SIP-adus Workshop 2021

Session 6
Cyber Security

# New Cyberattack and Proactive Survey Methodologies for Automotive Industry

Shinichi Kan (PwC Consulting LLC)

9-10, November, 2021

SIP

Cabinet Office

# INDEX

# 1

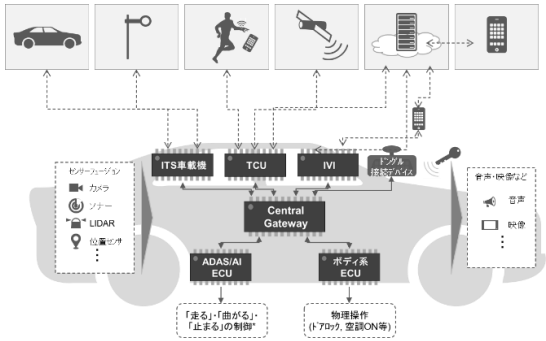
# Introduction

# Background and Research Objective

In order to deal with changes in the security environment due to the development of autonomous driving systems and new international regulations, we are performing two research activities.

## Changes in automotive security

Security risk in connected-system are increasing




## New international regulation

UNECE WP29　UN-R155/R156

World forum for harmonization of vehicle regulations working Party 29(WP29)

## Activity a. Development of IDS Evaluation Method and Guideline

Research Question : What methods, procedures, environments are required to evaluate in-vehicle IDS?

## Activity b. Research on connected car threat intelligence and initial response support

Research Question :What kind of method is available to collect and accumulate threat information for vehicles?
:What information required to support initial incident response for vehicles?

# 2

# In-vehicle IDS

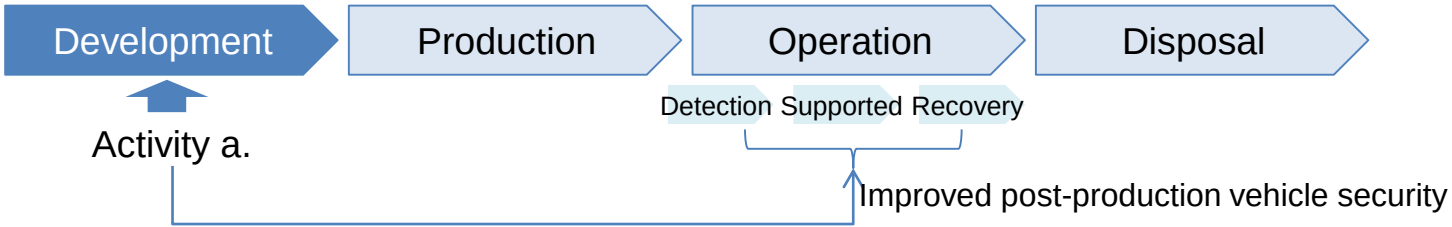
# In-vehicle IDS

In this research, we are investigating the evaluation method of in-vehicle IDS, as a cyber attack detection method, and establish “IDS evaluation guideline”.

| Regulations | Industry Practices |
| --- | --- |
| WP29 UN-R155 sets requirements for the manufacturers / suppliers to make the vehicles can detect and respond to cyberattacks. | In regulation, specific detection accuracy is not defined, and it is necessary for the manufacturer to determine the standard. |

