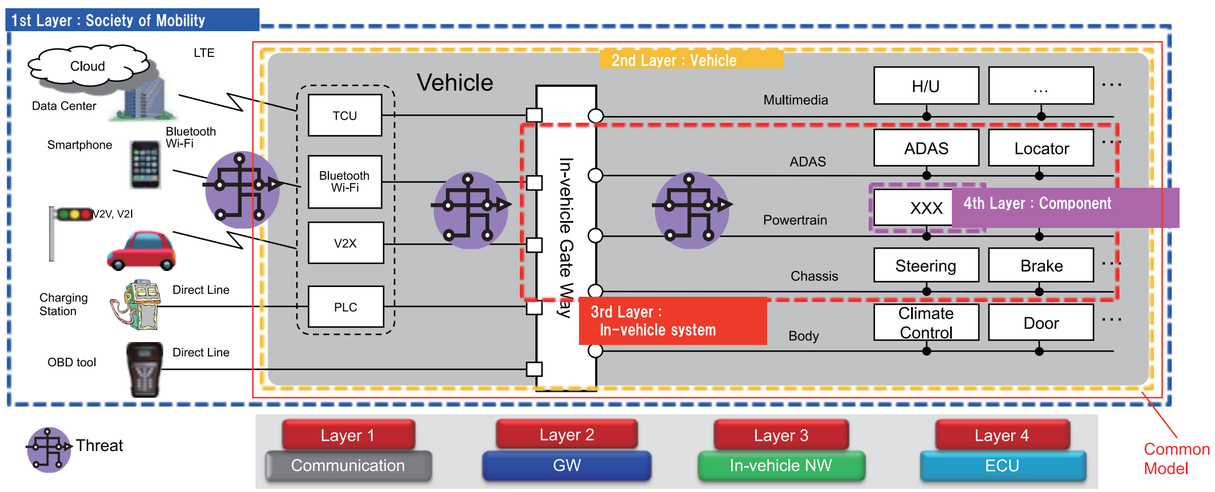
SIP-adus Workshop 2017
on Connected and Automated Driving Systems

# Cyber Security

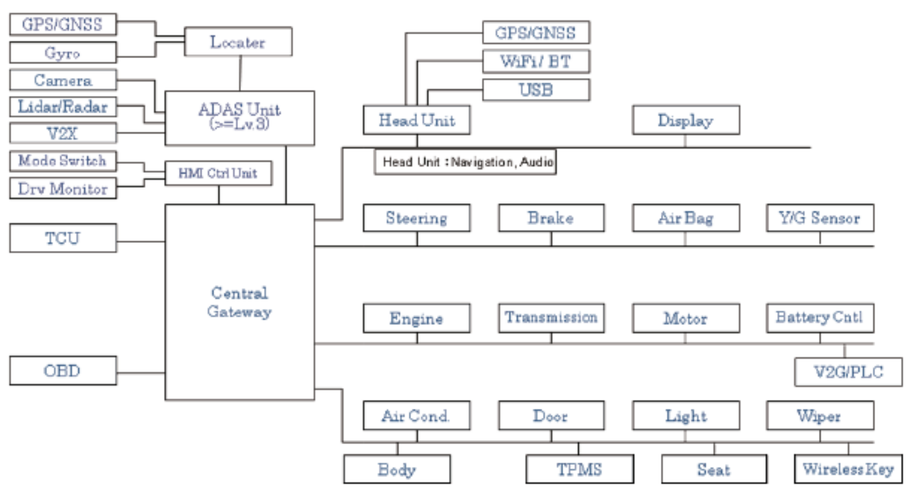
## Evaluation and Certification of Automotive Cyber Security

### ■ Back Ground and Objectives of the Project

Utilization of communication such as V2X is expected to obtain information such as dynamic map and local situation for Automated Driving. Meanwhile, the external connectivity through the communication makes Cybersecurity as an important issue. So, requirements for Automotive Security will be elicited by building common models for Automated Driving System and following threat analysis, and to study validation / evaluation technologies, methods, and criteria for component level to vehicle level, then summarize the requirements for test beds. In addition, the methods of omitting certificate verification is studied.




**Layered Structure for Automotive Cyber Security**




**Common System Architecture set in the Project**

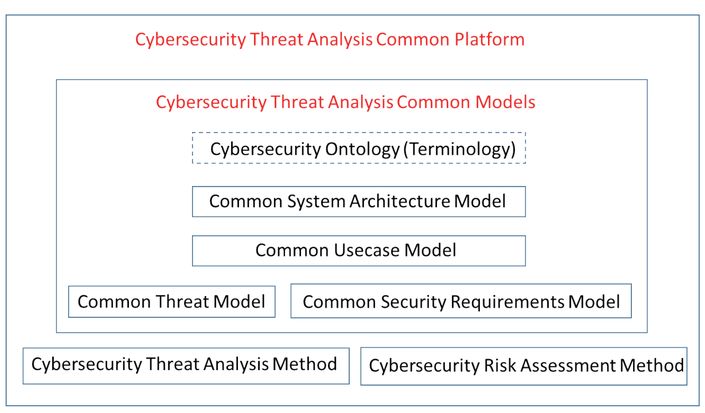
In the Project, we focus "in-vehicle" system which is shown as the 2nd to 4th layers in the above "Layered Structure."

1) Threat analysis : To develop "Threat Analysis Platform," Preliminary specification of data formats were determined.

