motor vehicles. Research[9] shows that a typical CAN bus is highly susceptible to attacks that exploit vulnerabilities such as a lack of authentication or encryption, which may lead to vehicle takeover or sensitive data breaches.

## MOBILE APPS

In our increasingly mobile world, many OEMs offer mobile apps that enable customers to connect to their vehicles. Some of these apps let users locate their vehicle, open the doors, and start the engine. Hackers can exploit app coding vulnerabilities, how the app communicates, or how it stores data.

The fallout from mobile app attacks ranges from the breach of sensitive information to potential safety threats. In 2018, for example, one auto maker[10] inadvertently exposed the personal details of more than 50,000 app users in an unsecured cloud storage bucket.


[7] CPO Magazine , [8] Pen Test Partners , [9] University of Washington , [10] Bleeping Computer

## Proactive Cybersecurity in Automotive Manufacturing

Automotive companies need a more proactive approach to handle the deluge of threats they now face. Our recommendations cover critical aspects of defense-in-depth, and align with NIST's Cybersecurity Framework (CSF).

### ASSET INVENTORY AND RISK ASSESSMENT

Proactive security starts with overcoming visibility gaps. What plant floor assets reside on the network? What software is used within OT environments, and what are the particular risks to those assets and software? Automotive companies can't protect what they don't know about.

A thorough inventory and risk assessment can help guide you toward the most important fixes before malicious actors can exploit any glaring weaknesses.

The initial steps you can take align with the Identify category of NIST's CSF, designed to help focus and prioritize security protections on the highest priority vulnerabilities. The goal is to secure the highest value business assets first, based on recognized threats and risks posed to the organization.

### PATCH MANAGEMENT

Patch management in OT is challenging because any level of downtime is costly and is avoided, and patching out-of-date software often necessitates taking a machine out of operation.

In most cases, taking an inventory of assets and conducting a risk assessment will flag multiple plant floor devices running outdated operating systems. These steps will also reveal unauthorized assets lurking on the network, exposing the organization to critical vulnerabilities.

A proactive security approach must include methodical patch management to address vulnerabilities in line with the Protect function of NIST's CSF. Automotive companies need processes to handle patching with minimal operational interruption. Some companies opt for an Infrastructure-as-a-Service approach, which greatly simplifies patching and other operational and cybersecurity management processes.

Security teams should consider these factors in determining patching prioritization:

- The potential risk to assets if a vulnerability is exploited
- The importance of any vulnerable device or system to the overall manufacturing process
- The security protections provided by each patch.

## LOGICAL NETWORK ZONING AND CPWE

Network architecture plays a vital role in the security of connected IT and OT environments. Attacks can propagate from individual machines, in switches and other plant-floor components into the IT network, as well as the other way around – from IT to OT networks. This often drives the decision to take production systems offline during IT security incidents.

In the previous exploit example of a vehicle's TCU breach, the OEM did not have proper network segmentation in place. Logical network zoning helps improve create the right zoning strategies for more holistic plant-wide security, protecting operations against a range of attacks.

A proven reference architecture, such as Converged Plantwide Ethernet (CPwE), also provides a solid foundation for proper network segmentation, so threat actors can't exploit vulnerabilities and move between IT and OT environments.

Often, OT architectures emerge from functional and efficient production designs, rather than having security built in from the start. OT systems are created to be deployed and to run smoothly. There's often little or no focus on how a particular design decision could impact network security.

What automakers need are smooth OT systems with the right cybersecurity protections safeguarding them. Even as the number and severity of attacks rises, it's still important to maintain smooth and secure information flow to maximize reliable uptime.

CPwE uses an Industrial Demilitarized Zone (IDMZ) to securely share information between IT and OT systems, while simultaneously shielding production systems from malicious traffic coming from corporate IT systems or the internet. Front and back firewalls provide strong protection and enforcement of security policies, providing traffic inspection across all networks.

## CONTINUOUS THREAT DETECTION AND RESPONSE

Threat detection and response delivers critical armaments in any organization's security defenses.

While a proactive approach to automotive cybersecurity starts with prevention steps that improve cyber resiliency, implementing threat detection and incident response controls can help businesses detect attacks quickly, respond to threats and help prevent propagation, and recover affected systems faster in the event of a breach.

Threat detection solutions should continuously identify threat signatures, such as anomalous devices and activity on the network. Baselines of normal user activity and traffic flows can prove useful in analysis and can shorten the time to detect incidents, especially in complex networks with high levels of IT/OT convergence.

Detecting attacks in real-time also allows for rapid incident response, such as quarantining devices or removing access, helping automotive manufacturers avoid damage escalation.

## Rockwell Automation Cybersecurity Expertise for the Automotive Industry

At Rockwell Automation, our industrial-strength cybersecurity services protect the automotive manufacturing processes you and your customers rely on daily. Our proactive approach covers the entire cybersecurity lifecycle, from assessment through recovery - so your organization can be prepared before, during, and after an attack.

We offer deep understanding of production operations leveraging insights from more than 100 years of industrial automation. Starting with a thorough inventory and risk assessment, we can help you gain clear visibility into the installed architecture, network infrastructure, and vulnerabilities present in your environment.

Our experience with Converged Plantwide Ethernet ensures holistic defense-in-depth to help block threats from propagating between IT and OT operations. And industrial-strength detection and response using a 24/7 OT Security Operations Center (SOC) can help stop attacks before malicious actors disrupt operations.

To learn more about how proactive automotive security strategies can protect against cyberattacks, contact us today.

Connect with us.

**rockwellautomation.com** — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846



Publication GMSN-WP004A-EN-P – May 2022