BACK TO A SUSTAINABLE FUTURE
21
RESILIENT CONNECTIVITY FOR SUSTAINED RECOVERY AND ECONOMIC GROWTH

INLAND TRANSPORT COMMITTEE

UNECE

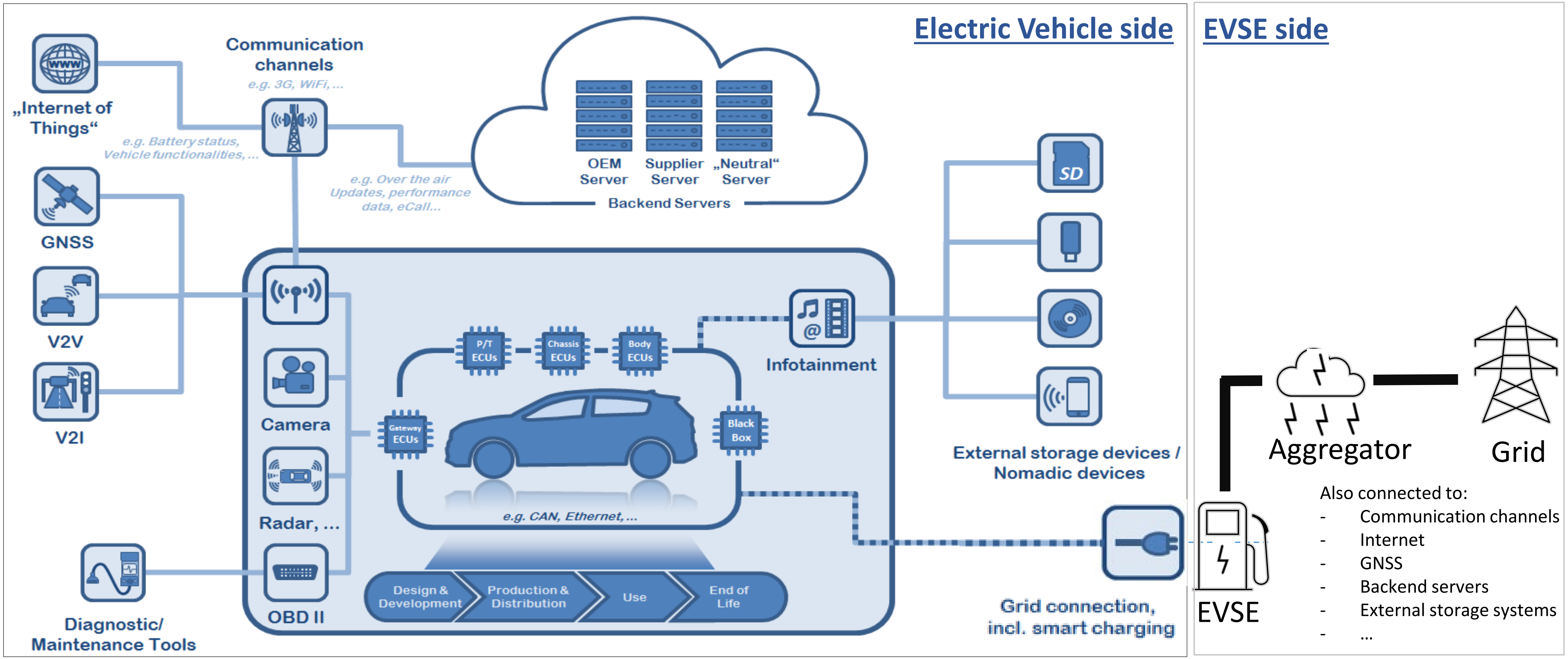
ITC/WP.5

5 September 2023
Geneva, Palais des Nations

Cyber security of Electric Vehicles and their Supply Equipment

François E. Guichard
UNECE

The subject of the day (simplified view)



Also connected to:

- Communication channels
- Internet
- GNSS
- Backend servers
- External storage systems
- …

