Submitted by FIA Document No. ITS/AD-10-06
(10th ITS/AD, 16 November 2016, agenda item 3-1-2)

FIA MOBILITY & TOURISM

Gerd Preuss,
FIA Representative at
UNECE, WP 29

A WORLD IN MOTION

Data Protection and Cyber Security in Automated Driving ITS-AD Meeting, November 2016

FEDERATION
INTERNATIONALE
DE L'AUTOMOBILE

FIA.COM

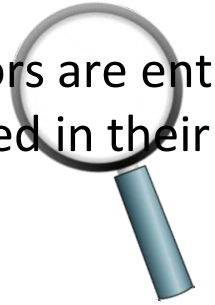
- Summary
- Basic Principles of Data Protection
- Functional Safety vs Cyber Security
- Cyber Security in Vehicles

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 systems like the ones described in Regulation 79 (ACSF)
- Data Protection and Cyber Security must be implemented in the technical design of a vehicle and the infrastructure (V2V; V2I)
- Vehicle Owner/Driver has the right to decide about what date is being sent/received from/to his vehicle, unless legal requirements like in the case of Automated Emergency Call System (AECS) are in place
- Certain data are per se primarily of a technical nature, it may be associated with the vehicle owner or driver via VIN and consequently constitutes personal data to which the Data Protection rules apply

Basic Principles for Data Protection

- **Transparency**
  Vehicle owners and/or operators are entitled to know what data is collected, transmitted, stored and received in their vehicles



- **Data minimization and earmarking**
  The principles of data minimization and earmarking data for specific uses should be mandatory requirements in the development of the applications

- **Freedom of Choice**
  The vehicle owner/driver must be able to decide, with whom he shares or does not share his vehicle related data and from who he obtains data related services

Basic Principles for Data Protection

- **Privacy by Design through Pseudonymisation of Data**

Even though certain data (e.g. actuation of the turn indicator) is per se primarily of a technical nature, it may be associated with the vehicle owner or driver via the Vehicle Identification Number and consequently constitutes personal data to which the Data Protection rules apply

Personal Data
Company Data of others than the VM
VIN
Location

} enable the VM to record profiles of drivers

These data shall be pseudonymised in any data transfer from / to the vehicle to ensure non monitoring by one party e.g. VM

Functional Safety vs Cyber Security

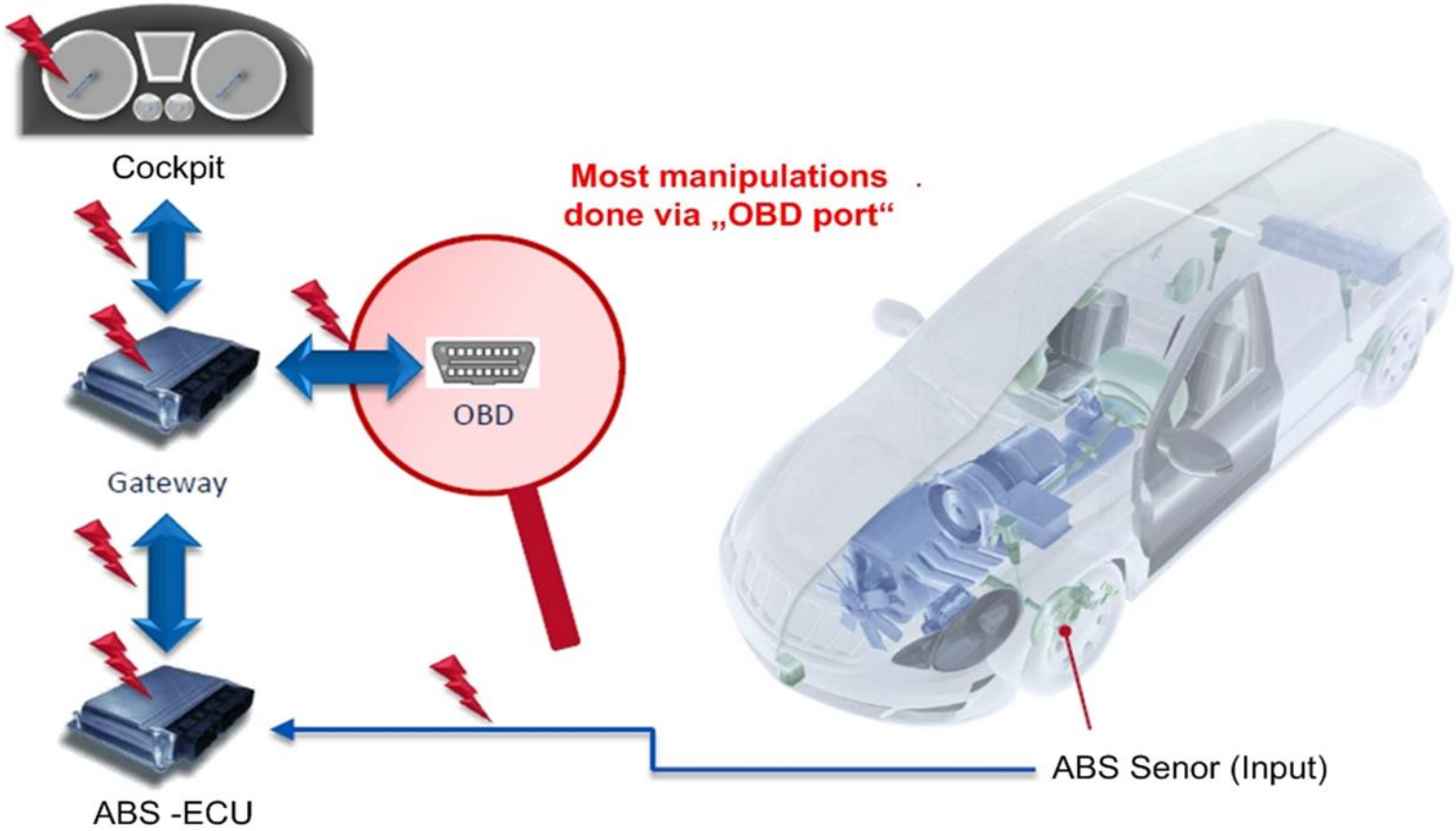
- **Functional Safety vs Cyber Security**
  Current vehicles are designed to fulfill highly sophisticated functional safety, e.g. ABS, ESP, ACSF

