# UN REGULATION 155 ON CYBERSECURITY AND ITS IMPACT WITH REGARD TO ELECTRIC VEHICLES

Kai Frederik Zastrow, Senior Fellow Regulation Certification Standards (Stellantis)

Pilot of Cluster 4 Cybersecurity & Software Updates, International Organization of Motor Vehicle Manufacturers (OICA), industry mirror of UNECE/GRVA/IWG CS&OTA

# Global Automotive Standards and Regulations to address Cybersecurity and SW updates

**WP.29 World Forum for Harmonization of Vehicle Regulations**
- UN Regulation 155 on Cyber Security
- UN Regulation 156 on SW updates
- UN Recommendations on cyber security and software updates

**ISO TC22/SC32/WG11 - Cybersecurity**
- ISO/SAE 21434 Cybersecurity Engineering

**ISO TC22/SC32/WG12 – Software update**
- ISO 24089 Software Update Engineering

**National Discussions**
- UK BSI PAS 1885:2018
- …

**European Union**
- Cybersecurity Act
- General Data Protection Regulation
- NIS Directive (Network and Information Security)

**China**
- Cybersecurity Law & Data Security Law
- Personal Information Protection Law
- Information Security: SAC/TC 260
- Automotive: SAC/TC 114/SC 34/WG Cyber

**USA**
- NHTSA Cybersecurity Guidelines

**UN Regulations (adopted in June 2020) are worldwide consensus:**
Developed under GRVA (chaired by Germany, Japan and China)
/ IWG Cybersecurity & OTA issues (chaired by UK, Japan and USA).
=> **Japan** and **European Union** are the first regions that make the regulations mandatory in their territory.

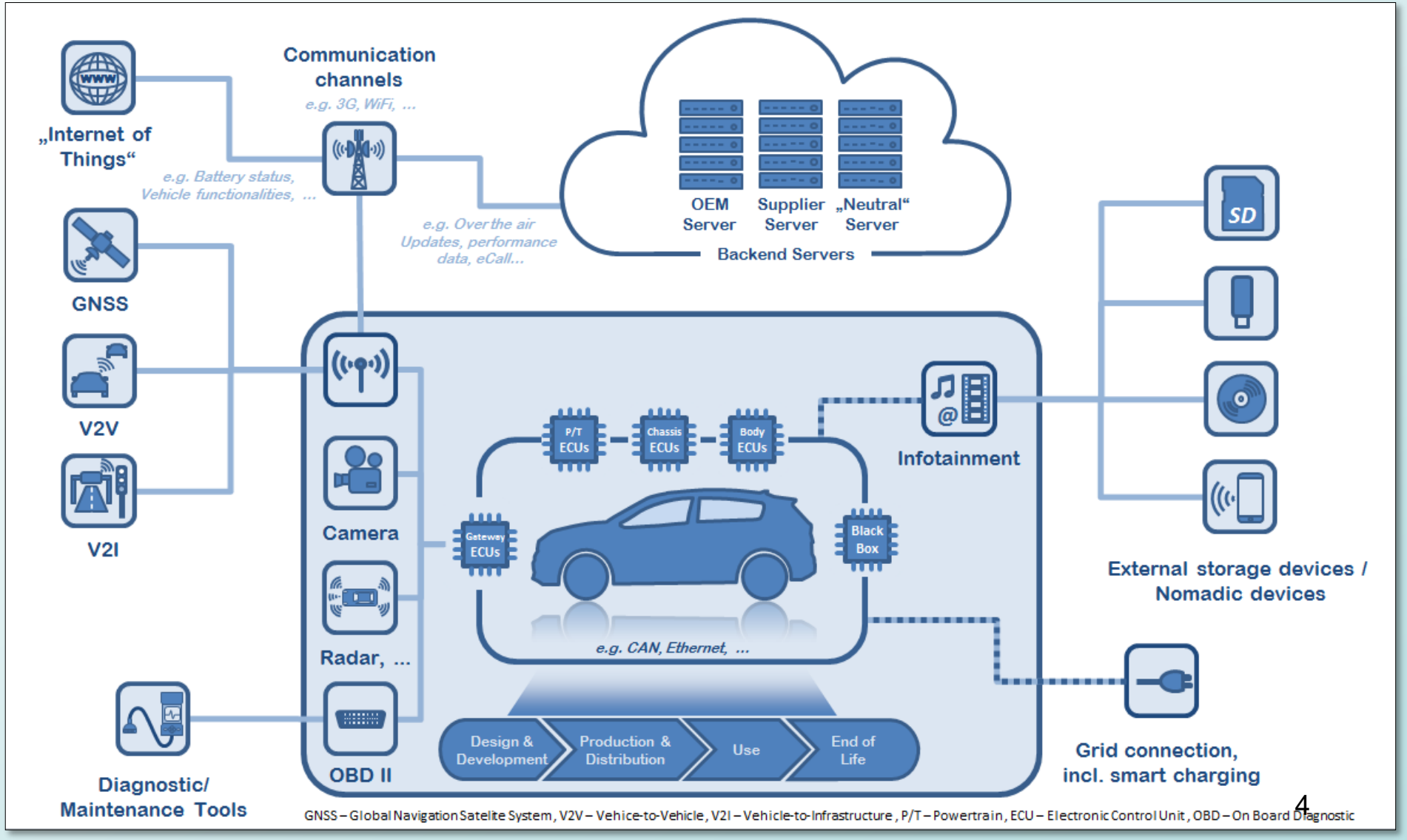
# Why cybersecurity regulation?

