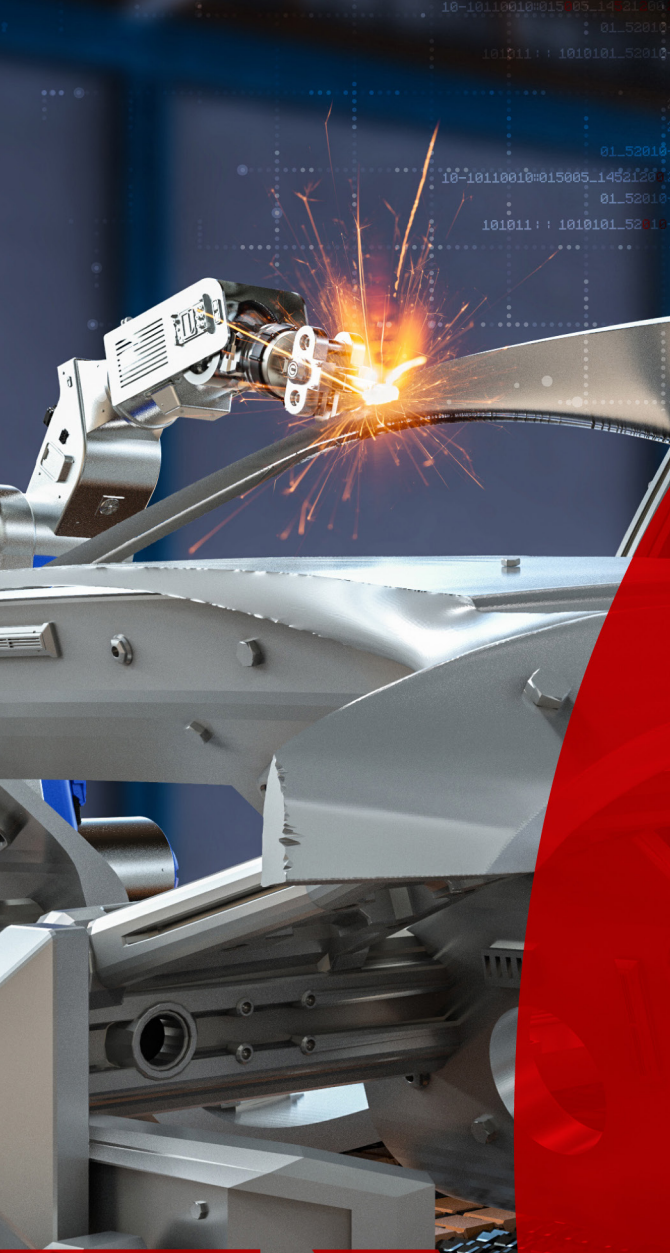
TXOne Networks

2023 /Q1



Mitigating Cyber Risks in Automotive Supply Chain:

An Analysis of ISO/SAE 21434 Guidelines

txOne networks

TXOne Networks

Mitigating Cyber Risks in Automotive Supply Chain:

An Analysis of ISO/SAE 21434 Guidelines

txOne networks

Mitigating Cyber Risks in Automotive Supply Chain:
An Analysis of ISO/SAE 21434 Guidelines

Table of Contents

Introduction

Recent advancements in autonomous driving, connected cars, electric vehicles, and ride-sharing services have dramatically impacted the automotive industry. According to McKinsey,[1] today's automotive systems have reached 100 million lines of code, surpassing even large software platforms such as Boeing 787, Mac OS, and Facebook. The technology of software-defined vehicles (SDV) is becoming more prominent, leading to an increase in vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) connectivity and the development of smarter applications that enhance customer experience and create new revenue streams for automotive original equipment manufacturers (OEMs). Industry experts predict that 60% of the future automotive value chain will come from software and content services.[2]

However, in 2022, the rise in complexity and new attack vectors have brought new challenges to the entire smart mobile ecosystem. Not only has the frequency and complexity of attacks increased but also hacking tools and knowledge have become more advanced. Fortunately, with the implementation of UNECE WP.29 R155, automotive OEMs are working closely with suppliers and cybersecurity companies to establish a robust cybersecurity management system (CSMS) structure, testing process, and compliance certification work to create a trustworthy smart mobile ecosystem. The security of the vehicle itself is not the only consideration; the entire product life cycle of the vehicle must also be protected, from development through production, to after-sales maintenance. This article provides security guidelines for automobile production to prevent the introduction of vulnerabilities and threats into the production process.

