The 12th Japan ITS Promotion Forum

Automated Driving Systems

Cyber Security

Takashi Imai

SIP-adus International Cooperation Working Group

Toyota Info Technology Center Co., Ltd.

SIP

Cabinet Office

<Translated Version>

SIP-adus' Activities and Cooperation with Industrial Groups

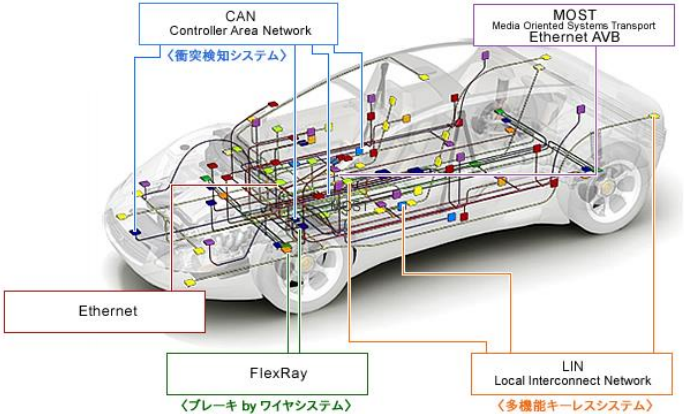
1. Vehicle Security Trends
2. Initiatives by Automotive Industry Organizations
3. Auto ISAC
4. Study of Cyber Security R&D Scenarios

Vehicle Composition

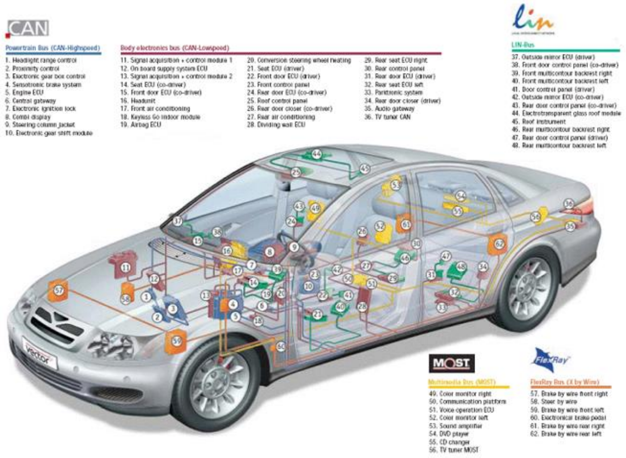
◆The car systems consist of many electronic control units (ECU).

◆They are linked by several on-board LAN depending on the characteristics and particularities of each application.

◆Among them, the CAN (Controller Area Network) protocol is the de facto standard of on-board LAN. It is used to support the various car functions associated with "acceleration, steer, and braking."



https://www.renesas.com/ja-jp/solutions/automotive/technology/networking.html

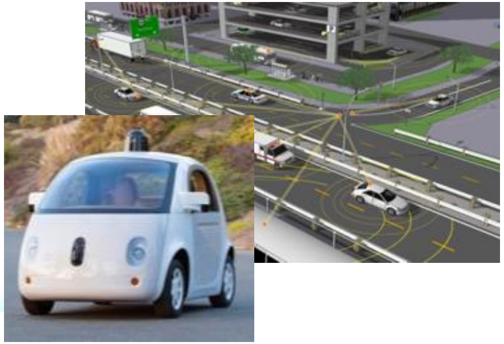


http://monoist.atmarkit.co.jp/mn/articles/0805/09/news152_2.html

Vehicle Advancement

◆Development into a vehicle system that provides "safe and comfortable mobility" while supporting the basic functions of "acceleration, steer, and braking"

◆Achieved with onboard ECUs (computers) that communicate each information interactively



・**An age of "automated driving" and "connected vehicles"**

The ECUs conduct operations based on sensor information.

・Detection of obstacles and other items around the car with various sensors

・Support driver with ADAS (Advanced Driver Assistance System) (collision prevention, etc.)

・Support by CAN
・Power steering, etc.
・Mandatory OBD-II

・All operations performed by the driver

Vehicle Security Trends

Vehicle scenarios	*Advanced driver assistance, Automated driving* Level 3 Level 4 *Connectivity* V2V V2G Use of Big Data V2X
Environmental changes surrounding vehicles	Expanding vehicle external communications, from stand alone control to cooperative control Spread of carry-in devices, expanding cooperative functions with vehicles Expanded use of standardized technologies (e.g., AUTOSAR, Linux, Ethernet, etc.)
Cyber Security	Increase cracking risk

Security countermeasure

Connected vehicle

Source: JasPar

◆The hacking capability against vehicles is growing year by year.

FCA recall of 1.4 million cars

Targeted vehicle
Vehicles equipped with **Uconnect (network connection services)**

Attack description*
Control of display, steering, and gear shifting by remote control from a PC

*No actual accidents were caused by the remote attack

'13 **Conducted by boarding the vehicle** (communication injection)

'15 **Successful remote hacking** (during low-speed driving)

'16 **Control of vehicle using maintenance mode** (when driving)
*Injection of communication through diagnostic connector

Targeted vehicle
FCA Jeep
Attack description
・**Injection of maintenance command from diagnostic connector**
・**Control of steering by spoofing regular ECU**

Targeted vehicle
Tesla Model S
Attack description
Control of brake operation in a moving vehicle by remote control from a PC

