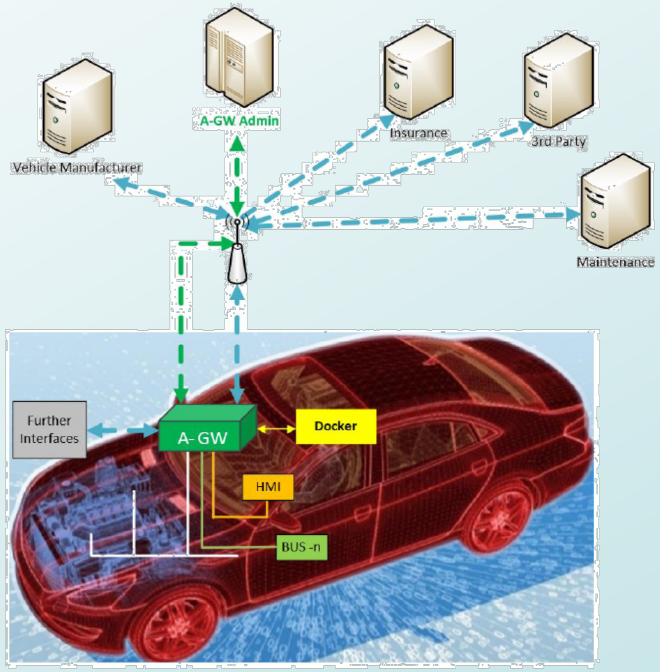
Informal document **GRVA-07-36**
7th GRVA, 21-25 September 2020
Agenda item 5(a)

OICA comments on WP.29-181-10



Source: WP.29-181-10

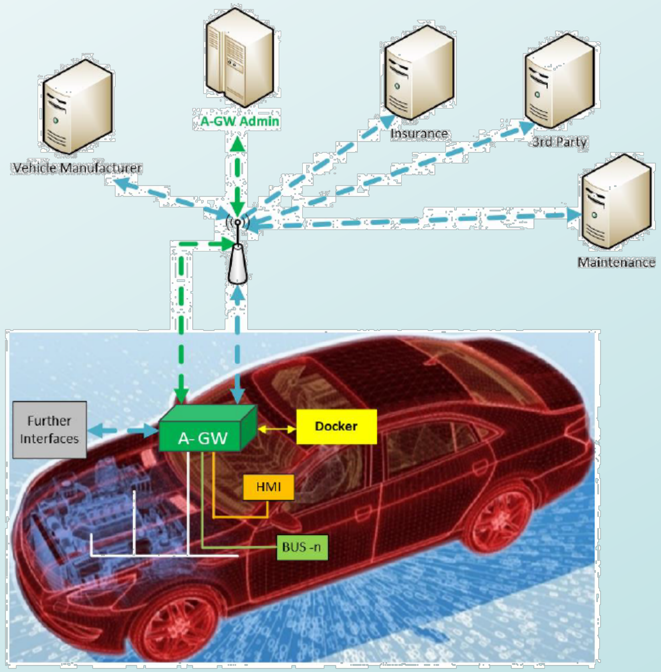
*: document WP.29-181-10, OTP = Open Telematics Platform

Content overview

FIA proposal on OTP Protection profile of an Automotive Gateway*

- Access to and modification of software and data on the vehicle by authorized third parties (non-restricted/unlimited read/write access)

- Introduction of an “Automotive Gateway” to be installed in each and every vehicle as “one and only” connection to the “outside world” (incl. every authorized third party)



Source: WP.29-181-10

- Introduction of an “Automotive Gateway Administrator” (neutral entity) as exclusive authorization body granting access

- Introduction of a Protection Profile for this Automotive Gateway (incl. Common Criteria)