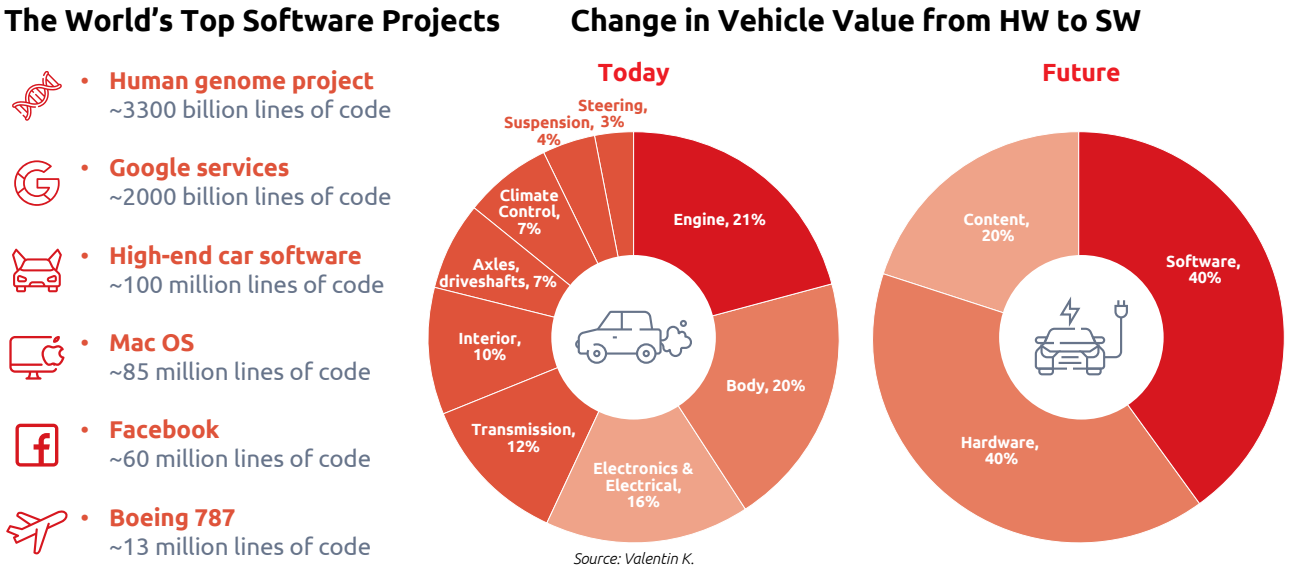


Figure 1: A Paradigm Shift for the Automotive Industry

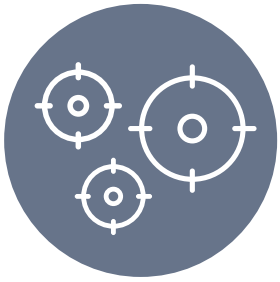
[1] *Ondrej Burkacky, Johannes Deichmann, Benjamin Klein, Klaus Pototzky,Gundbert Scherf, Cybersecurity in automotive, GSA and McKinsey, March 2020.*

[2] *V V Savchenko, S N Poddubko, "Development approach to a method for monitoring of driver's ability of resumption of control over the vehicle by on-board systems in automatic mode", IOP Conference Series: Materials Science and Engineering, 2018.*

Automotive Industry Cybersecurity Challenges

Rapid Digital Transformation

The global manufacturing industry is actively pursuing digital transformation, and one of the fastest growing sectors is the automobile manufacturing sector. Digitizing the automotive manufacturing process improves productivity, enhances quality, and optimizes plant operations. For example, in 2017, Honda Motor Co. deployed over 700 robots in its East Liberty factory in Ohio for automated welding and steel plate processing, which included some remotely controlled operations.[3] Engineers on the production line primarily monitored the automation process. In 2019, GAC Trumpchi's automobile factory in Yichang, China achieved the impressive speed of 46 seconds for body assembly.[4] To achieve better results, many factories have begun integrating IT and OT systems to enable data analysis of operational processes. However, these advancements also increase cybersecurity risks. A Frost & Sullivan survey of 300 manufacturers, including those in the automobile industry, found that 94% of them believed that IT security incidents also affect the OT environment. This is particularly true when manufacturers lack a comprehensive enterprise industrial network cybersecurity plan.



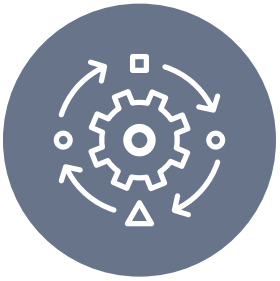
Expanding Attack Surface

According to research by McKinsey, future cars will have at least 150 or more Electronic Control Units (ECUs) and run 100 million lines of code. It is estimated that the amount of software code will reach over 300 million lines by 2030. A single new car can generate 25 GB of data per hour, or 4,000 GB of data per day. These data repositories have the potential to be worth up to $750 billion by 2030. Beyond the software development of the new car itself, it is important to pay attention to where new cars will be connected in the future, including the infrastructure they will be connected to (such as production facilities). The more infrastructure a car is connected to, the greater the attack surface becomes. For example, electric vehicle charging stations, V2X communication, road signs, and other off-vehicle communications can all become points of entry for attacks. Therefore, the potential target of an attack is not only the number of connected cars, but also the number of services and infrastructure that hold sensitive data that attackers may seek to exploit.

[3] *Toyoki Nakanishi,"For US autoworkers, robots are the job killers, not trade", Nikkei Asia, June 2017.*
[4] *Baden," 46 seconds to assemble a car!", ABB, October 2020.*

Legacy Systems Unable to Update Security in Real-time

The automotive industry, like other manufacturing sectors, faces challenges with legacy systems. These outdated computers are closely linked to production equipment and replacing them can result in unexpected downtime. However, carrying on without any changes leaves them vulnerable to hacker attacks, making it a high priority issue to address.



Complex Automotive Supply Chain Ecosystem

The supply chain in the automotive industry is complex, with OEMs relying on a variety of globally distributed third-party manufacturers for key components, including software and electronic components. As the proportion of software and services in vehicles increases, automakers are facing an increasingly complex software supply chain, leading to a changing threat landscape. Ensuring the integrity of the automotive manufacturing supply chain is crucial to prevent the introduction of threats or vulnerabilities into the production process. However, recent supply chain shortages and failures have prompted the automotive industry to seek new suppliers, which can further increase the risk of automotive networking, as they are bringing in untested and new players. In fact, a Frost & Sullivan survey of 300 manufacturers found that 47% of OT cybersecurity incidents come from new assets containing vulnerabilities or malicious programs, highlighting the importance of vulnerability management. Unfortunately, the same survey also revealed that 79% of automakers and tier 1 suppliers perform poorly in vulnerability management.

