A proposal for approach to proceed work in Cybersecurity TF

Japan

(Security TF of ITS/AD 21. Dec. 2016)

Background

１. Recent vehicles install electric actuators for the mechanism to control steering, breaking… Such electric actuators are commanded by ECUs. This means that there is a potential to control these mechanism by the results of ECUs’ processing without drivers intentions. This is a common concern for vehicles include conventional and automated drive vehicles.

２. Information and entertainment services which are provided by on board systems require a variety of connections between the vehicles and off-vehicle/on-vehicles devices. On the other hand, such connections could increase the threat of attacks.

Background

3. Personal data, such as ID, destination, should be protected carefully.

Clarifying necessary measures in WP.29 are required. The “Guidelines on measures ensuring cybersecurity and data protection of connected vehicles and vehicles with Automated Drive Technology” was developed as the first step.

Proposed work items

a. Construction of revised version of the “Cybersecurity guideline”

This item includes additional possible items such as, OTA, software integrity etc…

b. Construction of proposal for the next step

The next step includes a proposal of guidance to suggest necessary measures on security for relevant IWGs in WP.29, to ITS/AD.

Work item
a. Revision of “Cybersecurity guideline”

a. Revision of “Cybersecurity guideline”

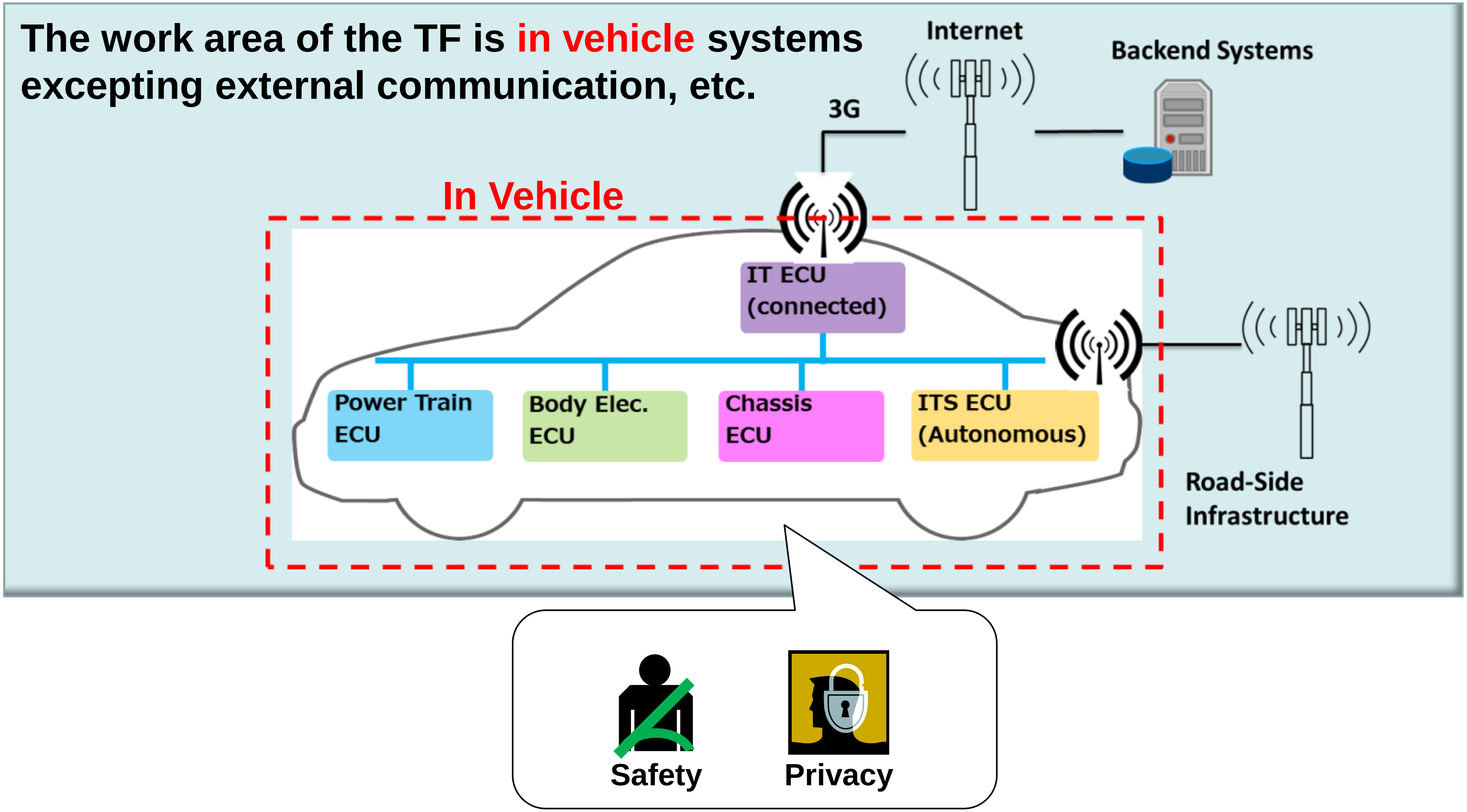
Step 1
Review of the “Cybersecurity guideline” by ITS/AD