*: document WP.29-181-10, OTP = Open Telematics Platform

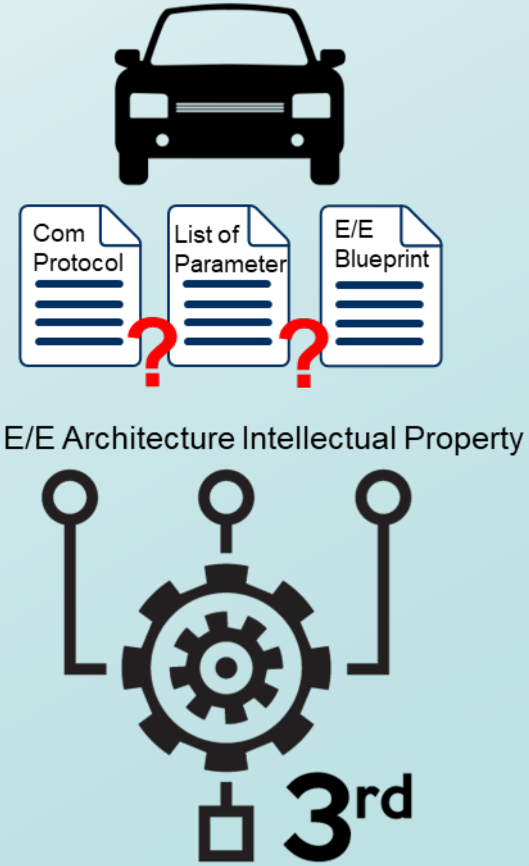
Issues identified

Access to & modification of data by 3rd parties (1/3)

- **Would this concept of unrestricted read-write-permissions require providing the detailed information (VIN-based) on internal vehicle communication of each and every vehicle on the road (e.g. communication matrix)?**

  If yes:

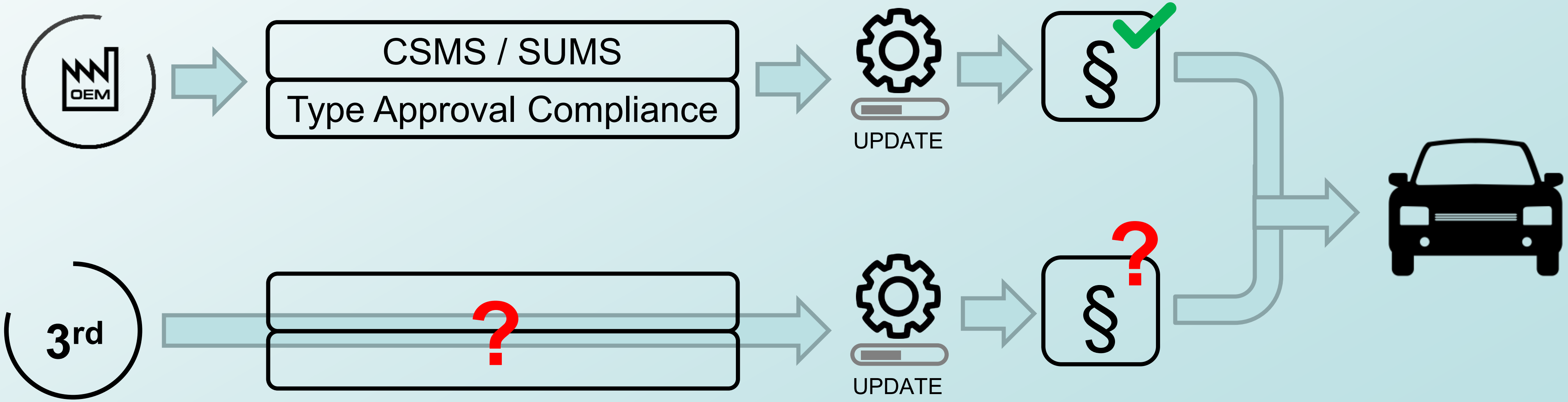
  - The requirement is far beyond existing Repair & Maintenance Information requirements
  - The capability and the way to access specific data depends on the specific configuration of each individual vehicle. It is hence VIN-based (depending on the trim level and options chosen, it may change after SW updates).
  - Intellectual property will be concerned.
  - How does a third party know which type of data is available on which individual vehicle?
  - Safety/security risk (see next pages)



Issues identified

Access to & modification of data by 3rd parties (2/3)

- **Changing software/data without OEM involvement creates**
  - Safety and security issues (operational and functional safety, cyber security etc.)
  - Responsibility / liability issues (Who will be held responsible in case of an accident?)
  - Change of type approval relevant software/data will affect the conformity of vehicles in the field
- **Tracking of software/data modifications**
  - Who is documenting 3rd party software/data modifications on each vehicle?
  - Will the 3rd parties be obliged to have a Cyber Security Management System and a Software Update Management System?