The Automobile Manufacturing Cyber Threat Landscape

In 2017, several automakers' operations were impacted by the WannaCry ransomware attack. Tracking the attacks in the automotive industry from 2020 to 2022, we found that ransomware attacks are still ongoing. The industry is now considering how to prevent the introduction of vulnerabilities or threats into the production process to avoid indirectly causing vehicle cybersecurity incidents. Automakers must shift away from traditional safety deployment models and adapt quickly. According to research, 49% of the top 100 automakers stated that their factories are "highly vulnerable" to ransomware attacks.[5] Hackers' current methods of targeting the automotive industry's supply chain will become more and efficient, distributing ransomware through spam or spoof emails that disguise malware as software updates that victims might download.

Figure 2: Security Incidents in the Automobile Manufacturing Industry in 2020-2022

[5] *Blackkite, "Ransomware Risk: Automotive Manufacturing In 2021", Blackkite, June 2021.*

Common Initial Access Attacks

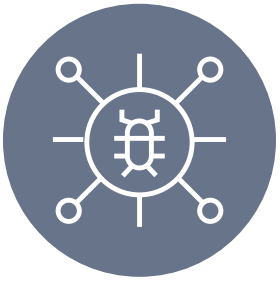
1. Utilize Public-Facing Applications

Hackers may exploit weaknesses in internet-facing software to gain access to the ICS network. Internet-facing software include user applications, operating systems, etc. Organizations often inadvertently expose vulnerabilities through remote management and visibility. Hackers may use network vulnerability scanning tools such as Shodan to find open ports and services and then attack network applications with publicly known vulnerabilities which may grant the ability to enter the ICS network or even direct access to the ICS environment. For example, the Sandworm hacker group became known for their attacks on Ukrainian electric companies in 2015 and 2016 and was suspected of initiating the NotPetya attack in 2017.[6] In the past, they used HMIs directly exposed to the internet to attack. Additionally, the Remote Procedure Call (RPC) vulnerability also existed in some old HMI software. ***However, according to Google researchers in 2018, Sandworm has begun to set its sights on the automotive industry as another target for their attacks.***[7]

2. Exploitation of Remote Services

Hackers may initially enter the IT network, and then use remote service communication protocols (such as RDP, SMB, SSH, and others) used by the enterprise intranet to move between IT or OT assets and network segments. In 2021, the EKANS ransomware attack targeted a large international automobile manufacturer. At first, many believed that the ransomware attack in the ICS environment was only due to an accidental spread from the IT network to the ICS environment.[8] However, the EKANS attack method challenges such claims, as it seemed to have a certain understanding of the process and function of HMI software, historical clients, and industrial control systems. Thus, it could be considered a weapon specifically designed for industrial control systems. It can disable security software processes to avoid detection and remove backups from the system to make it more difficult to restore files. In the second half of 2022, LockBit 3.0 launched a new wave of attacks. These are representatives of the famous Ransomware as a service (RaaS) category of attacks, and even pioneered the ransomware "bug bounty program" and deploying Cobalt Strike.[9]

[6] *Nicole Sganga, "Russian military hackers targeted Ukrainian power company, Ukrainian officials say", CBS News, April 2022.*
[7] *Cynthia Brumfield , "Russia's Sandworm hacking group heralds new era of cyber warfare", CSO, November 2022.*
[8] *Phil Muncaster, "EKANS Ransomware Detected with ICS-Specific Functions", Infosecurity Magazine, February 2020.*
[9] *Trend Micro Research," Ransomware Spotlight: LockBit", Trend Micro, February 2022.*



3. External Remote Services

This is distinct from exploiting remote services. Hackers may directly target and use external remote services as the initial entry point for attack. Especially during COVID-19, remote service applications in factories have become widespread, providing hackers with the opportunity to use VPN, VDI, and other remote service gateways to manipulate the connection and credential verification of these services.

While technologies such as VPN and VDI provide remote access to corporate networks, they can also increase the attack surface and likelihood of attacks because hackers can use stolen VPN credentials to carry out attacks. Therefore, more and more companies are turning to Zero Trust Network Access (ZTNA) solutions to replace traditional remote access VPNs.[10]

4. Spear Phishing Attachments

Hackers may use spear phishing attachments to lure specific targets into social engineering traps. In June 2022, a ransomware attack on the U.S. subsidiary of a Japanese auto hose maker forced the company to shut down its computerized production controls. As a precaution, a message was posted on the company's website advising customers to be cautious of any messages that may appear to be from the company, warning them that these may be spoof (fraudulent) emails instead.

