C/Ↄ CYBELLUM

Intro to

Automotive Cybersecurity Regulations

ISO SAE INTERNATIONAL enisa

As vehicles have come to rely heavily on software and an increasingly complex software supply chain, the cyber threat landscape continues to evolve, making security and safety standards more critical than ever.

Industry-wide recognition of automotive cybersecurity risks has pushed regulators and industry leaders to double-down on regulation. The recent adoption of UNECE WP.29 R155, and the ISO/SAE 21434 standard put the responsibility over cybersecurity squarely on the manufacturer's shoulders, requiring them to manage the risks associated with suppliers, service providers, and other organizations.

In order to help automotive product security pros navigate the different regulatory requirements and standards meant to help the automotive industry ensure vehicles
are secure throughout development, all the way to post production, we've put together this overview of today's top automotive cybersecurity standards and regulations.

The evolution of automotive regulation

Early in the 1980's US government regulatory bodies saw the benefit of General Motors' On-Board Diagnostics port (ODB) – which provided direct access to engine performance and other data monitored and collected by cars, and quickly moved to standardize it across manufacturers and mandate its adoption.

The expansion of the OBD port gave birth to protocols like ISO 9141, and later, SAE J1979/ISO 15031-5 which dictate the requirements for interchange of digital information between on-board emissions-related Electronic Control Units (ECUs) and external test systems.

The standardized SAE OBD II made it easy for technicians to provide effective service for a wide range of vehicles quickly and accurately. It also provided accurate performance data that enabled manufacturers and automotive suppliers to improve their products while monitoring compliance with emissions standards.

Vehicles' expanding attack surface

According to McKinsey, late-model cars run 100 million lines of code on 150 or more ECUs. By 2030, the amount of software will reach more than 300 million lines. A late-model car can generate 25 gigabytes of data per hour and 4,000 gigabytes per day. That data trove could be worth as much as $750 billion by 2030.

A typical car can utilize the services of more than seven individual networks running a wide variety of communication and control protocols from traditional CAN to SAE J1850 to Media-Oriented Systems Transport (MOST). Add a smartphone and Bluetooth, WiFi, and additional communication protocols also enter the vehicle environment. Soon, vehicles will be talking to one another via Vehicle-to-Vehicle protocol (V2V) and with external objects like street signs via Vehicle to Everything (V2X) communications. This year, 237 million connected cars cruise the roads in the United States, EU, China, and Japan. That number will rise to over 800 million by 2035.

The growing treasury of apps and data, coupled with non-stop connectivity create a very large attack surface and render each car a highly attractive target for hackers.

International cybersecurity regulations and standards

Relatively new to the world of cybersecurity, automobile manufacturers have been dealing with cybersecurity issues individually. But with the escalating frequency of cyberattacks on cars – increasing of 225 percent from 2018 to 2021 – manufacturers need to combine efforts and to seek protective regulations, standards, and guidelines that will cover the entire industry.

International bodies have been quick to fill the void. They are working feverishly to ensure that cybersecurity becomes the focus of manufacturers across every level of the automotive supply chain.

Early regulatory and standards bodies were national (US and Japan) and regional (EU), but momentum has been shifting toward international bodies. Below, we survey these bodies and their body of work.

Note: A "regulation" is legally binding within all the countries that sign up to the regulation (aka "contracting parties"). "Standards" and "Guidelines" are not legally binding but, ideally, become common practice in the industry.

ISO 26262 standard - road vehicles - functional safety

First published in 2011 and somewhat unrelated to today's cyber reality, ISO 26262 is limited to safety-related systems that include one or more electrical or electronic (E/E) systems installed in passenger cars with a maximum gross vehicle mass of up to 3500 kg.

The safety standard addresses hazards resulting from malfunctions of E/E safety-related systems, but does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, etc., unless directly caused by malfunctioning behavior of E/E safety-related systems.

Some of the original goals and definitions of ISO 26262 serve as a basis for later regulations. For example, 26262 defines a complete automotive safety lifecycle that includes management, development, production, operation, service, decommissioning. It also covers functional safety aspects of the entire development process, including activities such as requirements specification, design, implementation, integration, verification, validation, and configuration.

ISO/SAE 21434 standard - road vehicles - cybersecurity engineering

Published in 2020, ISO SAE 21434 takes the structure of ISO 26262 – that addresses the entire lifecycle of road vehicles – but focuses on the cybersecurity management and risk assessment of the modern vehicle. Unlike 26262's limitation to E/E systems, 21434's scope includes all electronic systems, components, and software in the vehicle, plus all external connectivity.

The standard holds automotive manufacturers and suppliers responsible for demonstrating due diligence in the implementation of cybersecurity and for applying cybersecurity management throughout the supply chain to support it. It defines minimum requirements for processes and activities to enable cyber control and promotes cooperation between all parties involved in the value chain of automotive industries.

