CYBELLUM

ISO/SAE 21434 FAQ

Frequently Asked Questions About the ISO/SAE 21434 Standard for Automotive Cybersecurity Engineering

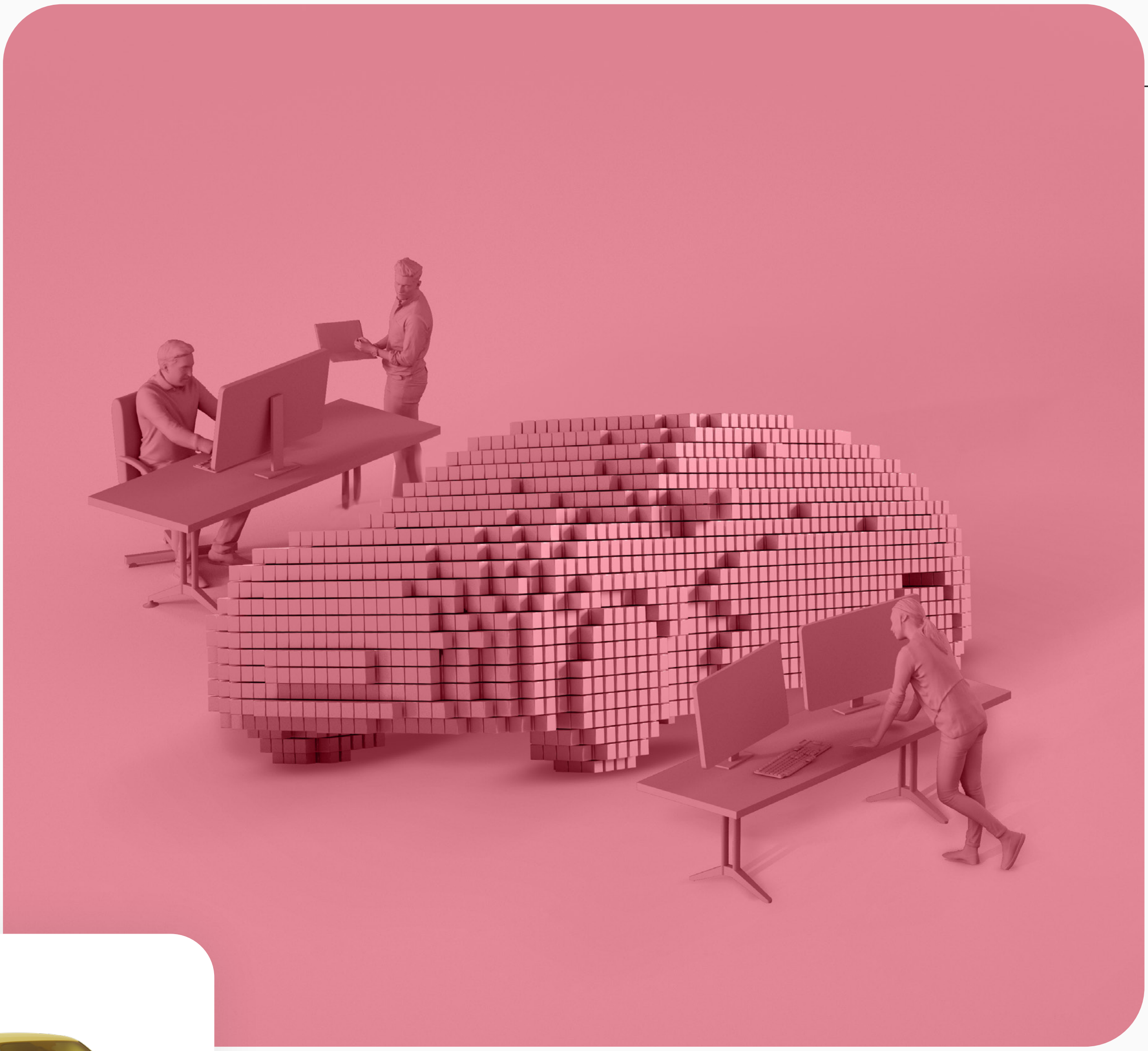

Table of Contents

Q1: What is ISO/SAE 21434 all about?

The standard is designed to help the automotive industry define a structured process to ensure cybersecurity is incorporated into the design of road vehicles, including systems, components software and connections to any external device or network.

The standard specifies the cybersecurity risk management requirements for the design, development, production, operation, maintenance, and decommissioning of road vehicle electrical and electronic (E/E) systems.

Q2: Who was involved in creating the standard?