Furthermore, in 2022, we have observed a trend of ransomware disguising itself as legitimate operating system update programs. In April 2022, the Magniber ransomware gained attention for masquerading as a Windows update file in order to trick victims into installing it. Alarmingly, by September 2022, it had also begun spreading via JavaScript.[11]

[10] *Sandra MacGregor," Gartner: Zero Trust Will Replace Your VPN by 2025", Datacenter Knowledge, Oct 2022.*
[11] *Lawrence Abrams, "Fake Windows 10 updates infect you with Magniber ransomware", BleepingComputer, April 2022.*

5. Supply Chain Compromise

Hackers may gain access to the ICS system environment through infected products, software, or workflows in the supply chain. This type of attack is called "supply chain compromise". Manipulation of a product (such as equipment or software) or its delivery mechanism occurs most often before the asset owner receives it. Adversaries tamper with these products and mechanisms with the goal of data or system compromise once infected products are introduced into the target environment. For example, a world-renowned automotive OEM suffered cyberattacks on component suppliers. Because the OEM's external parts management system was connected to some of the component suppliers' servers, 14 factories in Japan had to suspend operations, disrupting a total of 28 production lines.[12] Another way is to use the temporary assets of the ICS external network as the initial target. These temporary assets can be brought into the ICS environment through supplier personnel and would utilize a supplier or contractor with access to bring in removable media (test kits, USBs, infrastructure hard drives, etc.)

Table 1:
*Threat Scenarios Which are Related to "**Production Tool[s] or Equipment**"*

Threat Scenario	Example of Attack Path	Example of Mitigation
Production tool or equipment used to attack a vehicle or extract data	Abuse of privileges by staff (insider attack)	The principle of least privilege is applied to production tools or equipment systems
	Unauthorized internet access to the server (enabled by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	Network trust list technology is utilized on production tools or equipment systems to prevent unauthorized access
	Unauthorized physical access to the server (conducted by USB sticks or other media connecting to the server)	By implementing system security hardening design and access controls, it should be impossible for unauthorized personnel to gain access to personal or system-critical data

[12] *CNN, "Cyberattack on Toyota's supply chain shuts its 14 factories in Japan for 24 hours", CNN, March 2022.*

Threat Scenario	Example of Attack Path	Example of Mitigation
Vehicle related data held on ICS/ OT computers being lost or compromised ("data breach")	Abuse of privileges by staff (insider attack)	The principle of least privilege is applied to production tools or equipment systems to minimize the risk
	Unauthorized internet access to the server (enabled by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	Security controls are implemented on the ICS/ OT computer systems that store vehicle production data to prevent unauthorized access
	Unauthorized physical access to the server (conducted by USB sticks or other media connecting to the server)	Through system design and access control, it should not be possible for unauthorized personnel to access personal or system-critical data
	Information breaches can occur due to unintentional sharing of data, such as administrative errors or storing data on servers in garages	Security controls are applied to backend systems to prevent data breaches

Table 2:
*Threat Scenarios Which are Related to "**Unintended Human Actions**"*

Threat Scenario	Example of Attack Path	Example of Mitigation
Legitimate actors are able to take actions that would unwittingly facilitate a cyberattack	An innocent victim, such as an owner, operator, or maintenance engineer, may be deceived into taking actions that unintentionally load malware disguised as an executable system update, or enable an attack	Security measures must be put in place to define and control user roles and access privileges, in accordance with the principle of least privilege
	Defined security procedures are not followed	Organizations can use app locking as a means of ensuring that security procedures, including logging actions and access related to security feature management, are defined and followed

Table 3:
*Threat Scenarios Which are Related to "**Risk Caused by a Third Party**"*

Threat Scenario	Example of Attack Path	Example of Mitigation
Pre-installation of malicious programs in devices, and entry into the facility through device installation	Damage caused by a third party; sensitive data may be lost or compromised due to malicious programs on new devices or tools	Automotive original equipment manufacturers (OEMs) take active measures to secure their supply chain and ensure compliance with appropriate guidelines by their suppliers
Severe vulnerabilities in products supplied by third-party vendors	Software-enabled supply chain attacks, which typically exploit "software vulnerabilities" to disrupt, disable, or destroy supply chain systems, processes, or operations	
Compromising a third party's software update system	This kind of attack occurs when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor delivers it to their customers; the compromised software then corrupts the customer's data or system	

Regulations and Standards Driving the Evolution of Automotive Cybersecurity

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. 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 and R156 Over-The-Air Software Update (OTA) on June 24, 2020, which 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 organization.