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

- FIA member ADAC proved, 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.
  The consequences hereof are to the detriment of the consumer.

Functional Safety vs Cyber Security

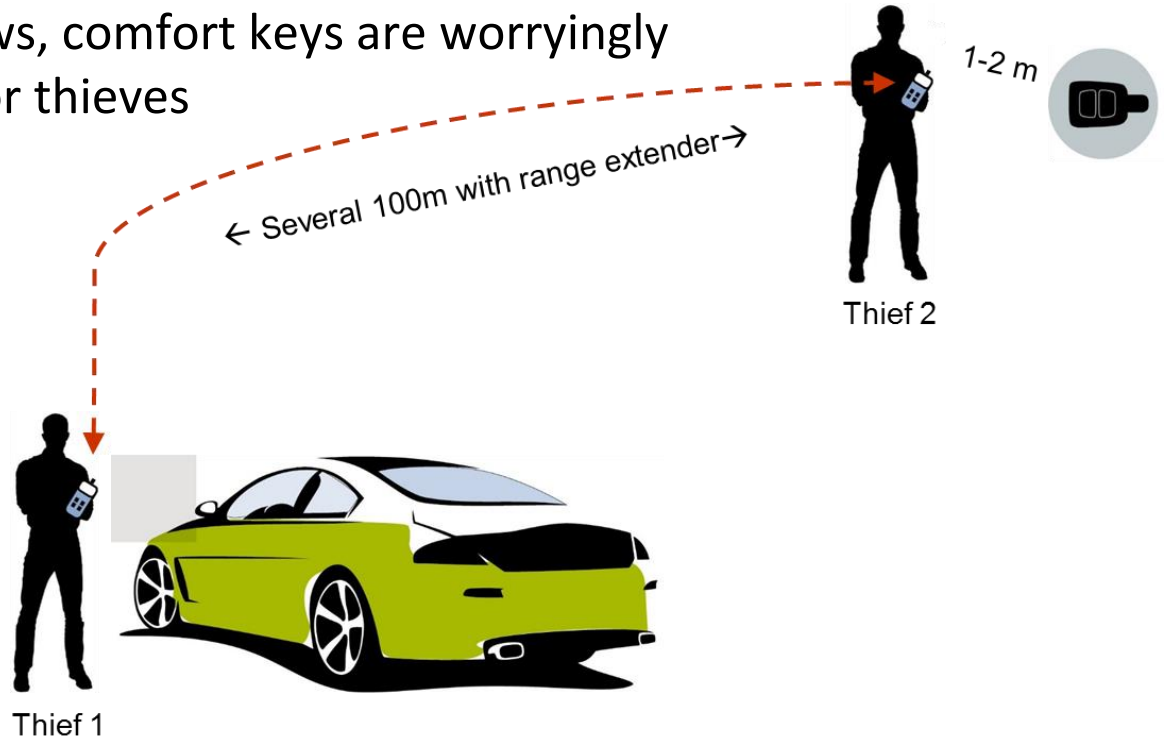
- **Mileage Fraud**



Functional Safety of the odometer is ok; but
lacking cyber security leads to manipulation

