Cybersecurity regulations
Impact on OEMs and suppliers

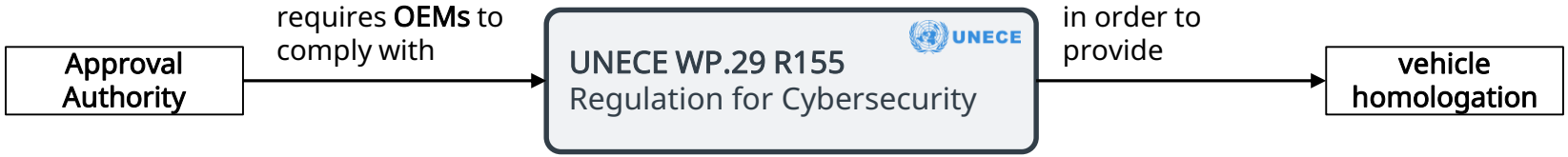
May 2021

Index

- UNECE WP.29 R155 regulation
- Impact of R155 on OEMs
- Impact of R155 on suppliers
- ISO/SAE 21434 as demonstration of cybersecurity management
- Marelli activities to achieve compliancy with cybersecurity regulations

UNECE World Forum for Harmonization of Vehicle Regulations (WP.29)

- Defines the process of **type approval** and mutual recognition of wheeled vehicles, equipment and parts
- The type approval process requires the compliance with **more than 60 vehicle functional system regulations**
- **R155 Cybersecurity is one of the system regulation to comply with**



R155 - Cybersecurity
Two levels of requirements

	Requirements
Organization	• Establish a Cybersecurity Management System (**CSMS**), which ensures security is adequately considered during development, production and post-production phases • Manage dependencies with ***suppliers*** in processes related to cybersecurity
Vehicle type	• Manage vehicle cyber risks, *including **supplier**-related risks* • Securing vehicles by design to mitigate risks along the value chain • Detecting and responding to security incidents across vehicle fleet

January 2021
- Regulations enter into force

July 2022
- Regulations mandatory for new vehicle types

July 2024
- Regulations mandatory for new vehicle produced

R155 - Cybersecurity
Two levels of certificates

	Certificates

Organization	• Certificate of Compliance for **CSMS**
	  • achieved through an assessment of the manufacturer carried out by Approval Authority
	  • valid for a maximum of three years

Vehicle type	• Type approval certificate of the Vehicle type • granted through **document checking** and **testing** activity of the vehicle carried out by Approval Authority

January 2021
- Regulations enter into force

July 2022
- Regulations mandatory for new vehicle types

July 2024
- Regulations mandatory for new vehicle produced

Certificate of Compliance for CSMS (1/3)
VDA Automotive Cybersecurity Management System Audit

- VDA volume defines the questionnaire and rating scheme which can and should be applied to the CSMS audit of OEM and supplier
- Each question is rated in levels of 0, 4, 6, 8 or 10 points
- An overall rating is calculated as $\frac{sum\ of\ all\ points\ obtained}{sum\ of\ possible\ points}$
- The audit results passed if
  - the overall rating is greater than or equal to 90
  - no question received rate below 4 points

Number of points	Risk assessment from the point of view of the process/process step	Rating the fulfilment of individual requirements
10	Process requirements and specifications are observed	Requirements fully met
8	Minor deviations in the process that do not affect the fulfilment of the following process or customer requirements	Requirements largely met[1]; minor deviations
6	The process partially does not meet the defined requirements, with impact on the following process or the customer	Requirements partially met; greater deviations
4	The process does not meet the defined requirements, with significant impact on the following process or the customer	Requirements inadequately met; major deviations
0	The process is not suitable to ensure fulfilment of the defined requirements	Requirements not met

Certificate of Compliance for CSMS (2/3)
VDA Automotive Cybersecurity Management System Audit

Example – Question about the Cybersecurity management and guidelines for auditor

Q1.1	**Is a cybersecurity policy defined for the CSMS area of application?**
Relevant minimum requirements	
The organisation defines a cybersecurity policy that includes a) acknowledgment of road vehicle cybersecurity risks; b) the executive management's commitment to manage the corresponding risks. The organisation assigns and communicates the responsibilities to achieve and maintain cybersecurity in accordance with its product portfolio for the relevant phases of the product lifecycle and grants the corresponding authorisation while providing required resources.	