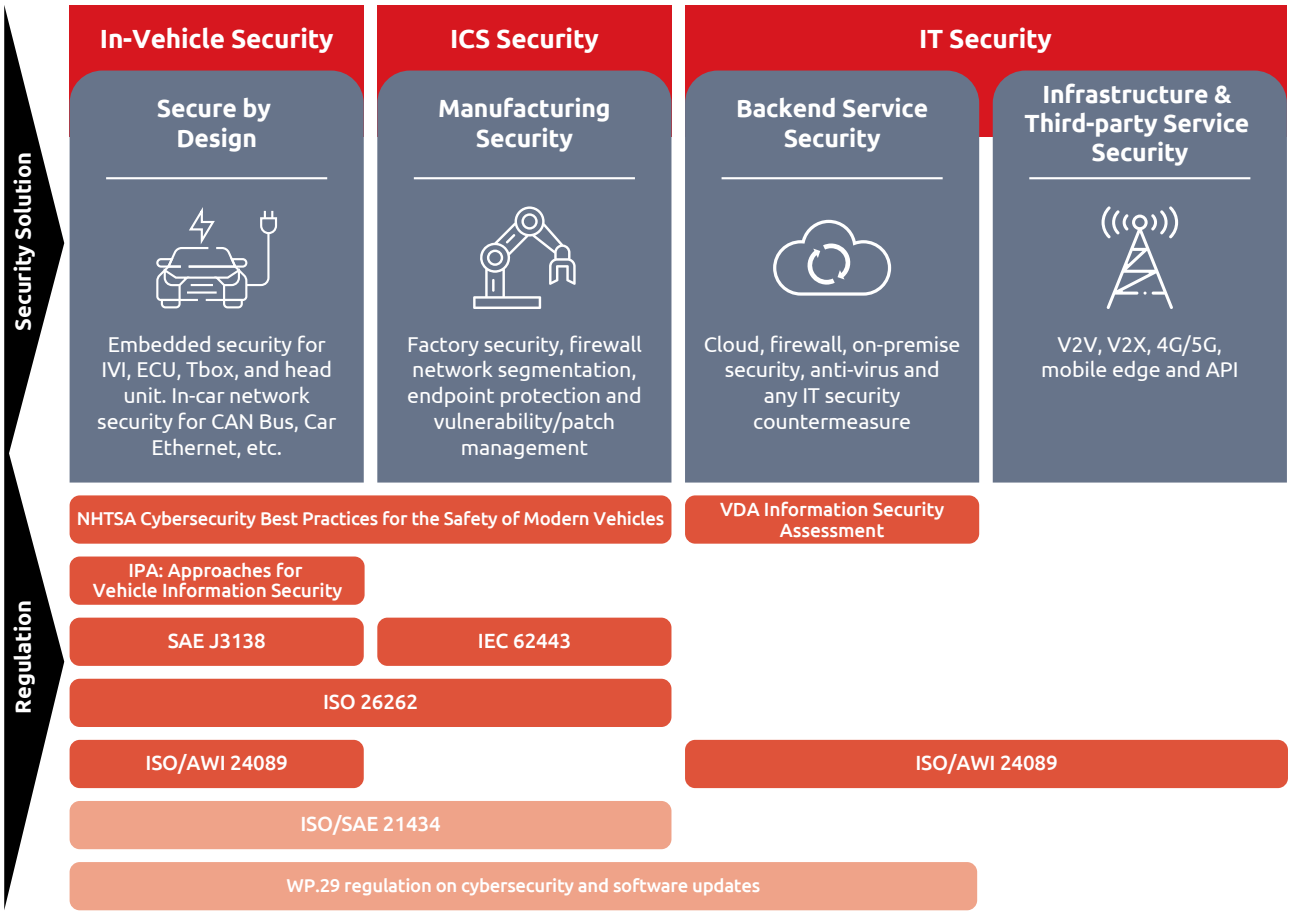


Figure 3: Regulations and Complicated Security Solutions Needed

Background Knowledge on UN Regulation No. 155

UN R155 was binding for new cars on the global market until July 2022. For conventional vehicles, the regulation will apply until 2024. This puts enormous pressure on OEMs and their supply chains, as certification is required to launch a car on UNECE's market. Type approval for OEMs is divided into 3 main requirements:[13]

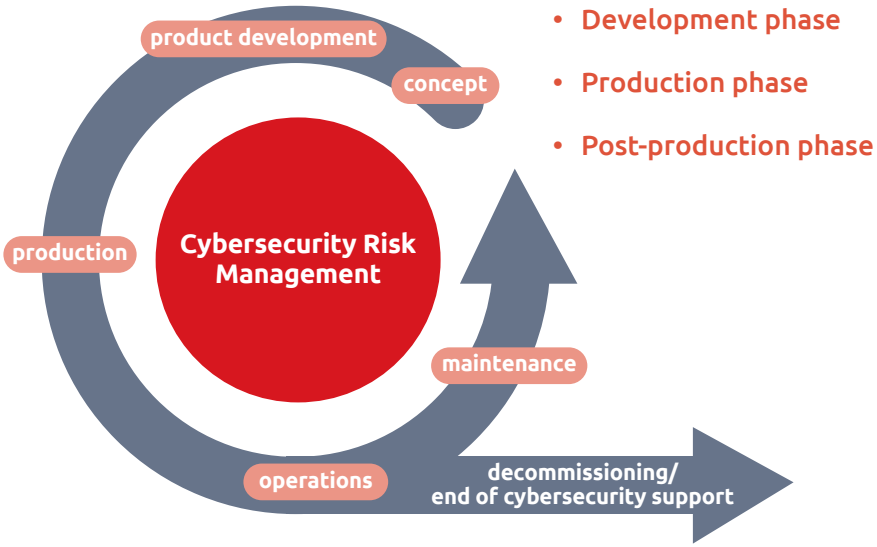
- **OEMs must implement a Cyber Security Management System (CSMS)**
- **Evidence that vehicle architecture design, risk assessment procedures, and cybersecurity control implementation are properly executed for a specific vehicle type**
- **The regulations and Annex 5 chapters provide examples of threats as well as the mitigation measures and security controls that could be implemented**

UN R155, a regulation binding type approval for 64 member states of the United Nations Economic Commission for Europe, requires vehicle manufacturers (OEMs) to implement a certified Cybersecurity Management System (CSMS) for any connected vehicle. Without it, manufacturers would not be able to obtain model approval. The new CSMS requirements set new standards for managing cybersecurity risks throughout a vehicle's lifecycle, including security by design, vulnerability mitigation, supply chain risk management, and incident management. OEMs are accountable for managing the CSMS throughout the automotive value chain and suppliers must also comply with CSMS principles. CSMS certification is a prerequisite for vehicle type approval and must be revisited every three years. However, UN R155 does not provide specific guidelines for implementation, but the ISO/SAE 21434 standard offers clear organizational, procedural, and technical requirements for cybersecurity throughout the vehicle lifecycle.

