Informal document **GRRF-82-07**
82nd GRRF 20-23 September 2016
Agenda item 9(c)

FIA MOBILITY & TOURISM

Gerd Preuss,
FIA Representative at
UNECE, WP 29

A WORLD IN MOTION

Data Privacy and Cyber Security in (partly) Automated Driving GRRF Meeting, September 2016

FEDERATION
INTERNATIONALE
DE L'AUTOMOBILE

FIA.COM

- Summary
- Basic Principles of Data Privacy
- Data Privacy by Design and in R79
- Next Steps

Summary

- FIA welcomes, that data protection and cyber security are regarded as topics of high importance in ITS-AD as a general (technical) requirement
- Both topics are also relevant for partly automated driving like ACSF
- Data Protection must be implemented in the technical design of a vehicle
- Vehicle Owner/Driver has the right to send/receive Data from/to his vehicle, unless legal requirements like Automated Emergency Call System (AECS) are in place
- Data from the vehicle, that are related to VIN or the number plate are personal related data
- In ACSF no data storage (DSSA) is necessary, delete DSSA paragraphs

Basic Principles for Data Protection

- **Transparency**
  All data that are sent from/ received by a vehicle should be accessible for the vehicle owner/driver, e.g. via websites or directly via the infotainment system

  Independent assessments on the data records from/to the vehicle on compliance with the privacy policies should be encouraged at national level

  Every data transfer from / to the vehicle needs the consent of the driver/owner, unless legal requirements like AECS are in place

- **Data minimization and earmarking**
  Not all data that can be collected is actually needed for the purpose for which it is collected. Therefore, the principles of data minimization and earmarking data for specific uses should be mandatory requirements in the development of the applications

Basic Principles for Data Protection

- **Freedom of Choice**

  The vehicle owner/driver must decide, with whom he shares or does not share his vehicle related data and services, unless for legal purposes like AECS or tachograph. This requires a non discriminatory access to in-vehicle-data for all stakeholders

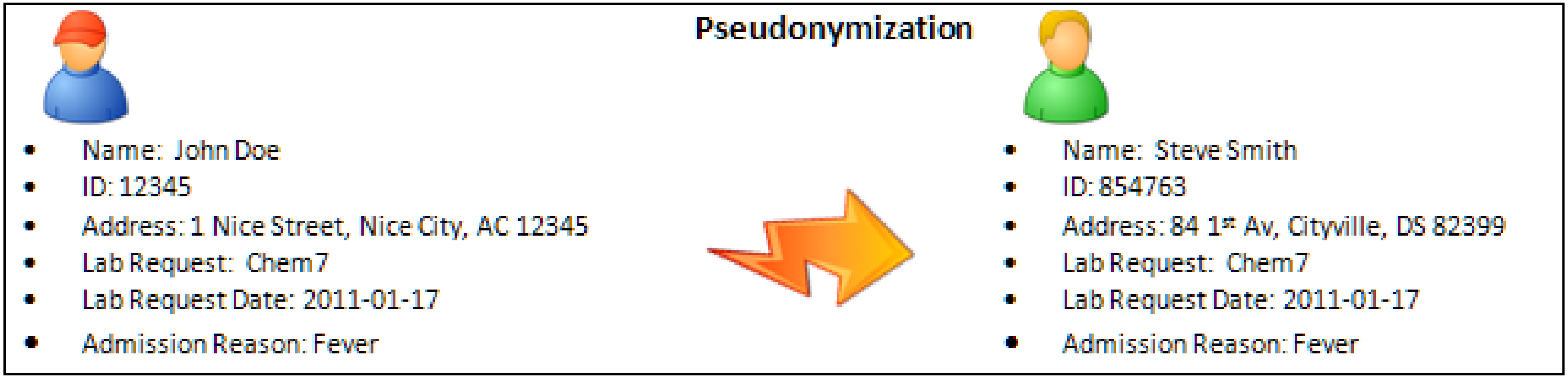
- **Security**

  Vehicles shall not only be safe, but also secure. The current fleet is not secure enough against hacking (e.g. odometer fraud, theft of vehicles with keyless go systems).
  FIA proposes to develop a protection profile according to common criteria according to ISO / IEC 15408 for vehicle security.