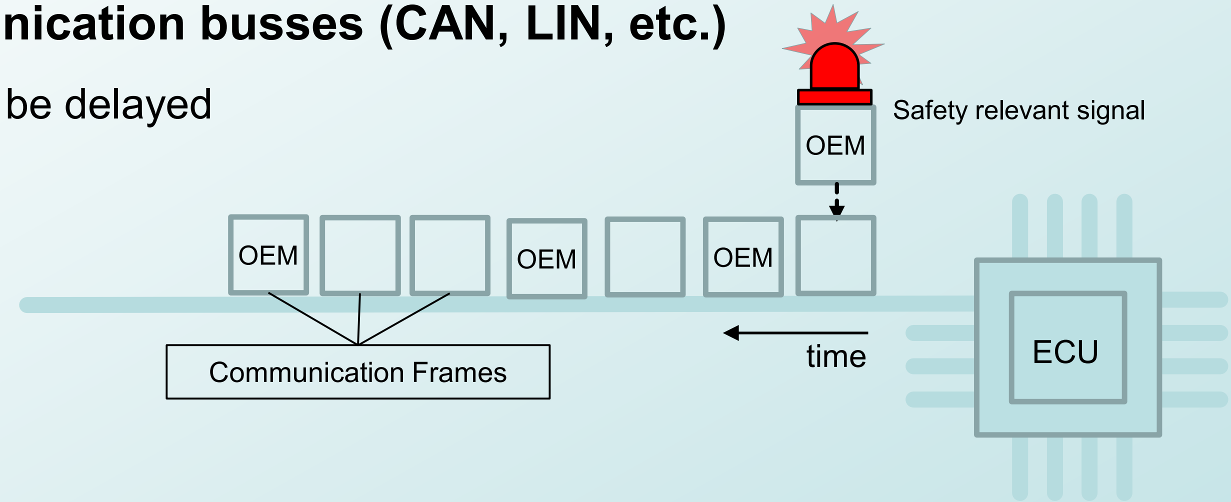


Issues identified

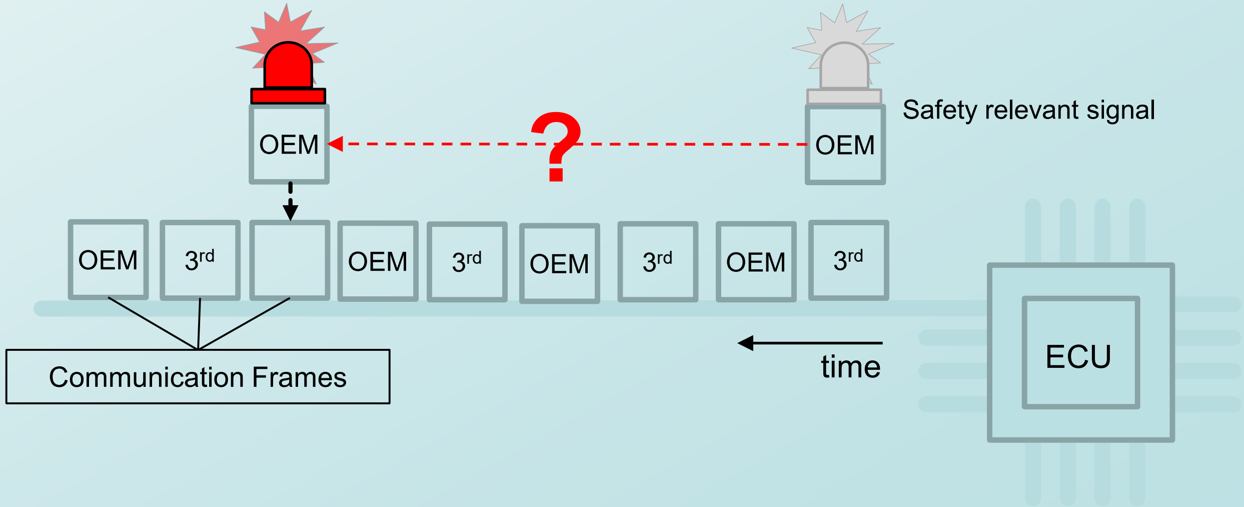
Access to & modification of data by 3rd parties (3/3)