ISO/SAE 21434 Provides Guidance for UNECE WP.29 R155

The International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE) have released their standards, which were designed by industry experts and considered to be the most advanced in the automotive industry. These standards provide guidance for cybersecurity, and compliance with ISO/SAE 21434 can aid automakers in using common frameworks and processes to make their products safer. To standardize the implementation of UN R155, ISO/SAE 21434 focuses on providing guidance on good techniques for addressing cybersecurity-related verification, including clauses related to cybersecurity management, project-dependent cybersecurity management, continuous cybersecurity activities, threat and risk assessment methods, and cybersecurity within the concept product development and post-development stages of road vehicles. Additionally, these standards require that not only OEMs, but also Tier 1 suppliers and other critical suppliers comply with cybersecurity engineering requirements. These standards primarily focus on the following aspects:

[13] *UN Regulation No. 155 , "Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system", E/ECE/TRANS/505/Rev.3/Add.154, March 2021.*



Previous research has primarily focused on the ISO/SAE 21434 risk analysis methodology (clause 8) and the concept phase of development (clause 9). However, less attention has been given to production security (Article 12). The questions that arise are: How to implement a Cybersecurity Management System (CSMS) in post-development and how to prevent the introduction of vulnerabilities in the production process? This paper briefly discusses the necessary measures and tools that should be integrated into an organization's processes to ensure compliance with ISO/SAE 21434. In fact, 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". The specific requirements include:[14]

1. [RQ-12-01] **A production control plan shall be created that applies the cybersecurity requirements for post-development (including production phase and post-production phase).**

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

3. [RQ-12-03] **The production control plan shall be implemented.**

[14] *ISO/SAE, Road vehicles — Cybersecurity engineering, ISO/SAE, August 2021.*

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. These practices also enable the assessment and verification of cybersecurity compliance for third parties such as automotive tier1 and tier2 suppliers, thus improving security throughout the entire supply chain; for example, by establishing reliable security testing processes between OEMs and suppliers.

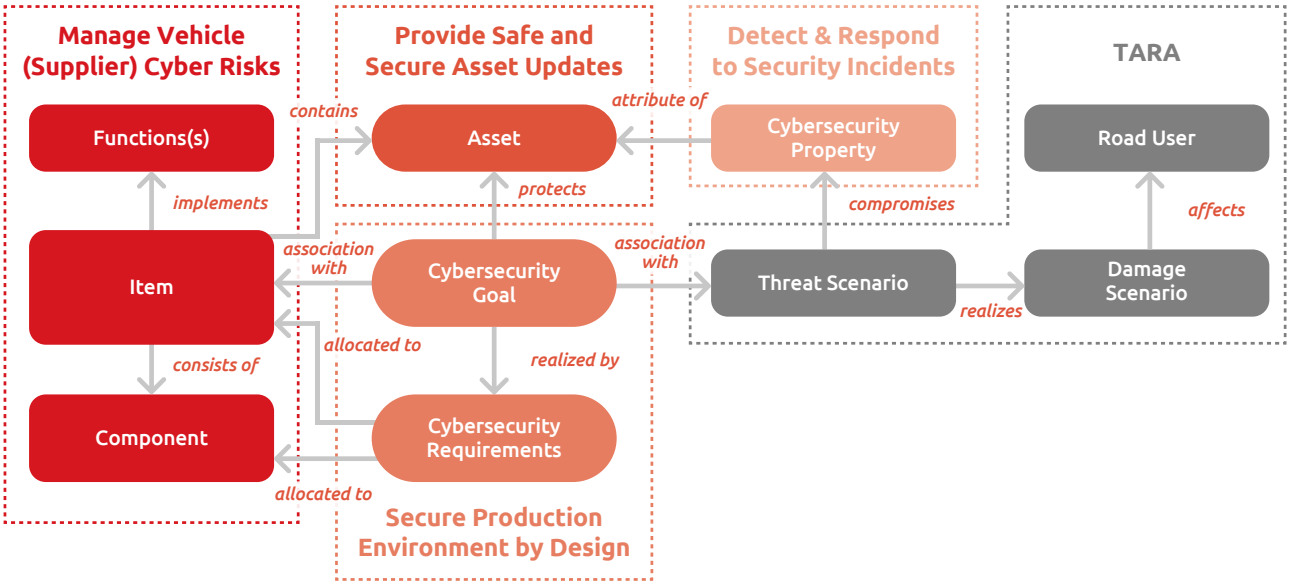


Figure 5. Relationship between ISO/SAE 21434 and R155 CSMS: Risk Focus

Ensuring Cybersecurity in Automotive Production through ISO/SAE 21434 Standards

1. Manage Vehicle Supplier Cyber Risks

Automakers often rely on supply chain partners to provide and maintain production tools and equipment. Compliance with UNECE WP.29 has added complexity, as automakers must now align their ICT supply with regulatory requirements. To ensure compliance, supply chain partners must adhere to secure product development processes and automotive OEMs must ensure that devices and software entering production facilities are secure.

- **Verify That Third-Party Production Equipment Complies with Security Requirements**

  Integrity check of supply chain equipment: Automakers must conduct integrity checks on supply chain equipment to confirm that all purchased commercial, open-source, and third-party systems or software components are free of malware.

