Proposals for General Guideline for eSecurity

1, Introduction

- Since automated driving technology for vehicles are in the process of being enhancement, a cyber-attack risk via an internet etc. will rapidly tend to increase in the world. (The attacker potentially access to such automated driving technology for vehicles, and it can be attacked many vehicles.)
- In an activity of WP29, WP29/GRRF/ACSF IG has been developing the amendment of R79 for ACSF. After the date of entry into force of this amendment, the vehicles with more advanced automated driving technologies will be deployed to the future market.
- In other aspects from automated driving, the protection of individual information may be violated by cyber-attack to vehicles.
- Having regard to the near future situations, WP29 should establish a general guideline in terms of vehicle construction for considering the cyber security to the manufacturer.
- The protection measures for the cyber-attack need to be taken appropriately depending on each automated driving technology. Besides, the security measures must be ever developed for protecting from a new type of cyber-attack which will be escalating day by day.

2, Proposal

2.1 Guideline for relevant activities on eSecurity in WP29

- This guideline specifies for the Category E under examinations of R79 amendment for the time being. This guideline will need to review before the introduction of automated driving technologies of level 3 or higher in the future.
- The guideline does not describe specific cyber security technologies, management requirements of cyber security and so on for the vehicle in view of followings.
  (1) The guideline should not give a hint for cyber-attack to the attackers.
  (2) The measures for cyber security need to be continuously advanced depending on a new type of cyber-attack.
  (3) Since automated driving technologies as well as the related cyber security measures are still evolving, automotive cyber security measures can not be defined one way at this moment.
- When UN Regulation with regards to the cyber security would be considered in the future, the appropriate requirements should be developed with thorough consideration of specific issues in case of cyber security for practical test procedures for type approval and the criteria, etc..

2.2 Guideline for general cyber security measures for vehicles

1. The vehicle manufacturers shall design to protect appropriately the on board information including the programs, the personal data, etc.

2. The vehicle shall be designed to avoid fraudulent manipulation to the software of automated driving technology as well as fraudulent access of the board information caused by cyber-attacks through;
   - wireless connection
   -wired connection via the diagnosis port, etc.

3. When the system for automated driving technology detects fraudulent manipulation by the cyber-attack, this shall be warned to the driver and stop the function of automated driving system.

4. Vehicles should have a function to discriminate on-board networks from any (network) channels which are connectable to other vehicles or off-vehicle objects.

5. Drivers can take over vehicle control in any case of automated driving. Control systems of vehicles should be designed to allow giving control initiatives to drivers during or after cyber-attack. As the principal in Automated Driving of WP29, drivers are obliged to pay attention to vehicle control in any cases.(for Level 3)