13th Japan ITS Promotion Forum

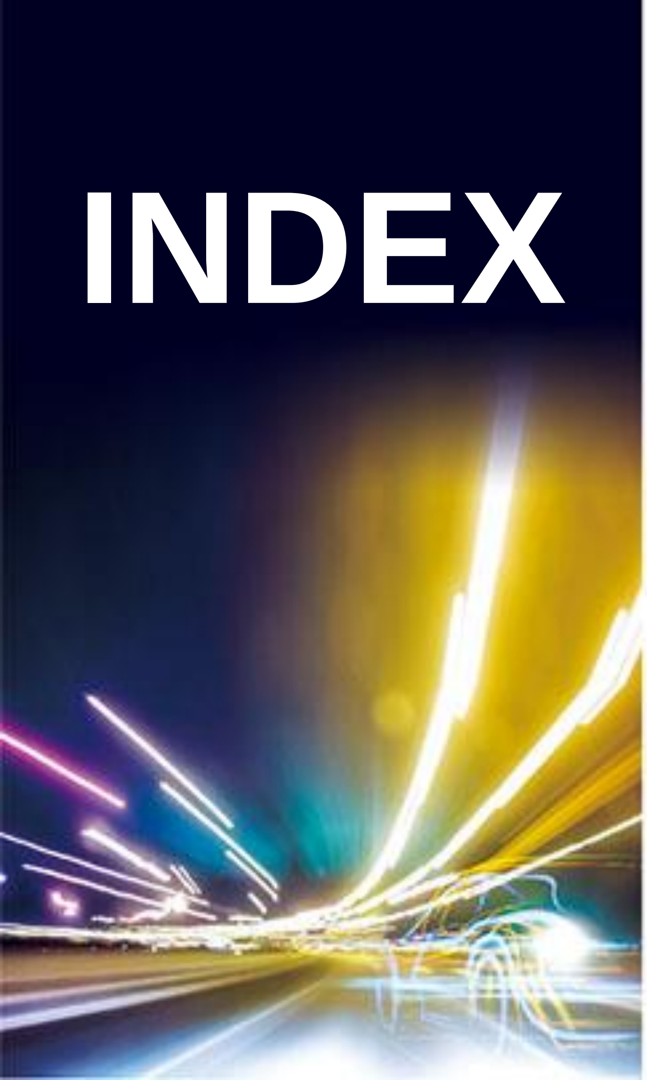
Automated Driving Systems

Cyber Security

Takashi Imai

SIP-adus International Cooperation Working Group

Toyota Info Technology Center Co., Ltd.



INDEX

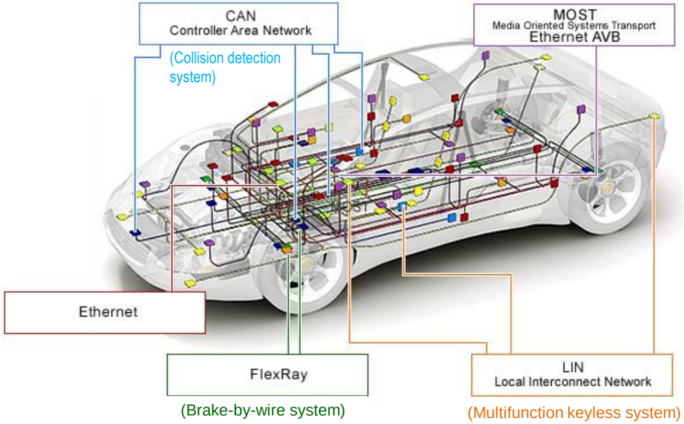
Industry Trends and SIP-adus Activities

1. Vehicle Security Trends
2. Initiatives by Automotive Industry Organizations
3. SIP-adus Initiatives

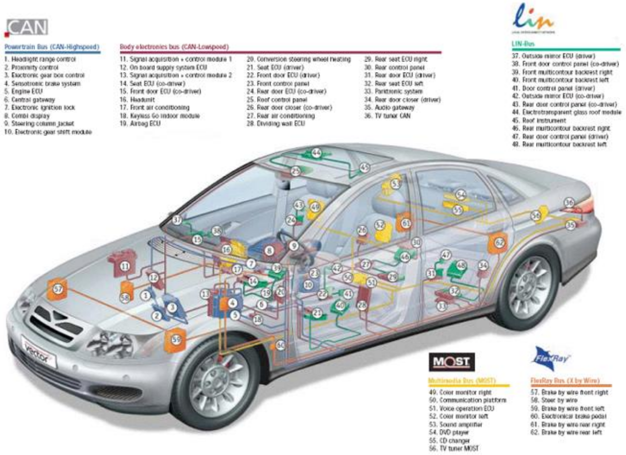
Vehicle Security Trends

Vehicle Composition

- The car systems consist of many electronic control units (ECU).
- They are linked by several onboard LAN depending on the characteristics and particularities of each application.
- Among them, the CAN (Controller Area Network) protocol is the de facto standard of onboard LAN. It is used to support the various car functions associated with “acceleration, steering, and braking.”


CAN
Controller Area Network
(Collision detection system)
MOST
Media Oriented Systems Transport
Ethernet AVB
MOST
Ethernet
FlexRay
(Brake-by-wire system)
LIN
Local Interconnect Network
(Multifunction keyless system)

