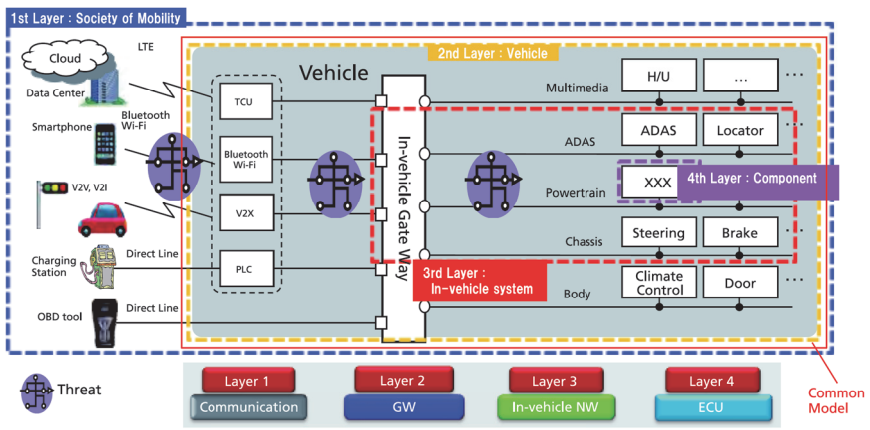
Evaluation and Certification of Automotive Security

[Back Ground and Object of Project]

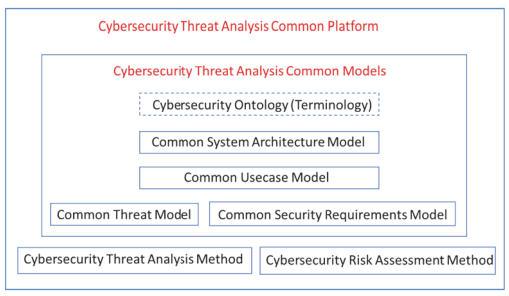
Utilization of communication such as V2X is expected to obtain information such as dynamic map and local situation for Automated Driving. Meanwhile, the external connectivity through the communication makes Cybersecurity as an important issue. So, requirements for Automotive Security will be elicited 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.

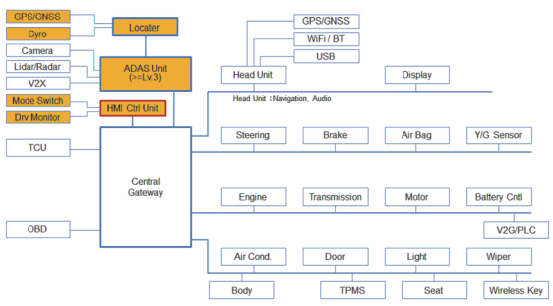


[Target of Project] In the 2nd to 4th layers, four(4) research subjects are set.

1) As a preparation for threat analysis with use of common system architecture, use case formulation and its model for automated driving, previously-achieved project information is organized and analyzed. Also, preliminary case of common system architecture is formulated and confirmed if the requirement for the use of threat analysis is satisfied.
2) To study validation / evaluation methods and criteria in every layer such as component level, in-vehicle system, external-vehicle cooperative system and vehicle level, in this year, security evaluation methods and attack cases in the other industries are investigated. In addition, as a component level, preliminary evaluation environment is formulated and the attack test to the ECU is done.
3) In order to study the method of certificate-verification omission for V2X communication, investigate the case examples that have been reported so far and simulation in PC is achieved to evaluate the performance of the methods. As a result, a concern against DDoS attack is confirmed with currently proposed methods.
4) With a focus on the security of V2X communication, technical trend and opinions to the legal regulation in overseas are investigated.