Illustration - Source: OICA / IWG on CS/OTA – Icons from Powerpoint

Agenda

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

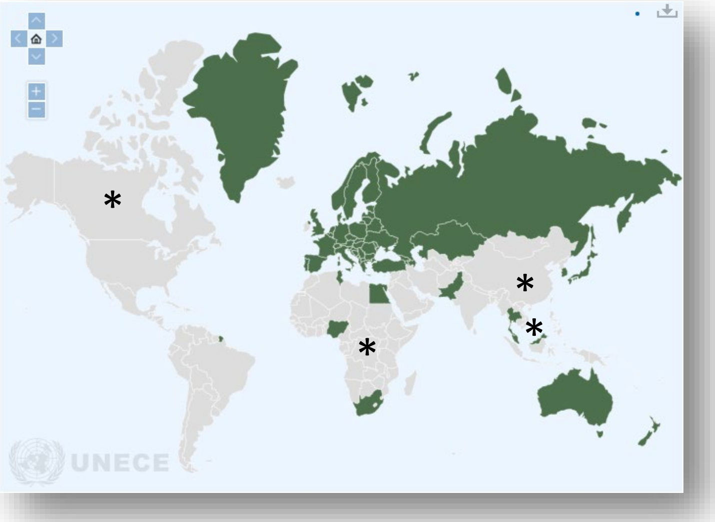
2. Deliverables produced by WP.29

3. Takeaways

Frameworks – relevant UNECE’s multilateral Agreements (WP.29)

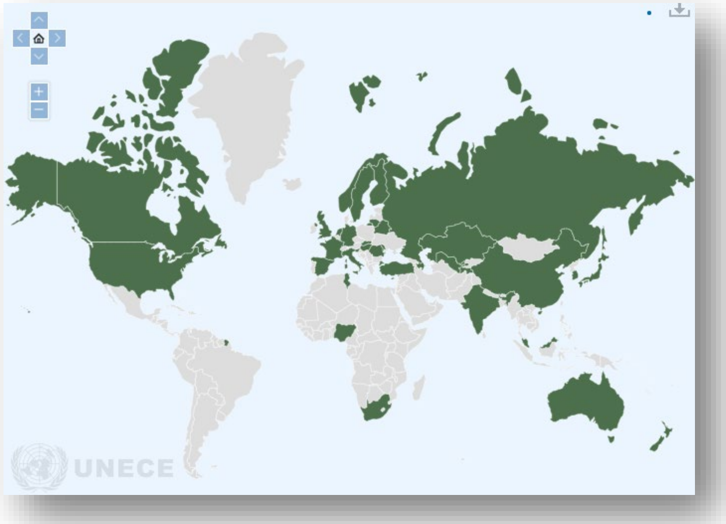
1958 Agreement:

- “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



Starting point - cyber security at UNECE

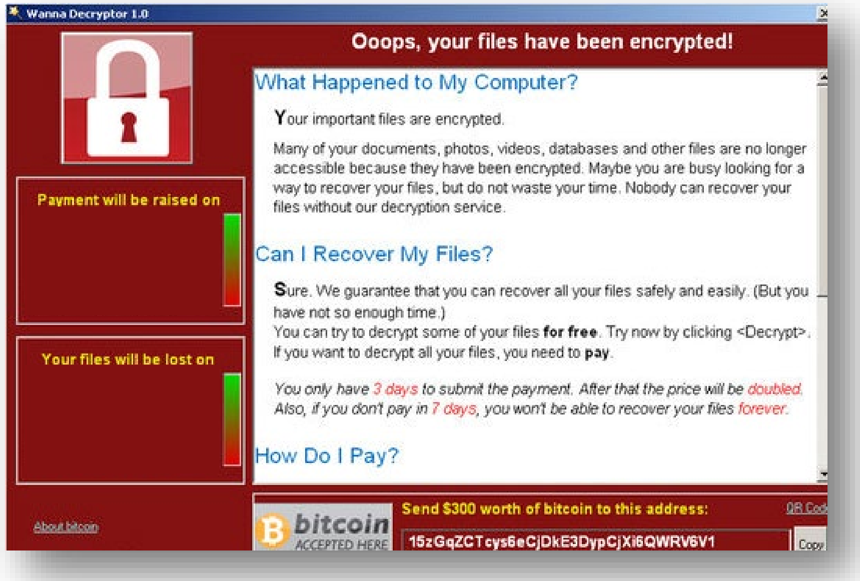
UNECE hosts the World Forum for Harmonization of Vehicle Regulations (WP.29)

