

INLAND TRANSPORT COMMITTEE

UNECE

ITU workshop “Security of ITS and CAV”

Chongqing, China

7 September 2026

Latest regulatory updates in CAV security

François E. Guichard

UNECE

Agenda

1. Introduction
   - UNECE
   - Starting point - cyber security at WP.29
   - 3 key considerations

2. Deliverables produced by WP.29

3. Takeaways

Presentation of UNECE

UNECE is:

- a United Nations agency
- part of the UN Secretariat
- One of the five regional economic commissions of the United Nations established under UN ECOSOC
- Located in Geneva, Switzerland
- Custodian of 60 Conventions for inland **transport**
- UN ECOSOC gave a regional and an inter-regional mandate to UNECE regarding transport





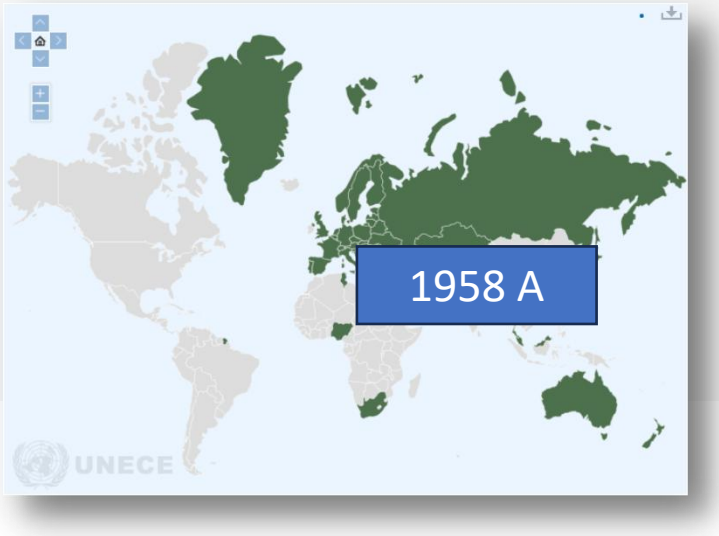
The WP.29 framework



Incl. their sub-systems and parts

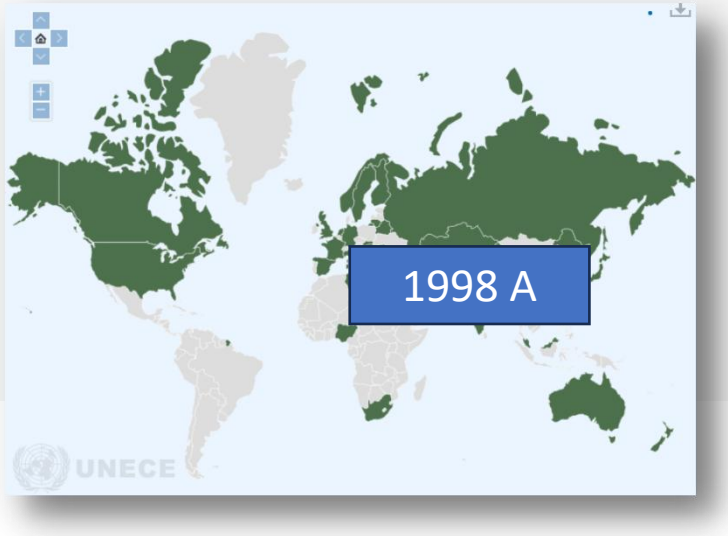
1958 Agreement:

- “UN Regulations”
- Directly applicable by the Countries and stakeholders/industry
- Mutual recognition of Type Approvals



1998 Agreement:

- “UN Global Technical Regulations”
- Requires transposition in national law
- No administrative procedures -> suitable for:
  - Self Certification
  - Type Approval