'17 **Control of vehicles by remotely striking numerous vulnerabilities**

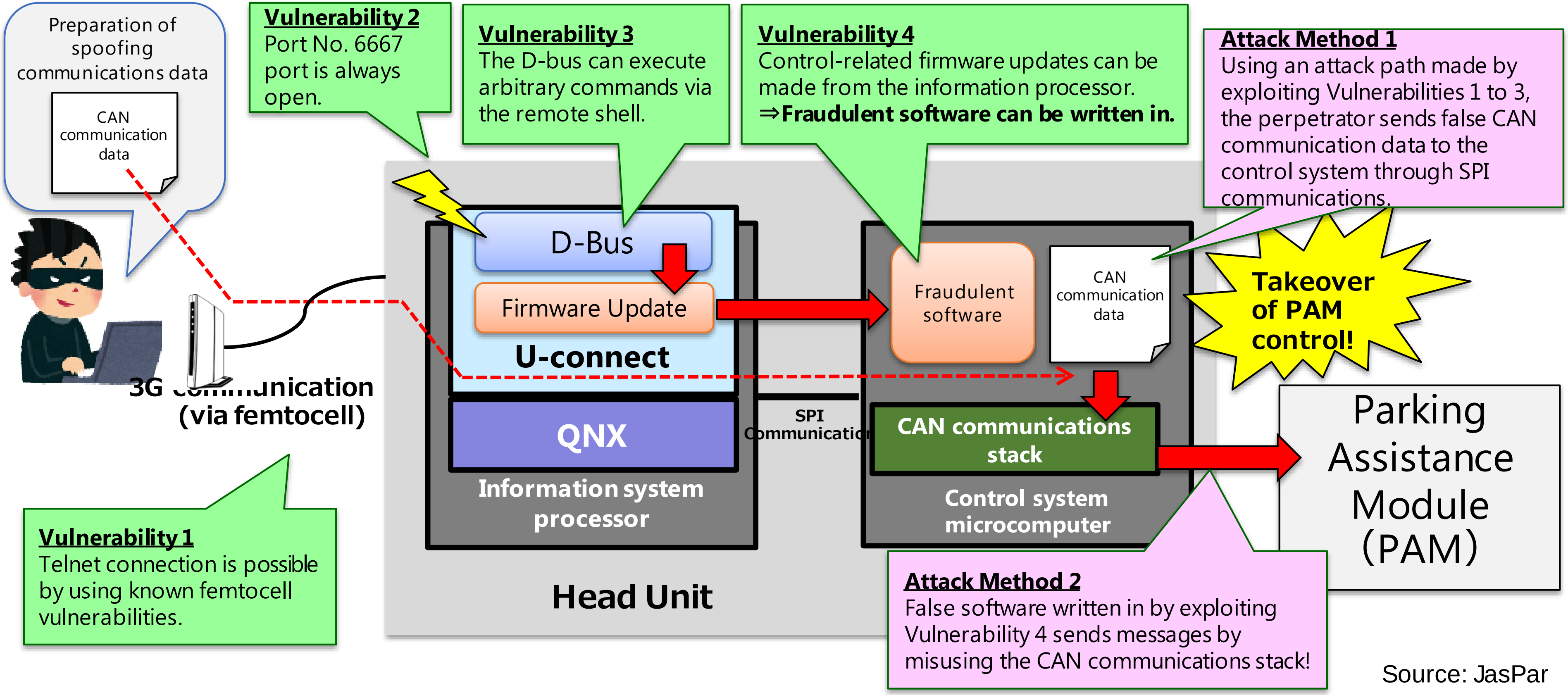
Targeted vehicle
Tesla Model X
Attack description
Same as the Model S (Attack striking new vulnerabilities)

*Attack made by analyzing communications beforehand

Source: JasPar

How Was Vehicle Control Taken Over?

- The perpetrators opened an attack path by exploiting several vulnerabilities in the head unit, sent a false message to the CAN bus, and took control of the PAM.

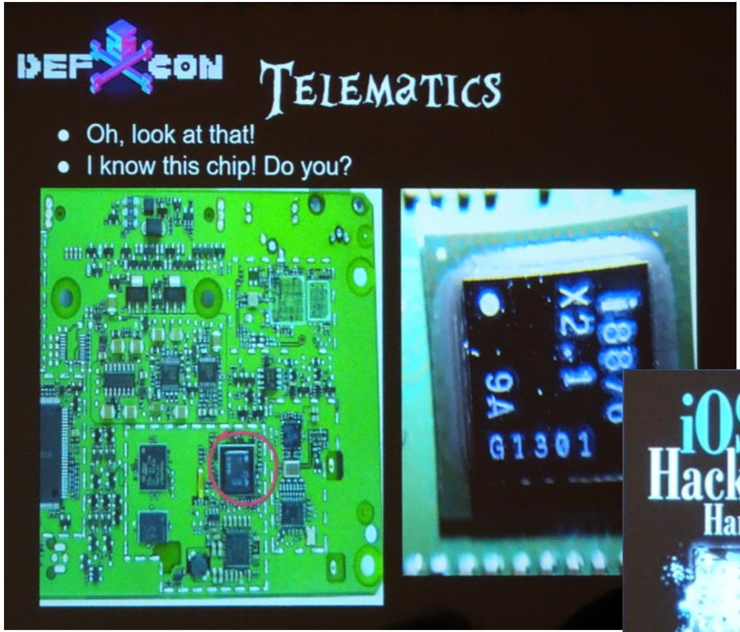


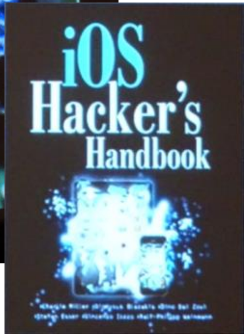
Source: JasPar

Noteworthy Technologies at Black Hat

Hardware hacking

- Analysis of telematic control units removed from discarded vehicles
- Equipped with the same chip as the iPhone, allowing successful remote attack using known vulnerabilities





SIEM(Security Information Event Management)

- Detection and visualization of occurring threats
- Automation of incident responses in accordance with pre-established rules is possible
- Many exhibits at business booths

Source: JasPar

List of Hacking Incidents Involving Vehicles (2017 Except)

◆ Hurdles to hacking are becoming lower as a result of automobile connectivity and access to CAN communications ⇒ Security measures against increasing cases of hacking are essential!

Time	Manufacturer	Summary	Source
February 2017	Many auto manufacturers	A vulnerability survey of the mobile phone apps of auto manufacturers found that door locks of several manufacturers can be opened.	Kaspersky Lab
April 2017	Bosch-made dongle	Engines could be stopped remotely by exploiting a vulnerability in a Bosch-made driver log connector and sending a message to the CAN bus.	ARGUS
April 2017	Hyundai	Car locations could be identified, door locks opened, and engines started by exploiting a vulnerability in the "Blue Link Mobile" app.	Rapid7
June 2017	Subaru	A vulnerability in the STARLINK app was discovered that allowed access to a vehicle's use history, sounding of its horn, and unlocking of its doors.	Aaron Guzman (researcher)
June 2017	Honda	PCs at Honda's Sayama Plant were infected by the WannaCry ransomware, temporarily shutting down the production line. Production of over 10 million vehicles was affected. Production of over 10 million vehicles was affected.	Nihon Keizai Shimbun, others
July 2017	Tesla	A remote hacking attack against the Tesla Model X was successful. Brakes, door locks, mirrors, and other components could be operated by attacking the CAN bus.	Keen Security Lab（China）
August 2017	BMW, Ford, Nissan	A vulnerability in a TCU that uses 2G circuits was discovered, and there was concern that arbitrary codes would be executed in the baseband wireless processor.	McAfee

Source: JasPar

Vehicle Security Trends: Summary

◆ Many incidents of attacks on control systems through wireless communications that link cars with the outside are being reported.