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

Hackers Remotely Kill a Jeep on the Highway—With Me...
It's not fun to have your two ton SUV's brakes hacked,

June 2015 – hacked Jeep

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



Wanna Decryptor 1.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Payment will be raised on

Your files will be lost on

Send $300 worth of bitcoin to this address:

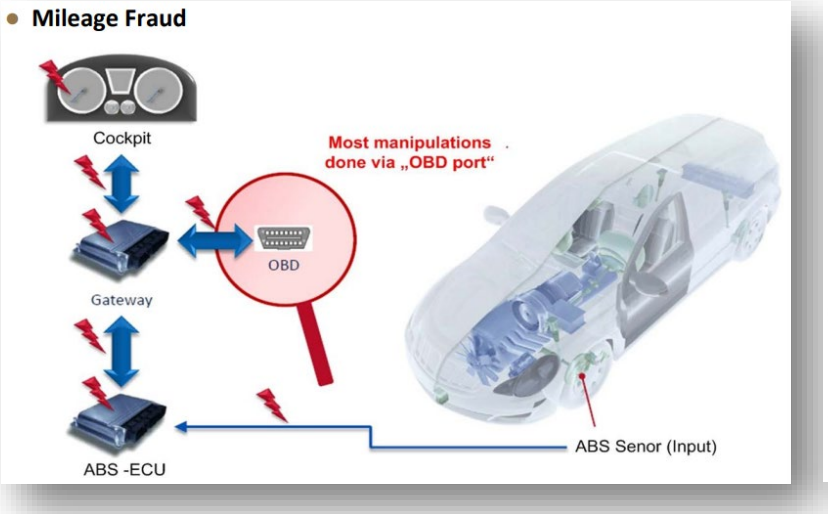
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