Inspect supply chain OS of equipment for policy compliance: They should also test or check the equipment for compliance and determine if executable code testing is needed to uncover vulnerabilities not identified in previous reviews, analysis or testing, and if so, which type of testing should be used. Additionally, all discovered threats and suggested remediation actions must be recorded and organized in a process or issue tracking system.

Analysis of SBOM and its vulnerabilities: Ideally, obtain provenance information (e.g., SBOM, source composition analysis, binary software composition analysis) for each software component and analyze that information to better assess the risk that the component may introduce.

- **Identify and Assess Supply Chain Cybersecurity Posture**

  To address cybersecurity risks throughout the supply chain, companies should first develop and define requirements during the planning phase. Automotive OEMs typically conduct risk assessments of potential suppliers, and it is common practice for them to conduct more robust due diligence research on potential suppliers and/or products using cybersecurity questionnaires to generate a supplier risk profile.

  In addition, businesses can use Requests for Information (RFIs) to conduct initial screening of potential suppliers and collect cybersecurity verification information. One example of a standard used in the automotive industry is the "VDA Cybersecurity Committee Cybersecurity Assessment" (VDA ISA) established by the German Automobile Industry Association (VDA). This standard is managed by the ENX Association through the Trust Information Security Assessment Exchange (TISAX) mechanism and provides a single security framework specific to the automotive industry to assist multiple suppliers, OEMs, and partners in the supply chain to assess cybersecurity.

- **Proactively Monitor the Cybersecurity Posture of the Supply Chain**

  In addition to conducting questionnaire surveys, enterprises should monitor supply chain cybersecurity risks in real-time and can do so with a dedicated third-party security rating tool. The security rating tools can leverage big data from the network and mathematical models to transform supply chain threat intelligence into quantitative cyber risk indicators, such as social information exposure, darknet discussion, DNS health level, IP reputation, credential leakage, system patching, network security, endpoint security and so on.

2. Apply Security Controls to Production Environment

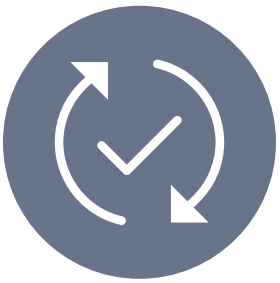
Asset hardening is a crucial step in eliminating attack methods and they include measures such as hardening network services and patching system vulnerabilities, as well as shutting down non-essential services such as applications, user permissions, user accounts, network services, network ports, and other unnecessary system functions. This approach extends the life of assets and protects aging assets, thereby minimizing opportunities for attackers to gain access to mission-critical computers and preventing malicious programs from running.

To deploy endpoint protection software on production line equipment, organizations can leverage advanced malicious program detection functions in our endpoint solution. In addition to detecting specific threats, implementing our application lockdown and behavior monitoring tools can prevent the execution of script files and unauthorized system changes. This is important to minimize disruption to production.

Implementing least-privilege control for production line equipment involves intelligently identifying key task processes, giving production-related applications the priority level required for their work, and performing detection of abnormal operational behavior. This can be achieved through learning, detection, and authorization of day-to-day operational actions, as well as monitoring vulnerable legitimate processes under least-privilege control to ensure quick operations and resource availability for essential tasks.

To disable redundant or unauthorized services and software, organizations can use application trust lists to lock down applications, configurations, data, and USB ports on assets. This helps prevent unauthorized application execution and ensures that only trusted users and applications can change configurations or data.

Plant managers must also be prepared to counter threats spread over the Internet by dividing an organization's OT network into easily defended areas. This can be achieved by defining executable instructions based on trusted industrial control communication protocols or determining which assets can communicate with each other based on specific IP policies. This allows factory networks to tighten network access controls, use better packet analysis, and make it more difficult for hackers to gather information or move across factory networks. This way, plant managers can achieve dynamic network isolation through next-generation IPS and firewall devices.



3. Provide Safe and Secure Asset Updates

- **Suppliers must continually patch management**

  Based on the critical vulnerability analysis, the supplier should establish a scope for vulnerabilities and then deploy, verify, and validate mitigating measures such as security upgrades and corrective configuration recommendations for that vulnerability. This should be used to provide customers with the supplier's patch management policy, which should be continually evolving.

- **Maintain a list of organization-approved commercial software components and component versions**

  To mitigate the likelihood of enterprises using software with high-risk vulnerabilities, enterprises should maintain a list of organization-approved commercial software components and component versions with their provenance data. They should assess the EOL status and deploy virtual patching as necessary. For instance, Windows XP and Windows 7 are examples of end-of-support operating systems. When Microsoft stopped issuing updates and patches, these OSes became more vulnerable to security threats. Thus, vendors should avoid developing the product with end-of-support OSes like Windows XP and Windows 7.

- **Verify software components and versions after any maintenance updates**

  From the moment an asset is put into its intended production use, it begins to age and depreciate, and regular maintenance begins. This entails not only repairs but also ongoing software configuration changes, system upgrades, and security updates to keep assets in sync with the changing factory field. Sometimes this is also necessary in order to maintain compliance with company security policies.

4. Detect & Respond to Security Incidents

An automotive manufacturing line may require many machines and systems to be connected to the network, providing attackers with additional initial access techniques such as Internet Accessible Devices or wireless intrusions. At this time, the factory security team needs a clearly visible platform to manage the cybersecurity of many devices in real-time, so that when an attack occurs, managers can discover and deal with it promptly.