- Risk of cyberattacks
  - **Safety/Security/Environmental impact**:
    - Hacker may
      - **be** the **vehicle user**
      - **manipulate** existing vehicle software
      - get access to **private/confidential data** (incl. location and charging history)
      - use vehicle for **criminal actions**
  - **Economic impact:**
    - Economic risk for vehicle manufacturer, e.g. for recalls

- Objective of the regulation
  - **Protect the vehicle from cyber-attacks**

# Cybersecurity concerns the **whole vehicle**

⇒ **Cybersecurity cannot be covered by certification of only some specific components**

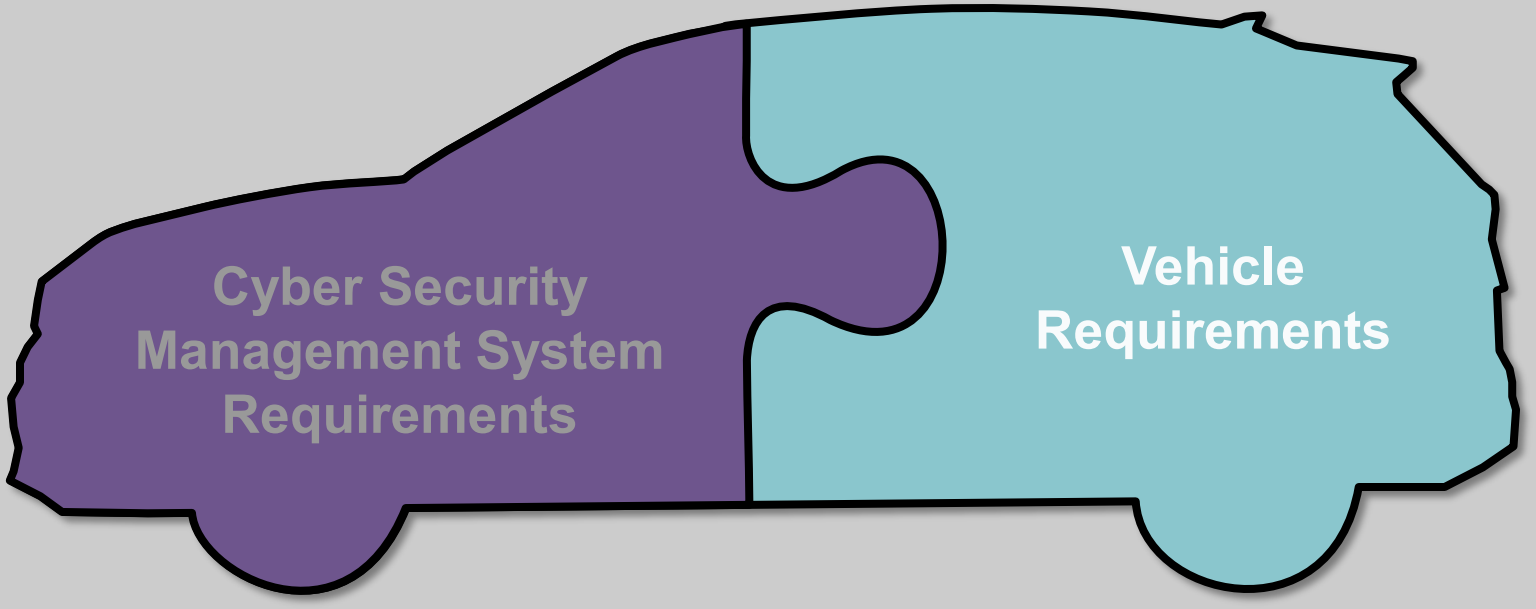


# UN Regulation 155 on Automotive Cybersecurity

Split approach for the cybersecurity assessment:

i) Assessment and certification of vehicle manufacturer **Cyber Security Management System**

ii) Assessment and certification of **vehicles**

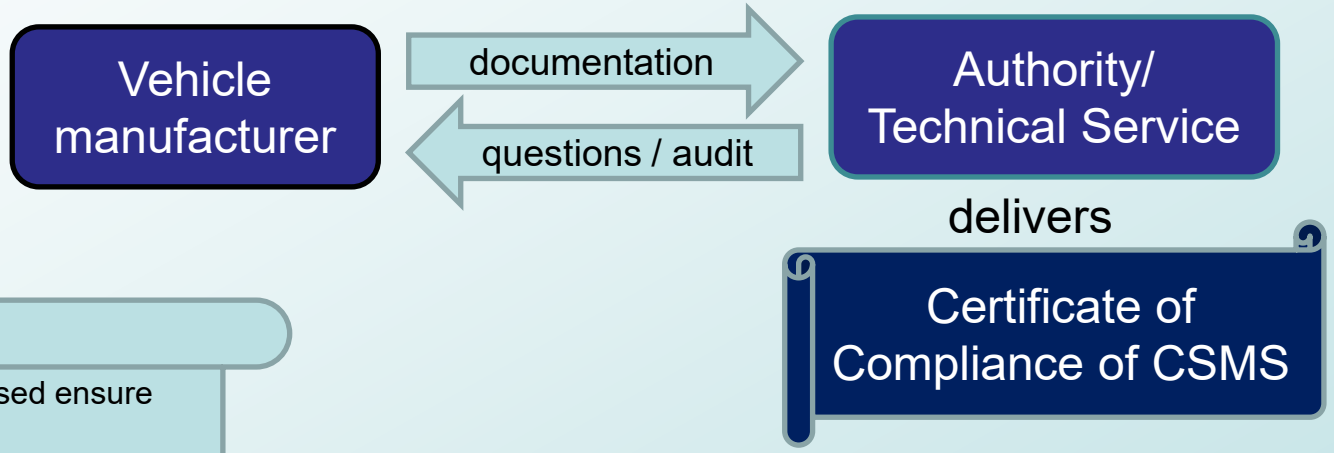



Organizational structure & processes

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

# 7.2 Requirements for the CSMS Cyber Security Management System

7.2.2.1. Vehicle manufacturer shall demonstrate that their Cyber Security Management System considers:
- Development phase
- Production phase
- Post-production phase




7.2.2.2. Vehicle manufacturer shall demonstrate that processes used ensure security including:
a) manage cyber security
b) identification of risks to vehicle types (see Annex 5, part A)
c) assessment, categorization and treatment of the risks identified
d) verify that the risks identified are appropriately managed
e) testing the security of the system
f) ensuring that the risk assessment is kept current
g) monitor for, detect and respond to cyber-attacks on vehicle types and assess whether the cyber security measures implemented are still effective
h) Provide relevant data to support analyses of attempted or successful attacks

7.2.2.3. The vehicle manufacturer shall demonstrate that mitigation happen in a reasonable timeframe

7.2.2.4. The vehicle manufacturer shall demonstrate that monitoring of vehicles is continual.

7.2.2.5. The vehicle manufacturer shall demonstrate how he manages dependencies with contracted suppliers and service providers in regards of the requirements of paragraph 7.2.2.2