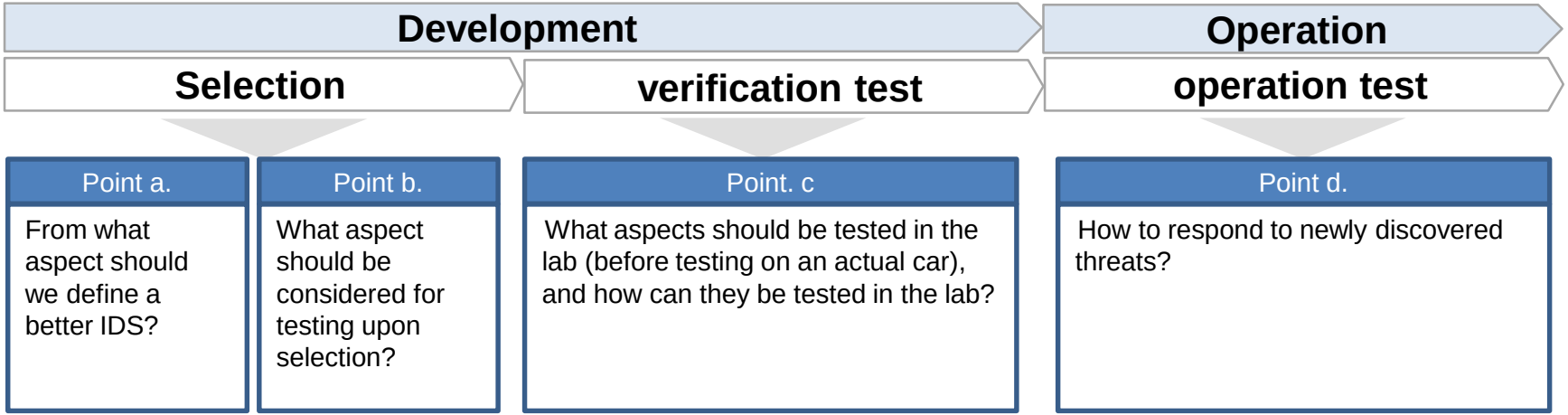
## Objective and approach

Establish IDS evaluation guideline contributes to post-production security in automotive industry.



# Scope of the IDS evaluation guidelines

Following activities 1~3 are performed in IDS selection, in-lab IDS behavior verification, defect identification and not only respond to new threat, also maintain vehicle operation.

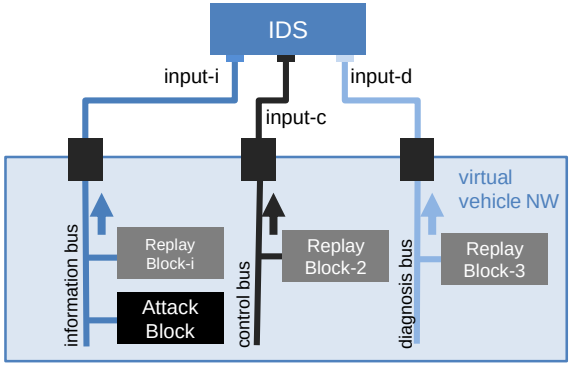



| # | Activity | Point |
|---|---|---|
| 1 | Examine the evaluation perspectives based on the specifications | a |
| 2 | Examine basic test cases (test requirements, prerequisites, test environment, test procedures, etc.) | a, b, c |
| 3 | Examine methods to identify the detection function required for IDS from attack cases | d |

# (Example)Test environment

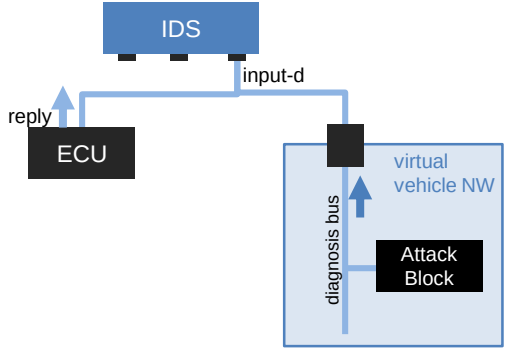
The test environment used in the basic test case is as follows. A simulation environment is used for those that required input of a message indicating the state of the vehicle (stopped, running etc.), and a testbed environment is used for those that required input of a response from the ECU.

## Simulation




Used for test cases that require input of car status messages (speed, steering angle, etc.) and do not require input of ECU responses.

## Testbed




Used for test cases for that require input of response from the ECU. This environment is mainly for the detection of attacks diagnosis service.

