GRVA Informal Working Group on Cyber Security and Over-The-Air Issues

Dr Darren Handley

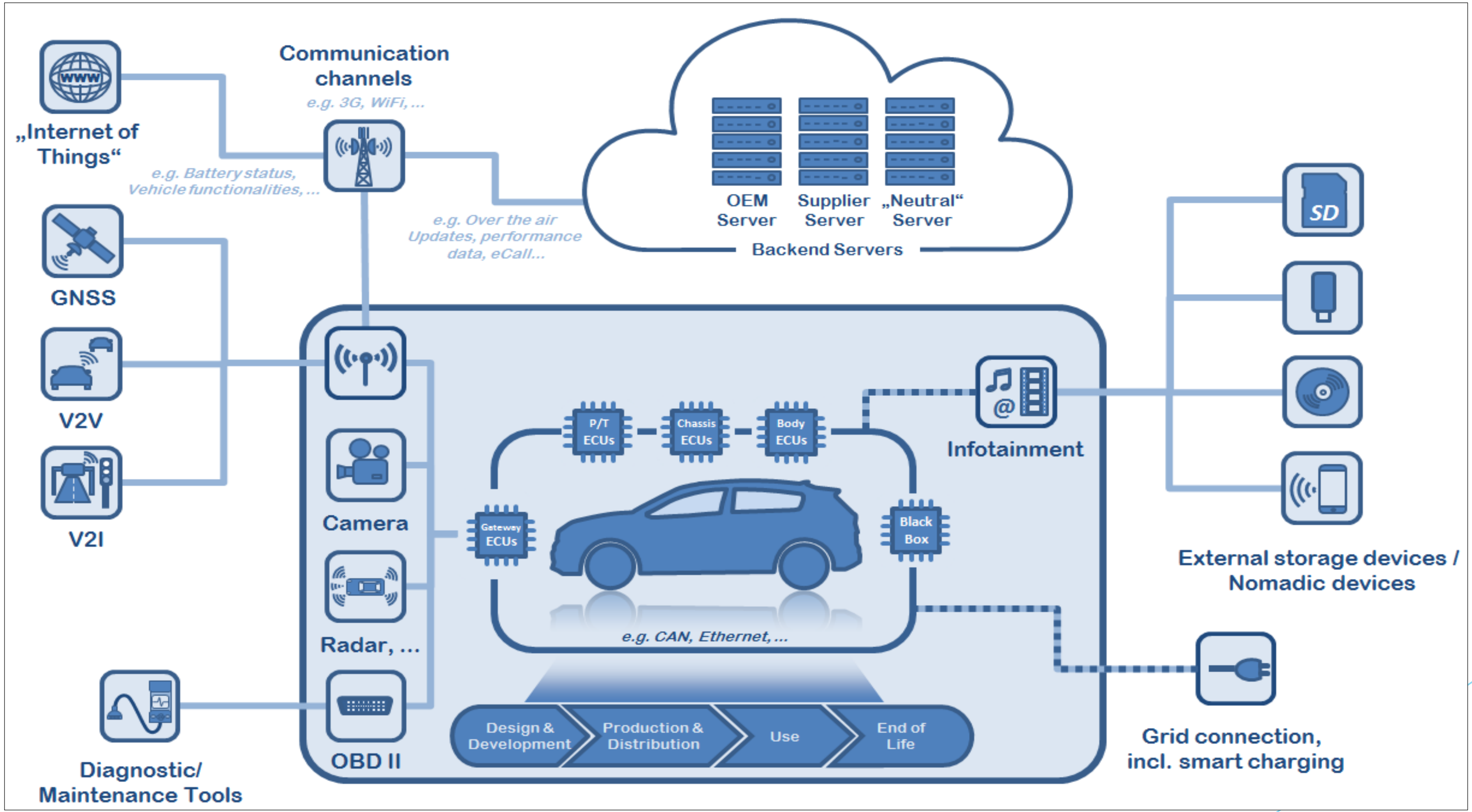
Contents

- Overview of the UNECE
  - Task Force on Cyber Security and Over-The-Air Issues
- Cyber security regulation
  - Overview
  - How assessments may be made
- Conclusions