UNECE

Starting point - cyber security at UNECE

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

WP.29 was made aware of the cyber security risk back in 2015



June 2015 – hacked Jeep

Source: https://www.youtube.com/watch?v=MK0SrxBC1xs

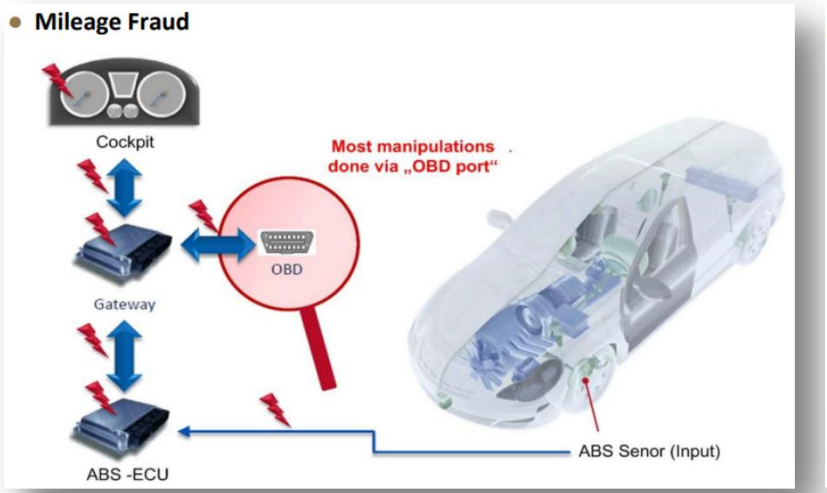


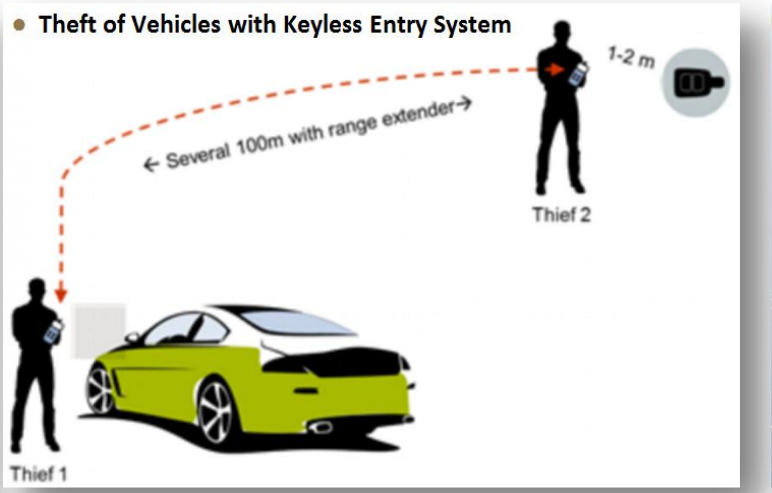
Mai 2017 - Wannacry

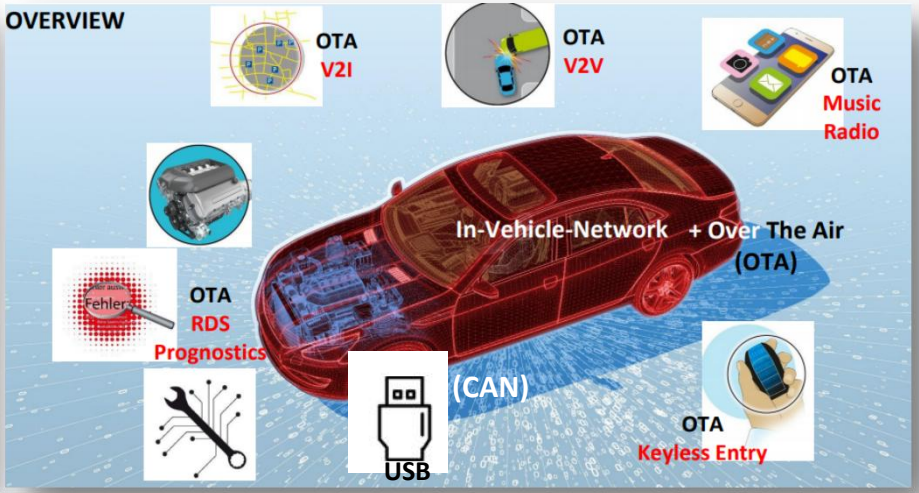
Source: screenshot

Starting point - cyber security at UNECE

-FIA presented the following cases:





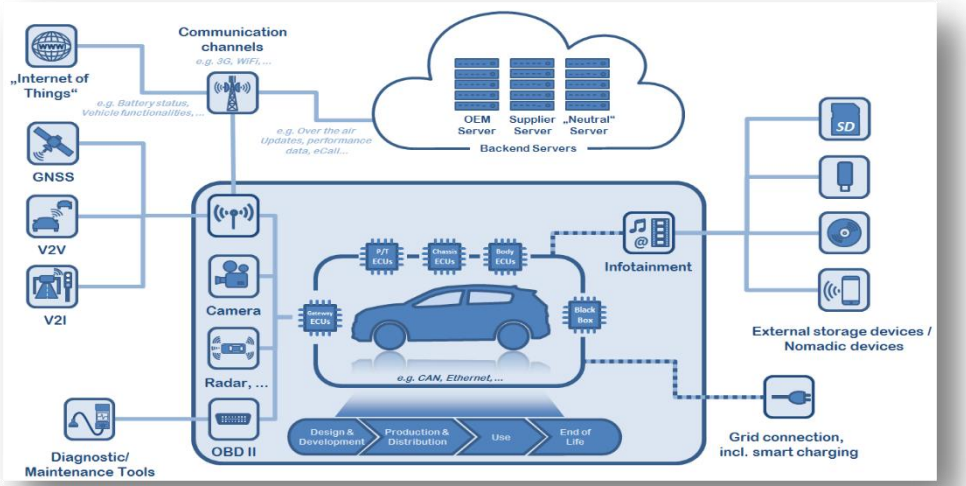


-G7 – Transport ministers

Recalled the importance of addressing cyber security and data protection at national, regional and international leve

WP.29's assessment





Action was deemed necessary
- Task force on cybersecurity and OTA issues
- Part of the Framework Document on Avs

Technical considerations
- Scope of the vehicle
- Needs at the level of the organization

Agenda

1. Introduction

2. Deliverables produced by WP.29
   - Open regulatory body / working group
   - Requirements
   - Ecosystem
   - Continuous exchange

3. Takeaways

UNECE (WP.29/GRVA) deliverables on Cyber Security

- Guidelines on cyber security and data protection adopted in 2016

- UN Regulation No. 155 (Cyber Security and CSMS)
  - Adopted in June 2020
  - Entry into Force in January 2021

- UN Regulation No. 156 (Software Update and SUMS)
  - Adopted in June 2020
  - Entry into Force in January 2021

- Cybersecurity and Software Update recommendations
  - Adopted in June 2022
  - Preparation for potential activities under the 1998 Agreement

Key aspects supporting cyber security in automotive at UNECE



Open body

No governance reform, but:
Looked for specific expertise
Open to new approaches
Inclusiveness
“Test phase” before adopting the regulation



Requirements

Level playing field
Organization / Processes
Product at system level
It includes:
- Supply chain
- Lifecycle and Lifetime requirements
- Monitoring
- Reporting



Ecosystem

Approval Authorities
Technical Services

Voluntary standards fully aligned with the requirements



Continuous exchange

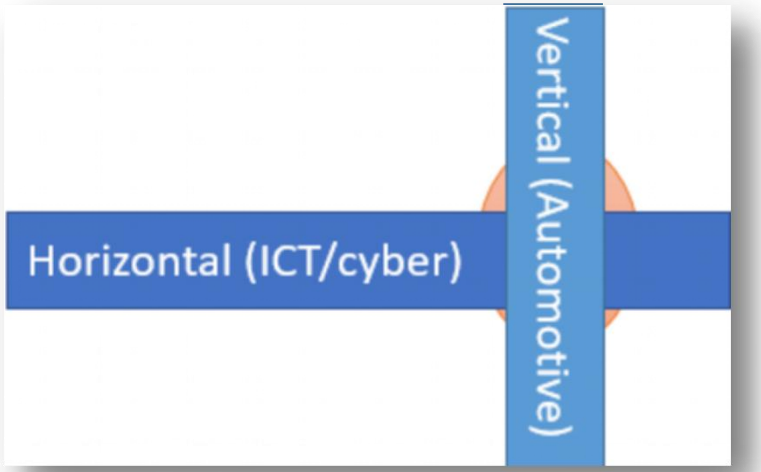
Implementation of the requirements
Review of new risks

“Open” body

UNECE worked within the existing legal frameworks to address cyber security (making OEM accountable)