- **Issue of increased traffic on communication busses (CAN, LIN, etc.)**
  - Delivery of safety relevant signals may be delayed

With **limited** access for third parties



With **unlimited** access for third parties



Issues identified

Automotive Gateway administration (1/2)

➢ **Purpose of the Automotive Gateway Administration: Granting authorized access for 3rd parties**

- Who should this entity be?
- Will this entity take over responsibility for safety/security and compliance to vehicle type approval?

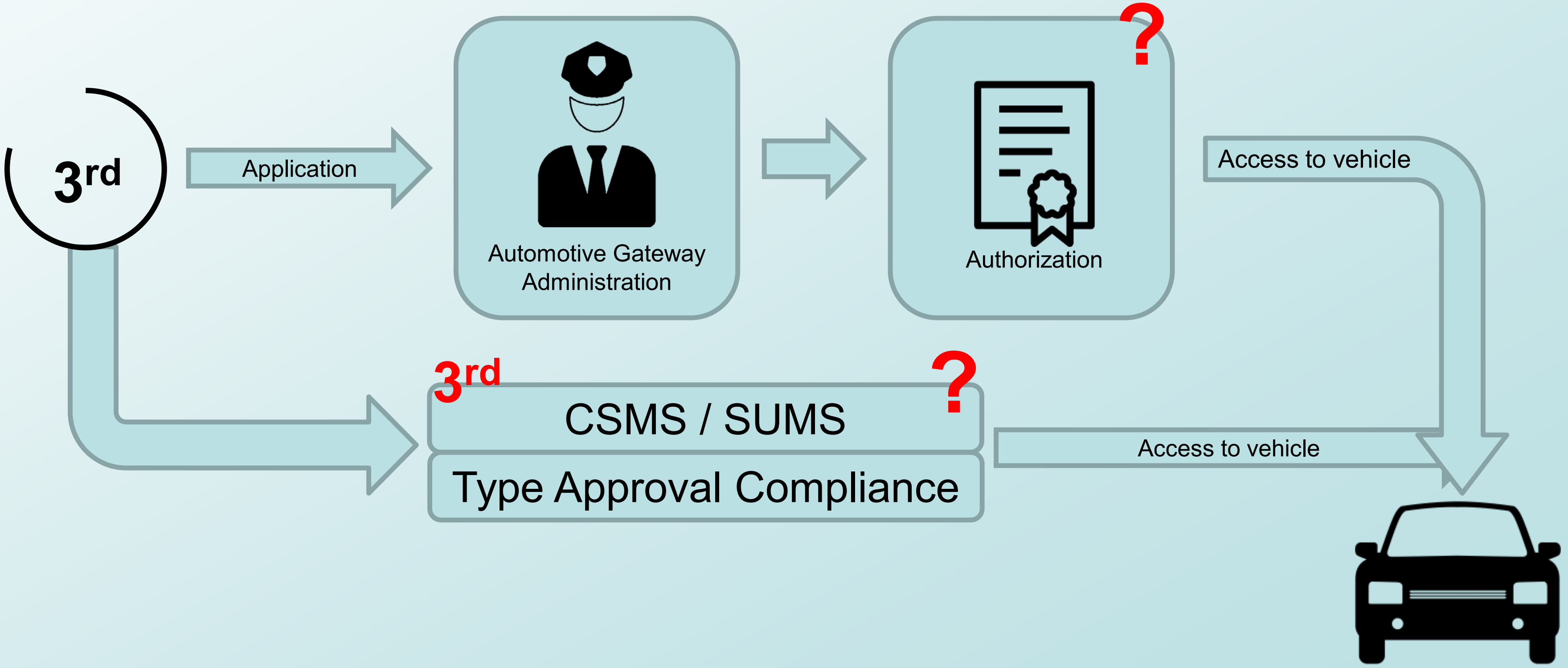
- On which legal basis should this entity act?
  Access to data is **NOT** regulated on UN level