2) Study on validation / evaluation methods and criteria : "Evaluation board" or "Evaluation system" were developed and security counter-measures with some security levels such as key length were implemented. Attacker teams evaluated difficulties with some evaluation methods in each level. The evaluation results are expected to help to consider "criteria."

3) Study on the method of certificate-verification omission for V2X communication : "Prioritized certificate verification" method was proposed.

### ■ Threat Analysis Platform




- A common and integrated platform will be developed for automotive industry to support HARA and analysis of security requirements.
- Multi-staged attacks and defenses in depth strategy will be able to be analyzed and developed.
- Preliminary specification of support tools were set for developing tools.

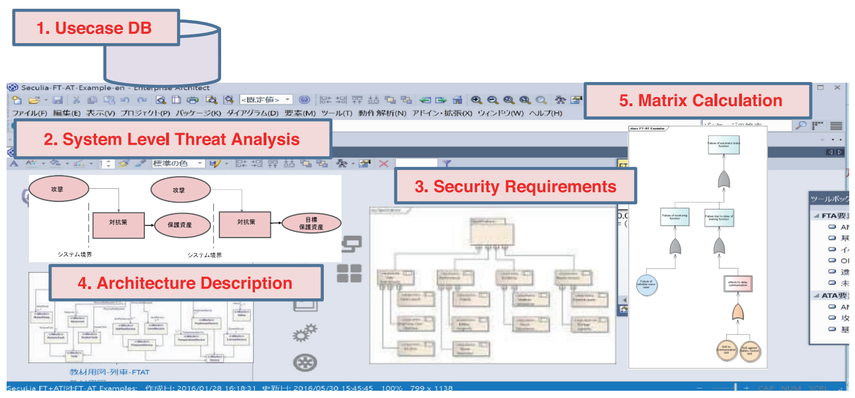
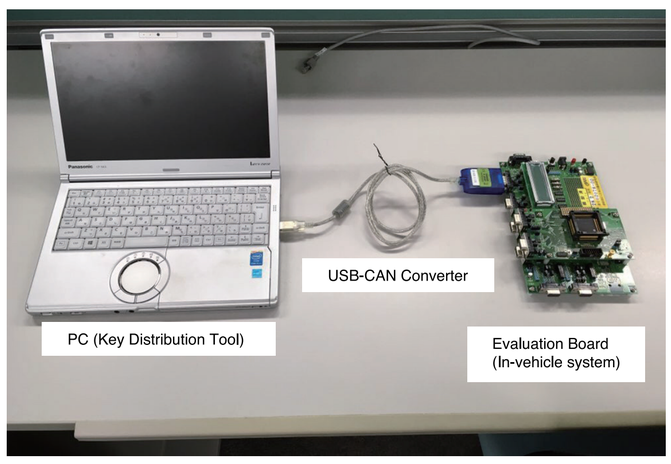


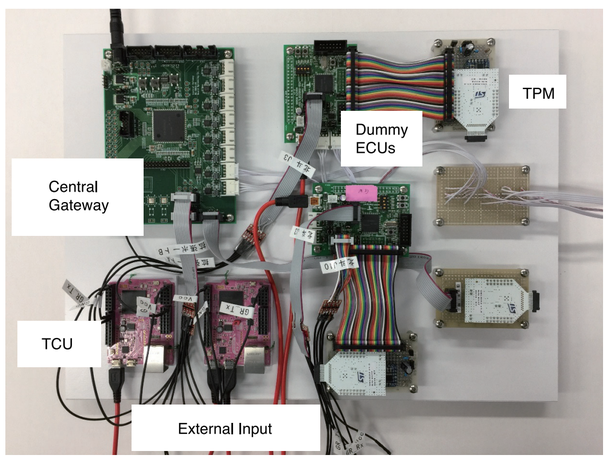

**Image of Support Tools**

### ■ Study on Validation/Evaluation Methods and Criteria




Evaluation study with use of the dummy in-vehicle system at some security levels (key length, randomness)

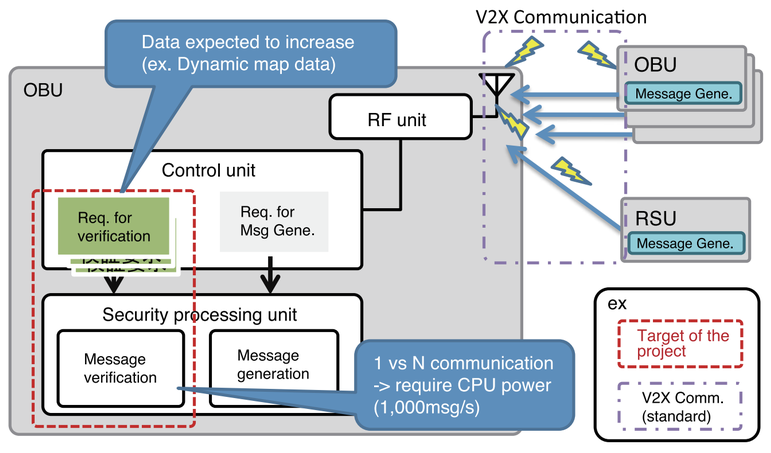
- S/W rewrite through CAN
- Key Distribution Procedure




Multi-layered "dummy" in-vehicle system is studied for general purpose evaluation which includes ;

- TCU (Tele-Communication Unit)
- External Input (Control Signal)
- Central Gateway
- Dummy ECU (Steering ECU)

### ■ Study on Omitting Certificate Verification of V2X Communication




Proposed "Prioritized certificate verification" method for omitting message verification was simulated, and simulation results show that the method achieves the requirement of V2X (1,000msg/s) target