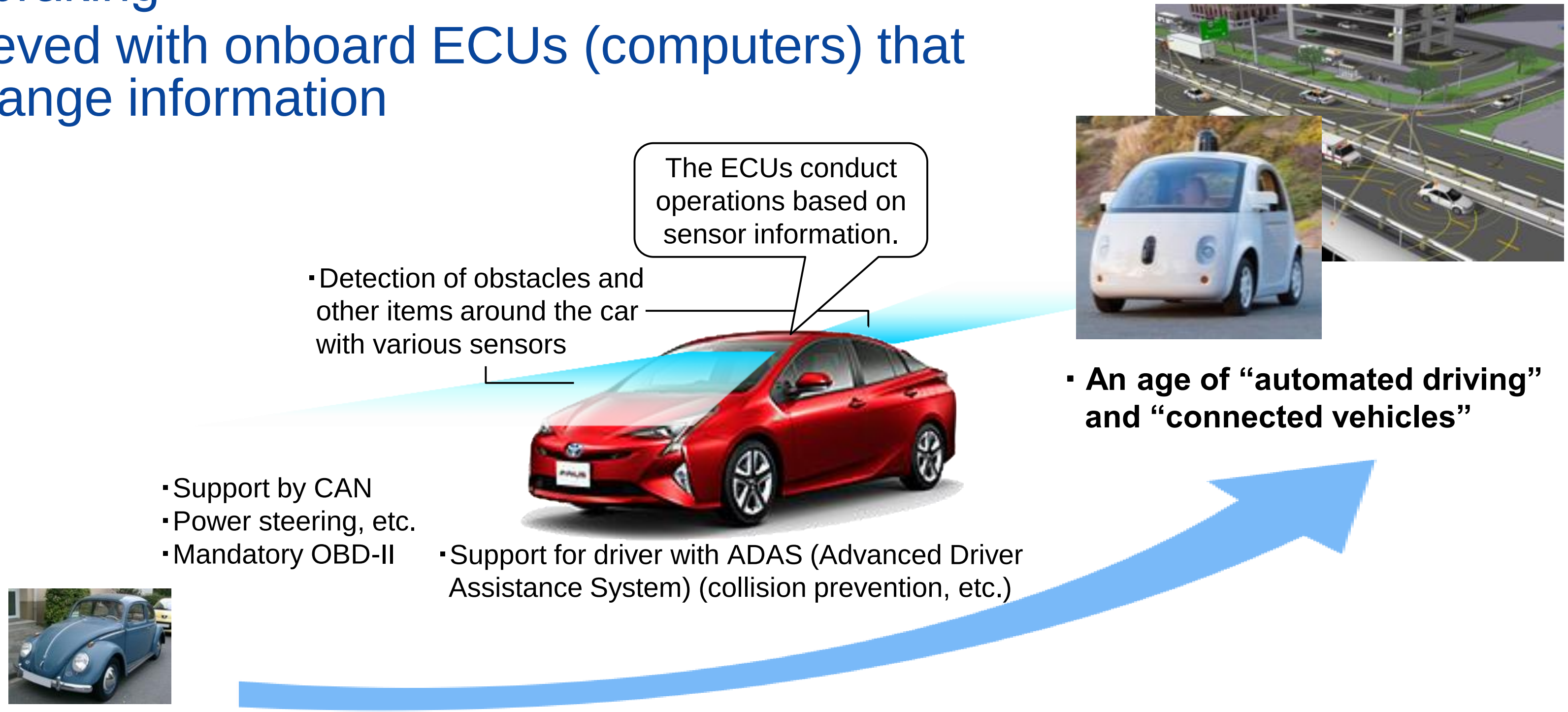
https://www.renesas.com/ja-jp/solutions/automotive/technology/networking.html


CAN
Powertrain Bus (CAN-Highspeed)
1. Headlight range control
2. Proximity control
3. Electronic gear box control
4. Sensotronic brake system
5. Engine ECU
6. Central gateway
7. Electronic ignition lock
8. Combi display
9. Steering column jacket
10. Electronic gear shift module
Body electronics bus (CAN-Lowspeed)
11. Signal acquisition + control module 1
12. On board supply system ECU
13. Signal acquisition + control module 2
14. Seat ECU (co-driver)
15. Front door ECU (co-driver)
16. Headunit
17. Front air conditioning
18. Keyless Go indoor module
19. Airbag ECU
20. Conversion steering wheel heating
21. Seat ECU (driver)
22. Front door ECU (driver)
23. Front control panel
24. Rear door ECU (co-driver)
25. Roof control panel
26. Rear door closer (co-driver)
27. Rear air conditioning
28. Dividing wall ECU
29. Rear seat ECU right
30. Rear control panel
31. Rear door ECU (driver)
32. Rear seat ECU left
33. Parktronic system
34. Rear door closer (driver)
35. Audio gateway
36. TV tuner CAN
lin
LIN-Bus
37. Outside mirror ECU (driver)
38. Front door control panel (co-driver)
39. Front multicontour backrest right
40. Front multicontour backrest left
41. Door control panel (driver)
42. Outside mirror ECU (co-driver)
43. Rear door control panel (co-driver)
44. Electrotransparent glass roof module
45. Roof instrument
46. Rear multicontour backrest right
47. Rear door control panel (driver)
48. Rear multicontour backrest left
MOST
Multimedia Bus (MOST)
49. Color monitor right
50. Communication platform
51. Voice operation ECU
52. Color monitor left
53. Sound amplifier
54. DVD player
55. CD changer
56. TV tuner MOST
FlexRay
FlexRay Bus (X by Wire)
57. Brake by wire front right
58. Steer by wire
59. Brake by wire front left
60. Electronical brake pedal
61. Brake by wire rear right
62. Brake by wire rear left
Vector

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, steering, and braking”
- Achieved with onboard ECUs (computers) that exchange information



・All operations performed by the driver

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

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

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

The ECUs conduct operations based on sensor information.

▪ **An age of “automated driving” and “connected vehicles”**

Vehicle Security Trends

Vehicle scenarios	*Advanced driver assistance, automated driving* Level 3 Level 4 *Connection* V2V V2G Use of big data V2X
Environmental changes surrounding vehicles	Expanding vehicle external communications, from standalone 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	Increased risk of cracking

Security counter-measures
Connected vehicle

Source: JasPar

Vehicle Security Trends

◆ The ability to hack vehicles is growing year by year.