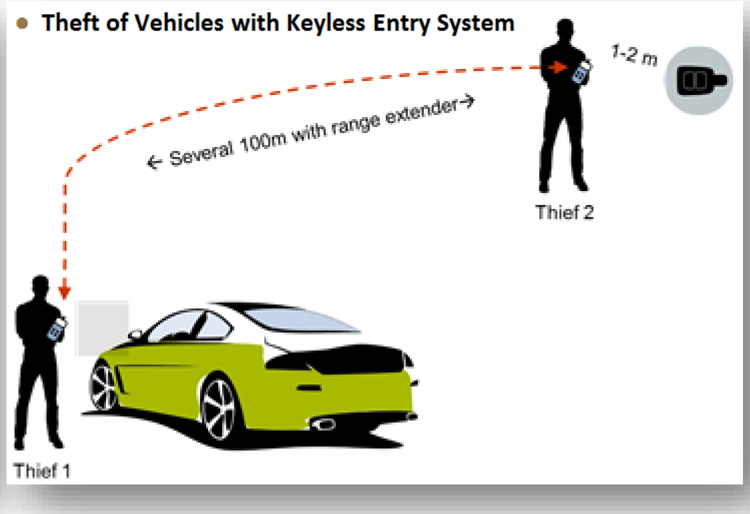
Mai 2017 - Wannacry

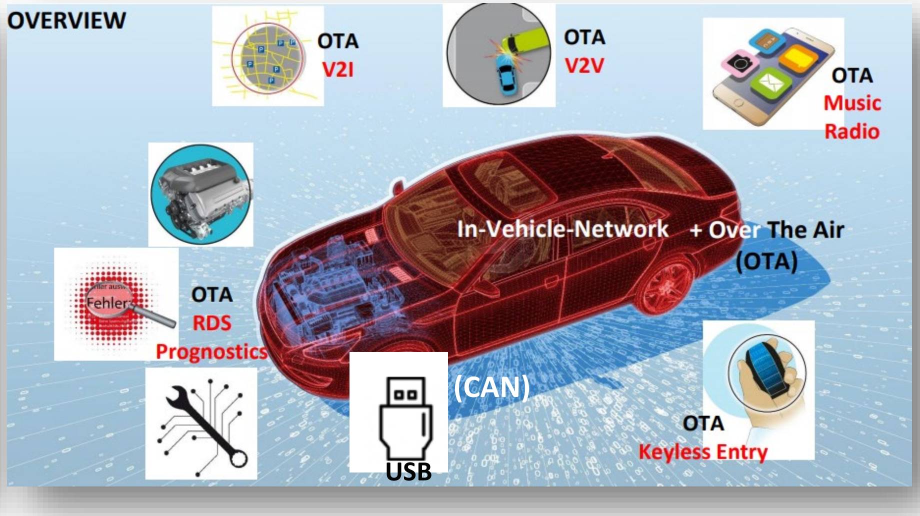
Source: screenshot

Starting point - cyber security at UNECE

-FIA presented the following cases:




Theft of Vehicles with Keyless Entry System
1-2 m
← Several 100m with range extender→
Thief 2
Thief 1