Issues identified

Automotive Gateway administration (2/2)

➢ **Qualification/certification of 3rd parties receiving authorization**

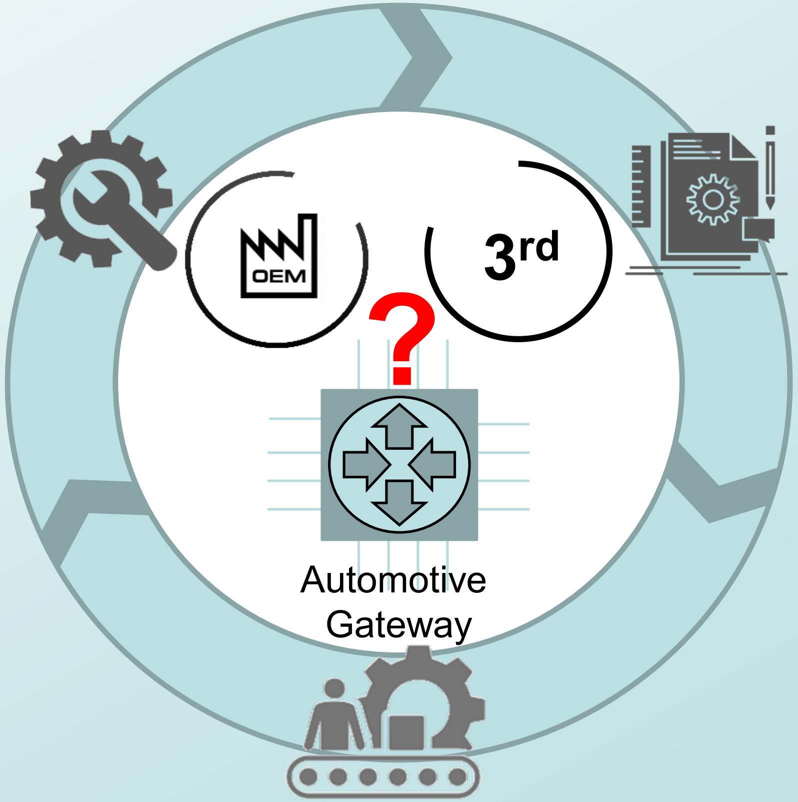
- On which basis?
- How will safety and security be covered?
- How will Type Approval Compliance be covered?
- Will the 3rd parties be obliged to have a Cyber Security Management System and a Software Update Management System?



Issues identified

Automotive Gateway device (1/4)

- Who is developing / manufacturing / certifying / maintaining this component?



Issues identified

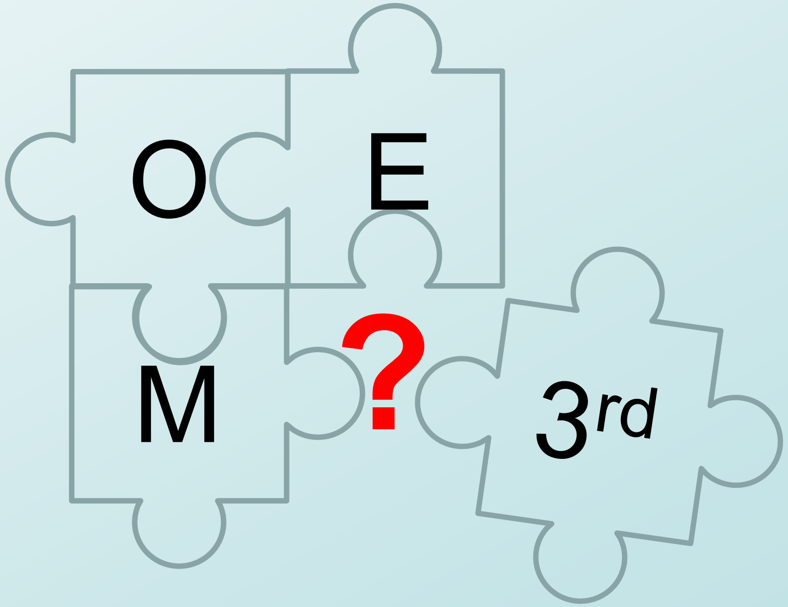
Automotive Gateway device (2/4)

- Who is overall responsible for the component incl. its safety and security?