Data Privacy by Design

- **Pseudonymisation of Data**

  Personal Data, Company Data of others than VM, VIN and location enable the VM to record profiles of drivers.
  These data shall be pseudomised in any data transfer from / to the vehicle to ensure transparency



Pseudonymization

- Name: John Doe
- ID: 12345
- Address: 1 Nice Street, Nice City, AC 12345
- Lab Request: Chem7
- Lab Request Date: 2011-01-17
- Admission Reason: Fever

- Name: Steve Smith
- ID: 854763
- Address: 84 1st Av, Cityville, DS 82399
- Lab Request: Chem7
- Lab Request Date: 2011-01-17
- Admission Reason: Fever

Data Privacy by Design

- **Data Storage in ACSF (see R79 Draft 5.6.1.8) ?**

  FIA sees no need for data storage in the framework of ACSF

  In any category of ACSF resp. UNECE R79, the driver is responsible for the operation of the vehicle

  Only in fully automated driving vehicles, the recording of event data is necessary

Cyber Security in Vehicles

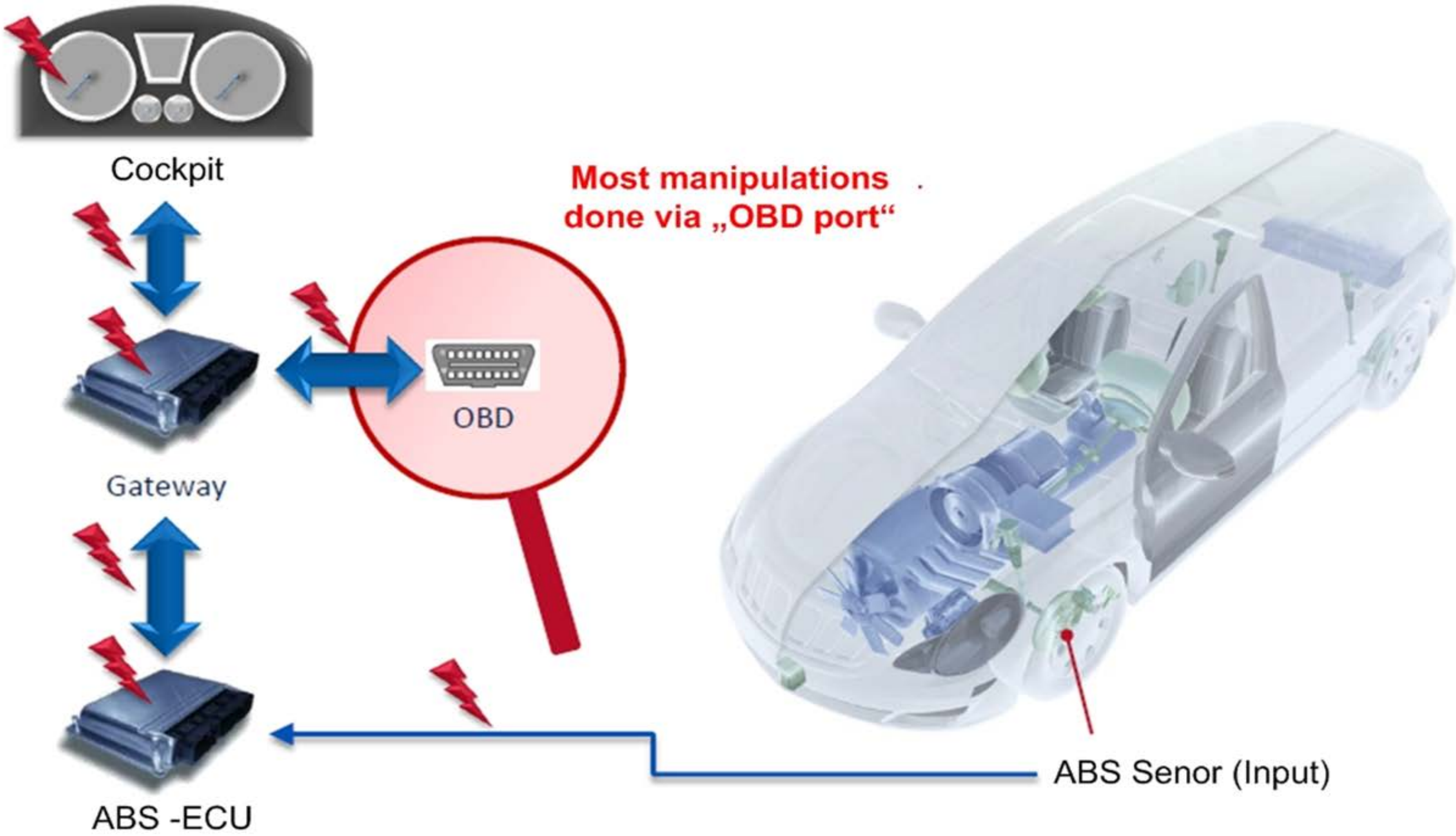
- **Functional Safety vs Vehicle Security**
  Current vehicles are design to fulfill highly sophisticated functional safety, E. G. ABS, ESP, ACSF.