◆ There are concerns about attacks via Wi-Fi, which has been the target of attacks longer than cellular communications networks and Bluetooth.

◆ Attention and expenditure will be needed to combat external hacking in the age of self-driving cars.

◆ Full security evaluations and secure design processes are required.

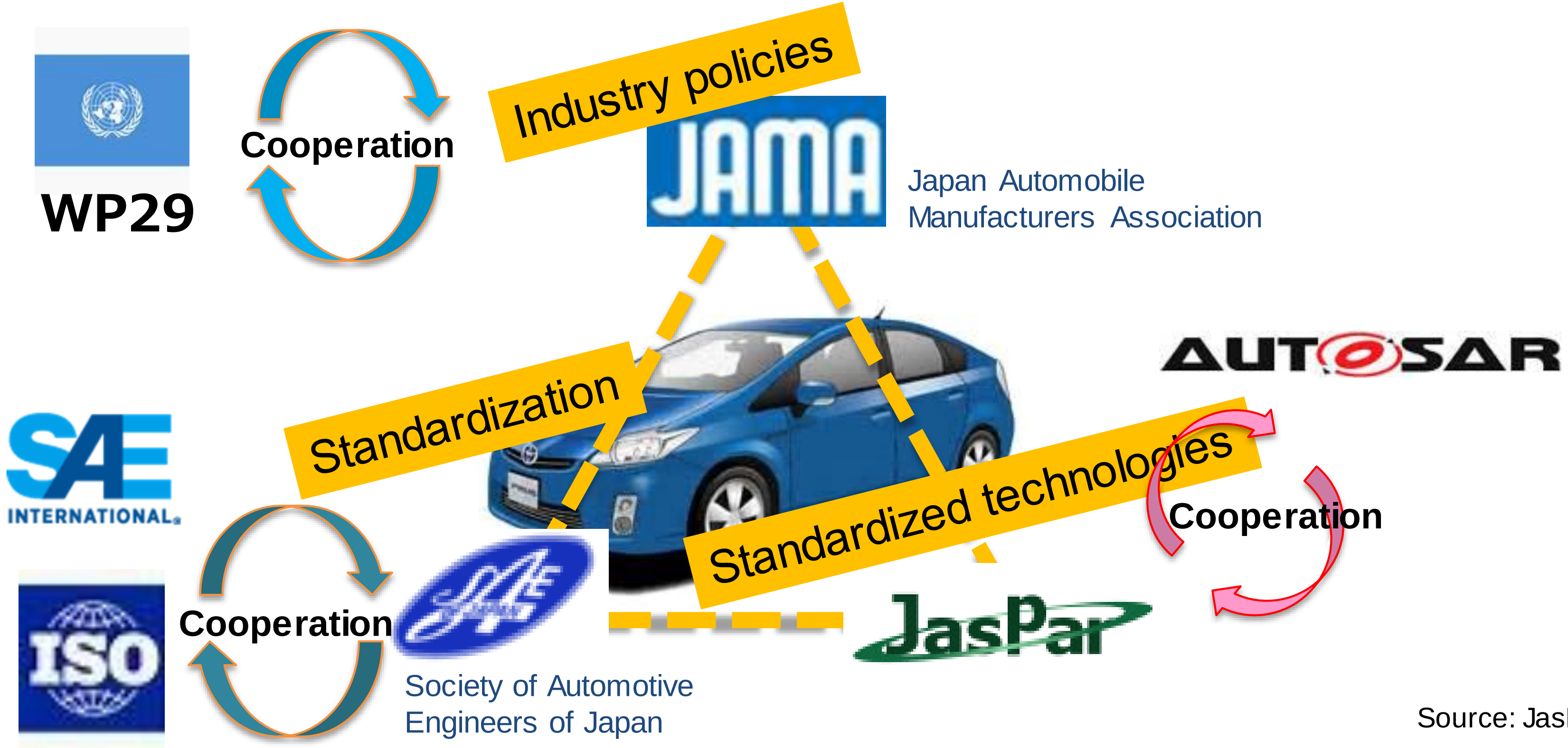
◆ Difficulties in cyber security for vehicles

1. Unlike the IT industry, auto manufacturers also handle **customer safety**.
2. As opposed to **"functional safety" (random accidents)**, how should **"Cyber security" (malicious intent)** be viewed?
3. Cars have a **long life cycle**.

Issues pertaining to the cyber security of vehicles are an area of cooperation, rather than an area of competition. Active cooperation among OEMs and industrial organizations will continue.

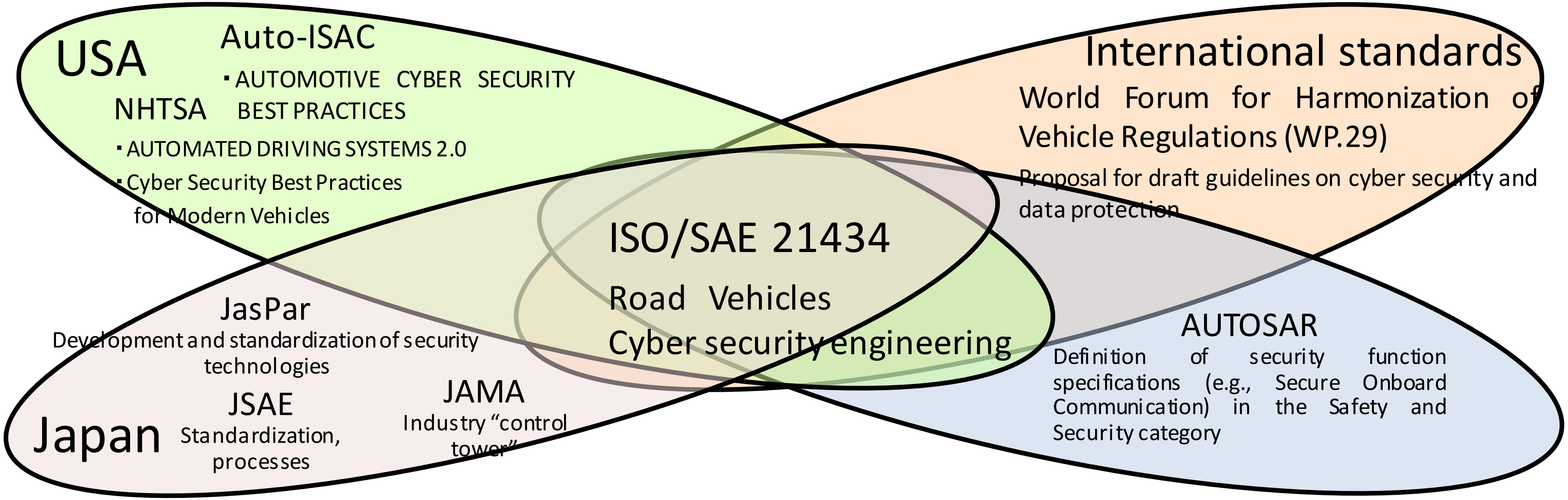
◆ Organizational roles are generally as follows:

Planning: JAMA　Requirements: JSAE　Design: JasPar　Operation: JAMA



Source: JasPar

Developments in Security-Related Standardization/Legislation



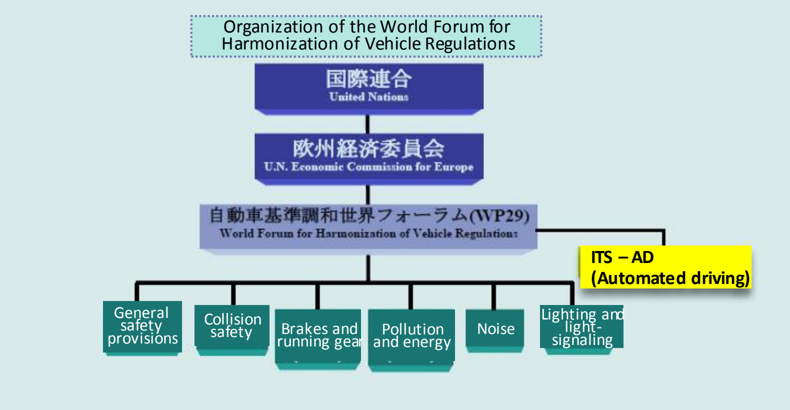
Organization name	Outline of activities
NHTSA	Formulation of regulations and guidelines for self-driving cars (including security requirements)
Auto-ISAC	Central organization for sharing information on incidents/vulnerabilities in the automobile industry
ISO/SAE 21434	Formulation of vehicle security standards through the Joint Working Group of ISO (Europe) and SAE (USA)
WP.29	Security and data protection guidelines for self-driving cars and connected cars
AUTOSAR	Formulation of security function requirements as an electronic platform specification

Source: JasPar

Developments in Security-Related Standardization/Legislation

WP.29: Cyber security and data protection

- Self-driving cars Cyber security guidelines
- Demand for "driver warnings" and "safe vehicle control" whenever a "cyber attack from outside" is detected
- Also, demand for "protection from leaks and fraudulent use of personal information (privacy)"



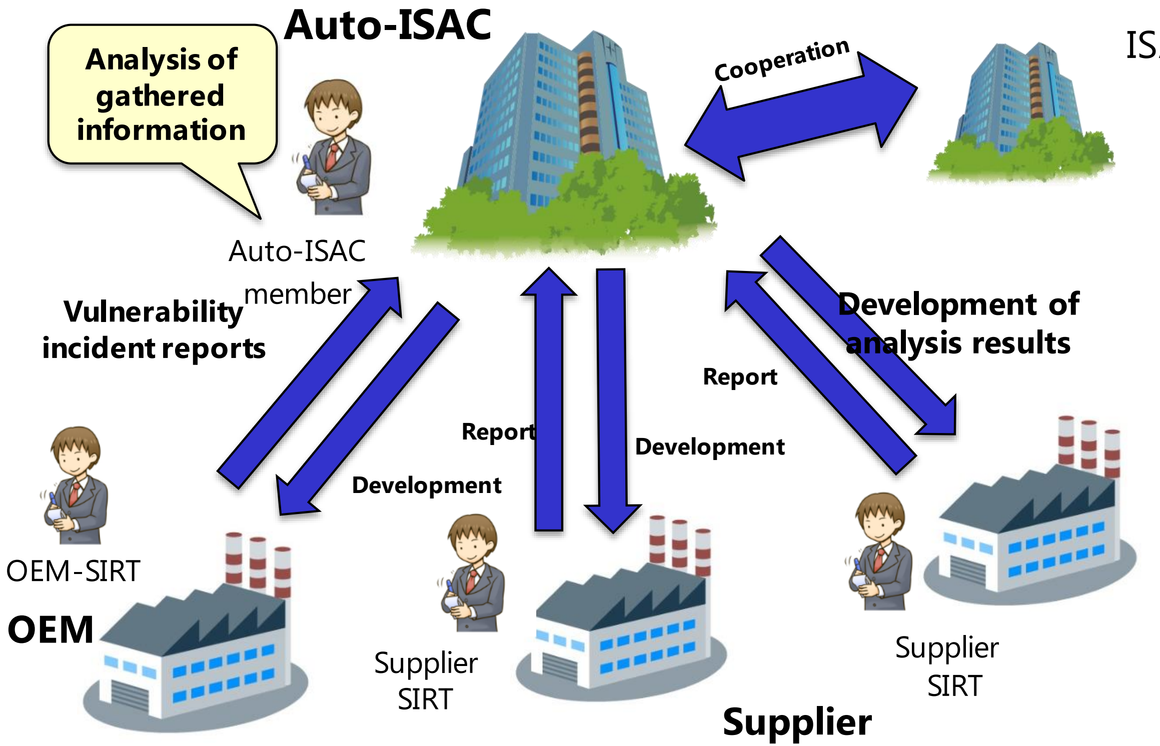
ISO/SAE 21434: Road Vehicles – Cyber security engineering

- ISO proposal concerning cyber security development processes for automobiles
- Being discussed in the ISO and SAE Joint Working Group (the world's first)
- Scheduled to be issued in 2020

Source: JasPa

Auto ISAC

- The Alliance of Automobile Manufacturers and Global Automakers joined to establish the Automotive Information Sharing and Analysis Center (Auto-ISAC) in response to the growing number of reports of hacking in the United States.