UNECE invited automotive and ICT/Telecommunication experts
ITU role was acknowledged – Annex 5

The stakeholders tested the outcome of the work with volunteering vehicle manufacturers







Draft, for internal use only, copyright UNECE, F Guichard

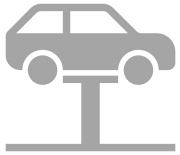
Key aspects related to cyber security requirements (automotive)



Management System

Obligations regarding the organization

(Processes are in place)



Product

TARA

Verification that the product implements the organization processes



Monitoring

Manufacturer monitors attempted and successful attacks

Data collected to support forensics



Reporting

Manufacturer reports to the Authority that issued the approval

➔The industry voluntary standards ISO/SAE 21343 and ISO/PAS 5112 support the implementation of these requirements

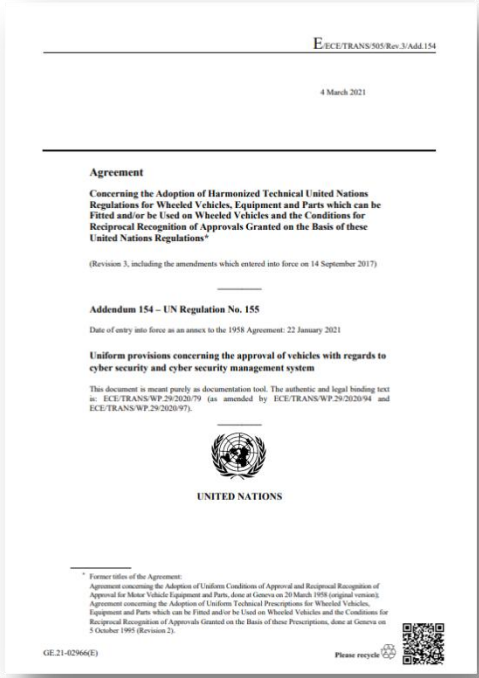
Draft, for internal use only, copyright UNECE, F Guichard

Requirements in UN Regulation No. 155 – Annex 5

Annex 5 lists:

- Vulnerabilities
- 69 attack vectors and 24 mitigations

  - Part A: threats, vulnerabilities and attack methods
  - Part B: mitigations (vehicle systems)
  - Part C: mitigations (external systems like back-end servers, cloud infra.)



E/ECE/TRANS/505/Rev.3/Add.154

4 March 2021

Agreement

Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations*

(Revision 3, including the amendments which entered into force on 14 September 2017)

Addendum 154 – UN Regulation No. 155

Date of entry into force as an annex to the 1958 Agreement: 22 January 2021

Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

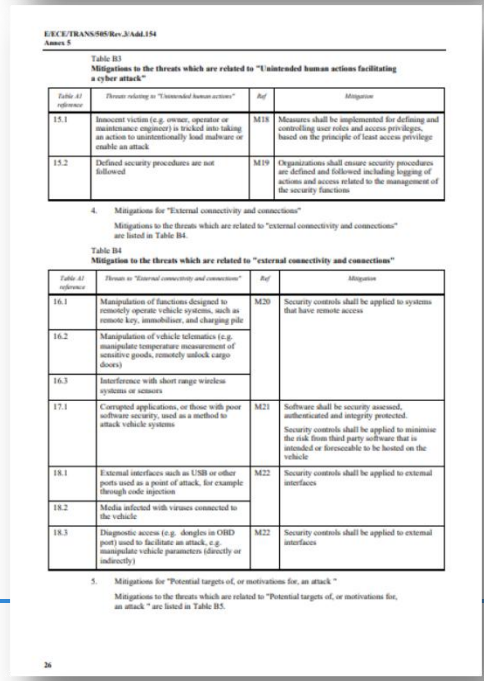
This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).

UNITED NATIONS

* Former titles of the Agreement:
Agreement concerning the Adoption of Uniform Conditions of Approval and Reciprocal Recognition of Approval for Motor Vehicle Equipment and Parts, done at Geneva on 20 March 1958 (original version);
Agreement concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions, done at Geneva on 5 October 1995 (Revision 2).

