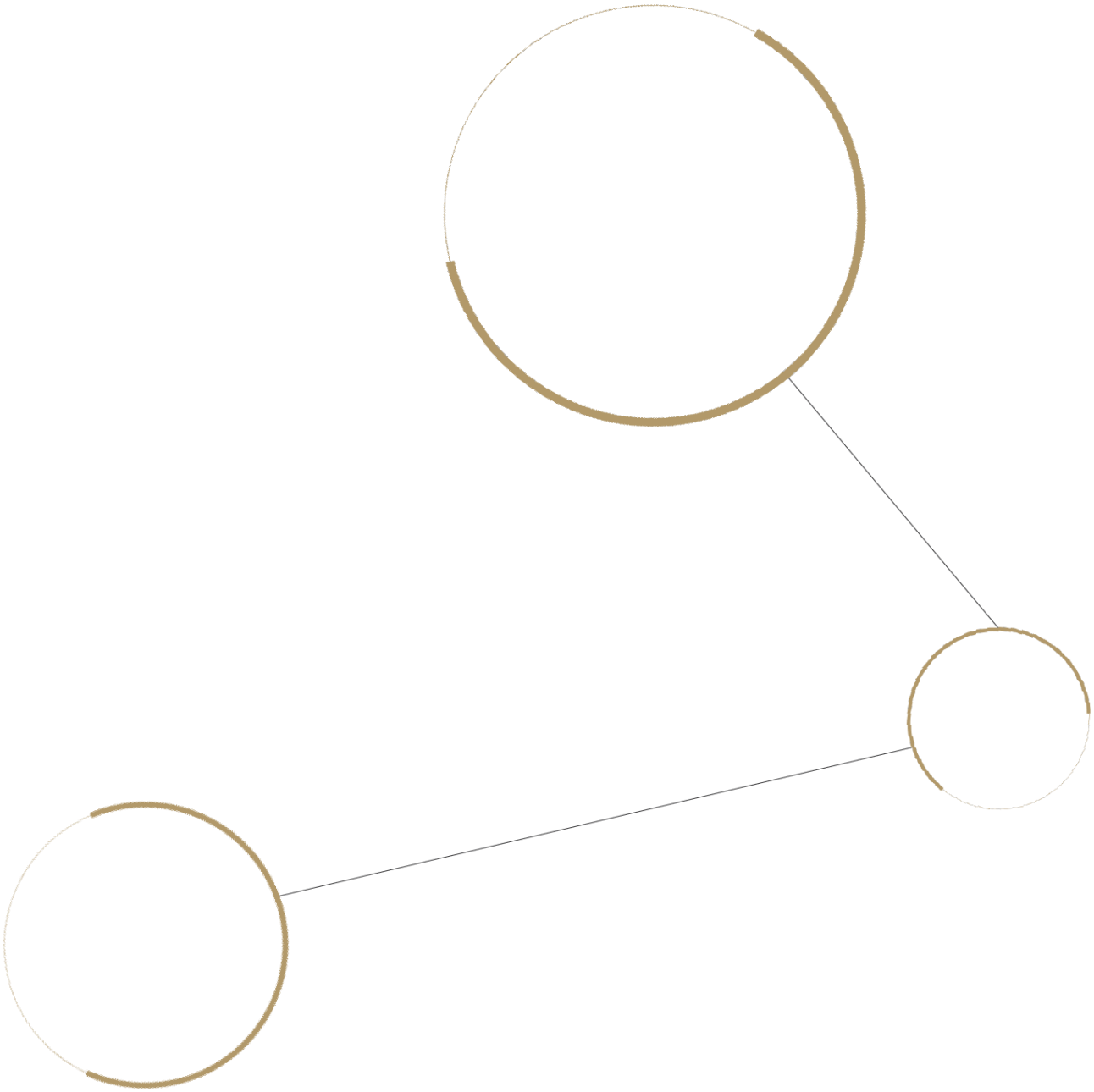
CYBELLUM

UNECE WP.29 FAQ

Frequently Asked Questions About the UNECE WP.29 GRVA Automotive Cybersecurity Regulations