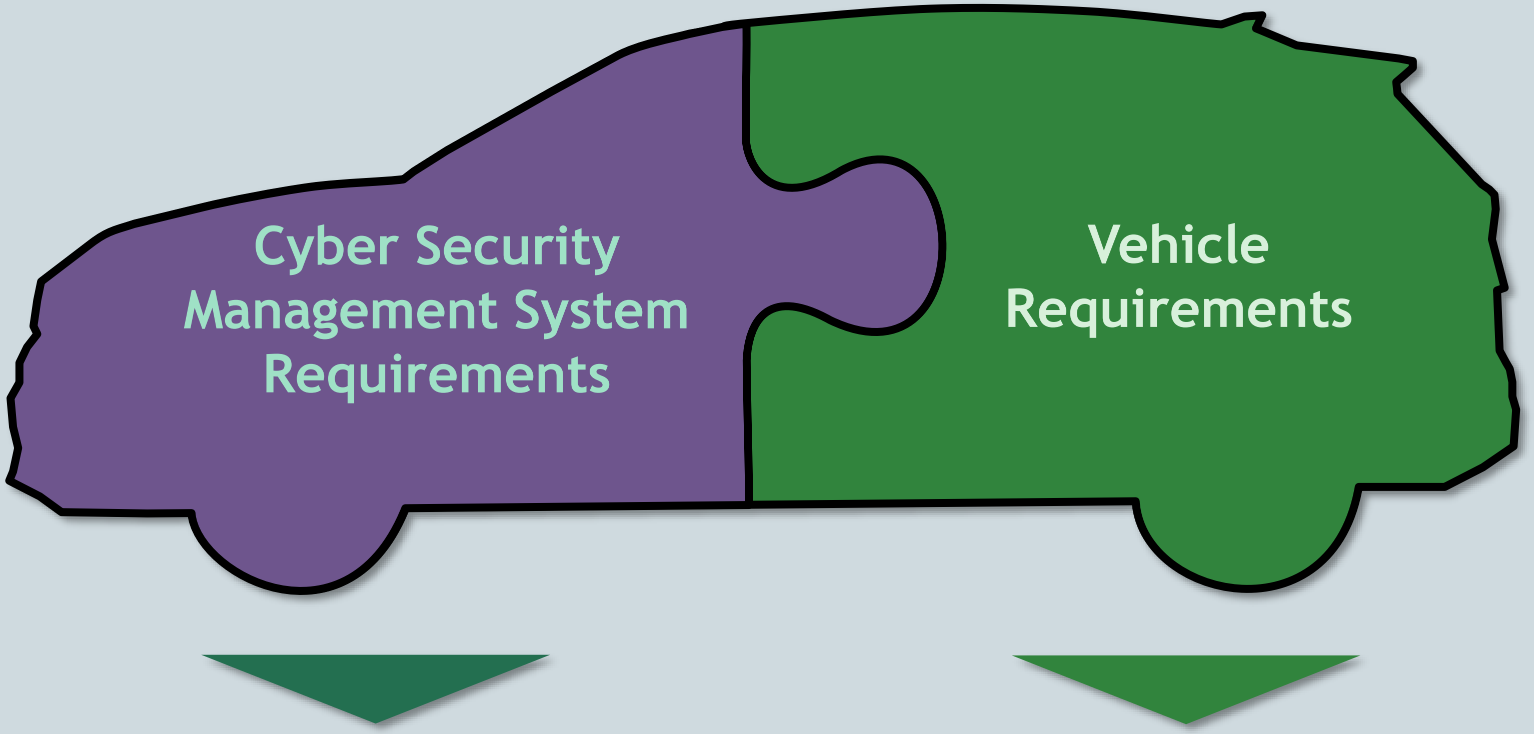
UNECE and the Task force

- On 21st December 2016 a task force was established to address Cyber Security and Software Over-The-Air Issues
- The task force contains experts from Contracting Parties and NGO‘s (CITA, FIA, ITU, OICA, CLEPA, ISO and others)
- Nineteen physical meetings have been held to formulate proposed regulations plus over thirty ad-hoc meetings (plus many side meetings). Typically 30-50 people attend.
- The current status is that a cyber security regulation for vehicles has been adopted by WP.29 under the 1958 agreement.

The vehicle ecosystem



The cyber security regulation



Cyber Security Management System Requirements

Vehicle Requirements

Organizational structure & processes

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

Cyber Security Management System

- This requires vehicle manufacturers to have, at an organisational level, the following:
  - Processes to identify and manage cyber security risks in the design of a vehicle
  - Processes to verify that the risks are managed, including testing
  - Processes to ensure that risk assessments are kept current
  - Processes to monitor for cyber attacks
  - Processes to assess if cyber security measures remain effective in light of new threats or vulnerabilities identified
  - Processes to respond to attacks
  - Processes to support analysis of successful or attempted attacks
- These processes must cover the period of a vehicle's life from its conception to the last of its type

Type Approval Requirements

- For every vehicle type that is declared and approval sought, the following must be provided:
  - Evidence that the CSMS applies to the vehicle type, particularly for vehicles in the field
  - The risk assessment for the vehicle type, identifying what is critical and the risks posed to them
  - Mitigations to reduce the risks identified to a justifiable level
  - Evidence, through testing, that the mitigations work as intended
  - Measures to detect and prevent cyber attacks
  - Measures to support data forensics
  - Monitoring activities specific for the vehicle type
  - Reporting the outcome of monitoring activities for a vehicle type to the relevant type approval authority and confirmation the mitigations implemented remain effective

Conclusions

- The regulations are based on the principle of risk-reduction not risk-elimination
- The regulation focuses on the vehicle but requires the vehicle risk assessment (and design) to take into account external risks, such as Intelligent Transport Systems.
- As vehicles become more automated and reliant on external data sources and communications, the security of those externalities will be as important as the security of the vehicle. The vehicle therefore needs to be designed (and maintained) with an awareness of the dependence it has on those externalities and how to manage the risks from them.
- People designing Intelligent Transport Systems need to consider the end-end security of their systems and how it may affect the security and operation of vehicles using them (and those not).