The ISO/SAE 21434 Standard is a result of the efforts of a joint working group of more than 100 experts from 14 nations and 82 industry organizations across public, private, and government sectors, representing the SAE Vehicle Cybersecurity Systems Engineering Committee and the ISO Technical Committee 22, Sub-committee 32, Working Group 11.

Using four main working groups focusing on risk management; product development; production, operation, maintenance, and decommissioning and process overview, the ISO/SAE 21434 draft was born.

Q3: When will the finalized standard be released?

The standard was released as a draft on 12th February 2020, and its development and final release is expected at the beginning of 2021.

Q4: Where can I get a copy of the standard?

You can find it on the ISO or SAE websites.

Q5: What is the relationship of this standard to SAE J3061 and ISO 26262?

SAE International and ISO had previously worked on automotive safety and security related standards on their own:

- ISO 26262 had set functional safety standards and the new cybersecurity standard echoes its structure by covering the complete vehicle engineering cycle (from design through development to validation and maintenance).
- SAE J3061 was developed by SAE in 2016 to set the foundation for cybersecurity standards. The new ISO/SAE 21434 standard can be viewed as a much more extensive and up-to-date evolution of that standard.

Q6: How is the ISO/SAE 21434 standard related to the UNECE WP.29 regulation?

Although WP.29 does not mention the ISO/SAE 21434 standard, it is understood that if an OEM and its supply chain can demonstrate compliance against this standard framework, then that compliance can be used to demonstrate compliance with the WP.29 regulation.

As an international automotive cybersecurity framework with explicit controls, ISO/SAE 21434 will likely be the framework most OEMs and Tier-1 suppliers align or certify to.

A mapping of the WP.29 CSMS requirements to the ISO/SAE 21434 standard is available here.

Q7: How is the standard structured?

The first four clauses of the standard highlight the scope (Clause 1), references (Clause 2), definitions (Clause 3), and general considerations (Clause 4) of the standard. The bulk of the standard requirements are covered in Clauses 5-14, where:

- Clauses 5 and 6 focus on the management of cybersecurity and include the implementation of organizational cybersecurity policies, rules, and processes for overall cybersecurity management and for project-dependent cybersecurity management (similar and relevant to the WP.29 CSMS regulation).
- Clause 7, titled "Continuous Cybersecurity Activities" defines activities that provide information for ongoing risk assessments and vulnerability management of vehicles.
- Clause 8 titled "Risk Assessment Methods" defines methods to determine the extent of the cybersecurity risk.
- Clauses 9-14 cover the requirements throughout the full lifecycle of a vehicle, with the "Concept Phase" (Clause 9) "Product Development Phases" (Clauses 10 and 11), and the "Post-Development Phases" (Clauses 12-14).
- In Clause 15, titled "Distributed Activities", the standard details the requirements for supplier management, and defines the interactions, dependencies, and responsibilities between customers (OEMs) and suppliers (Tier 1 and 2s) for cybersecurity activities.

The standard also includes 10 Annexes (A-J) which are all informative and used to provide additional information to the main body of the document for several reasons, for example:

- When the information or table is very long;
- To set apart special types of information;
- To present information regarding a particular application of the document.

Q8: Which types of vehicle components does the standard apply to?

According to Clause 4 titled "General Considerations", the standard is limited to cybersecurity relevant items and components inside or on the vehicle perimeter including aftermarket and service parts.

Systems outside the vehicle perimeter can be considered for cybersecurity purposes but are not in the scope of the standard. The following are examples of what can be considered for the vehicle level as a whole:

- The vehicle E/E architecture
- The cybersecurity cases of the cybersecurity relevant items and components

Q9: What’s within the scope of the standard?

ISO/SAE 21434, in draft form as of May 2020, is a baseline for vehicle manufacturers and suppliers to ensure that cybersecurity risks are managed efficiently and effectively. The standard was specifically developed to ensure the safety and security of the ultimate road-user/driver, and as such, the determinant levels of risk and corresponding cybersecurity measures are set based on the final impact on the driver.

It provides a standardized cybersecurity framework, establishes cybersecurity as an integral element of engineering throughout the lifecycle of a vehicle from the conceptual phase all the way through decommissioning, ensures that cybersecurity is considered in post-production processes (software updates, service and maintenance, incident response, etc.), and calls for effective methods of lessons learned, training, and communication-related to automotive cybersecurity.

More specifically, the scope of the standard includes:

1. Specific requirements for cybersecurity risk management
2. A cybersecurity process framework
2. Common language to help manufacturers and organizations communicate their cybersecurity risk

Q10: What’s out-of-scope for the standard?