ISAC in other fields

- Auto-ISAC is the central organization for sharing information on cyber threats to electronic automotive parts, onboard networks, and other various items in real time throughout the entire industry.
- The Security Incident Response Team (SIRT) of each company is responsible for making reports to Auto-ISAC and receiving information released by it.

Source: JasPar

Establishment of Auto-ISAC (Information Sharing & Analysis Center) (January 2016)

✓ **ISACs have been established under government leadership in major infrastructure and industrial sectors.**

・PDD63 (order by President Clinton) = Directive to establish information-sharing bodies in 18 important infrastructure sectors (1998)

(Banks/finance, electric power, waterworks and sewerage systems, transport, communications, nuclear reactors, military industries, etc.)

・Establishment of the large-scale Auto-ISAC by major OEMs, suppliers and others (January 2016; 38 OEMs and suppliers)

・The House of Representatives instructed the NHTSA to begin studies toward formulating a bill that will require security measures for vehicles (2017)

Establishment of Auto-ISAC (January 2017)

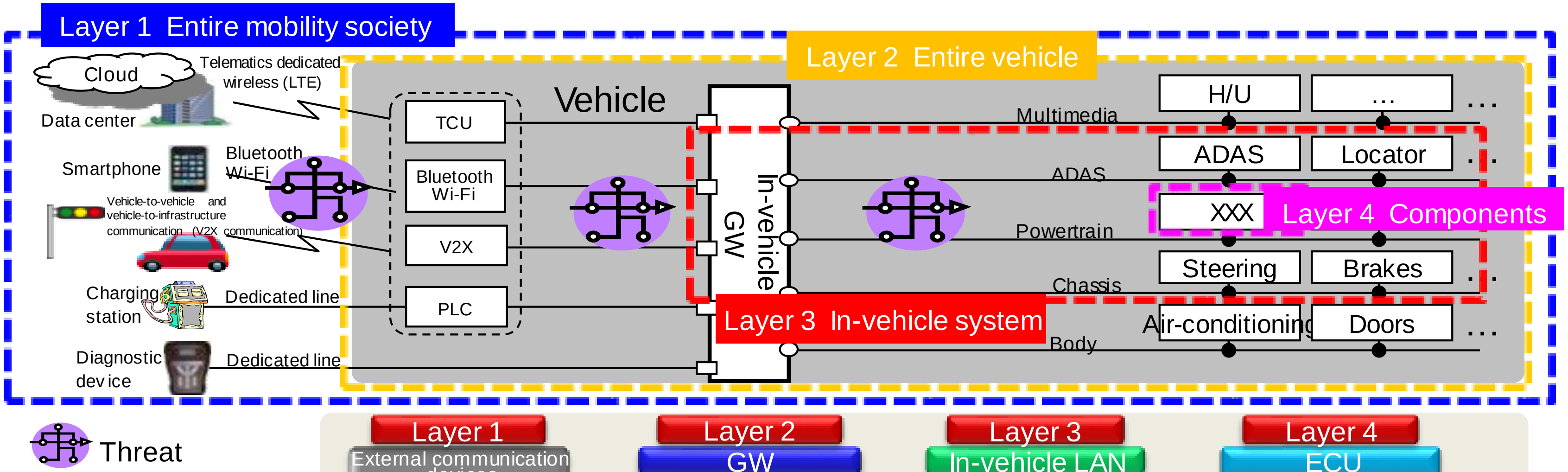
・METI Cyber Security Management Guidelines = Demand that industry reinforce its responses in 10 areas (2015)

・The initial aim was to start small and quickly, given predictions that cyber attacks in Japan would be infrequent over the short term.

・Full-scale activities in line with Item 8 of METI's demand, "**Participate in and effectively use information-sharing activities"** began in April with the establishment of a working group (11 OEMs in Japan) under JAMA's Safety & Environmental Technology Committee.

Source: JasPa

◆ An agreement by Japan's automotive industry concerning the standard on-board system structure to be studied
Study focused on vehicles (Layer 2 and below) with consideration for industry standards and international standards



Layer 1	Layer 2	Layer 3	Layer 4
External communication devices	GW	In-vehicle LAN	ECU
Encryption	Access control (filtering)	Tempering detection	Secure programming
Digital signature	Key management	Encryption	Secure storage
Access control (Authentication, filtering)	ECU authentication		Secure boot
	Anomaly detection		
	Secure log		

Examples of security measures

TCU: Telematics Communication Unit
PLC: Power Line Communication
GW: Gateway
H/U: Head Unit
ADAS: Advanced Driver Assistance Systems
ECU: Electronic Control Unit

For data center security, Proceeding to study by SIP "Server Security in Key Infrastructure"

The Sub-Working Group's Four-Year Plan

- ◆ To build a common model for automated driving systems, formulate security requirements through threat analysis, and aim to build an evaluation environment (test bed) and standardize evaluation methods.
- ◆ For V2X communication, to research simplification of signature verification and aim for standardization.

		FY2015	FY2016	FY2017	FY2018
① Examine common model ・Threat analysis		Research	Develop, determine, derive	Develop prototype	Build, evaluate, improve
②Evaluation technology and evaluation environment	a) Component, in-vehicle system	Develop and research standards for target of component evaluation	Develop component evaluation environment and target of system evaluation	Complete component evaluation technology, develop system evaluation environment	Complete system evaluation technology, test bed trial run
	b) Vehicle external link system ・ Vehicle level	Research ICT attack cases Research audiovisual countermeasure sections	Countermeasure technology evaluation pointers and research and development of indicators	Verify evaluation pointers and indicators	Provide feedback on verification results and create guidelines
	c) Evaluation based on communication protocol	Research (protocol specifications, attack methods)	Examine evaluation methods and evaluation standards	Develop and improve evaluation environment through simulator	
	d) Evaluation using actual device	Research attack methods against components	Research attack methods against vehicles Research attack methods against systems	Research attach methods against mobility society	
	e) Research authentication by third party	Research authentication in other industries	Examine automotive application	Examine third-party authentication body	
③ Simplify V2X signature verification		Desk study	Communication evaluation Standardization activities	Mounting test Examine V2X operation	Comprehensive verification test
④ V2X overseas research and sharing of information		Research overseas trends Examine framework for information sharing	Operate framework for information sharing		

User Friendliness（JAMA)