’13

Conducted by boarding the vehicle
(communication injection)

*Attack made by analyzing communications beforehand

Source: KASPERSKY DAILY

’15

Successful remote hacking
(during low-speed driving)

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 accidents were caused by the remote attack

’16

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

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

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

’17

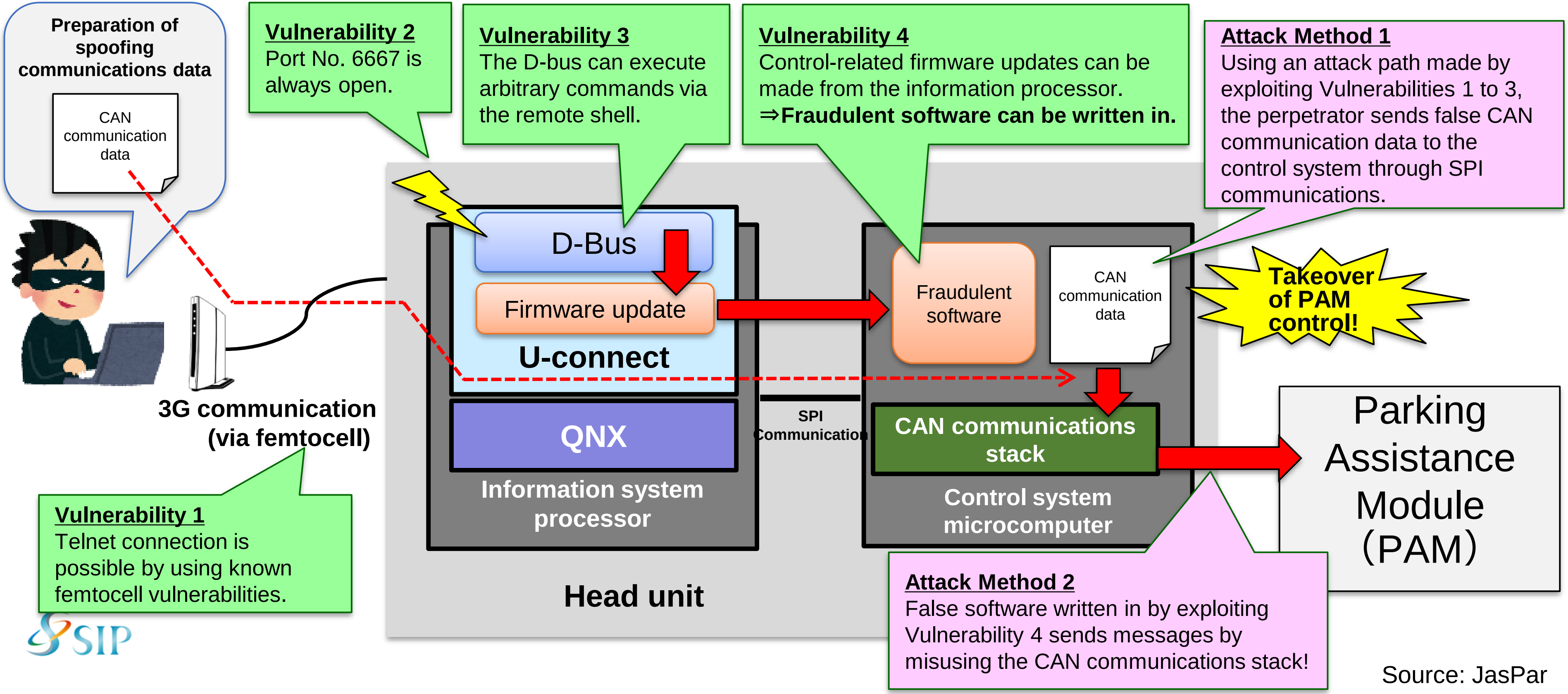
Control of vehicles by remotely attacking numerous vulnerabilities

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

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.



Preparation of spoofing communications data

Vulnerability 1
Telnet connection is possible by using known femtocell vulnerabilities.

Vulnerability 2
Port No. 6667 is always open.

Vulnerability 3
The D-bus can execute arbitrary commands via the remote shell.

Vulnerability 4
Control-related firmware updates can be made from the information processor.
⇒**Fraudulent software can be written in.**

Attack Method 1
Using an attack path made by exploiting Vulnerabilities 1 to 3, the perpetrator sends false CAN communication data to the control system through SPI communications.

Attack Method 2
False software written in by exploiting Vulnerability 4 sends messages by misusing the CAN communications stack!

Source: JasPar

2

Initiatives by Automotive Industry Organizations

Initiatives by Industry Organizations

◆ Difficulties in cyber security for vehicles

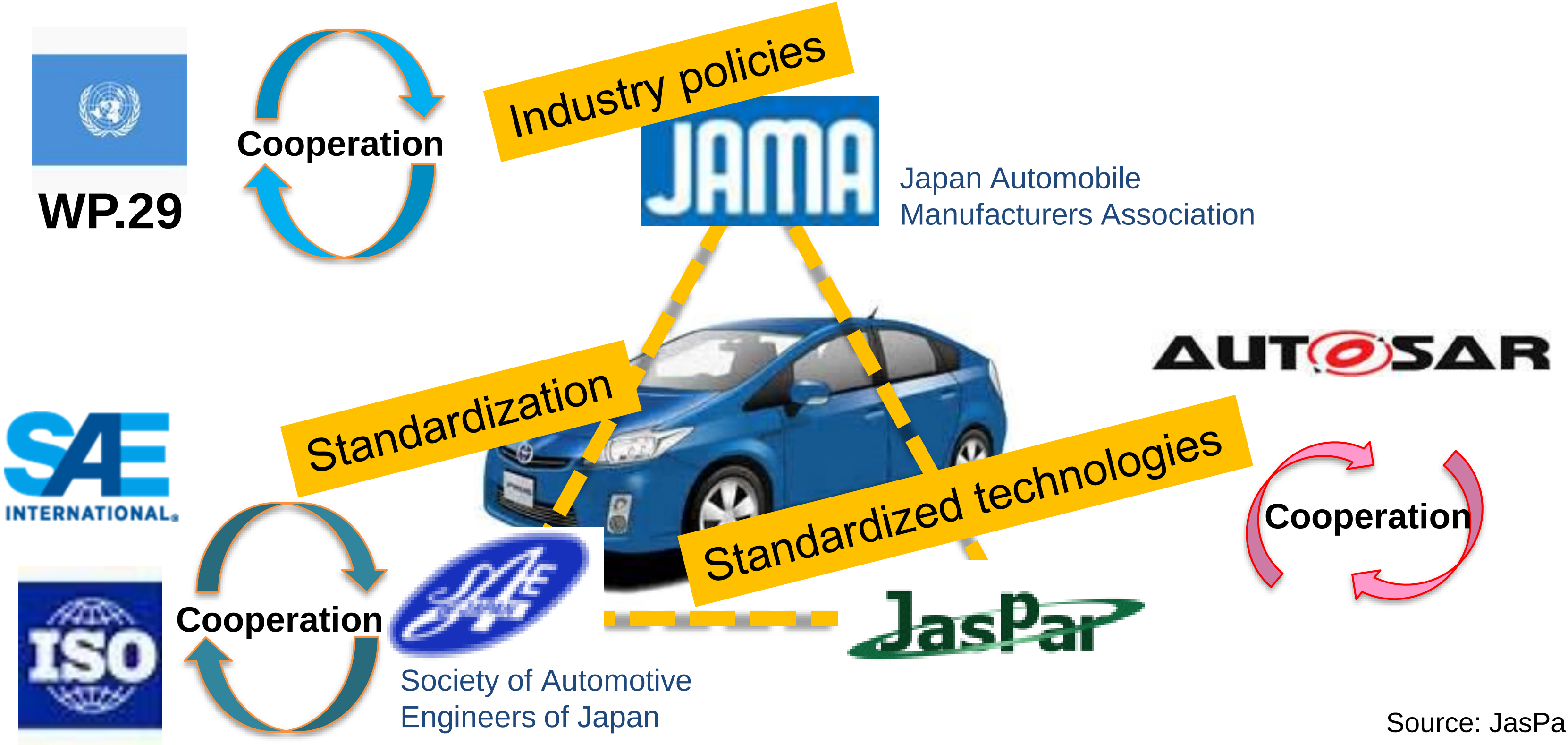
1. Unlike the IT industry, auto manufacturers also handle **customer safety**.
2. As opposed to **“functional safety” (random accidents)**, how should **“cyber security” (malicious intent)** be viewed?
3. Cars have a **long life cycle**.