# 7.3. Requirements for vehicle types

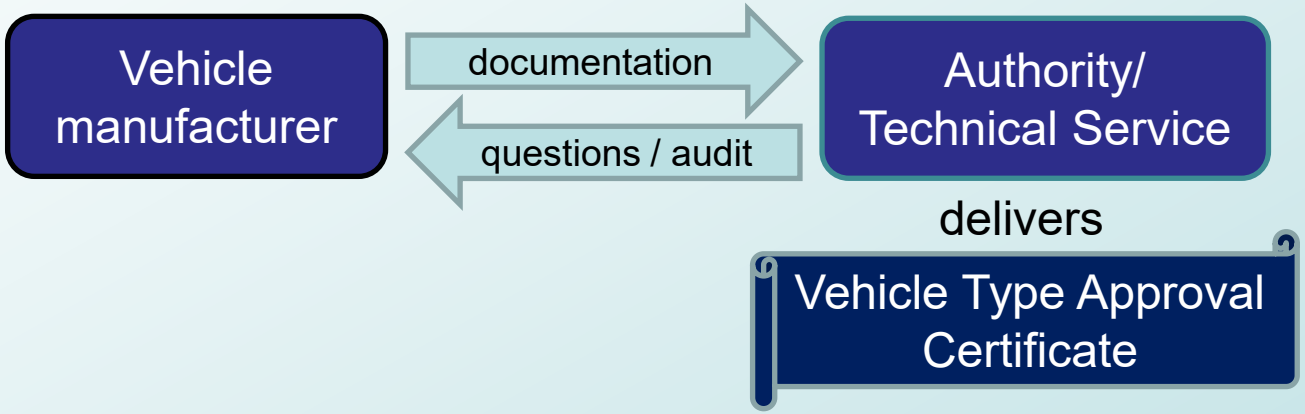
7.3.1. Vehicle manufacturer shall have valid Certificate of Compliance relevant to the vehicle type being approved.

7.3.2. Manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks

7.3.3. Vehicle manufacturer shall demonstrate an exhaustive risk assessment => Annex 5, part A

7.3.4. Vehicle manufacturer shall demonstrate proportionate mitigations => Annex 5, part B & C.

7.3.7. Vehicle manufacturer shall implement measures to detect and monitor cyber-attacks, provide data forensic for analysis of attempted attacks.




## 7.4 Monitoring and Reporting

7.4.1. Vehicle manufacturer shall report at least once a year, or more frequently if relevant, the outcome of the monitoring activities.

7.4.2. The Authority shall if necessary require to remedy any detected ineffectiveness.
If the response is not sufficient, the CSMS may be withdrawn.

# Annex 5, Part A: List of threats

Table A1

**List of vulnerability or attack method related to the threats**

| *High level and sub-level descriptions of vulnerability/ threat* | | | *Example of vulnerability or attack method* | |
|---|---|---|---|---|
| 4.3.1 Threats regarding back-end servers related to vehicles in the field | 1 | Back-end servers used as a means to attack a vehicle or extract data | 1.1 | Abuse of privileges by staff (**insider attack**) |
| | | | 1.2 | **Unauthorized internet access** to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) |

| *High level and sub-level descriptions of vulnerability/ threat* | | | *Example of vulnerability or attack method* | |
|---|---|---|---|---|
| 4.3.5 Threats to vehicles regarding their external connectivity and connections | 16 | Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications | 16.1 | Manipulation of **functions designed to remotely operate systems**, such as remote key, immobilizer, and charging pile |
| | | | 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 |