- ◆Common Architecture Model
- ◆Use Cases of Automated Driving （JAMA）
- ◆Thread Info.（JPCERT/CC, Auto-ISAC）
- ◆Evaluation（Attack）Info. （Auto-ISAC)

Threat Analysis Tool

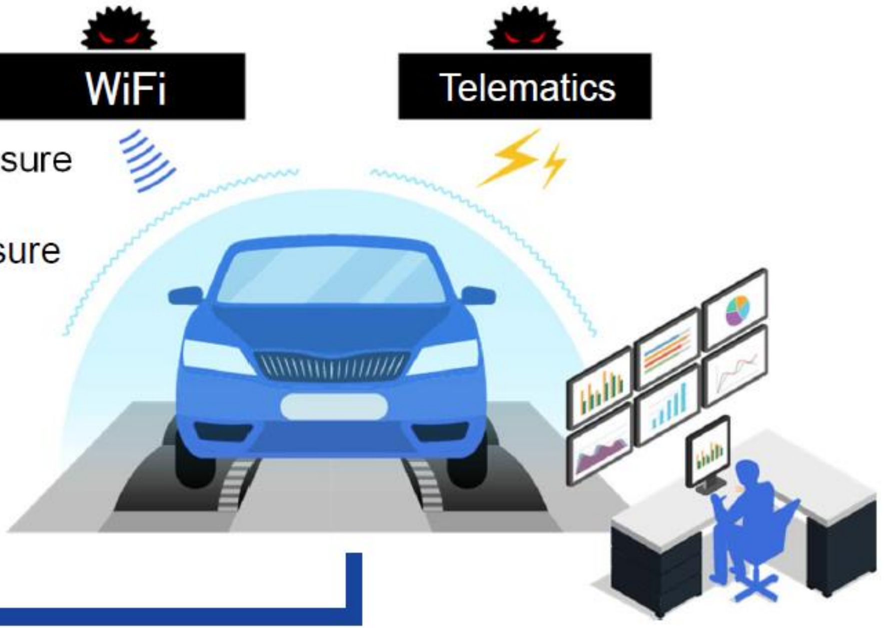
- ◆Countermeasure
- ◆Level of Countermeasure

Comparison with Current Threat Analysis (JasPar)

Vulnerability Evaluation

WiFi

Telematics



Cyber Security Evaluation Guideline

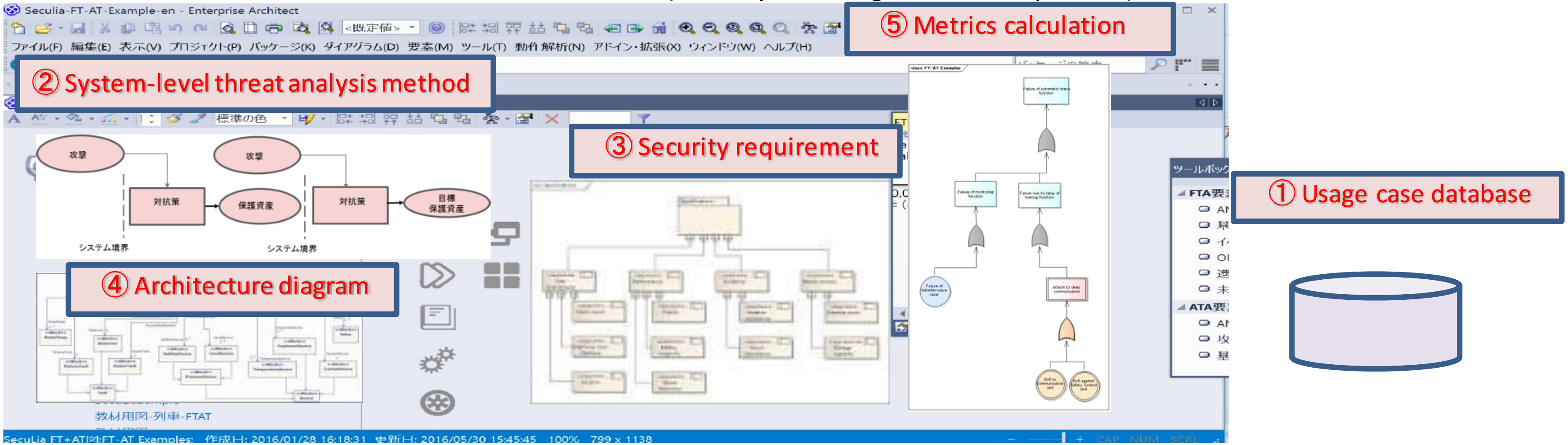
◆ Examine methods to analyze threats from cyber attacks

- Incorporate defense-in-depth, multi-stage attack strategy
- Check against threat database (Auto-ISAC, NVD, etc.)
- Link with JasPar analysis specification

◆ Development of integrated analysis tools

- Creation of analysis tools integrated into functional safety
- Develop industry standard tools linked to JAMA, JasPar

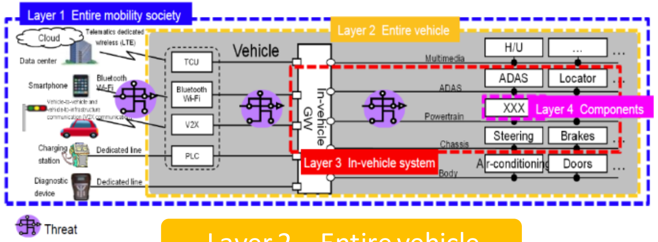
Overview of all tools (Conceptual diagram at completion)



◆ Development of vehicle evaluation guidelines

SIP-adus: Improper implementation oriented evaluation guidelines
JasPar: Design oriented guidelines

Consolidation of knowledge and experience in evaluation of actual devices is required.



Layer 2 Entire vehicle

⇒ Aim to integrate the above and achieve international standardization

a) Wiretapping on communication
b) Port scan
c) Fuzzing
d) Penetration
e) Jamming

Ⅰ Threat analysis study
Ⅱ Evaluation guidelines preparation
Ⅲ Large-scale field operational tests

January-April 2017	May-August	September-December	January-April 2018	May-August	September-December	January-March 2019

Public invitation for the test (selection of 3 companies)

Ⅰ Threat analysis study Conducted competitively by 3 companies

Stage gate screening (determination of FY2018 entrusted entities)
Ⅱ Guidelines preparation

Participant recruitment

Test preparations

Ⅲ Large-scale field operational tests

Ⅱ Guidelines update

◆ Development of vehicle evaluation guidelines (continued)

Current outcomes

- ◆ Introduction of R&D based **on 3-company competition** to formulate evaluation guidelines
- ◆ Selection of **1 evaluation vendor** following **stage-gate screening** (March) by a technical committee of experts based on the guidelines and ability to evaluate actual devices

⇒ Each commissioned company uses **a different approach**, which will clarify the **points of guideline formulation.**

Synopsys, Inc.