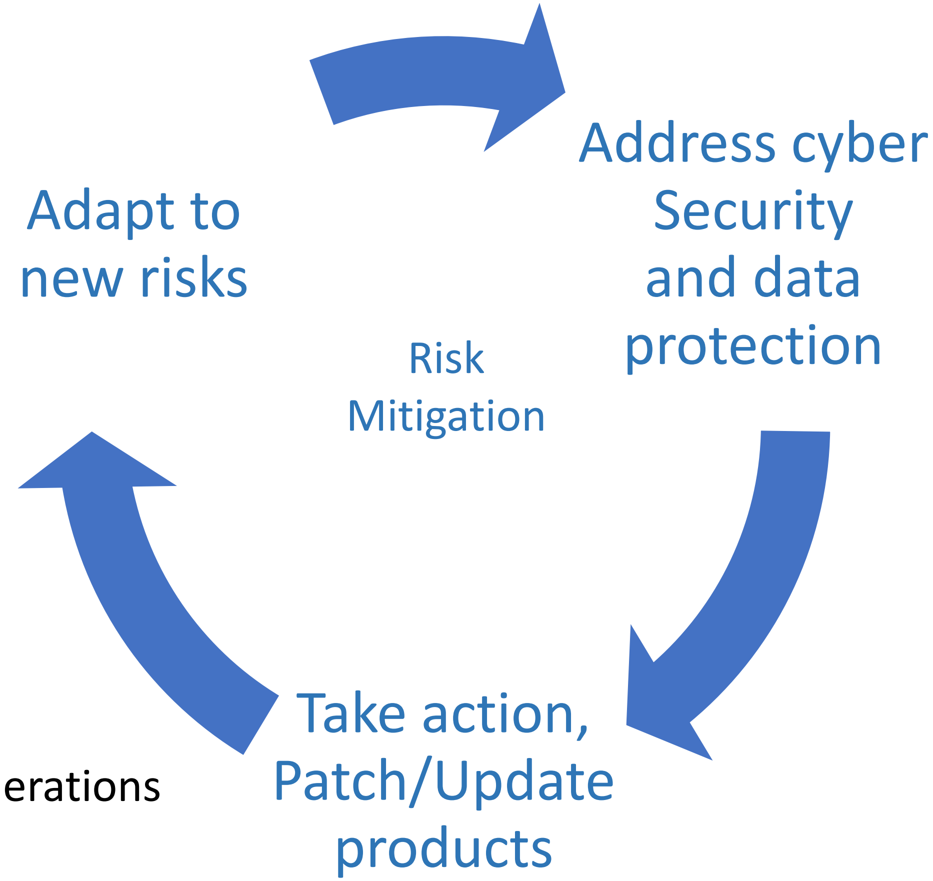
-G7 – Transport ministers

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

Illustration - Source: slides presented by FIA at WP.29 and GRVA sessions

Consideration of three essential elements

- ➔ Reporting on successful or attempted attacks
- ➔ Upgrade standards and regulations



Adapt to new risks

Address cyber Security and data protection

Risk Mitigation

Take action, Patch/Update products

- ➔ Prepare the organization
- ➔ Perform TARA
- ➔ Cascade down requirements across supply chain
- ➔ Secure and test the product

…while supporting legitimate access to data

- ➔ Life cycle and lifetime considerations
- ➔ Software update incl. OTA
- ➔ Update the TARA, keep it current
- ➔ Monitor

Agenda

1. Introduction

2. Deliverables produced by WP.29
   - Task Force on CS/OTA
   - 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
  - Japan and EU apply the regulation on the mandatory basis (2022/2024)

- UN Regulation No. 156 (Software Update and SUMS)
  - Adopted in June 2020
  - Entry into Force in January 2021
  - EU apply the regulation on the mandatory basis (2022/2024)

Key aspects related to cyber security in automotive at UNECE

"Open" bodies

No reform

Looked for specific expertise

Open to new approaches

Testing before adoption of the requirements

Requirements

Organization / Processes

Product at system level

Includes:

- Supply chain
- Lifecycle and Lifetime requirements
- Monitoring
- Reporting

Ecosystem

Approval Authorities

Technical Services

Voluntary standards fully aligned with the requirements

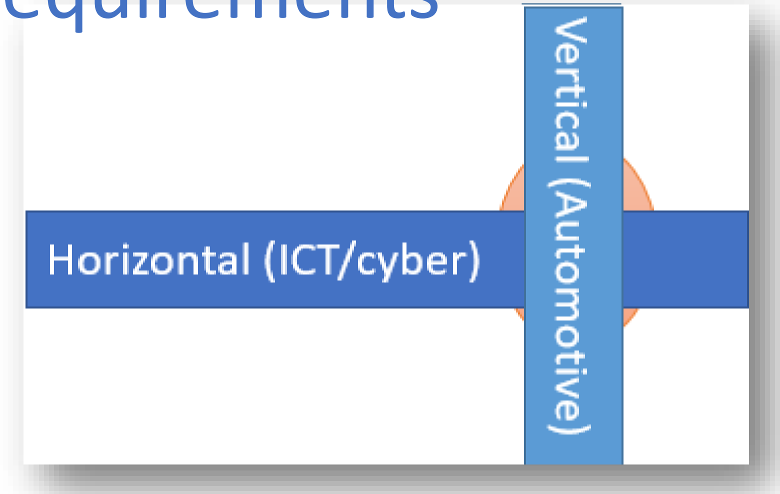
Continuous exchange

Implementation of the requirements

Review of new risks

“Open” bodies agreed on cyber specific requirements

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



UNECE invited automotive and ICT/Telecommunication experts

ITU SAE INTERNATIONAL ISO Etc.