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.

SIP

Initiatives by Industry Organizations

- Organizational roles are generally as follows:
  Planning: JAMA Requirements: JSAE Design: JasPar Operation: JAMA

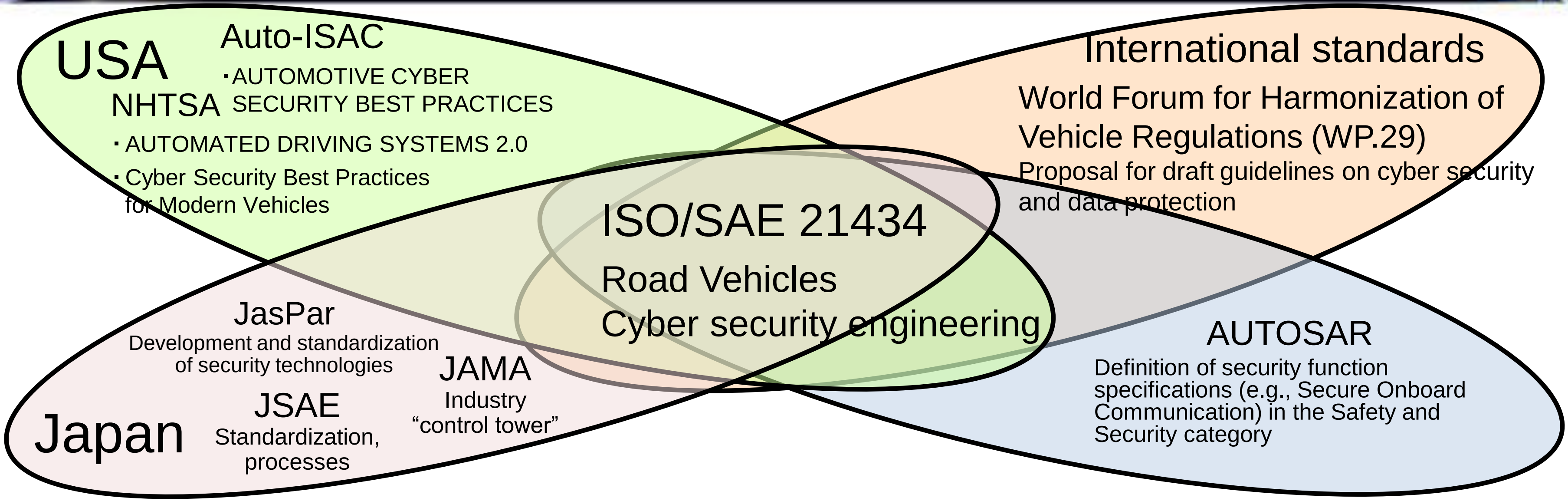


Japan Automobile Manufacturers Association

Society of Automotive Engineers of Japan

Source: JasPar

Developments in Security-Related Standardization/Legislation



USA

Auto-ISAC

・AUTOMOTIVE CYBER SECURITY BEST PRACTICES

NHTSA

・AUTOMATED DRIVING SYSTEMS 2.0

・Cyber Security Best Practices for Modern Vehicles

International standards

World Forum for Harmonization of Vehicle Regulations (WP.29)

Proposal for draft guidelines on cyber security and data protection

ISO/SAE 21434

Road Vehicles

Cyber security engineering

Japan

JasPar

Development and standardization of security technologies

JAMA

Industry "control tower"

JSAE

Standardization, processes

AUTOSAR

Definition of security function specifications (e.g., Secure Onboard Communication) in the Safety and Security category

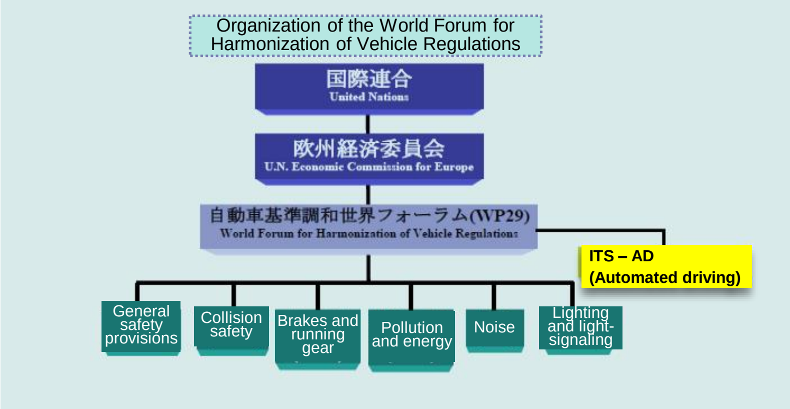
Organization name	Outline of activities
NHTSA	Formulation of regulations and guidelines for self-driving cars (including security requirements)
Auto-ISAC	Central organization for sharing information on incidents/vulnerabilities in the automobile industry
ISO/SAE 21434	Formulation of vehicle security 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)”