Functional Safety vs Cyber Security

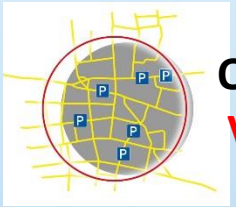
- **Theft of Vehicles with Keyless Entry System**
  ADAC engineers managed to hack the keyless vehicles in a matter of seconds and to drive off, leaving no visible trace of a break-in or theft. Because of their obvious security flaws, comfort keys are worryingly easy prey for thieves



Functional Safety of the keyless entry system is ok; but
lacking cyber security leads to theft

Cyber Security in Vehicles

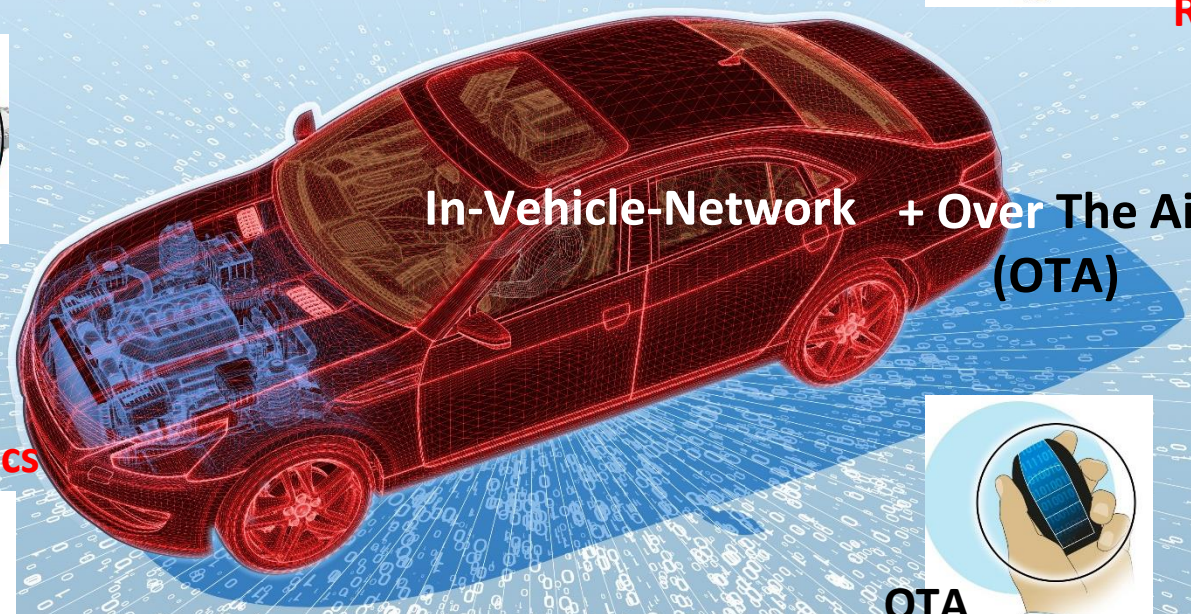
OVERVIEW



OTA
V2I

OTA
V2V

OTA
Music
Radio

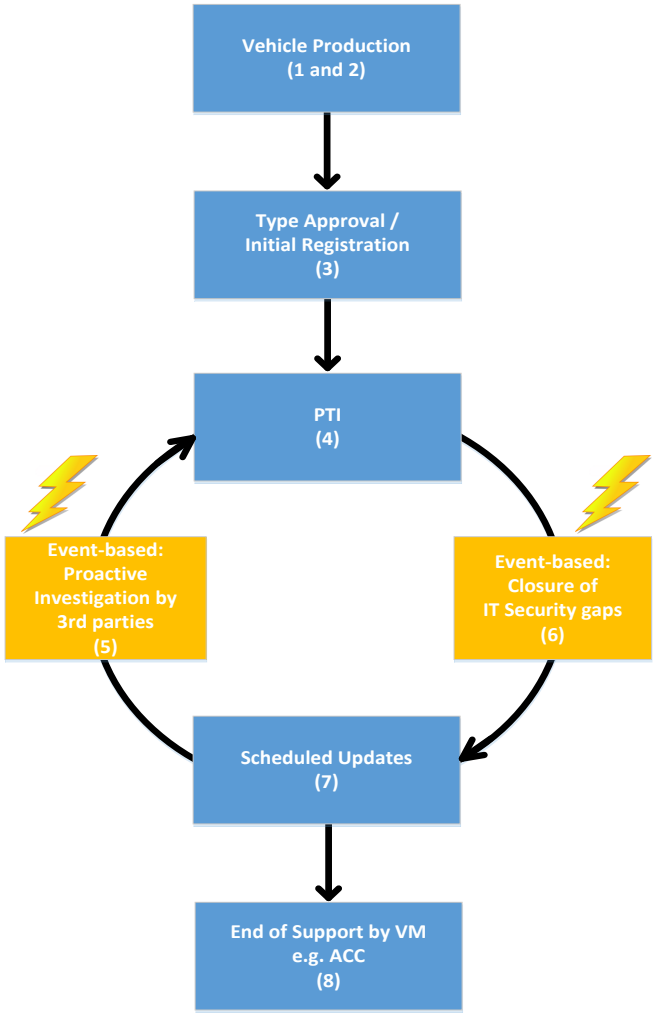


In-Vehicle-Network + Over The Air (OTA)

OTA
RDS
Prognostics

OTA
Keyless Entry

Cyber Security in Vehicles



- Cyber security starts with the technical design of a vehicle