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

Key aspects related to cyber security requirements (automotive)

Management System

Obligations for 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

Each 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

The ecosystem

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

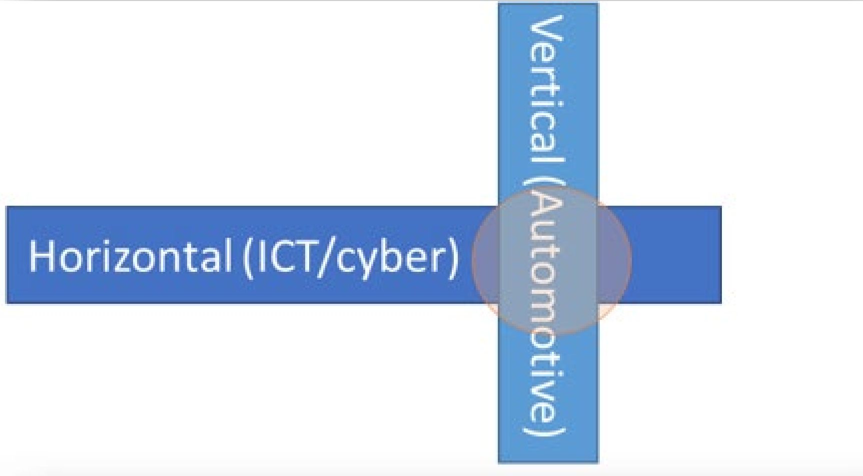
Since the entry into force, UNECE observed many announcements for:

- 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



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

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

-The Authorities meet in recurrent meetings (“workshops”) to discuss the implementation (last one: yesterday)

Agenda

1. Introduction

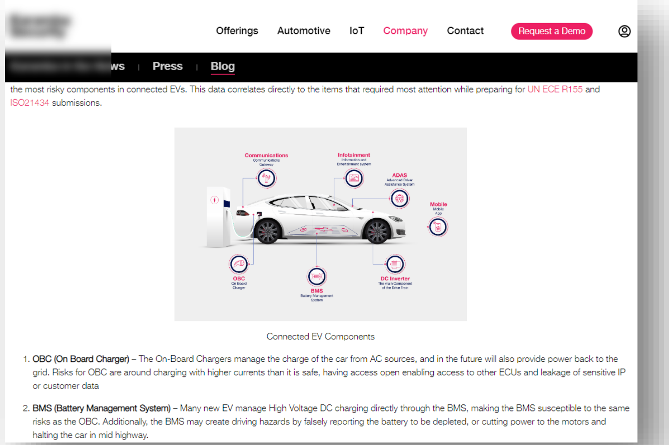
2. Deliverables produced by WP.29

3. Takeaways
   - Current status
   - Achievements
   - Open items

Takeaways – Current status for EVs and EVSE

Vehicle side
(OEM and Tier 1)

Standard commercial solutions available to address the most pressing issues for EVs, e.g.:
-OBC
-BMS
-Infotainment
-Communication hub/gateway
-ADAS
-DC inverter
-Mobile applications