Organization of the World Forum for Harmonization of Vehicle Regulations

国際連合
United Nations

欧州経済委員会
U.N. Economic Commission for Europe

自動車基準調和世界フォーラム(WP29)
World Forum for Harmonization of Vehicle Regulations

ITS – AD
(Automated driving)

General safety provisions

Collision safety

Brakes and running gear

Pollution and energy

Noise

Lighting and light-signaling

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: JasPar

3

SIP-adus Initiatives

Objective and Overview of SIP-adus Security Measures

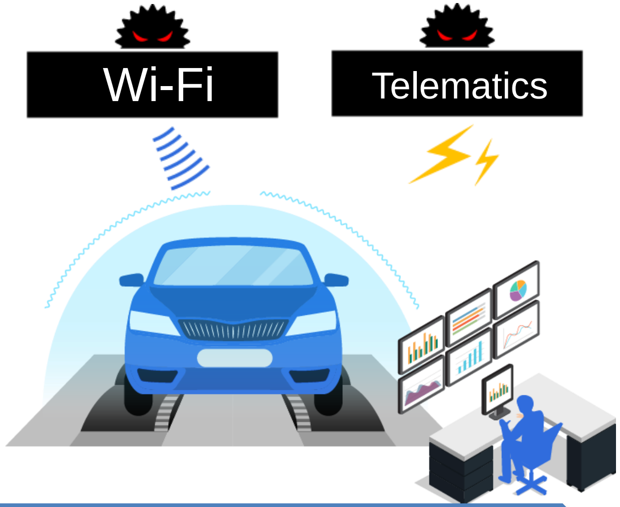
Objective: Establishment of guidelines for evaluating the cyber security defense performance of vehicles

(1) Threat analysis

- ◆ Investigation of system configurations, such as automated driving demonstrations conducted in the world
- ◆ Investigation of known vulnerabilities and incidents
- ◆ Risk/Impact analysis

(2) Formulation of security evaluation guidelines

(3) Verification by FOTs with domestic OEM



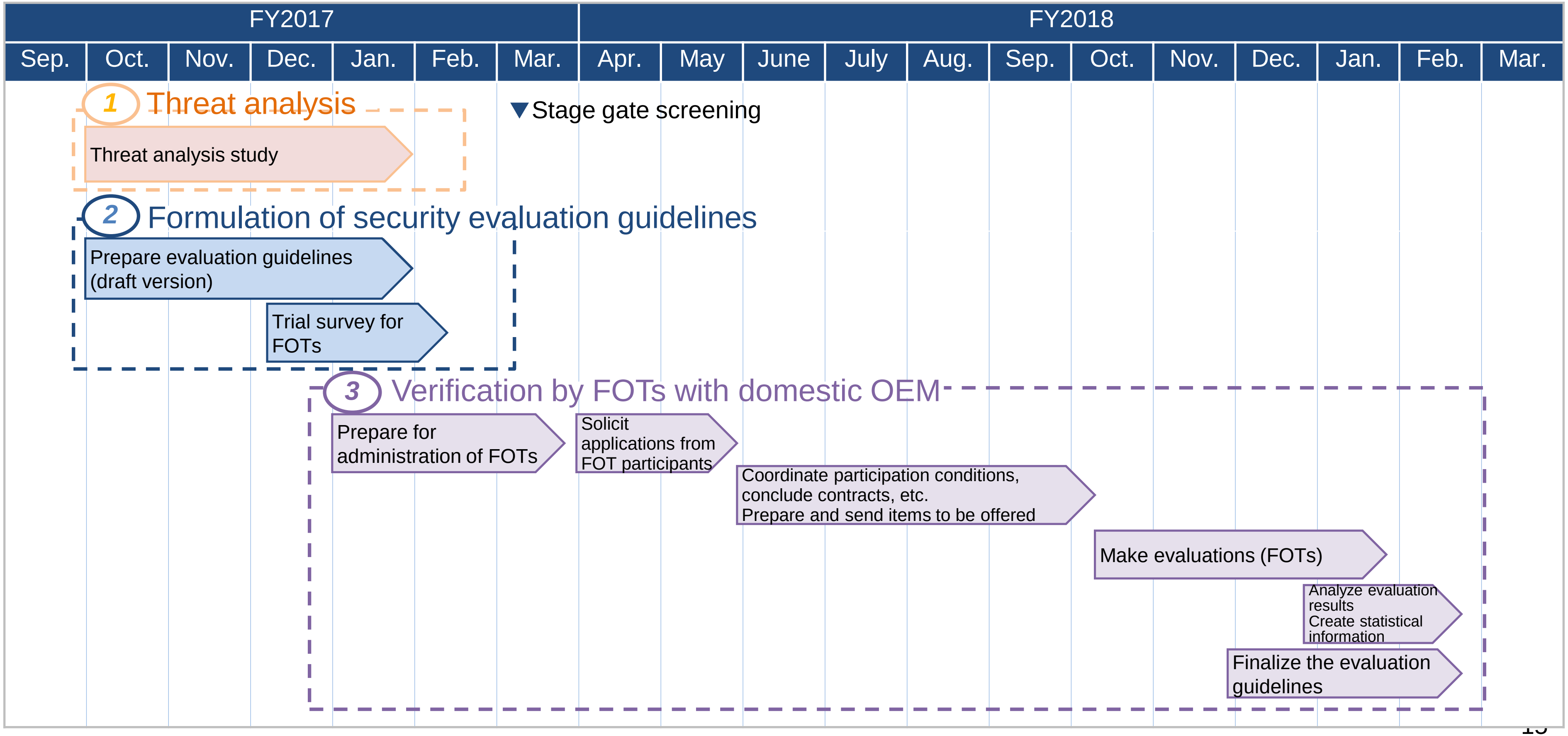
Guidelines were competitively formulated by each of three leading security vendors.