GE.21-02966(E)

Please recycle



E/ECE/TRANS/505/Rev.3/Add.154
Annex 5

Table B3
Mitigations to the threats which are related to "Unintended human actions facilitating a cyber attack"

Table A1 reference	*Threats relating to "Unintended human actions"*	*Ref*	*Mitigation*
15.1	Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack	M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege
15.2	Defined security procedures are not followed	M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions

4. Mitigations for "External connectivity and connections"

Mitigations to the threats which are related to "external connectivity and connections" are listed in Table B4.

Table B4
Mitigation to the threats which are related to "external connectivity and connections"

Table A1 reference	*Threats to "External connectivity and connections"*	*Ref*	*Mitigation*
16.1	Manipulation of functions designed to remotely operate vehicle systems, such as remote key, immobiliser, and charging pile	M20	Security controls shall be applied to systems that have remote access
16.2	Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)		
16.3	Interference with short range wireless systems or sensors		
17.1	Corrupted applications, or those with poor software security, used as a method to attack vehicle systems	M21	Software shall be security assessed, authenticated and integrity protected. Security controls shall be applied to minimise the risk from third party software that is intended or foreseeable to be hosted on the vehicle
18.1	External interfaces such as USB or other ports used as a point of attack, for example through code injection	M22	Security controls shall be applied to external interfaces
18.2	Media infected with viruses connected to the vehicle		
18.3	Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)	M22	Security controls shall be applied to external interfaces

5. Mitigations for "Potential targets of, or motivations for, an attack "

Mitigations to the threats which are related to "Potential targets of, or motivations for, an attack " are listed in Table B5.

26

The ecosystem

Using the existing legal framework led to the possibility to promptly implement cyber requirements in Automotive.

Since the entry into force, UNECE observed many announcements for:

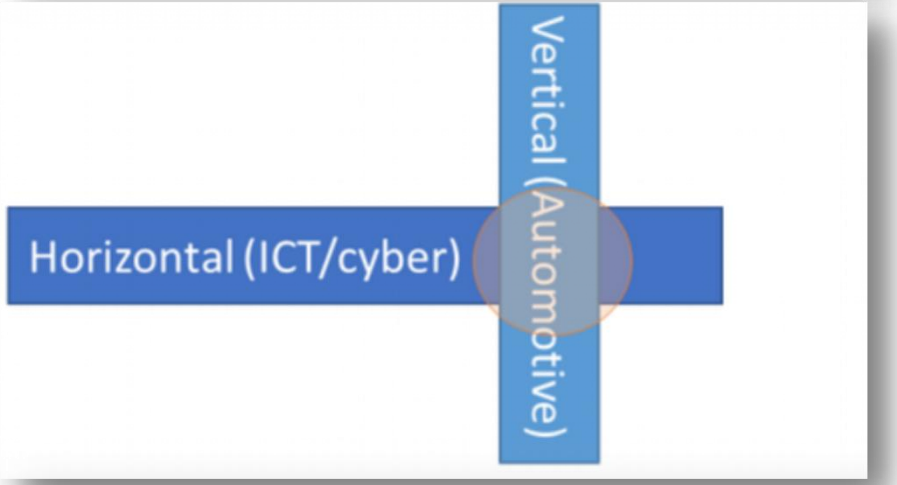
- Merger and acquisitions
- Partnerships
  (e.g. Fujitsu + Upstream Security, Siemens + Karamba)
- Profit opportunities. The “cyber market” will grow and double to reach USD 10 Bio. In 2030 -- source: McKinsey

Industry (voluntary) standards are fully aligned with the regulatory requirements – developed in parallel
See ISO/SAE 21434 (engineering) and ISO/PAS 5112 (audits)

Some figures:

-58 Approval Authorities notified to UNECE

-43 Technical Services nominated by their Authorities and notified to UNECE





Draft, for internal use only, copyright UNECE, F Guichard

Continuous exchanges among relevant parties

- The drafting group (IWG on CS/OTA) got its mandate updated.