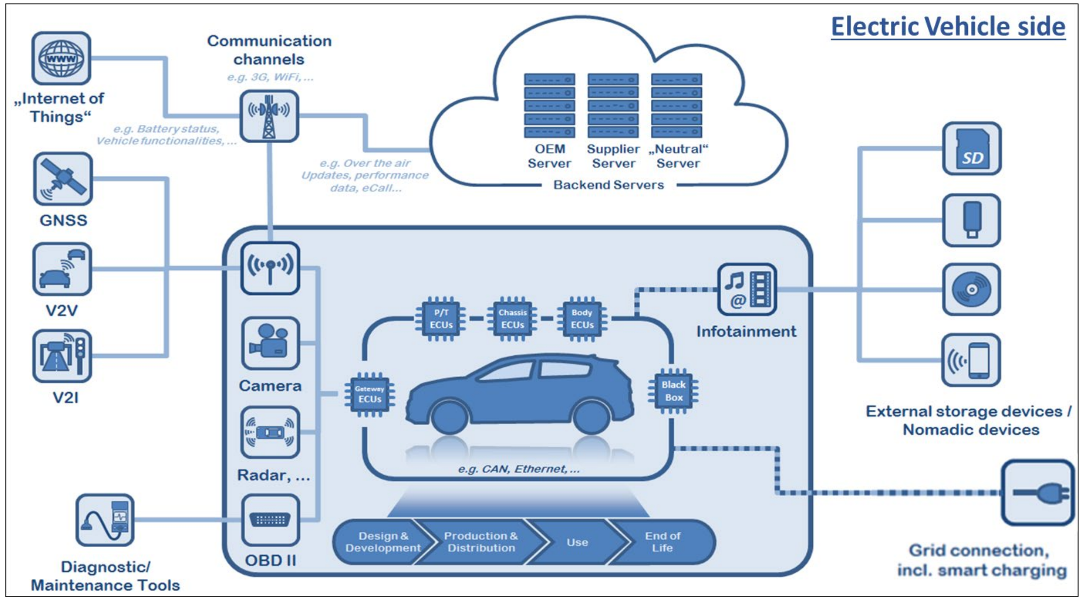


the most risky components in connected EVs. This data correlates directly to the items that required most attention while preparing for UN ECE R155 and ISO21434 submissions.

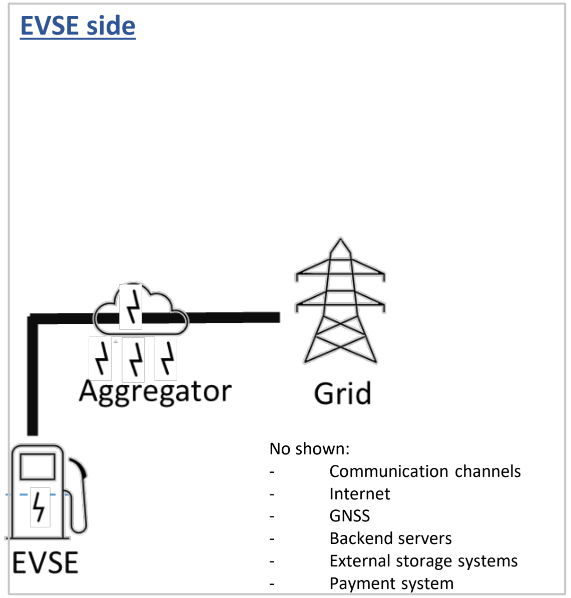
Connected EV Components

1. **OBC (On Board Charger)** – The On-Board Chargers manage the charge of the car from AC sources, and in the future will also provide power back to the grid. Risks for OBC are around charging with higher currents than it is safe, having access open enabling access to other ECUs and leakage of sensitive IP or customer data
2. **BMS (Battery Management System)** – Many new EV manage High Voltage DC charging directly through the BMS, making the BMS susceptible to the same risks as the OBC. Additionally, the BMS may create driving hazards by falsely reporting the battery to be depleted, or cutting power to the motors and halting the car in mid highway.

Electric Vehicle side



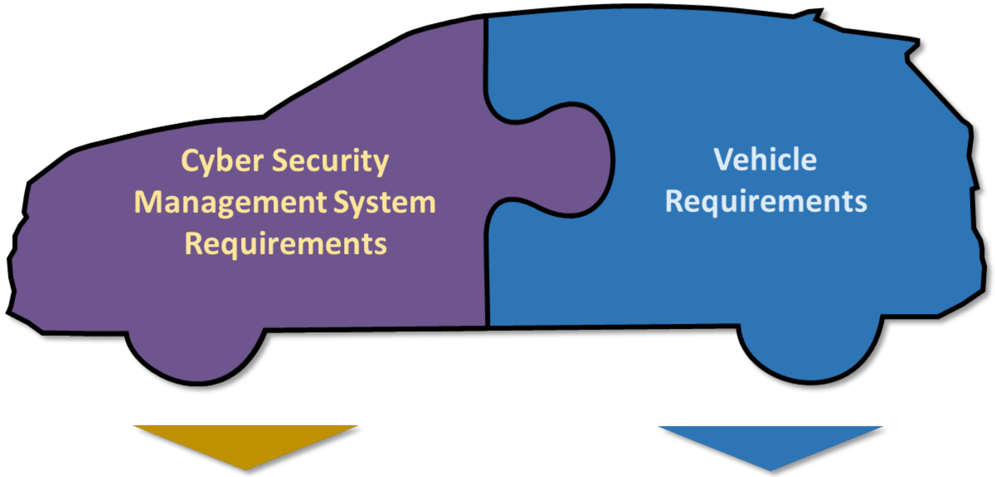
EVSE side



No shown:
- Communication channels
- Internet
- GNSS
- Backend servers
- External storage systems
- Payment system
- …