ISO/SAE 21434 does not dictate specific cybersecurity technologies or solutions, mandates around remediation methods, or cybersecurity requirements for telecommunications systems, connected backend-servers, EV chargers, or autonomous vehicles.

Instead, the standard heavily emphasizes risk identification methods and established processes to address the cyber-risks. Accordingly, if a compromised backend-server, charger, or autonomous vehicle leads to a direct risk to the road-user, it must be monitored, controlled, and mitigated.

This provides OEMs and their suppliers flexibility in implementing the technologies and solutions needed to adhere to the standard.

Q11: How is risk assessment performed according to the standard?

The standard requires OEMs and their suppliers to analyze new and emerging threats and risks throughout a vehicle's lifecycle to determine the extent to which a road user/driver could be impacted by a threat scenario. This general process of threat analysis and risk assessment is called "TARA". The standard's methods for effective risk assessment (TARA) include:

- Asset Identification - Know what could be harmed.
- Threat Scenario Identification - Know how the assets could be harmed.
- Threat Impact Analysis and Rating - Estimate the damage the threat could cause.
- Attack Path Analysis - which actions (in isolation or linked) could lead to a threat.
- Attack Feasibility Analysis and Rating - what's the likelihood of the damage/harm occurring.
- Risk Determination - how high is the risk caused by the threat.
- Risk Treatment Decision: how would you treat the specific risk.

ISO-SAE explains that the methods/"modules" listed are not connected to a particular phase of the vehicle's lifecycle and can be used in the order most appropriate for the OEM.

Q12: What does the standard require from Tier-1 & Tier-2 suppliers?

Clause 15 of the standard focuses on “distributed cybersecurity activities” and discusses the cybersecurity relationships between OEMs and Tier 1 and 2 suppliers.

An OEM is responsible for ensuring that their suppliers implement methods to ensure their products and components are cybersecure. There are three main strategies to develop a successful supplier-OEM relationship:

A. Evaluate: (Clause 15.4.1) “Demonstration and Evaluation of Supplier Capability”
As part of the supplier assessment and evaluation by the OEM, the supplier should supply a “Cybersecurity Record of Capability” which includes:
   - Evidence of their capabilities regarding cybersecurity
   - Evidence of continuous cybersecurity activities
   - A summary of previous cybersecurity assessments
   - Organizational audit results
   - Evidence of an information security management system
   - Evidence of the organization’s management systems

B. Confirm: (Clause 15.4.2) “Request for Quotation”
When an OEM purchases supplies and components from Tier-1 or Tier-2 suppliers, they should include in their quote:
   - A formal request that the supplier will comply with the standard
   - A list of the expectations of the cybersecurity responsibilities to be undertaken by the supplier
   - Details of the the cybersecurity goals or the set of relevant cybersecurity requirements for the supplier

C. Align: (Clause 15.4.3) “Alignment of Responsibilities”
The OEM and supplier must agree on the division and alignment of responsibility, through a process called CIAD “cybersecurity interface agreement for development”. The CIAD division of responsibility includes agreements on:
   - OEM and suppliers’ points of contact regarding cybersecurity
   - A joint tailoring of the cybersecurity activities
   - The identification of the cybersecurity activities that are to be performed by the OEM and by the supplier

The OEM and the suppliers should build the CIAD division of cybersecurity responsibilities using the RASIC model. Mentioned in Annex C of the standard and stands for:

- R (responsible): The organization that is responsible for getting the activity done
- A (approval): The organization that has the authority to approve or deny the activity once it is complete
- S (support): The organization that will help the organization responsible for the activity;
- I (inform): The organization that is informed of the progress of the activity and any decisions being made; and
- C (consult): The organization that offers advice or guidance but does not actively work on the activity.

Q13: How can Cybellum help you with the ISO/SAE 21434 standard?

Cybellum is highly active in the area of standards, regulations and best practices, chairing the Israeli representation for the ISO/SAE 21434 standard committee, leading the taskforce responsible for the standard' Use-case Annex and involved in other standardization efforts such as the upcoming ISO/WD PAS 5112 guidelines for auditing cybersecurity engineering, IAMTS study-group on cybersecurity and more.

Our solutions enables OEMs and their suppliers to develop and maintain secure products, helping them navigate compliance with the UNECE WP.29 regulation and ISO/SAE 21434 standard. Our platform is the foundation for a CSMS covering everything from risk assessment and ongoing monitoring to documentation and readiness for auditing.

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.