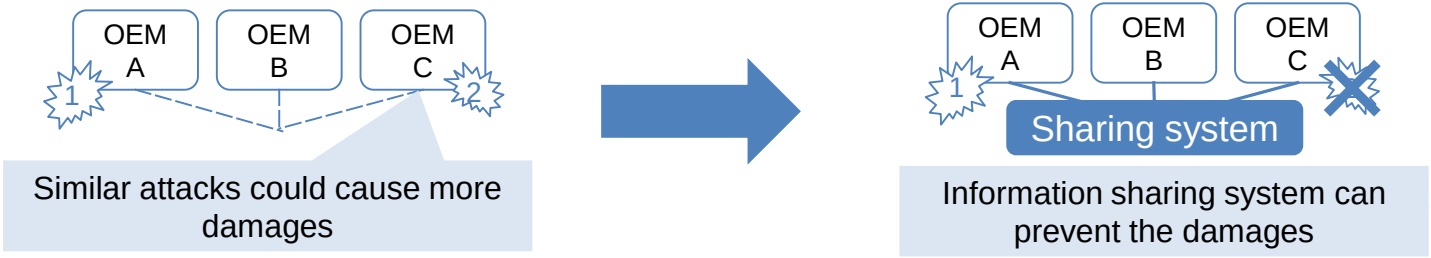
# 3

# Threat information sharing system

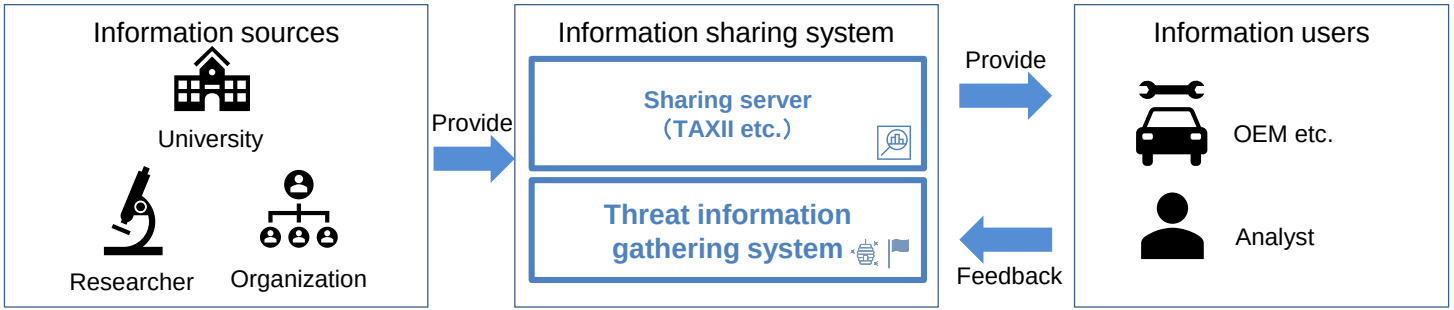
# Threat information sharing system

Researching the basic design of threat information sharing system in order to contribute to post-shipment security measures in automotive industry.

