UNECE task force on cyber security and over the air updates

Presentation by Dr Darren Handley

- Mandate
  - Task force initiated January 2017
  - Aim is to address Cyber Security issues, relevant for the automotive industry
  - Consider existing and developing standards, practice(s), directives and regulations concerning cyber security and their applicability to the automotive industry
  - Consider what assessments or evidence may be required to demonstrate compliance or type approval with any requirements identified

- Cyber security paper – what does it do?
  - Outline of process envisaged
  - What the output may look like
  - Timeline: complete paper by summer!

Cyber Security and the work of a UNECE task force

1. OEM gains approval of their cyber security procedures, covering:
   - Risk assessment process to be used is suitable
   - Suppliers will be managed appropriately
   - Risk monitoring and incident response plans are adequate

1. New Vehicle Type

2. OEM assesses possible cyber risks to the vehicle and its systems and designs in suitable mitigations

3. OEM records: the vehicle, it systems and key component parts; the risks posed to them; and the mitigations implemented or actions undertaken to reduce the risk to the vehicle

4. Type Approval Authority assesses actions undertaken by OEM based on the information supplied

5. Type Approval Authority provides type approval if satisfied

6. Type Approval Authority periodically validates that the processes used and decisions made by the OEM remain valid

2. 6. OEM has plans in place to respond should the risk profile of the vehicle change necessitating action (e.g. software update)

What the output of the task force looks like:

- Guidance section, describes process and procedures for cyber security:
  - Describes outcome based objectives (principles) organisations should look to achieve
  - Details various threats and mitigations OEMs and their suppliers should consider in the design and development of vehicle systems
- Regulation section, provides for:
  - Approval that an OEM has identified and assessed the cyber risks to a vehicle and applied appropriate mitigations in its design
  - Approval that an OEM has suitable processes to support the vehicle post production should the need arise.
- Key points:
  - The regulation would be based on a subjective assessment by an authority
  - It requires the OEM to detail how the systems in a vehicle may be attacked and what measures have been implemented to protect them