Examples for Q1.1

- Organisation specific policy/handbook for cybersecurity processes and activities (or similar) including commitment from the top management for ensuring cybersecurity
- Organisation chart, roles and responsibility matrix for cybersecurity organisation
- Guidelines for the communication of cybersecurity related information for external instances and relevant stakeholders
- Internal regulations for cybersecurity processes (e.g., directives, strategies, secure development handbook, security incident management handbook)
- Regular management reviews of cybersecurity aspects

Certificate of Compliance for CSMS (3/3)

ISO/PAS 5112 — Guidelines for auditing cybersecurity engineering

- Publicly Available Specification (PAS) is under development, currently approved in the 1st CD version
- Extension of ISO 19011 Guidelines for auditing management systems for the automotive domain

- It provides guidelines on
  - the management of an audit
  - the planning and conducting of management system audits
  - the competence and evaluation of an auditor and an audit team
- It gives an *example* of a questionnaire based on ISO/SAE 21434 objectives

Type approval certificate of the vehicle type (1/2)
R155 – Annex 5

1. **Document checks**
2. **Testing**

to verify

a) exhaustive risk assessment of threats (Annex 5, Part A)

b) risk treatment through proportionate mitigations (Annex 5, Part B and C)

c) capability to detect and prevent cyber attacks, to monitor threats and vulnerabilities and to provide data forensic

	Macro category	Category	Threats	Mitigations
Annex 5	inside the vehicle	Vehicle communication channels	Part A	Part B
		Update process		
		Unintended human actions facilitating a cyber attack		
		External connectivity and connections		
		Potential targets of, or motivations for, an attack		
		Potential vulnerabilities that could be exploited if not sufficiently protected or hardened		
		Data loss / data breach from vehicle		
		Physical manipulation of systems to enable an attack		
	outside of vehicle	Back-end servers		Part C
		Unintended human actions		
		Physical loss of data loss		

Type approval certificate of the vehicle type (2/2)
Example of Threats and related mitigations – Update process

Threat ID	Threats	Mitigations ID	Mitigations
12.1	Compromise of over the air software update procedures. This includes fabricating the system update program or firmware	M16	Secure software update procedures shall be employed
12.2	Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware		
12.3	The software is manipulated before the update process (and is therefore corrupted), although the update process is intact		
12.4	Compromise of cryptographic keys of the software provider to allow invalid update	M11	Security controls shall be implemented for storing cryptographic keys
13.1	Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features	M3	Security Controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP

UNECE WP.29 R155
Impact on suppliers

- **Requirements for the CSMS**
  - OEMs shall demonstrate that the CSMS manage potential dependencies with suppliers and their processes of cybersecurity management
- **Requirements for vehicle types**
  - OEMs shall demonstrate that the supplier-related risk are identified and managed

ISO/SAE 21434
Two levels of requirements

	Requirements
Organization	• Define methods for risk assessment and treatment and for vulnerability analysis and management • Define the interactions, dependencies and responsibilities between customers and suppliers for cyber security activities
Project	• Specify cybersecurity activities and their deliverables during design, development and post-development of a product

February 2020
- Draft International Standard

May 2021
- Final Draft International Standard

End 2021
- Publication (expected)

UNECE WP.29 cybersecurity regulation
and relation with ISO/SAE 21434

Marelli activities to achieve compliancy with CS regulations
Working Group on Cybersecurity

Marelli established a Working Group on Cybersecurity

MARELLI WORKING GROUP CS

- **Teams involved**
  - Technical Compliance & Regulatory
  - ICT
  - Business Units
  - Legal
  - Quality
  - Purchasing and Sales
- **Aim**
  - define a Global Procedure for Cybersecurity Management within November 2021

Marelli activities to achieve compliancy with CS regulations
Details

Cybersecurity management

Organizational structure
- roles and responsibilities

Cybersecurity culture
- training definition and scheduling

Cybersecurity activities during RFI/RFQ/CR
- supplier and customer management

Continuous cybersecurity activities

Vulnerability management
- policy and infrastructure for vulnerability monitoring and treatment

Incident response
- policy and infrastructure for event assessment and incident management

PKI and Key management
- policy and infrastructure for key and certificate management

Project-related cybersecurity activities

Pre-development cybersecurity
- Cybersecurity Interface Agreement

Cybersecurity development process
- TARA, Vulnerability Analysis, PenTest

Post-development cybersecurity
- Production, Operation and End-of-life

Thanks!