1) Common Models of Automated Driving for Threat Analysis





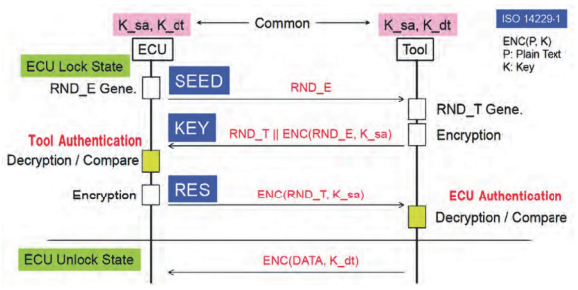
As a preparation for threat analysis, work-products in the last fiscal year were compiled and analyzed.

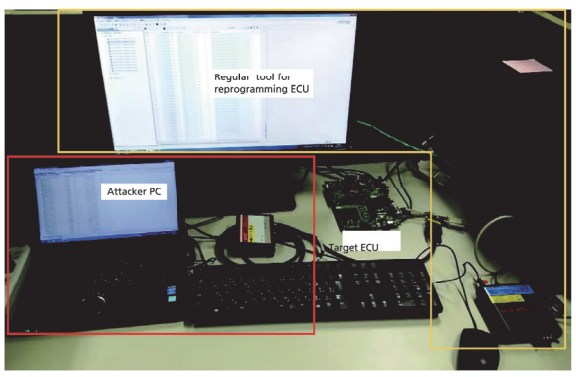
→ A common and integrated platform for cybersecurity threat analysis for automotive industry to support HARA and analysis of security requirements.

→ The whole process of threat analysis will be carried out based on common models, which include architecture model and use cases.

→ Multi-staged attacks and defense in depth strategy can be analyzed and developed.

2) Study Validation/Evaluation Methods and Criteria





Evaluation study started from component level with use of the evaluation board for S/W rewrite through CAN

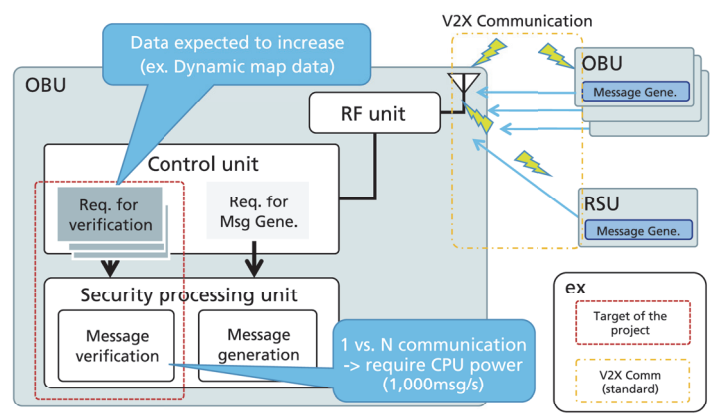
☐Evaluation system for component level
- ▶Re-programming module equipped
  - ・Security IP not used
  - ・Encryption key stored on RAM in μC
- ▶Randomness level for certificate
  - ・SEED initialize : 2 levels (Yes / No)
  - ・SEED entropy : 2 levels (4bit, 128bit)

☐Evaluation results

Attacks of spoofing through CAN successful at all levels

→ Further study planned at the next steps for investigating requirement to counter measures, including in-vehicle system level evaluation

3) Study Omitting Certificate Verification of V2X Communication



Investigated omitting methods and simulated

- ▶ Processing time for V2X (1,000msg/s) : US 3%, EU 24%
- ▶ "Prioritized certificate verification" proposed

→ Study on performance evaluation and analyzing, and investigate key/certificate management

[Future Plan]

Through the study of threat analysis and validation / evaluation technology, the direction of third-party validation /evaluation and third-party certification as for an automotive security should be studied and based on the obtained results, activity for global alliance (cooperation / coordination) is considered. In addition, for the large-scale demonstration test scheduled in 2017, security validation / evaluation and building test-bed which are necessary for the automated driving vehicle will be studied. Regarding the method of signature-verification simplification, with satisfying necessary security level, the method to reduce the device load is also studied and obtained results are studied to cooperate in the global alliance.

METI Ministry of Economy, Trade and Industry

SIP