Contents

Q1: What's the role of UNECE in vehicle cybersecurity? 2

Q2: What are the WP.29 GRVA regulations for CSMC and USMS? 2

Q3: What is the purpose of the WP.29 CSMS regulation? 3

Q4: Which types of vehicles does the WP.29 regulation apply to? 3

Q5: Does WP.29 affect vehicles that are already on the road? 3

Q6: Do "facelifts" of existing vehicles require new approvals? 4

Q7: When will the regulations be finalized and published? 4

Q8: Which countries are part of the UNECE and are affected by this regulation? 4

Q9: When will countries start implementing the regulations? 4

Q10: What are the implications on OEMs and their suppliers for noncompliance with the regulation? 5

Q11: What is the certification process for CSMS and Vehicle Type approval? 5

Q12: Where is the most updated text of the CSMS regulation? 6

Q13: How is the regulation document structured? 6

Q14: What are the main principles of CSMS approval? 7

Q15: What are the main principles of Vehicle Type approvals? 8

Q16: What types of cyber threats, vulnerabilities, and mitigations are covered by WP.29? 8

Q17: How is WP.29 related to the ISO/SAE 21434 standard? 9

Q18: How can Cybellum help you with the WP.29 regulation? 9

Q1: What's the role of UNECE in vehicle cybersecurity?

The United Nations Economic Commission for Europe is under the jurisdiction of the United Nations Economic and Social Council. It was established to promote economic cooperation and integration among its 56 member states. Within the UNECE lies the Inland Transport Committee (ITC), the UN platform to help efficiently address the global and regional needs for inland transport. One of the subsidiary bodies of the ITC is the WP.29, which was established on June 6, 1952, as the Working Party on the Construction of Vehicles. It renamed in 2000 as the World Forum for Harmonization of Vehicle Regulations (WP.29).

The objective of the WP.29 is to initiate and pursue actions aimed at the worldwide harmonization or development of technical regulations for vehicles and to develop regulations that are intended to improve vehicle safety, protect the environment, promote energy efficiency, and increase anti-theft performance.

In response to the growing prevalence of connected vehicles, the ITC recognized the importance of WP.29 activities related to automated, autonomous and connected vehicles at a session in February 2018. They requested that the WP.29 consider establishing a dedicated subsidiary working party specifically focused on connected vehicles. In June 2018, following this request, WP.29 decided to convert the Working Party on Brakes and Running Gear (GRRF) into the new Working Party on Automated/Autonomous and Connected Vehicles (GRVA).

Additional background information can be found here - http://www.unece.org/trans/main/wp29/faq.html

Q2: What are the WP.29 GRVA regulations for CSMC and USMS?

As of June 25, 2020, two new UNECE regulations had been adopted. The first regulation focuses on uniform provisions on the approval of cybersecurity and cybersecurity management systems (CSMS) in vehicles. The second regulation is on vehicle software update processes and software update management systems (SUMS), commonly known as "Over-the-Air" (OTA) updates.

The CSMS regulation is the focus of subsequent FAQs.

Q3: What is the purpose of the WP.29 CSMS regulation?

WP.29 CSMS is intended to minimize vehicle cyber risk. It, therefore, provides a comprehensive approach to automotive cybersecurity, based on the following key principles:

- An organizational framework and minimal cybersecurity requirements that impact all automotive players along the value chain.
- The responsibility for cybersecurity certification is on the OEM.
- Best practices must be incorporated into the design of vehicles.
- OEMs must provide reasoned arguments as to the cybersecurity of their vehicles.
- The cybersecurity of vehicles must be maintained continuously throughout all stages of the vehicle's lifecycle including post-production

Additionally, the regulation offers a non-conclusive list of cyber threats and corresponding mitigations.

It is highly focused on processes and governance, however, it doesn't include an explicit definition of how the regulatory requirements can be met nor does it mandate detailed technical measures.

This was done intentionally, to provide OEMs flexibility to decide how to ensure the cybersecurity of their vehicles. It is expected that, through the use of relevant standards (such as the ISO/SAE 21434) and by implementing appropriate measures, OEMs should be able to demonstrate how the principles of the regulation are met.

Q4: Which types of vehicles does the WP.29 regulation apply to?

The regulation applies to vehicles within the M and N categories (vehicles with at least 4 wheels), the O category (if fitted with at least one electronic control unit), and vehicles in categories L6 and L7 that are equipped with autonomous driving functions beyond level 3.

Q5: Does WP.29 affect vehicles that are already on the road?