To address this, ENISA released 'How to Secure the Connected & Automated Mobility (CAM) Ecosystem'. ENISA states "Today, connected vehicles, environments and infrastructures need to be designed with new capabilities and features. These capabilities and features should aim to provide:

- Increased safety
- Better vehicle performance
- Competitive digital products and services
- Improved comfort
- Environmental friendliness
- User-friendly systems and equipment convenient for its customers

Mistra C:2012 and Cert C guidelines

The C programming language is commonly used in automotive software. The MISRA C (2012) and CERT C guidelines (2011) are recommended within ISO/SAE 21434 for any projects using C.

The purpose of these guidelines is to prevent the use of C functionality that may cause critical or unspecified behavior. For example, strong typing ensures that there is an understanding of the language data types and thus prevents certain classes of programming errors. Defensive implementation techniques that allow the software to continue to function even under unforeseen circumstances are also part of the guidelines.

CERT C is a language security standard designed to identify vulnerabilities that are particular to cybersecurity. MISRA C:2012 1 defines a language subset that is applicable to both safety and security.

United nations regulations

The United Nations Economic Commission on Europe (UNECE) has become a major regulatory player. UNECE's World Forum for Harmonization of Vehicle Regulations adopted UN regulations on cybersecurity and software updates for connected vehicles.

54 signatory countries – which include the EU, South Korea, Japan, Turkey, and Russia – are now subject to the UNECE Working Party 29 (WP.29) regulations.

Formally known as WP.29 Cybersecurity and Cybersecurity Management Systems (CSMS), the new body of international regulations deals with four major areas:

- Managing vehicle cyber risks
- Securing vehicles by design to mitigate risks along the value chain
- Detecting and responding to security incidents across vehicle fleet
- Providing safe and secure software updates including over-the-air (OTA) and ensuring vehicle safety is not compromised

WP.29 puts the responsibility for cybersecurity certification on the manufacturer. It demands the incorporation of best practices in the design of vehicles and holds manufacturers responsible for the cybersecurity of their vehicles. It also requires ongoing cybersecurity for vehicles throughout all stages of the vehicle's lifecycle, including years of driving on the road.

WP.29 describes the types of cyberthreats which can be related to:

- Back-end servers
- Vehicle communication channels
- Vehicle update procedures
- Unintended human actions
- A vehicle's external connectivity and connections
- A vehicle's data and/or code
- Other vulnerabilities such as: compromised or insufficiently applied cryptographic tech, compromised parts or supplies, vulnerable software or hardware, vulnerable network design, unintended data transfers, and the physical manipulation of systems

Note: WP.29 does not apply to North American automakers who are not signatories as of this moment.

Relationship between WP.29 and ISO/SAE 21434

WP.29 and ISO/SAE 21434 are complementary. While WP.29 generally states what must be done to achieve compliance, ISO/SAE 21434 gives us the how. Here are some examples:

- CSMS: A cybersecurity management system (CSMS) is the first step toward compliance with WP.29. Manufacturers must implement a CSMS for monitoring security incidents, threats, and vulnerabilities. However, WP.29 does not describe how to set up a CSMS, but ISO 21434 explains implementation of cybersecurity policies, responsibility assignment, and management system maintenance to support cybersecurity activities.
- Risk management: WP.29 requires risk assessment and management across the entire lifecycle of a vehicle, but it does not explain how to do it. ISO/SAE 21434 provides details concerning risk assessment, risk analysis, and organization cybersecurity management.
- Securing the supply chain: WP.29 clearly states that manufacturers are responsible for cybersecurity management in the supply chain, however, it does not indicate how to verify components. It specifies some of the strategies that the OEMs can apply to manage the supplier-related risk, such as evaluating the supplier’s capability by considering supplier cybersecurity activity records and making a contractual agreement with suppliers to maintain and conduct cybersecurity activities throughout the vehicle lifecycle of the vehicles.

ENISA

The 2019 release of the European Agency for Cybersecurity’s (ENISA) ‘Good Practices for Security of Smart Cars’ defines the best practices to consider when developing and deploying connected vehicles.Since its publication there has only been a rise in cyber attacks targeting modern vehicles. While many vehicle hacks involve theft of property, increased connectivity threatens both brand confidence and consumer safety, since a hack into one ECU gives access to all other software components as well.

Compliance for Better Automotive Cybersecurity

With international bodies coming into the cybersecurity space, delivering regulations, standards, and guidelines, it looks like the public will be better cyber-protected in the vehicles they use. Over time, cybersecurity in vehicles will evolve to contend with the dynamic nature of cyber threats.

About us

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Top Automotive manufacturers such as Jaguar Land Rover, Nissan, Audi, and Faurecia use Cybellum's Product Security Platform and services to manage cybersecurity risk and compliance across business units and lifecycle stages. From SBOM to Vulnerability Management, CSMS Management, and WP. 29 Compliance Validation, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

Experience what product security can be. Book a demo.