It meets and reviews the regulation in order to identify necessary updates

It was tasked to address AI in the context of cyber security (no amendment to the regulation was deemed necessary)

- The Regulation was adopted together with an *interpretation document* to support the stakeholders in implementing the requirements

- The Authorities meet in recurrent meetings ("workshop") to discuss the implementation

Draft, for internal use only, copyright UNECE, F Guichard

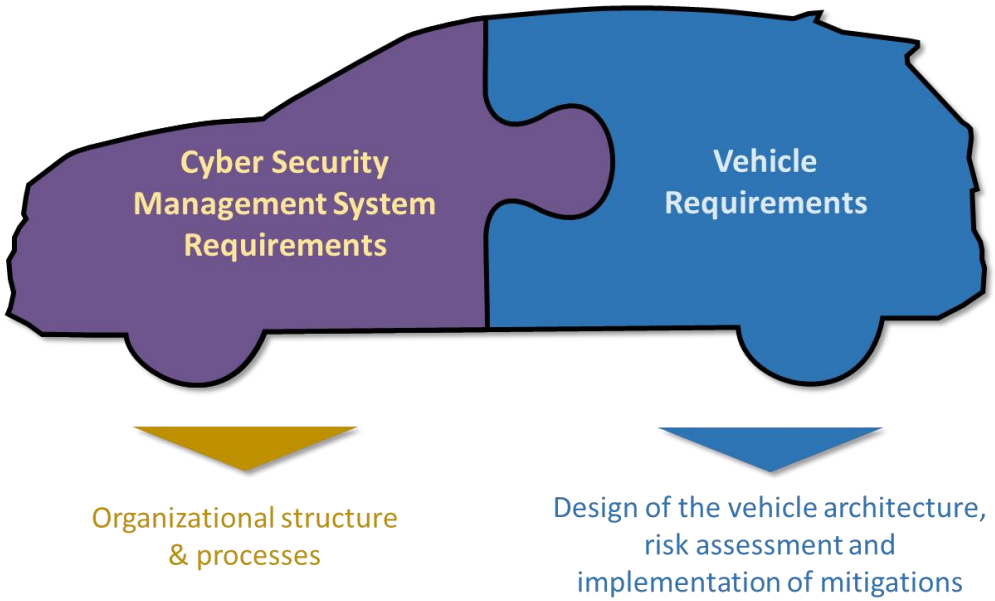
Agenda

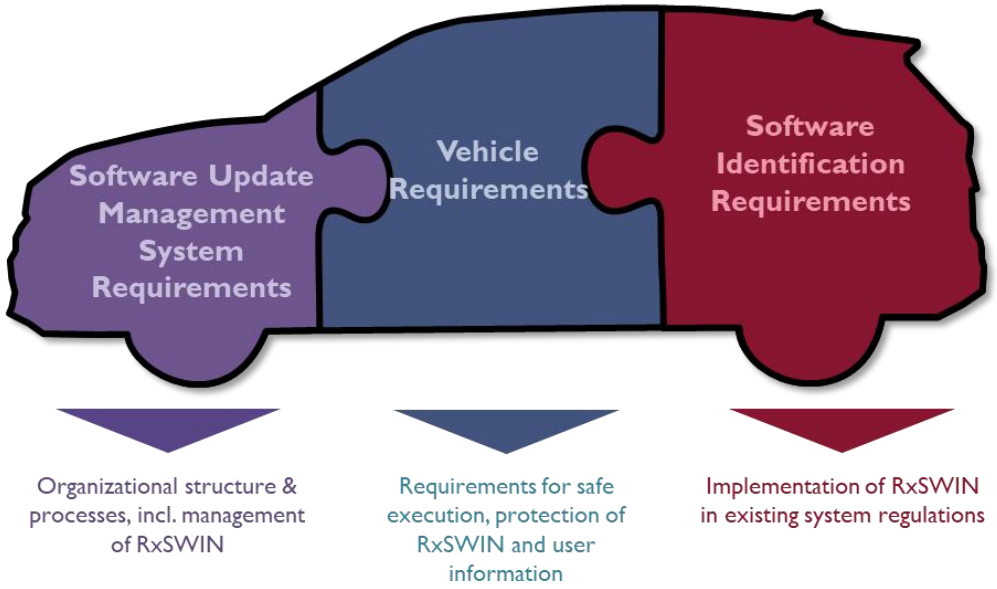
1. Introduction

2. Deliverables produced by WP.29

3. Takeaways
   - Scope
   - Overview
   - Open items

Takeaways - What we've done and recent addition





Vehicle categories covered: passenger cars, trucks, buses and coaches

Recent amendment: powered-two-wheelers were added in the scope of UN Regulation No.155