Issues identified

Automotive Gateway device (3/4)

- How to ensure proper implementation within the different vehicle architectures?



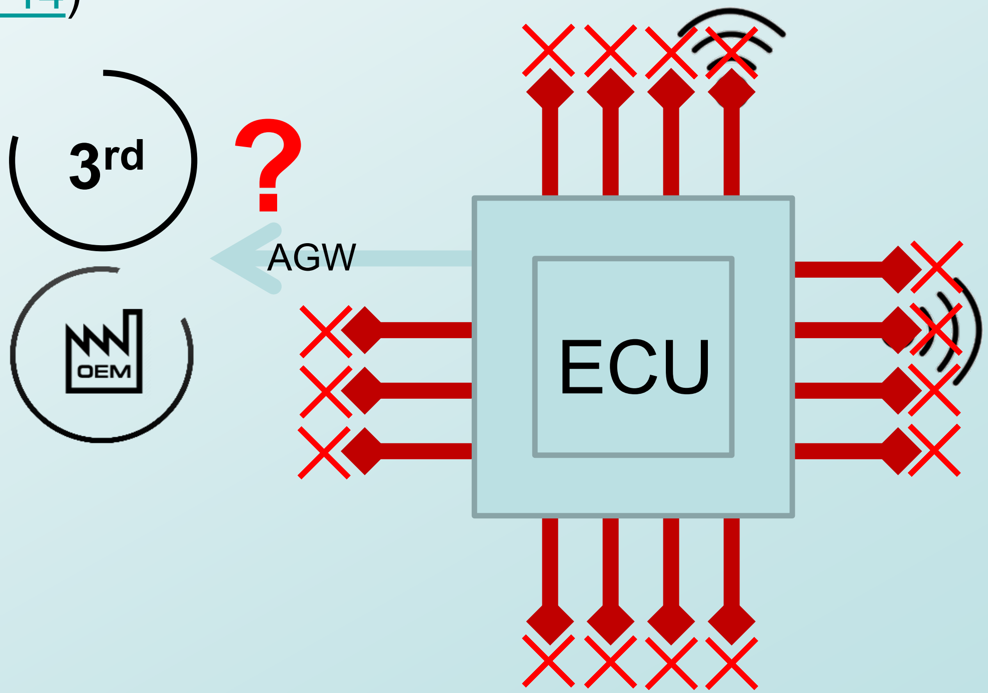
Issues identified

Automotive Gateway device (4/4)

- Is it the intention that the Automotive Gateway is the one and only communication channel between the E/E architecture and outside world?

- If yes, how is time critical communication ensured via this gateway (e.g. for ADAS)

- See also Annex (FIA Presentation TFCS 11-14)



Issues identified

Software/Data modifications by 3rd parties

- How will 3rd parties be required to follow the requirements of UN R 156 “Software updates”?
- How is a 3rd party required to conduct a risk assessment in context of safety and security before providing an update?
- How will the information on the software versions be documented and made available for the vehicles on VIN basis?
- How is compliance with Vehicle Type Approval ensured and who will be held responsible in case of non-compliance?