✓ Advantage of information sharing system

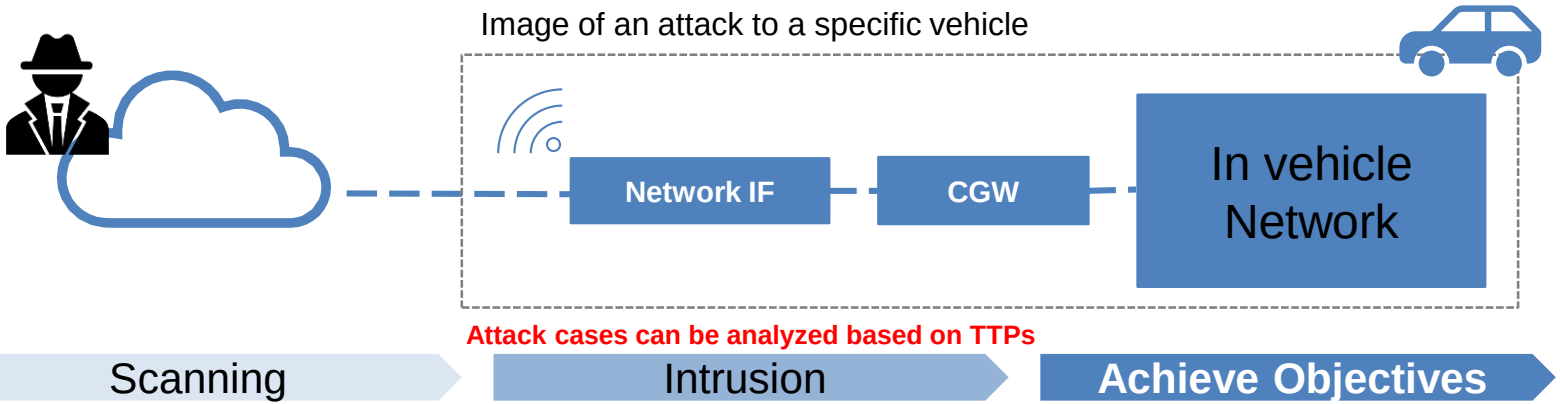



✓ Outline/schematic image of the system



# Hypothesis and evaluation method of the information sharing

Unlike IT systems, vehicles do not have common architecture for each OEM, so there is a high probability that a certain threat for a vehicle may not be applicable for another. On the other hand, analyzing the case will help identifying threat that is commonly applicable for any vehicles.

| | |
|---|---|
| Hypothesis | A case/threat for certain vehicle may still be applicable for other vehicles. |
| Analysis |  |
| Evaluation | Regardless of the vehicle type, evaluate whether threat information handled by the information sharing system can be utilized among stakeholders in the Automotive field such as OEMs. (We assume J-Auto-ISAC as a point of contact with the information sharing system.) |

# How to accumulate the threat information

In order to consider whether STIX / TAXII, which is widely used in the IT field, is sufficient as a method for collecting and accumulating threat information, we examined a list of threat information and try to describe it in STIX format.

**Objective**

- Find a method for accumulating threat information that can be used in the automobile field.

**Hypothesis**

- In the future, considering the utilization of threat information accumulated in the IT field, it is better to use the data standards and formats used in the IT field.
- The main data standards and formats widely used in the IT field are as follows.
  - STIX / TAXII
  - IODEF / RID
  - OpenIOC

**Approach**

- As a result of considering the frequency of use in the IT field and the variety of information that can be expressed, this study start to examines with STIX/TAXII.
- We try to consider whether STIX / TAXII is sufficient as a method for collecting and accumulating threat information of automobile field.

# 4

# Experiments of threat information observation

# Objective of the observation experiment

We will conduct a threat information observation experiment with reference to implementation examples in the IT field.

| | |
|---|---|
| Objective | • Establish a method for collecting and accumulating threat information in the automobile field. |
| Hypothesis | • In the IT field, various methods have been experimented and operated for actively collecting threat information on intention and attack methods of cyber attackers, which is useful for building cyber intelligence.<br>• In a connected system, it can be possible to collect threat information and build cyber intelligence by the same method.<br>(例) Honeypot / CTF / OSINT / Bug bounty / Monitoring |
| Threat Information | • Attributes of cyber attackers / TTPs |
| Approach | • Consider attack patterns on connected systems and evaluate the possibility of collecting threat information through actual observation experiments using threat information collection methods in the IT field. |

# Expectation on honeypot and CTF

The expectation of honeypot and CFT in this project is not to obtain specific threat, but to find out if are the methods beneficial to obtain car-related threat and organize them for future use.

**Background:**

- At the moment, attacks on connected cars are rare.
- In addition, no large-scale targeted attacks on connected cars, so-called attack campaigns, have been identified.

**Honeypot and CTF are used to find out the following:**

- Are there actually connected cars being accessed from the internet?
- Are there any devices that have been accidentally exposed to the internet?

- How do virtual attackers (CFT participants) attack cars?
- What motivates the (virtual) attackers?

# 5

# Future work

# Future work

We are now considering the use of STIX/TAXII for the information sharing system in automotive industry, and are planning honeypot experiments mimicking real products on markets.

Furthermore, Observation experiments are planed to conduct by holding a playground.

## *2020*

Fundamental Research

- Information sharing activity in IT field.
- Information collecting method in IT field.

## *2021*

Information sharing


Honeypot experiments

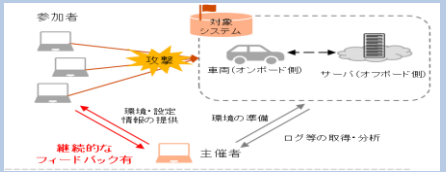

## *2022*

Information sharing system


Honeypot experiments

Expand Honeypot's type and variety

CTF(Playground)



# Thank you