- Finding technical missing points and making issues clear

Step 2
Develop countermeasures to the issues

Step 3
Drafting the amendment of the “Cybersecurity guideline”
(~mid of 2018?)

a. Revision of “Cybersecurity guideline”

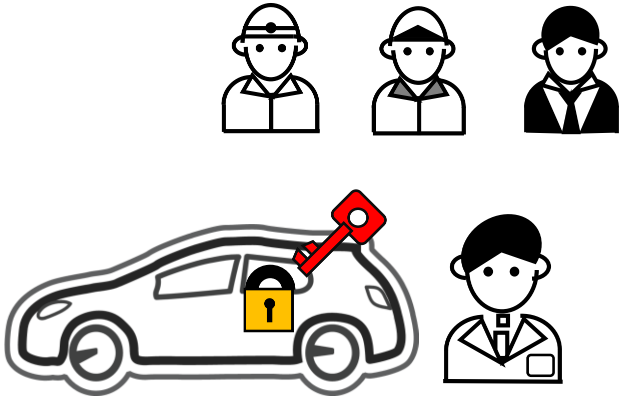


The work area of the TF is in vehicle systems excepting external communication, etc.

Reviewing the context of the “Cybersecurity guideline”

Major points in the preamble part

- The guideline is intended to present requirements to automotive manufacturers, component/system suppliers and service providers
- This guideline is intended as interim guidance until the completion of on-going research and collaboration activities and the development of more detailed globally harmonized requirements on cybersecurity and data protection.
- The manufacturer, supplier and service providers shall respect the principles of data protection by design and data protection by default
- For cybersecurity and data protection required steps shall be checked, e.g. system checks by external organizations.

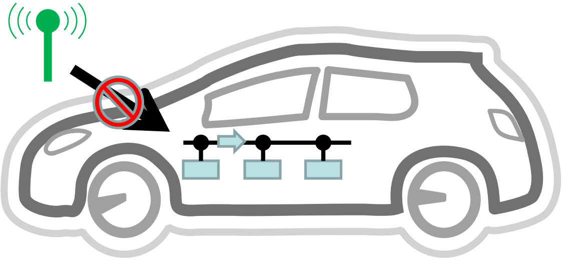


Reviewing the context of the “Cybersecurity guideline”

- The connection and communication of connected vehicles and vehicles with ADT
  - ➢ shall not influence on internal devices and systems generating internal information necessary for the control of the vehicle with appropriate measures.
  - ➢ shall be designed to avoid fraudulent manipulation to the software of connected vehicles and vehicles with ADT as well as fraudulent access of the board information caused by cyber-attacks through;