Draft, for internal use only, copyright UNECE, F Guichard

Thank you for your attention



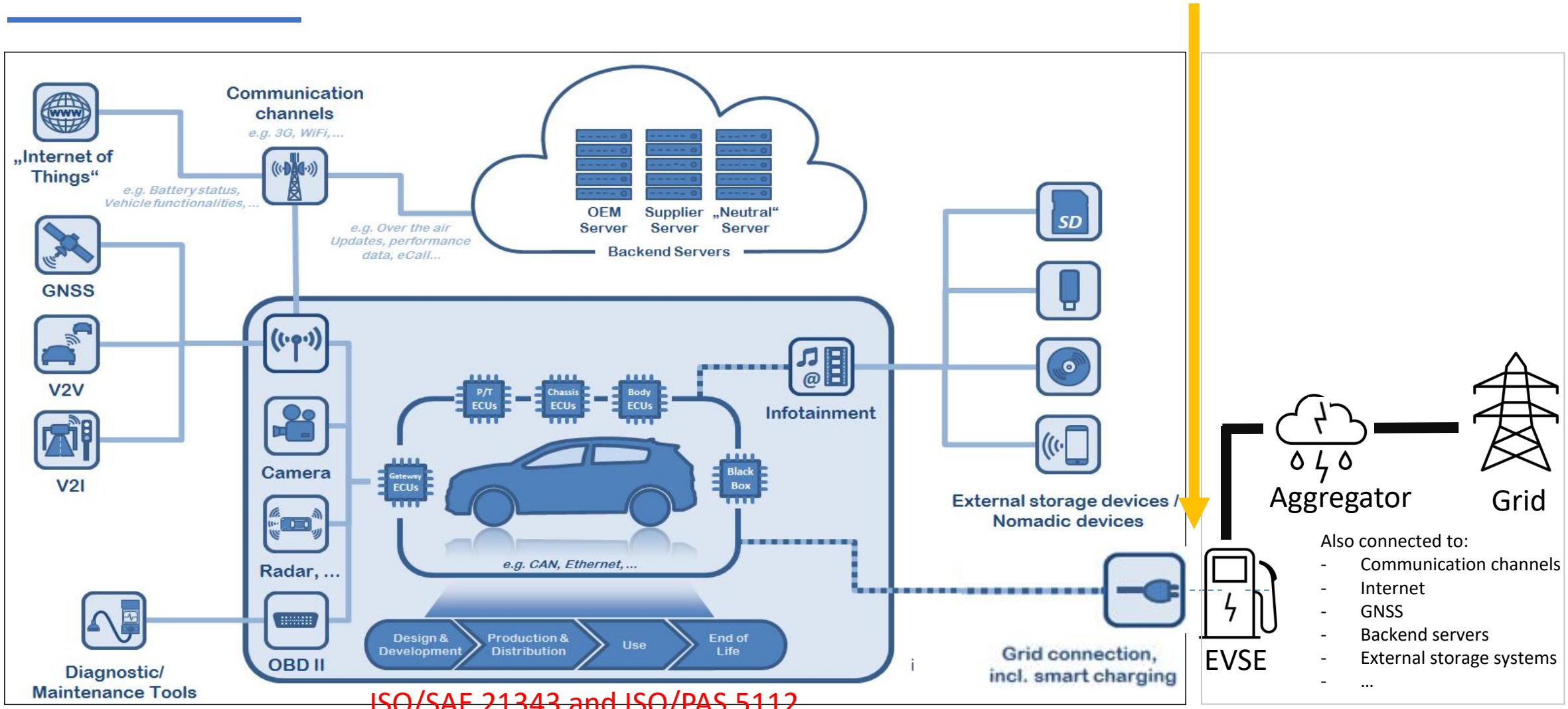
François E. Guichard
Secretary to the Working Party on Automated/Autonomous and Connected Vehicles
Francois.Guichard@un.org

UNECE

Draft, for internal use only, copyright UNECE, F Guichard

Takeaways

e.g. ISO 15118 Vehicle to grid communication interface



ISO/SAE 21343 and ISO/PAS 5112

Draft, for internal use only, copyright UNECE, F Guichard