Transmitted by the expert from France Document No. ITS/AD-08-06
(8th ITS/AD, 9 March 2016, agenda item 4)

French views on cyber-security with regards to type-approval on connected vehicles

Key issues :

- Number of connected vehicles will increase seriously in the next decade, even for lowcost vehicles, notably due to mandatory systems as ecall.

- The cyber risk shall be taken into account as soon as possible as a mandatory part of type-approval for a clarification of rules for the manufacturers and the suppliers

- Therefore, the common approach on cybersecurity should be an addition of requirements on cybersecurity directly to UN regulation

- As all new vehicles will in the future be concerned by this problem, it would be appropriate to include requirements on cybersecurity in ECE R10 (electromagnetic compatibilty) or ECE R116 (protection against unauthorized use), or to built a new dedicated UN regulation for M/N categories

- Requirements should be based on international standards already existing, notably for other activities than automotive industry

- Adding new requirements in automotive regulation will impose to the manufacturers cyber protection systems to be tested and validated before entering into service

- Question on over the air updated software version or new security patch for cars already in the market, shall be taken into account

French proposals :

<u>Recommendations for security of the next-generation car</u>

- Architecture and network security : all stakeholders must adopt as soon as possible a "secure by design" for the sofware and the hardware. This can result in partitionning, filtering, hardenning configurations, embedded security mechanisms, defence in depth, encryption, managing removable media....

- Required convergence of Safety and Security approachs : wich may be illustrated by a change in the "automotive safety integrity level" proposed in ISO 26262.

- Certify and qualify all sensitive devices : for exemple the electronic control units (ECUs).

- Ensure to upgrade softwares to fix vulnerabilities, even if this increases the attack surface : both ways of doing, via "On Bord Diagnostic" plug (OBD) or "Over The Air" (OTA). This two methods require strict and appropriate mesures.

- Operational security, supervision, detection and incident handling : use Intrusion Detection System (IDS) to detect and prevent attaks. Log all security events for forensic investigation and data analysis. The overall monitoring and response could be build in a near future on a Security Operating Center (SOC) and on a Computer Emergency Reponse Team (CERT) like in others fields.

All these recommendations and a risk analysis should contribute to a new frame of the repository for a car security approval.
Before the placing on the european market of a vehicle, an audit of compliance with these standards should be carried out (especially pentests).