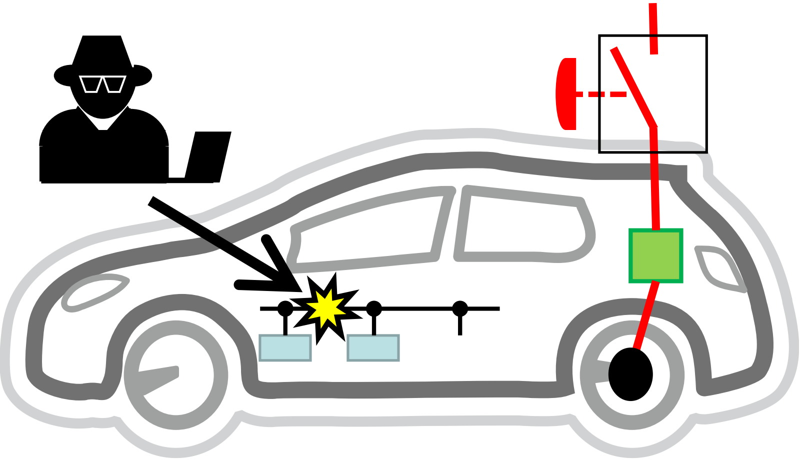
    - wireless connection / - wired connection

    via the diagnosis port, etc.
  - ➢ shall be equipped with measures to ensure a safe mode in case of system malfunction, e.g. by redundancy in the system.



Reviewing the context of the “Cybersecurity guideline”

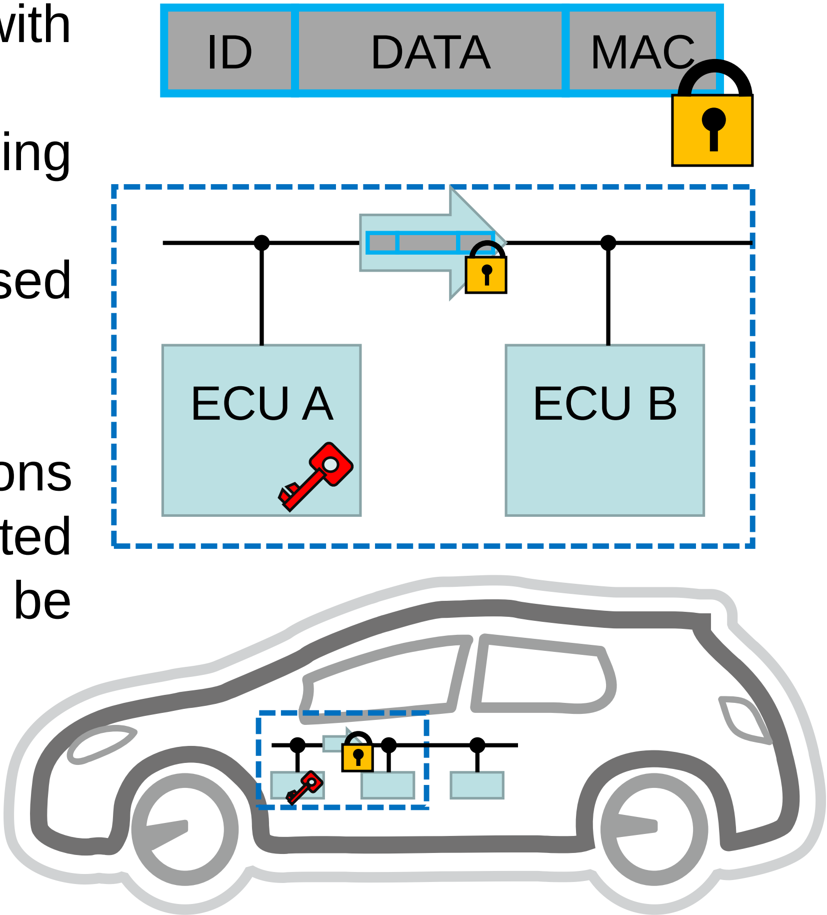
- When connected vehicles and vehicles with ADT detect fraudulent manipulation by a cyber-attack, the system shall warn the driver and control the vehicle safely according to the above requirements.



