Information on Joint ISO/SAE Standard to address Cyber Security

Submitted by the OICA Experts
UNECE IWG ITS/AD Adhoc Meeting

Geneva, 19.09.2016

Addressing Cyber Security

Why do we propose a separate „Automotive Security Engineering“ Standard:

- Security has more assets than only safety (Money, Law, Operational, etc.)
- It needs different expertise, knowledge, methods and aspects
- The risk models are different, security risks emanate from malicious human intelligence, safety risks a due to natural occurence
- An own standard is easier to manage and maintain than a combined one

Why the Industry proposes a standard for Automotive Security :

- It is a cross domain topic (hardware, software, systems engineering, etc.)
- It covers more aspects than only secure data communication (immobilizer, chiptuning, ecu hardening, DRM, privacy, etc.)

Main Parts to Cover by the New ISO/SAE* Standard

The Standardisation Proposal contains three main parts:**

Part 1 - Vocabulary

1 Scope
2 Normative references
3 Terms and definitions
  3.1 Security Vocabulary
  3.2 Automotive Engineering Vocabulary
  3.3 Roles in the automotive security process
4 Index in alphabetical order

Part 2 - Management and Supporting Processes

1 Scope
2 Normative references
3 Terms and definitions
4 Management of the Automotive Security Engineering Process
5 Supporting processes

Part 3 - Item Development

1 Scope
2 Normative references
3 Terms and definitions
4 Risk Analysis
5 Protection measures specification
6 Implementation
7 Verification and validation of security requirements
8 Release for production
9 Operational phase planning

---

* The agreement for an together standard is signed, therefore the coverage is worldwide over the different markets
**Main Chapters overview only, Subchapters are not illustrate