A developer of global security diagnostic tools that also has a presence in international standardization

PwC Consulting

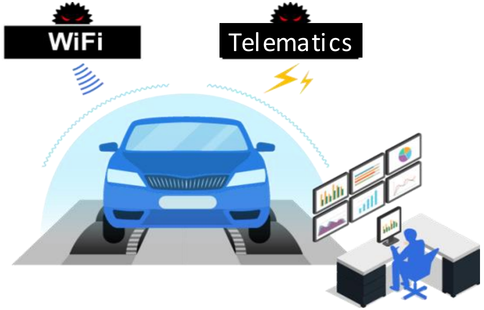
A company with a hardware hacking lab that can diagnose vulnerabilities in not only software but also hardware

Deloitte Tohmatsu Risk Services Co.

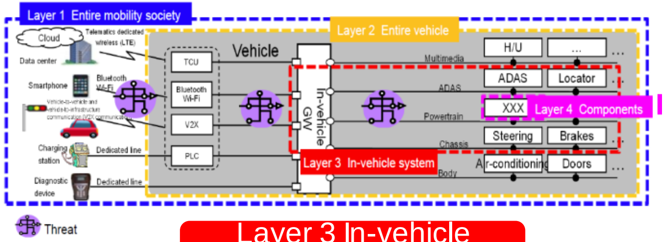
A specialist security company of the Deloitte Group, one of the world's most prominent general consulting networks

Next fiscal year

- ◆ Confirmation of the evaluation guidelines' validity and effectiveness through a **vehicle attack evaluation** by the selected evaluation vendor
- ◆ **Building of an Cyber Security evaluation system and international standardization** (with JasPar)



◆ Development of evaluation methods for in-vehicle communications (CAN)



Layer 3 In-vehicle system

① Using in-vehicle communication simulator, confirm

- Assumed attack methods
- Communications behavior during the attack

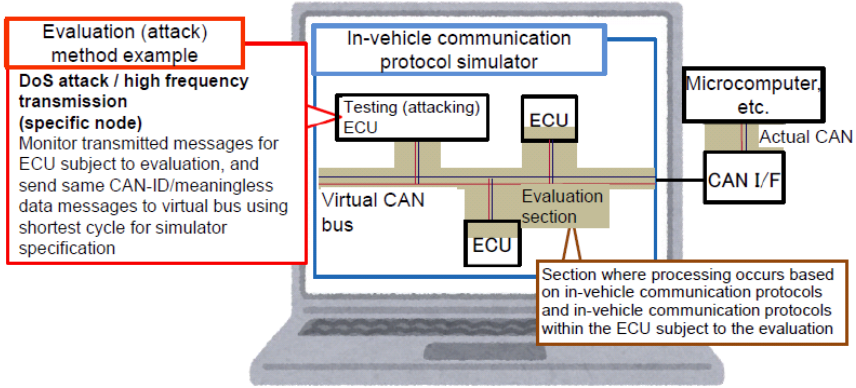
⇒ Building of virtual environments in addition to actual devices and simulation of attack

⇒ Scheduled for use as an evaluation database

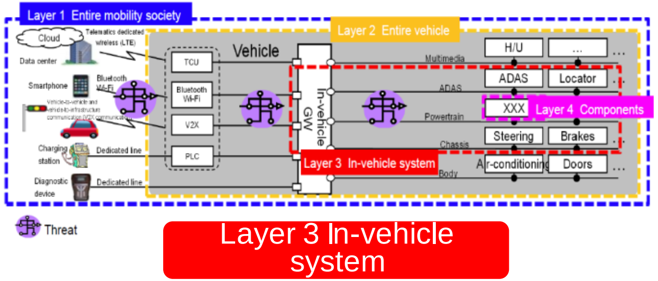
a) DoS attack
1) High-frequency transmission
2) Message collision
3) Transmission of malfunction message

b) Spoofing attack
1) Message replay
2) Message falsification
3) Transmission frequency falsification

⇒ Application to personnel training using simulator bench



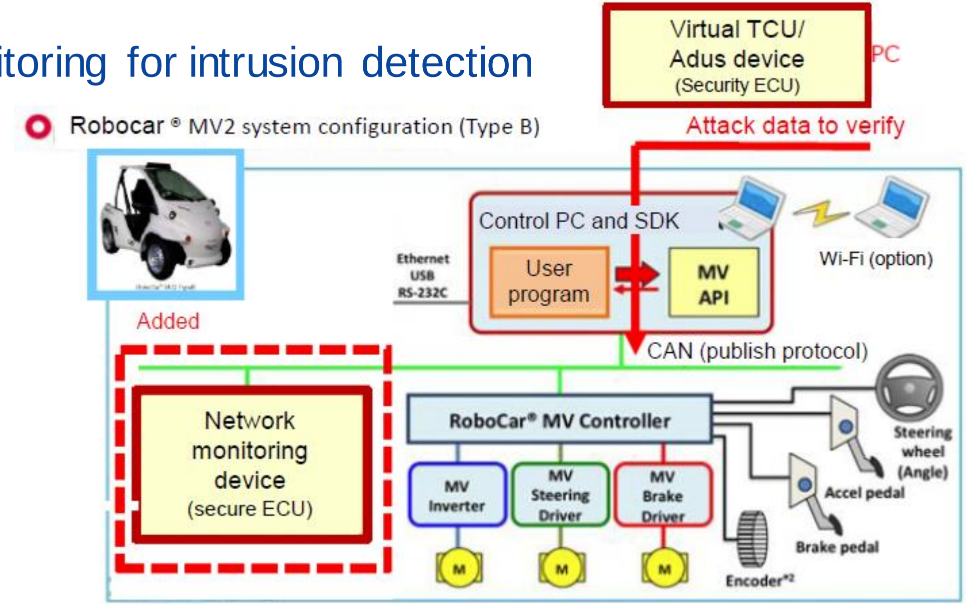
◆ Development of evaluation methods for in-vehicle communications (CAN) (continued)



② Intrusion detection guidelines

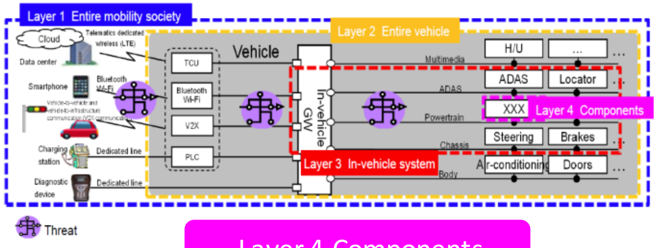
- CAN message cycle disturbance
- CAN message omission, etc.