(1) Deloitte Tohmatsu Risk Services, (2) Nihon Synopsys,
(3) PwC Consulting & Cyber Defense Institute

The best guidelines were selected and proven.

PwC Consulting & Cyber Defense Institute

Overall Schedule



FY2017: Sep. Oct. Nov. Dec. Jan. Feb. Mar.

FY2018: Apr. May June July Aug. Sep. Oct. Nov. Dec. Jan. Feb. Mar.

▼Stage gate screening

1 Threat analysis

- Threat analysis study

2 Formulation of security evaluation guidelines

- Prepare evaluation guidelines (draft version)
- Trial survey for FOTs

3 Verification by FOTs with domestic OEM

- Prepare for administration of FOTs
- Solicit applications from FOT participants
- Coordinate participation conditions, conclude contracts, etc. Prepare and send items to be offered
- Make evaluations (FOTs)
- Analyze evaluation results Create statistical information
- Finalize the evaluation guidelines

3

(1)

SIP-adus Initiatives

Threat analysis study

Objective of Threat Analysis and Implementation Approach

Objective: Identify overall threats including attacks from outside of vehicles such as V2X related to automated driving

1 Creation of a list of services and functions related to automated driving

- Investigate the information disclosed by automakers, auto parts manufacturers, IT companies, etc., investigate the services related to automated driving systems and connected cars, and identify the functions to achieve such services

Survey targets

Automakers (16 companies)

Auto parts manufacturers (4 companies)

IT companies (23 companies)

List of services and functions

	Service	Function
1	Driving and parking assist	Inter-vehicle distance control Lane-keeping control Inter-vehicle distance control (in cooperation with ITS) Platooning Automated driving (in cooperation with ITS) Automated driving (autonomous) Display of image around the vehicle for parking Automated parking Automated parking (linked with a smartphone)
2		…

Input:
- Information disclosed by automakers (16 companies), auto parts manufacturers (3 companies), and IT companies (23 companies) (by referring to websites, etc.)

Output:
- List of services and functions

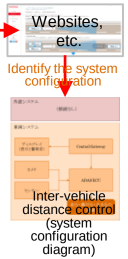
2 Determination of the expected system configuration for each function

- Conduct investigations based on the information disclosed by automakers and IT companies, and study the system configuration to achieve the functions

*The results of interviews with industry experts are also taken into account.

Expected system configuration for each function

	Service	Function
1	Driving and parking assist	Inter-vehicle distance control Lane-keeping control Inter-vehicle distance control (in cooperation with ITS) Platooning Automated driving (in cooperation with ITS) Automated driving (autonomous) Display of image around the vehicle for parking Automated parking Automated parking (linked with a smartphone)
2	…	…


Websites, etc.
Identify the system configuration
Inter-vehicle distance control (system configuration diagram)
Central Gateway
ADAS ECU

Input:
- List of services and functions
- Information about functions disclosed by main automakers and IT companies
- Opinions of experts in interviews

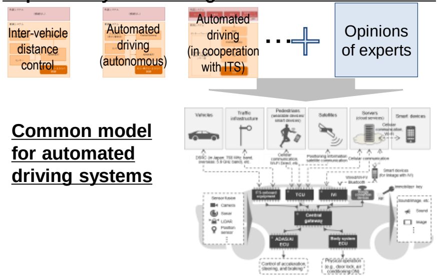
Output:
- Expected system configuration for each function

3 Identification of a common model for automated driving systems

- Identify the common model of automated driving systems in the threat analysis investigation by taking into account all the expected system configurations for each function

*The results of interviews with industry experts are also taken into account.

Expected system configuration for each function

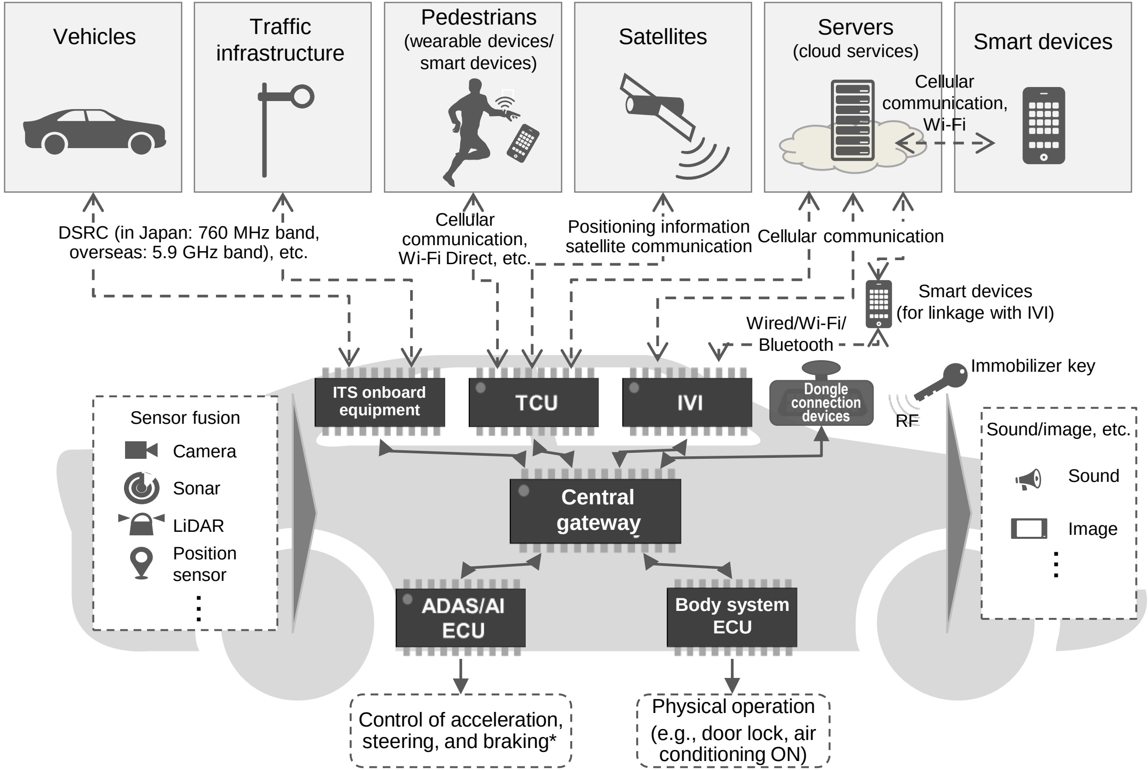


Common model for automated driving systems

Input:
- Expected system configuration for each function
- Opinions of experts in interviews