The visualization of cybersecurity can provide cybersecurity managers of factories with a comprehensive overview of network communication protocol monitoring, linking together global threat intelligence, abnormal behavior management, and asset life cycle management. This way, the platform can automatically generate alarms based on abnormalities or block threat behaviors, enabling cybersecurity teams to directly monitor their enterprise industrial control systems, ensuring the protection of the network and connected devices.

The success of incident response depends on tracking, compiling, and documenting system security incidents, including maintaining records about each incident; these records can include audit monitoring, network monitoring, physical access monitoring, user and administrator reporting, and reported supply chain incidents:

- **Endpoints detect and respond:** Stellar allows management from a single pane of glass with support for Syslog forwarding, indicators of compromise (IoC) integration, and centralized monitoring.
- **Networks detect and respond:** Our network defense platform gives comprehensive visibility of the connected, air-gapped, and standalone OT environment by using our Edge series products. Our network defense platform is a centralized management platform for multiple sites for each deployed Edge series product.
- **Assets inventory visibility:** The TMPS3 collected asset information can be converted to the CSV format through the centralized management program as an asset inventory or sent to a SIEM or log server for further asset management. This would allow operators to maintain OT asset inventory and identify impact levels, known vulnerabilities, and cyber risks.

5. Threat Analysis and Risk Assessment

Threat Analysis and Risk Assessment (TARA) is a threat modeling and risk assessment method provided by ISO21434, which is an important part of the standard. This method is similar to NIST SP-800-30 and ISO IEC 31010 and can be used to assess the feasibility or likelihood of an attack, as well as the related impact, to determine the severity level of risk.

The TARA approach begins with asset identification, where analysts need to determine the security attributes of each asset and identify damage scenarios and their impact. Assets are classified by standard Confidentiality, Integrity, and Availability (C, I, A) levels. Impact ranges from negligible to severe and fall into four categories: Security, Financial, Operations, and Privacy (S, F, O, P). It is important to consider that all these consequences should be calculated from the perspective of road users, rather than companies.[15]

Another angle of analysis is from the perspective of threats. Analysts need to determine the time required for each attack scenario to attack the vulnerability, the ability of the attacker, the knowledge acquisition of the attacked component, the access conditions for executing the attack, and the attacker's access to chances of equipment weakness, etc. Once the impact and attack feasibility are combined and calculated, the response strategy that the organization should adopt can be determined.

Annex 5 of R155 is an important part of the regulation containing the minimum set of threats and corresponding mitigations that must be considered for type approval. It is split into three parts:

- Part A contains vulnerability or attack method related to threats
- Part B contains mitigations to the threats intended for vehicles, including vehicle communication channels, update processes, unintended human actions, external connectivity, potential targets/ motivations, potential vulnerabilities, data losses/breaches, and physical manipulation
- Part C contains mitigations to the threats outside of vehicles including backend servers, unintended human actions, and physical loss of data

[15] *Jacob Wilson, "Automotive threat analysis and risk assessment method", Synopsys, November 2020.*

In response to ever-evolving cyber threats, the Auto-ISAC, located in the United States, has been focused on sharing and analyzing intelligence on emerging cybersecurity risks in vehicles since 2018. It aims to enhance vehicle cybersecurity capabilities in the global automotive industry by working together with other organizations. On October 11, 2022, European automotive organizations CLEPA and ACEA established the ISAC for European Automotives (Auto ISAC) to foster collaboration among automotive stakeholders and aid in the identification, detection, response, and recovery from cyber threats, vulnerabilities, and incidents in the automotive supply chain.[16]

As part of threat identification, we continue to monitor vulnerabilities and threats. In addition to assisting the industry in monitoring the latest threats and malicious programs with our IoT/ICS Threat Atlas platform, we also conduct exclusive analysis and research on ICS/OT vulnerabilities. This enables organizations to detect new vulnerabilities, and effectively manage large amounts of information through automation and a unified console. This helps organizations adopt an automated approach to face evolving threats to boost vulnerability management, threat awareness, and ICS/OT cyber threat intelligence.

[16] *CLEPA, "Automotive Information Sharing & Intelligence Centre on Cybersecurity to kick off activities", CLEPA, September 2022.*

Conclusion

Developing and implementing a vehicle cybersecurity management system for the development, production, and maintenance of vehicles is a crucial aspect of the global automotive industry. To meet the cybersecurity requirements of regulations and standards, organizations should use an asset risk centric approach as their key ICS/OT strategy. This includes ensuring integrity and security of the software on the system, providing lifetime protection for endpoints even when updates are not possible, reducing the risk of compromise of unpatched systems, and preventing unauthorized access to production systems through alternative secure software update methods.

However, as production infrastructure and IT networks become more interconnected, network defense is crucial in reducing the spread of threats. Enterprises must be prepared to implement network isolation policies and controls in the event of malware attacks. Continuous monitoring of production systems can prevent threats from spreading from ICS/OT systems to vehicle systems and having up-to-date threat and vulnerability intelligence can help product threat response teams respond to potential risks in a timely manner.

We work with partners in the automotive industry to provide comprehensive solutions from OT/ICS endpoints to the network, and a unified cybersecurity platform for OT visibility. At the same time, we are also actively assisting the automotive supply chain to ensure comprehensive management, automation, continuous monitoring, and deep data correlation of the entire supply chain to limit the opportunity for adversaries to disrupt the supply chain.

txone.com