⇒ Study of real-time monitoring for intrusion detection



Robocar ® MV2 system configuration example (Type B platform + control PC & SDK)

◆ Development of evaluation method for key distribution and reprogramming authentication



Layer 4 Components

Examine necessary standard target levels when reprogramming in accordance with on-board computer (ECU) security risk

- Encrypted algorithms
- Random bit number, entropy

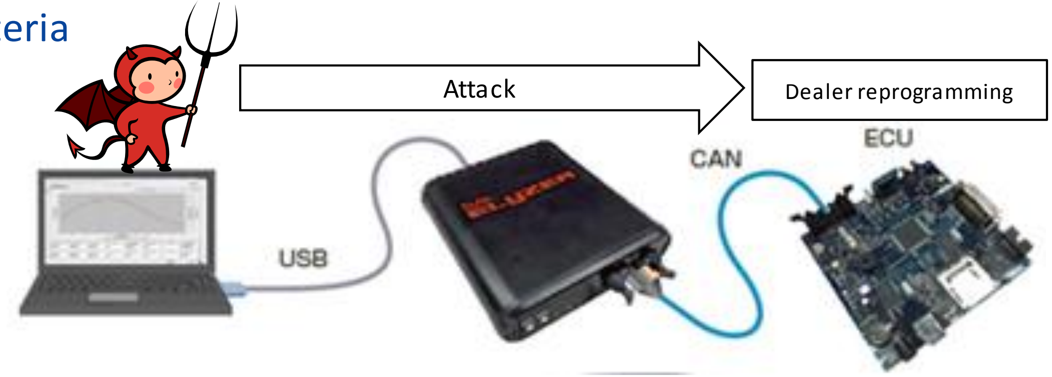
Assessment methodology

(1) Evaluation of actual device attack by evaluation board

(2) Study of key management in other industries*

*Bank ATMs, credit card payment terminals, smart meters

⇒ Calculation of costs associated with extraction (exposure) of confidential information and establishment of criteria



◆ Improving communications delays with V2X signature validation

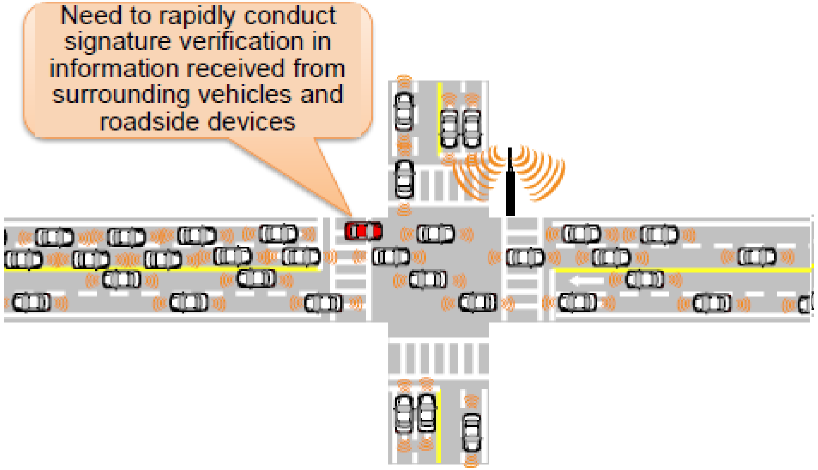
Background: Ensuring real-time information at time of V2X communication adoption

Research: Simplification of message signature verification process for messages in V2X communication

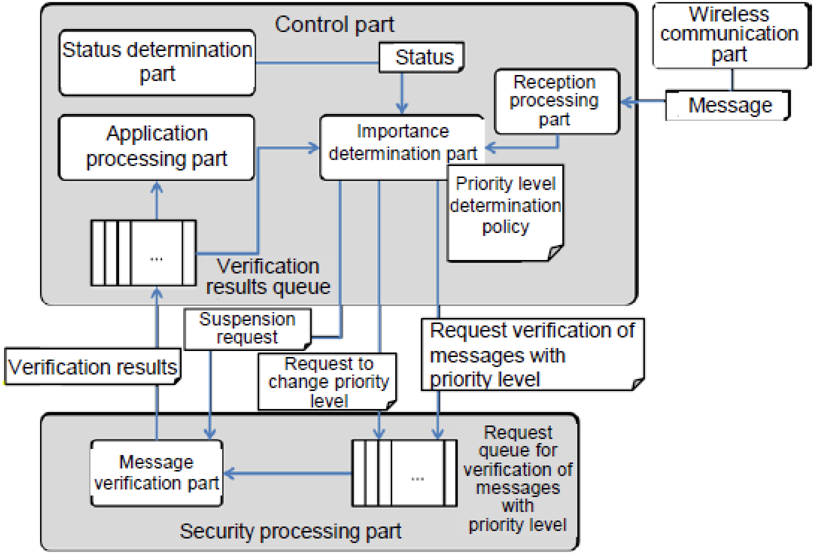
Target: 1,000 messages/second

⇒ Completion of performance targets for "message verification with priority levels"

- Confirm evaluation on actual devices
- Plan to move forward with standardization proposals, etc.. to ISO/TC204/WG16



Message verification method with priority levels



Results

1. Understanding built among OEMs and government bodies
   - Better understanding of areas of competition and areas of cooperation
   - Promotion of dialogue concerning legislation
2. Higher technical level/human resources development as an industry
3. Contribution to standardization proposals by Japan

Challenges

1. Reinforcement of cooperation among concerned organizations
   ⇒ Improvements are underway with the inclusion of JAMA and JasPar as members.
2. Continuity of SIP-adus' project outcomes
   - Sales and better usability of threat analysis tools
   - Updating of evaluation guidelines

   ⇒ Cultivation of standard evaluation organizations and businesses for the industry

Thank you