- Type approval authorities must be able to check the security of a new vehicle against a protection profile
- During the lifetime of the vehicle, PTI stations must check, if the proper software is installed
- Event based measures must close loopholes, once uncovered
- End of support must be defined

Cyber Security in Vehicles

- A **general risk analysis** e.g. failure mode and effects analysis (FMEA) including all risks inherent to end-to-end connections such as backend or car-to-X, third party interfaces such as telephone, smartphone, OBD or radio should be performed (1)

- **Technology neutrality** is a general requirement of technical regulations (2)

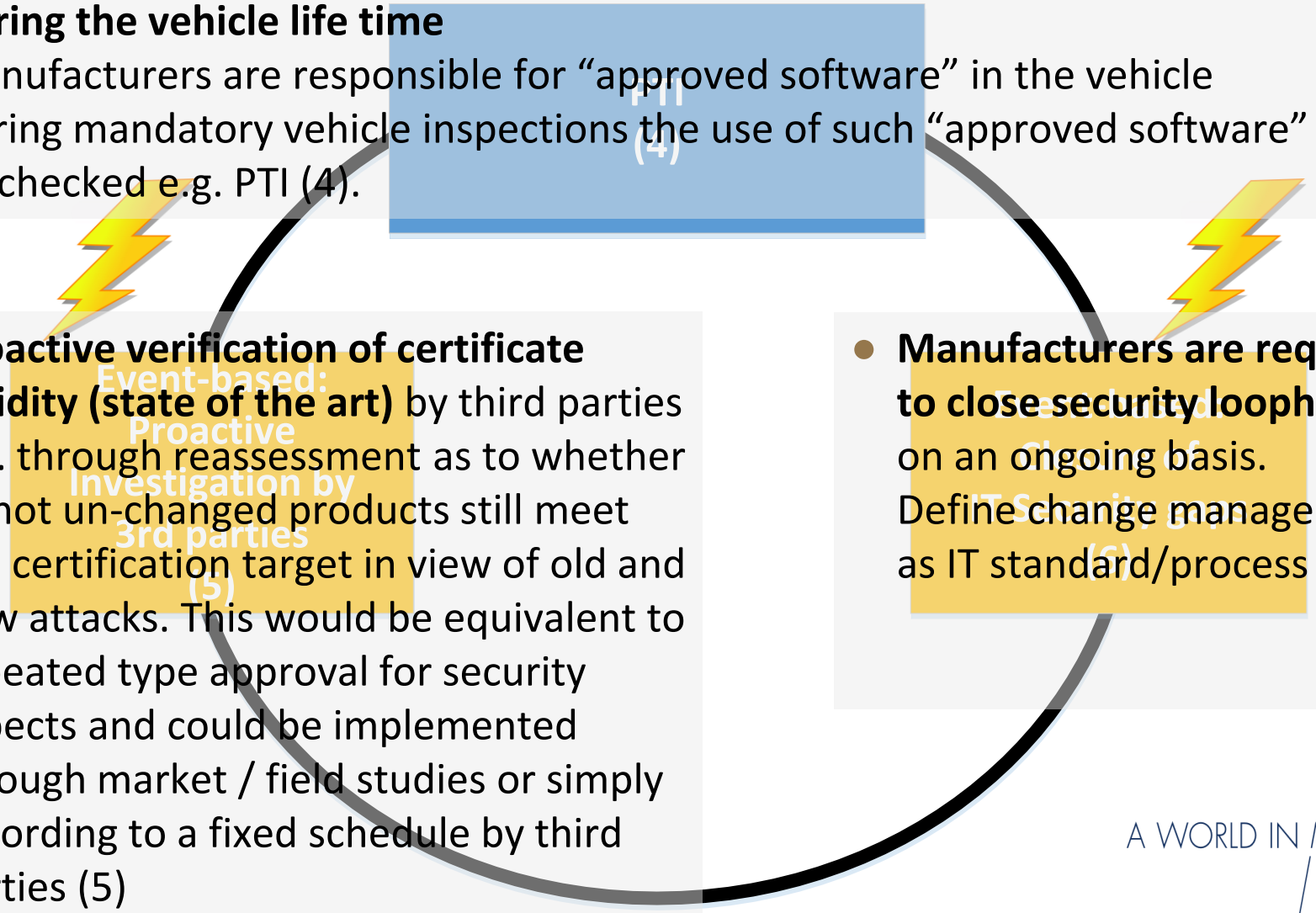
Vehicle Production
(1 and 2)