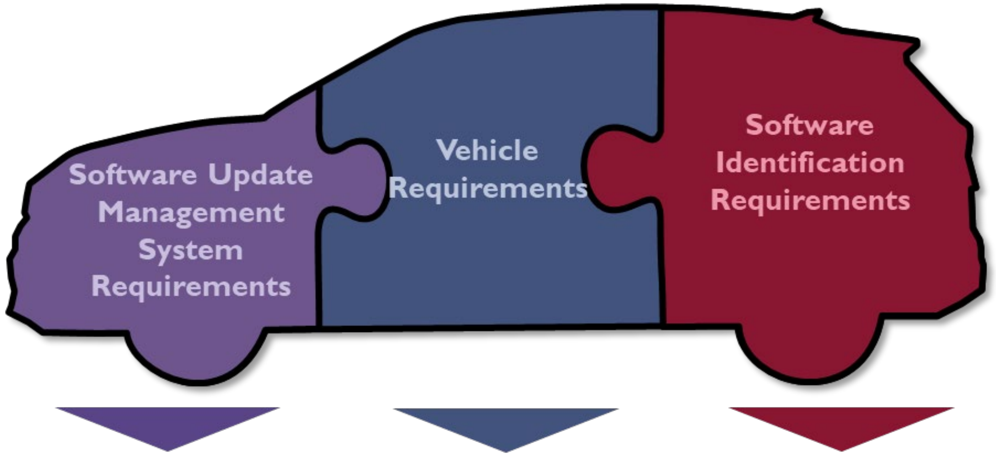
Illustration - Source: https://karambasecurity.com/blog/2022-01-30-ev-tara-compliance-iso-unece

Takeaways – Achievements and open points



Organizational structure & processes

Design of the vehicle architecture, risk assessment and implementation of mitigations


Software Update Management System Requirements
Vehicle Requirements
Software Identification Requirements

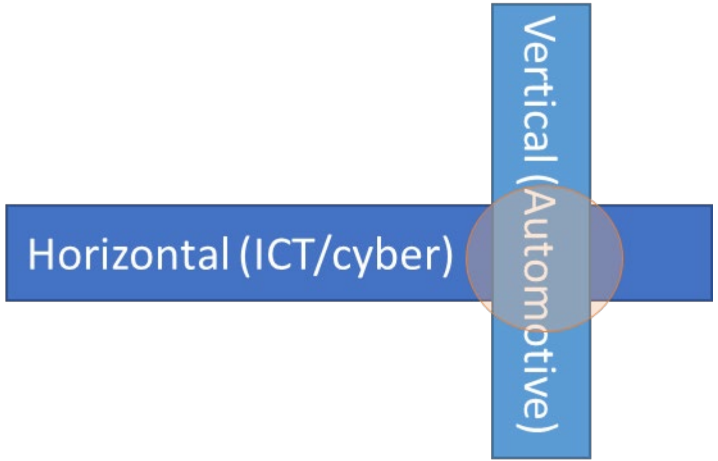
Organizational structure & processes, incl. management of RxSWIN

Requirements for safe execution, protection of RxSWIN and user information

Implementation of RxSWIN in existing system regulations

Vehicle categories covered: passenger cars, trucks, buses and coaches as well as L6 and L7 with ADS

Open: Agricultural vehicles and powered-two-wheelers



Thank you for your attention

Francois E. Guichard