Industry concerns on FIA proposal

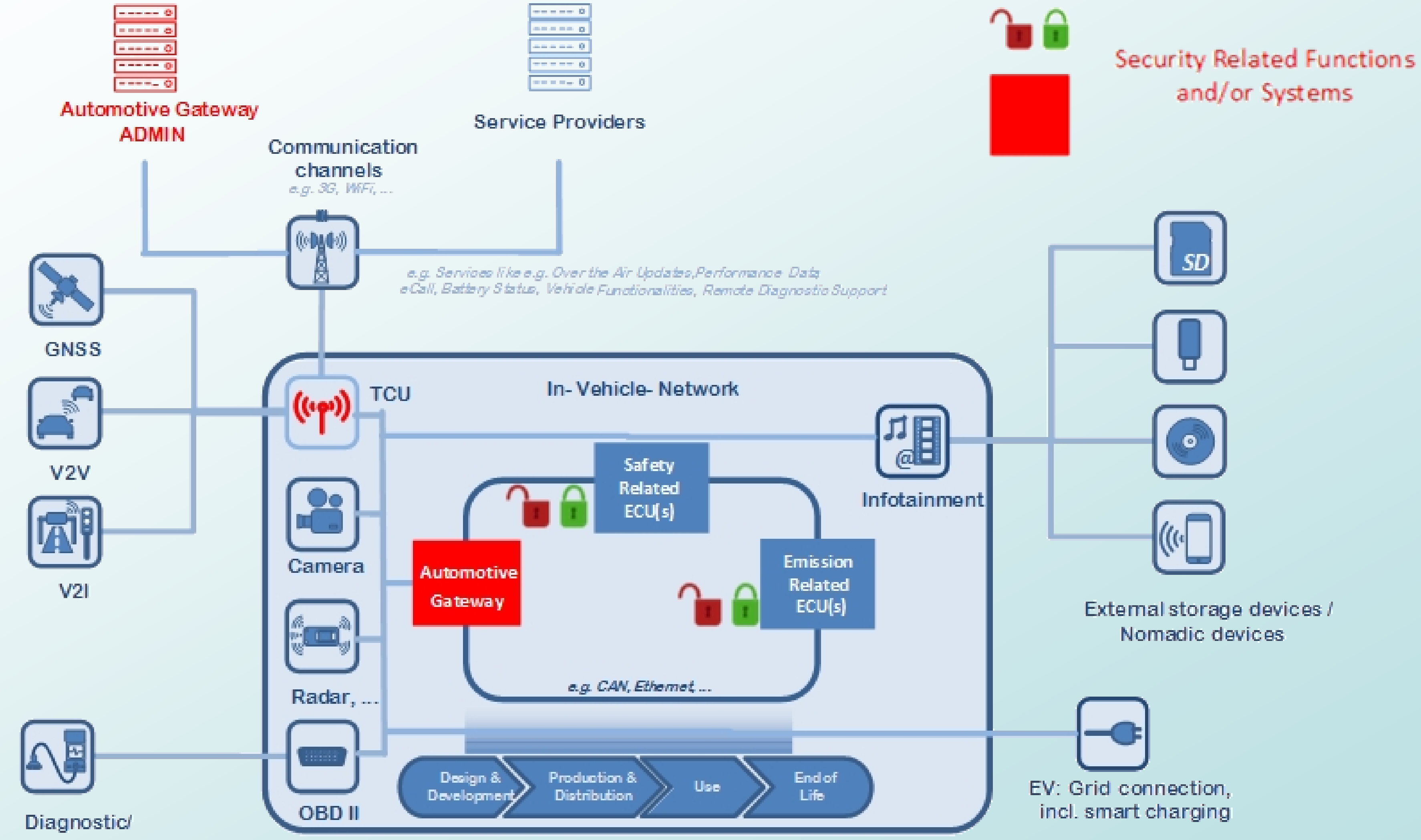
regarding OTP Protection profile of an Automotive Gateway

- **The Proposal is not technology neutral**
  - All vehicles would need to install a specific automotive gateway that responds to the requirements.
- **The Proposal requires the creation of a centralized and worldwide accepted agency**
  - Who shall create and finance this new agency?
  - Will this agency take the responsibility of vehicle safety/security and type approval compliance?
- **The Proposal creates new safety/security risks for the vehicle user**
  - Even if the communication with the automotive gateway is secured, it creates new safety risks for the vehicle user
  - Adding a new “door” to the system and “copy” the key for that door to all the authorized third parties creates more risk to “lose” the key
  - A vulnerability within the standardized access would not be limited to one vehicle but would impact all vehicles using this standardized access
- **The Proposal is not clear with regard to the responsibilities and compliance to vehicle Type Approval**

Annex

FIA Reference Model

TFCS-11-14



GNSS– Global Navigation Satellite System , V2V- Vehicle to- Vehicle , V2I– Vehicle to- Infrastructure , P/T– Powertrain , ECU– Electronic Control Unit , OBD- On Board Diagnostic