  In contrast to this, IT security in vehicles is not up to date. The Vehicle Manufacturers are in favor to develop their own IT security systems, while IT experts (BSI) support the method of the Common Criteria.

  ADAC proved from a consumer point of view, that mileage fraud of odometers and theft of vehicles with keyless go systems is easily possible, due to the fact, that these systems are functional safe, but not cyber secured.

Cyber Security in Vehicles

- **Mileage Fraud**



There are 20 - 40 control units on-board of a vehicle that either store this information or retrieve it from the CAN bus

Cyber Security in Vehicles

- **Mileage Fraud**

Neither expert technicians, OBD rationality testing nor odometer tampering devices can definitively prove that a vehicle’s mileage has been reduced tampered with.

Odometers should definitively be protected with a technical solution that would effectively lock out tampering devices.
Such locks could also protect the vehicle from the deactivation of other important features such as seatbelt reminders or ignition interlocks.

A holistic (cyber) security approach with harmonized rules to ensure quality is needed.

Cyber Security in Vehicles

- **Mileage Fraud**

  In June 2016 the Technical Committee Motor Vehicles has adopted a new Euro 6 Regulation succeeding Regulation 692/2008/EC, supplementing Regulation 715/2007/EC. In this EU Regulation a number of odometer tampering prevention measures have been incorporated, which is a first step in the right direction and which will be applicable in the EU by September 2017.

  Odometer fraud is a cross cutting issue in all domains of type-approval.

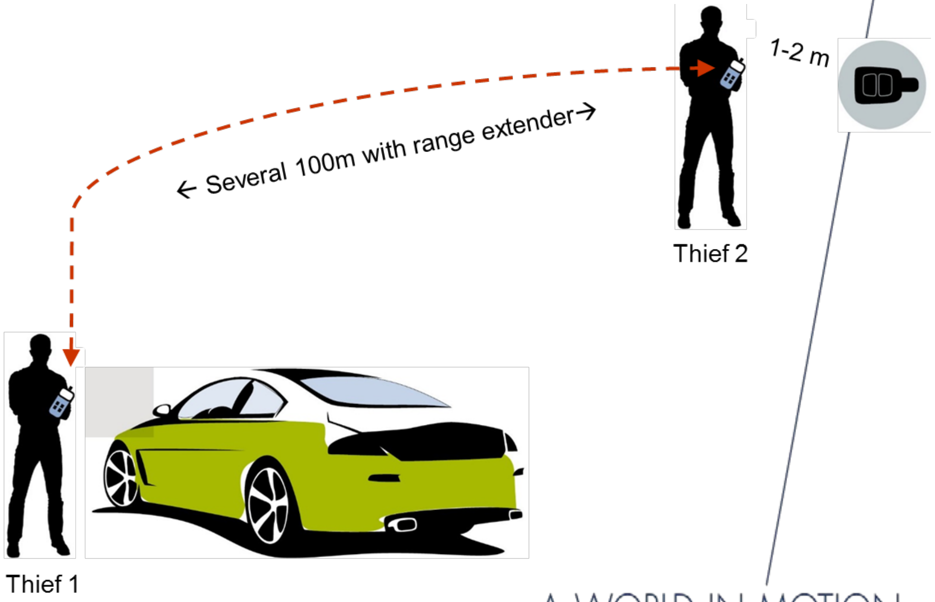
  A structural solution could be found if WP29 would give the mandate to GRSG and GRRF to address mileage fraud by amending UN Regulation No 39 (odometer and speedometer) and to do this within the shortest possible delays. Mileage fraud is an issue likely to occur on (partly) automated vehicles, but is today an actual, large scale problem for authorities and consumers alike on conventional vehicles.