The UN regulation on cybersecurity does not affect type approvals granted prior to the regulation's entry into force in a given country (i.e. not when it comes into force as a United Nations regulation). It also does not affect vehicles already on the road.

Q6: Do "facelifts" of existing vehicles require new approvals?

If a vehicle "facelift" includes the changing or replacement of a system(s) that could potentially affect the cybersecurity of the vehicle (e.g. infotainment, telematics), the vehicle manufacturer may be required to obtain a new whole vehicle type approval (WVTA) and /or an "extension" of the current WVTA held for the vehicle.

Q7: When will the regulations be finalized and published?

It is expected that the regulations will be finalized and published in early 2021. It will apply to the 54 member states (which excludes the US and Canada).

Q8: Which countries are part of the UNECE and are affected by this regulation?

Albania, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czechia, Denmark, Egypt, Estonia, European Union, Finland, France, Georgia, Germany, Greece, Hungary, Italy, Japan, Kazakhstan, Latvia, Lithuania, Luxembourg, Malaysia, Montenegro, Netherlands, New Zealand, Nigeria, North Macedonia, Norway, Pakistan, Poland, Portugal, Republic of Korea, Republic of Moldova, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Thailand, Tunisia, Turkey, Ukraine, United Kingdom of Great Britain and Northern Ireland.

Q9: When will countries start implementing the regulations?

According to a UNECE press release of June 25, 2020, Japan has indicated that it plans to apply these regulations upon entry into force (estimated in late 2021 or beginning 2022). The Republic of Korea has adopted a stepwise approach, introducing the provisions of the regulation on Cybersecurity in a national guideline in the first half of 2020, and proceeding with the implementation of the regulation in a second step. In the European Union, the new regulation on cybersecurity will be mandatory for all new vehicle types from July 2022 and will become mandatory for all new vehicles produced from July 2024.

Q10: What are the implications on OEMs and their suppliers for noncompliance with the regulation?

The regulation clearly indicates that the responsibility to prove that effective cybersecurity methods and processes were used, lies with the OEM; the OEM is responsible for ensuring cybersecurity processes are in place throughout the supply chain.

OEMs that do not comply with the regulations (once adopted by member countries) will not get type approval. They will face trade barriers and other complications that will impact the bottom line. Vehicle manufacturers that do acquire the necessary certification will get type approval, be able to sell their vehicles in the countries that adopted the regulation and can brand their companies as secure so that they can build mutual trust with their customers.

While Tier-1 and Tier-2 suppliers are not required to have their own compliance certificate, those that do not provide evidence to the OEM that they implemented all the necessary cybersecurity measures (thus not allowing the OEM to be certified) will most likely be cut off by the OEM and lose business.

In that context, it's important to remember that the regulation clearly demands cybersecurity measures throughout the lifecycle of the vehicle, which includes the development, production, and post-production phases. While the OEM can ensure cybersecurity measures are in place during the production phase, it must rely on its suppliers to provide cybersecurity measures during the development phase (of all the components, chips, parts, etc.) of the vehicle as well as the post-production phase e.g. for services such as OTA updates, smart services related to the connected car (remote unlock door or engine start), access control for software, and more.

Q11: What is the certification process for CSMS and Vehicle Type approval?

- The OEM implements an effective and regulatory compliant CSMS.
- The OEM submits an application for a Certificate of Compliance for CSMS to an Approval Authority or its Technical Service.
- The CSMS is then assessed by the Approval Authority or Technical Service
- The OEM signs a declaration of compliance.
- The OEM is issued a CSMS certificate of compliance valid for 3 years (after which a renewal is needed).
- The OEM develops vehicle architecture with CSMS involved.
- The individual vehicle type is assessed by the Approval Authority or Technical Service.
- Vehicle Type Certification is issued.

Q12: Where is the most updated text of the CSMS regulation?

It can be found here.

Q13: How is the regulation document structured?

The first six sections of the WP.29 regulation highlight the scope of the regulation (Section 1), defines the terms used in the regulation (Section 2), and elaborates on the application, markings, processes, and certifications related to formal regulatory approval (Sections 3-6). The regulation also includes details on how to approach vehicle modifications (Section 8), demands regarding production conformity and updates regarding continuity (Sections 9-11), and the method by which OEMs need to communicate their approval process with the UN Secretariat (Section 12).