Output:
- **Common model of automated driving systems in the threat analysis investigation**

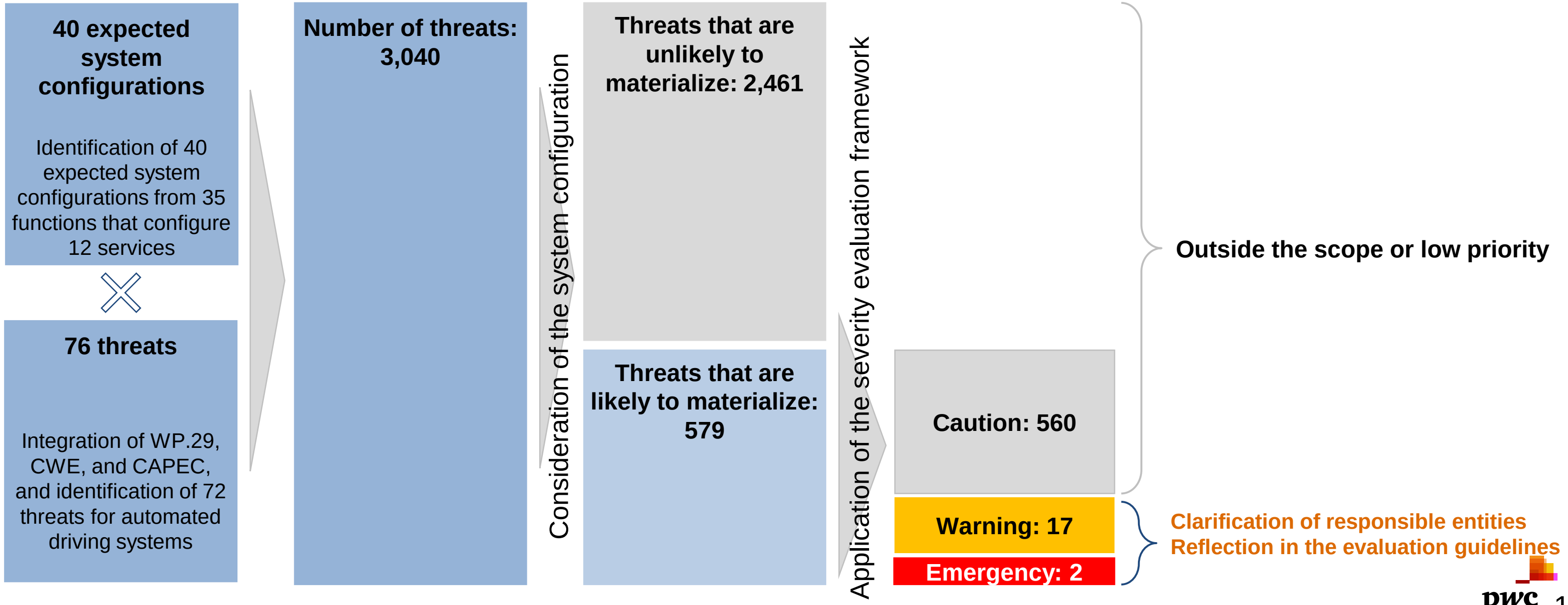
Common Model for Automated Driving Systems (Expected in the Early 2020s)


Vehicles
Traffic infrastructure
Pedestrians (wearable devices/ smart devices)
Satellites
Servers (cloud services)
Cellular communication, Wi-Fi
Smart devices
DSRC (in Japan: 760 MHz band, overseas: 5.9 GHz band), etc.
Cellular communication, Wi-Fi Direct, etc.
Positioning information satellite communication
Cellular communication
Smart devices (for linkage with IVI)
Wired/Wi-Fi/ Bluetooth
Immobilizer key
RF
ITS onboard equipment
TCU
IVI
Dongle connection devices
Sensor fusion
Camera
Sonar
LiDAR
Position sensor
⋮
Central gateway
Sound/image, etc.
Sound
Image
⋮
ADAS/AI ECU
Body system ECU
Control of acceleration, steering, and braking*
Physical operation (e.g., door lock, air conditioning ON)

*The topology of control functions for steering, braking, engine, etc. has been simplified because it does not affect the threat analysis results directly.

Overview of the Results of Threat Analysis (1)

- Identify threats that may materialize based on all the system configurations related to automated driving systems, apply a severity evaluation framework, and thereby identify threats that should be addressed with priority.
- Clarify the entities responsible for taking countermeasures against identified threats, and reflect threats that require countermeasures on the vehicle side in the evaluation guidelines.



40 expected system configurations

Identification of 40 expected system configurations from 35 functions that configure 12 services

×

76 threats

Integration of WP.29, CWE, and CAPEC, and identification of 72 threats for automated driving systems