Reviewing the context of the “Cybersecurity guideline”

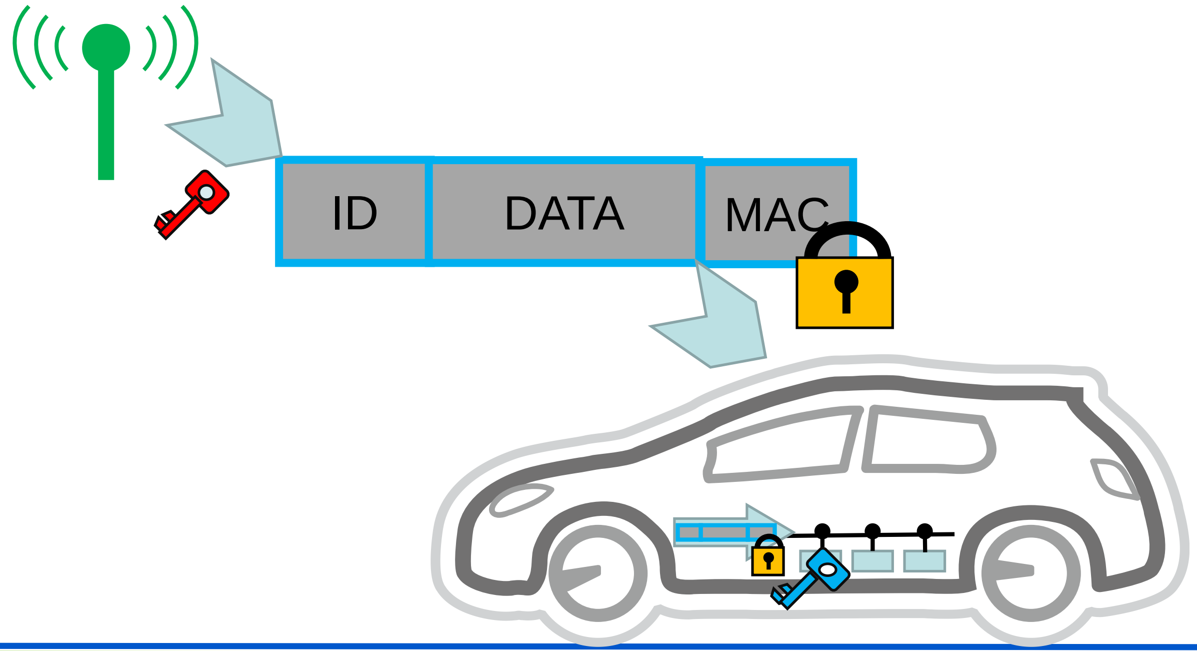
- Connected vehicles and vehicles with ADT shall be equipped with
  ➢integrity protection measures assuring e.g. secure software updates
  ➢appropriate measures to manage used cryptographic keys

- The integrity of internal communications between controllers within connected vehicles and vehicles with ADT should be protected e.g. by authentication.



Reviewing the context of the “Cybersecurity guideline”

- Online Services for remote access into connected vehicles and vehicles with ADT should have a strong mutual authentication and assure secure communication (confidential and integrity protected) between the involved entities.



Reviewing the context of the “Cybersecurity guideline”

Finding technical missing points and making issues clear

For example…

- “authentication” means ?

  MAC? or …

- security anchor should be defined?
- “redundancy” should be clarified?

…

Referring existing relevant standards

Work item
b. Construction of proposal for the next step

b. Construction of proposal for the next step

Discussion for the next step on cyber security

for example…

scenarios of implementation
of security measures on vehicles

….