The primary requirements of the regulation are largely discussed in Section 7, titled "Specifications" covering the Cyber Security Management System and Vehicle Type Approval:

- Cyber Security Management Systems (CSMS) include cybersecurity requirements for an OEM's organizational structure, processes, and governance. CSMS certification demands evidence from the OEM, including test reports and threat modeling, to prove that due diligence was performed in ensuring cybersecurity throughout the lifecycle of the vehicle.
- Vehicle Type approval involves testing the vehicle and certifying that the design of vehicle architecture, the risk assessment procedures, and the implementation of cybersecurity controls were executed correctly. In this approval process, an authority tests an individual type of vehicle to check if the cybersecurity measures were actually implemented.

In accordance with its aim to be practical and non-theoretical, in Annex 5, the regulation clearly stipulates that for both CSMS and Vehicle Type approvals, the OEM must take cyber threats, vulnerabilities, and related mitigations into consideration when implementing risk assessments and threat analysis. Many (but not all) of these risks and correlating mitigations are listed in three parts (A, B, and C) in Annex 5.

Q14: What are the main principles of CSMS approval?

The main principles involved in CSMS approval demand:

1. Lifecycle Implementation: Vehicle manufacturers must methodically implement cybersecurity measures at each stage of the vehicle lifecycle: development, production, and post-production phases.
2. Risk Assessment and Management: Security must be adequately considered in all OEM processes including the identification of risk (including the specific risks highlighted in Annex 5), assessment and treatment of risk, the effectiveness of cybersecurity measures, and the treatment of data gathered about cyber-attacks.
3. Cyber Threat and Attack Process: OEMs must have in place a process for effective monitoring, detection, and response to cyberattacks, cyber threats, and security vulnerabilities.
4. Timeliness: The processes used to manage cybersecurity must allow for timely response and mitigation of cyber-threats and vulnerabilities.
5. Data and Telematics Usage: Risk assessment and management must be continuously carried out to ensure that the OEM has the capacity to analyze and detect cyber threats, vulnerabilities, and cyber-attacks from vehicle data and vehicle telematics logs.
6. Supply Chain Management: The OEM must manage all the risks associated with contracted Tier 1 and Tier 2 suppliers, service providers, and/or sub-organizations.

Q15: What are the main principles of Vehicle Type approvals?

The main principles involved in Vehicle Type approval demand:

1. Application of CSMS: The OEM must prove that proper CSMS was applied to the specific vehicle type.
2. Tier 1 and 2 Supplier Management: It is the OEMs responsibility to identify and manage any risks related to its Tier 1, 2, or other suppliers.
3. TARA: An in-depth TARA (Threat Analysis and Risk Assessment) process must take place for every vehicle type, and include an assessment of the interactions the vehicle will have with external systems. Many of these threats are listed in the regulations Annex 5. Additionally, it is not enough for an OEM to assess the threat, rather it must also find appropriate and proportionate mitigations (which are also highlighted in Annex 5).
4. Threat Reporting: The OEM must provide periodic reports covering detected attacks and new threats.
5. Aftermarket Responsibility: The OEM must build measures to secure the vehicle with regards to aftermarket software, services, applications, or data.
6. Data and Telematics Usage: The OEM must have the ability to analyze the specific vehicle data related to attempted or successful cyber-attacks.

Q16: What types of cyber threats, vulnerabilities, and mitigations are covered by WP.29?

To help OEMs and their suppliers understand and assess the risks associated with connected vehicles, Annex 5 of the regulation lists 69 different attack routes due to 7 different cyber threats and vulnerabilities. To aid in the management of said risks, the regulation also offers 23 cybersecurity mitigations with the potential to secure a vehicle, its components, and back-end servers against these threats. It is important to note that while the list of threats, vulnerabilities, and mitigations is extensive, the regulation is quick to point out that it is not exhaustive.

The regulation includes detailed descriptions and examples of threats, and even goes as far as to offer specific examples of potential attack methods. The threats listed are divided into the following 7 categories: back-end servers, vehicle communication channels, vehicle update procedures, unintended human actions, external connectivity and connections, vehicle data/code, and other vulnerabilities.

Q17: How is WP.29 related to the ISO/SAE 21434 standard?

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.

Q18: How can Cybellum help you with the WP.29 regulation?

Cybellum 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.

Additionally, 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.

Done reading? Schedule a free consultation with one of our experts.