- **Verifiability / certifiability of type approval (3)**
  e.g. White box-principle: software screening by third parties based on internationally recognised protocols
  Stage 1: general risk analysis
  Stage 2: actually installed technical systems red

Type Approval /
Initial Registration
(3)

Cyber Security in Vehicles

- **During the vehicle life time**
  Manufacturers are responsible for “approved software” in the vehicle
  During mandatory vehicle inspections the use of such “approved software” should be checked e.g. PTI (4).

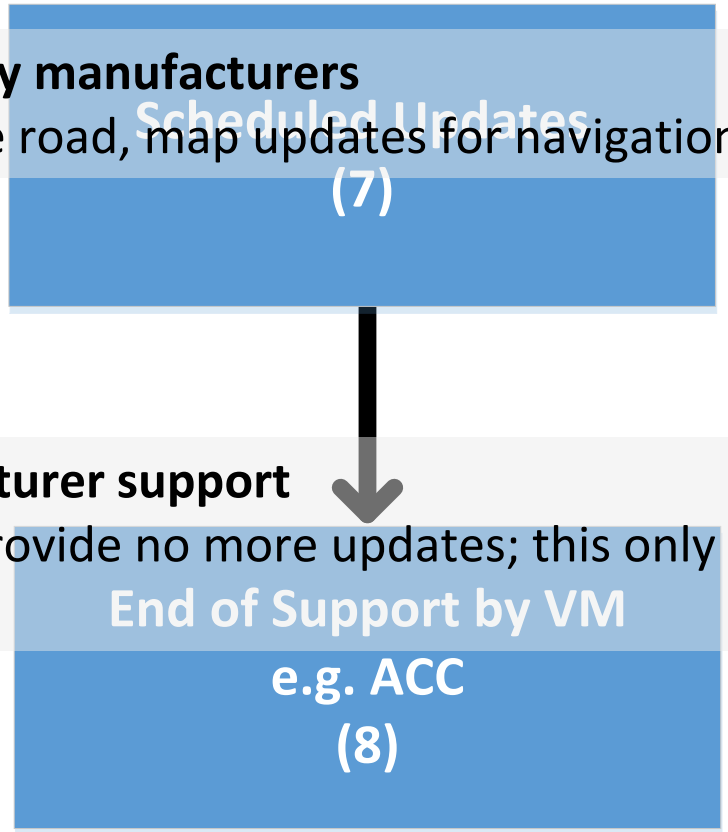


- **Proactive verification of certificate validity (state of the art)** by third parties e.g. through reassessment as to whether or not un-changed products still meet the certification target in view of old and new attacks. This would be equivalent to repeated type approval for security aspects and could be implemented through market / field studies or simply according to a fixed schedule by third parties (5)

- **Manufacturers are required to close security loopholes** on an ongoing basis.
  Define change management as IT standard/process (6)

Cyber Security in Vehicles

- **Scheduled updates by manufacturers**
  Amended rules of the road, map updates for navigation devices (7)



- **Phased out manufacturer support**
  Car manufacturers provide no more updates; this only affects assistance systems such as ACC (8)

While points 1, 2, 3, 4, 7 and 8 can be scheduled, points 5 and 6 are event-based and only occur after manipulation was uncovered

Cyber Security in Vehicles

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

- The type approval authority or a national accredited body must check the cyber security of the vehicle against a protection profile
  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

#SaveKidsLives

THIRD UN GLOBAL ROAD SAFETY WEEK

READ IT SIGN IT SHOW IT DELIVER IT ABOUT

Thank you for your attention