# Annex 5, Part B: Mitigations on vehicles

Table B1

**Mitigation to the threats which are related to "Vehicle communication channels"**

| *Table A1 reference* | *Threats to "Vehicle communication channels"* | *Ref* | *Mitigation* |
|---|---|---|---|
| 4.1 | Spoofing of messages (e.g. 802.11p | M10 | The vehicle shall verify the authenticity and |

| *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 | | |

# Annex 5, Part C: Mitigations outside the vehicle

Table C1

**Mitigations to the threats which are related to "Back-end servers"**

| *Table A1 reference* | *Threats to "Back-end servers"* | *Ref* | *Mitigation* |
|---|---|---|---|
| 1.1 & 3.1 | Abuse of privileges by staff (insider attack) | M1 | Security Controls are applied to back-end systems to minimise the risk of insider attack |
| 1.2 & 3.3 | Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) | M2 | Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP |
| 1.3 & 3.4 | Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server) | M8 | Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data |
| 2.1 | Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on | M3 | Security Controls are 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 |

# Requirements for the whole vehicle life cycle

- Vehicle manufacturer shall demonstrate that their Cyber Security Management System considers (§ 7.2.2.1):

a) Development phase

b) Production phase

c) Post-production phase

Post-production phase

Production phase

Development phase

# Conclusions

- UN R155 requires an exhaustive cybersecurity risk analysis and the implementation of appropriate mitigations.
- Cyberattacks must be reported to the approval authority.
- As more and more vehicles will be type approved according to R155 (mandatory for all first vehicle registrations from July 2024 in Japan & European Union), the reports to approval authorities will show the part of cyberattacks via the electric charging interface.
- According to those reports, additional measures may be introduced.
- UN R155 is part of a broader effort to address the cybersecurity challenges associated with the increasing connectivity and complexity of vehicles, including EVs. All stakeholders are expected to work together to implement and enforce these cybersecurity measures.

# ANNEX

# Link to UN documents

- UN Regulation 155 Cybersecurity https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
- Interpretation document on Cybersecurity https://unece.org/sites/default/files/2022-04/ECE-TRANS-WP.29-2022-61e.pdf
- UN Regulation 156 SW update https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update
- Interpretation document on SW update http://unece.org/sites/default/files/2020-12/ECE-TRANS-WP29-2021-060e.pdf
- Recommendations on uniform provisions concerning cyber security and software updates https://unece.org/sites/default/files/2022-04/ECE-TRANS-WP.29-2022-60e.pdf
- UN Regulation 157 ALKS (see chapter 9 with link to UN Regulations 155 and 156 and Annex point 19) https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems-alks
- Consolidated Resolution on the Construction of Vehicles (R.E.3), Annex 7: Provisions on Software Identification Numbers (integration of RXSWIN in system regulations) http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29/ECE-TRANS-WP29-2020-082e.pdf

# ISO 15118 Vehicle to grid communication interface

ISO/TC 22/SC 31 “Data communication” developed a series of standards for charging/discharging “Vehicle to grid communication interface”

- ISO 15118-1: General information and use-case definition
- ISO 15118-2: Network and application protocol requirements (TLS Transport Layer Security 1.2)
- ISO 15118-3: Physical and data link layer requirements
- ISO 15118-4: Network and application protocol conformance test
- ISO 15118-5: Physical and data link layer conformance test
- ISO 15118-6: Physical and data link layer requirements for differential Power Line Communication
- ISO 15118-8: Physical layer and data link layer requirements for wireless communication
- ISO 15118-9: Physical and data link layer conformance test for wireless communication
- ISO 15118-10: Physical layer and data link layer requirements for wired ethernet communication
- ISO 15118-20: 2nd generation network and application protocol requirements (TLS 1.3 ; bi-directional charging possible)

This standard (parts 2 & 20) includes secure communication protocols between the vehicle and the charging station.

# IEC 61851 Electric vehicle charging system

## IEC TC 69 developed a series of standards for electric vehicle conductive charging systems

- IEC 61851 covers the mechanical, electrical, communications, EMC and performance requirements for EV supply equipment used to charge electric vehicles, including light electric vehicles.
- IEC 61851 is divided into several parts as follows:
  - Part 1: General Requirements,
  - Part 21-14: Electric vehicle onboard charger EMC requirements for conductive connection
  - to an AC/DC supply.
  - Part 21-25: EMC requirements for OFF board electric vehicle charging systems.
  - Part 23: DC electric vehicle charging station
  - Part 24: Digital communication between a DC EV charging station and an electric vehicle
  - for control of DC charging

# Thank you!