Cyber Security in Vehicles

- **Theft of Vehicles with Keyless Entry System**
  ADAC engineers managed to hack the keyless vehicles in a matter of seconds and to drive off, leaving no visible trace of a break-in or theft. Because of their obvious security flaws, comfort keys are worryingly easy prey for thieves.

- It is easy to extend the range of the wireless communication between the key fob and the car by several 100m. In addition, similar technology can be used by thieves in order to disable immobilisers and alarm systems. Experts believe that off-the-shelf electronic components are all it takes to easily build a car theft device.

- **Lacking IT security allows "man in the middle" attack, functional safety allows theft!**



A WORLD IN MOTION

Cyber Security in Vehicles

- FIA proposes to pick up Cyber Security in type approval legislation, similar to functional safety requirements. FIA proposes WP29 to give combined mandate to GRRF & GRSG to establish new UN informal working group working on new Regulation on cyber security

- The type approval authority or a national accredited body must check the cyber security of the vehicle against a protection profile according to common criteria in ISO/IEC 15408.
  The vehicle manufacturer must meet this protection profile by his own proprietary measures against cyber attacks.

- Workshops and PTI Stations must be able to check during inspections, if the vehicle systems have been hacked or if any illegal software was installed, e.g by checking current hard- and software versions with informations from vehicle manufacturers

- The protection profile should be updated regularly

Next steps

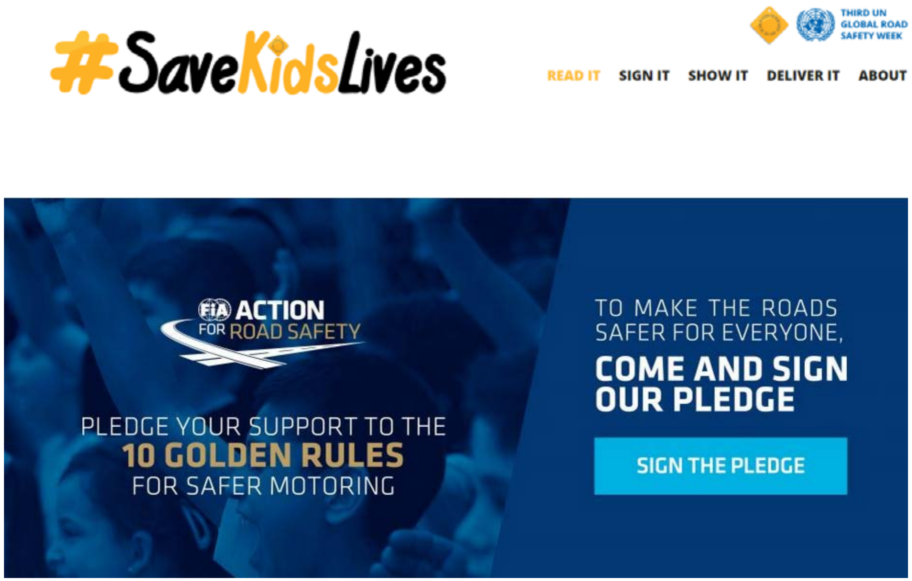
- FIA proposes a mandate from WP29 to GRRF & GRSG to establish a common informal working group. Goal: develop new UN Regulation for

  => cyber security

  => data protection

  => remote access to in-vehicle-data

  G7 determined, that cybersecurity and data protection is a growing concern from consumers; therefore all stakeholders have a responsibility to design appropriate regulation to ensure trust in new technology and connected vehicles



#SaveKidsLives

FIA ACTION FOR ROAD SAFETY

PLEDGE YOUR SUPPORT TO THE **10 GOLDEN RULES** FOR SAFER MOTORING

TO MAKE THE ROADS SAFER FOR EVERYONE,

COME AND SIGN OUR PLEDGE

01 BELT UP

02 RESPECT THE HIGHWAY CODE

03 OBEY THE SPEED LIMIT

04 CHECK MY TYRES

05 DRIVE SOBER

06 PROTECT MY CHILDREN

07 PAY ATTENTION

08 STOP WHEN I'M TIRED

09 WEAR A HELMET

10 BE COURTEOUS AND CONSIDERATE

Thank you for your attention