Number of threats: 3,040

Consideration of the system configuration

Threats that are unlikely to materialize: 2,461

Threats that are likely to materialize: 579

Application of the severity evaluation framework

Caution: 560

Warning: 17

Emergency: 2

Outside the scope or low priority

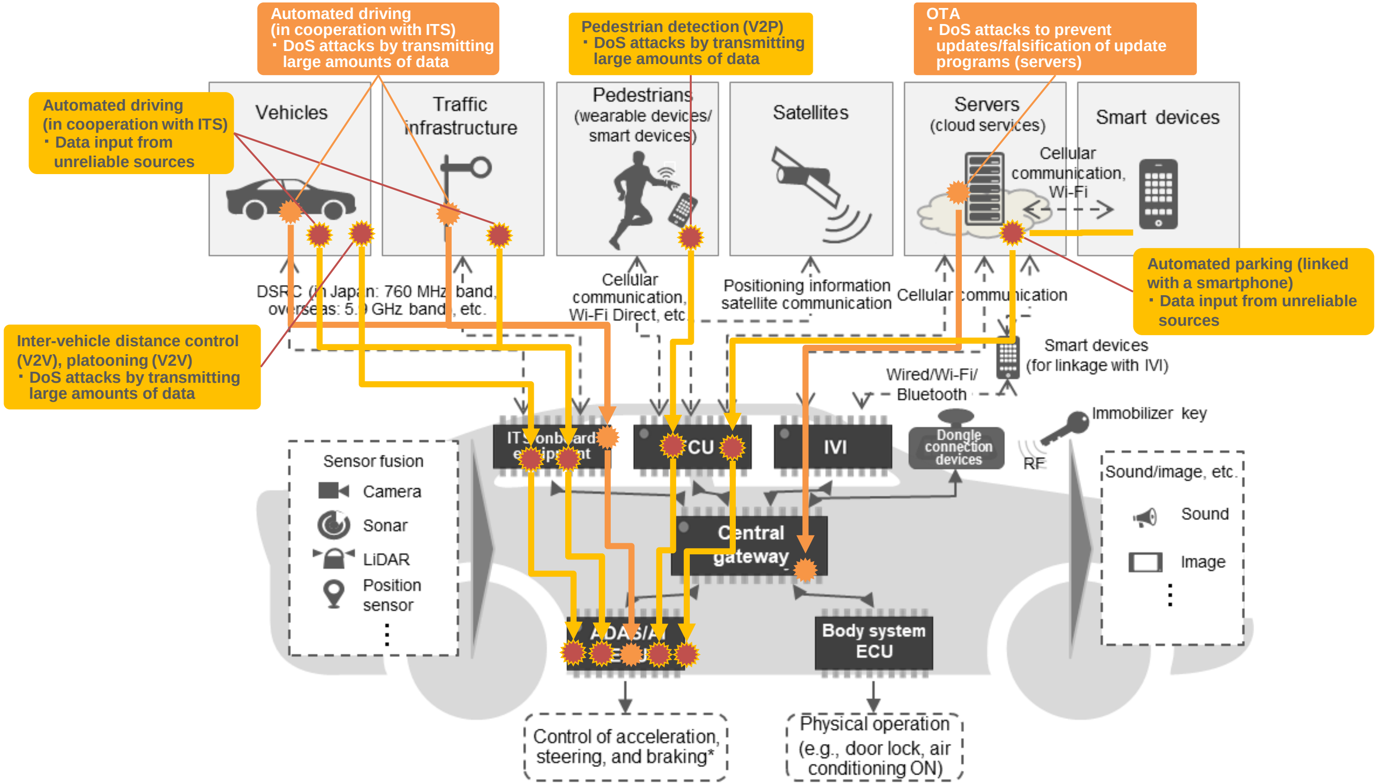
Clarification of responsible entities
Reflection in the evaluation guidelines

SIP

pwc

Overview of the Results of Threat Analysis (2)

Illustration of the common model for serious threats



Automated driving (in cooperation with ITS)
- DoS attacks by transmitting large amounts of data

Pedestrian detection (V2P)
- DoS attacks by transmitting large amounts of data

OTA
- DoS attacks to prevent updates/falsification of update programs (servers)

Automated driving (in cooperation with ITS)
- Data input from unreliable sources

Automated parking (linked with a smartphone)
- Data input from unreliable sources

Inter-vehicle distance control (V2V), platooning (V2V)
- DoS attacks by transmitting large amounts of data

Vehicles
Traffic infrastructure
Pedestrians (wearable devices/ smart devices)
Satellites
Servers (cloud services)
Smart devices
Cellular communication, Wi-Fi
DSRC (in Japan: 760 MHz band, overseas: 5.9 GHz band), etc.
Cellular communication, Wi-Fi Direct, etc.
Positioning information satellite communication
Cellular communication
Smart devices (for linkage with IVI)
Wired/Wi-Fi/ Bluetooth
Immobilizer key
RF
ITS onboard equipment
TCU
IVI
Dongle connection devices
Sensor fusion
Camera
Sonar
LiDAR
Position sensor
⋮
Central gateway
ADAS/AD ECU
Body system ECU
Sound/image, etc.
Sound
Image
⋮
Control of acceleration, steering, and braking*
Physical operation (e.g., door lock, air conditioning ON)

3

(2)

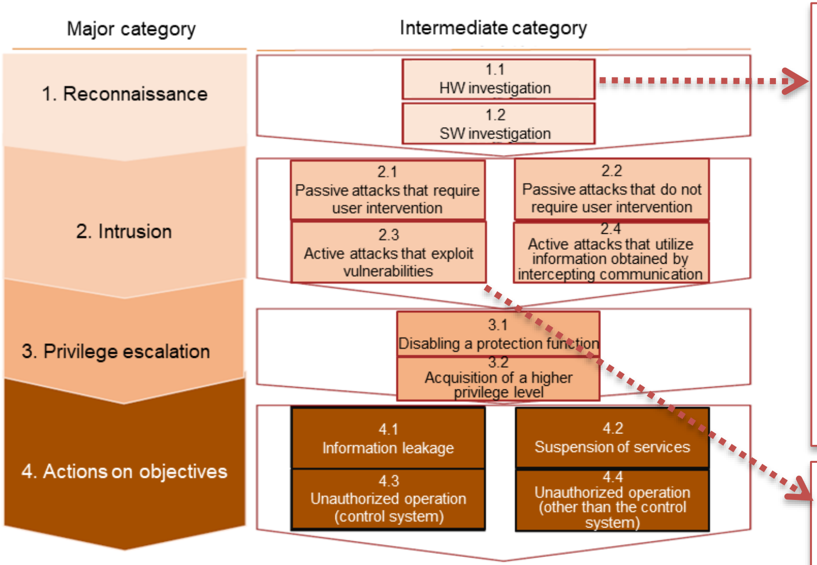
SIP-adus Initiatives

Formulation of security evaluation guidelines

Overview of the Guidelines

Conduct various cyber attacks to check that the security design information, etc. which is used as a foothold for intrusion into a vehicle is not stolen or that unauthorized operation does not occur due to attacks

Evaluation items



Major category | Intermediate category

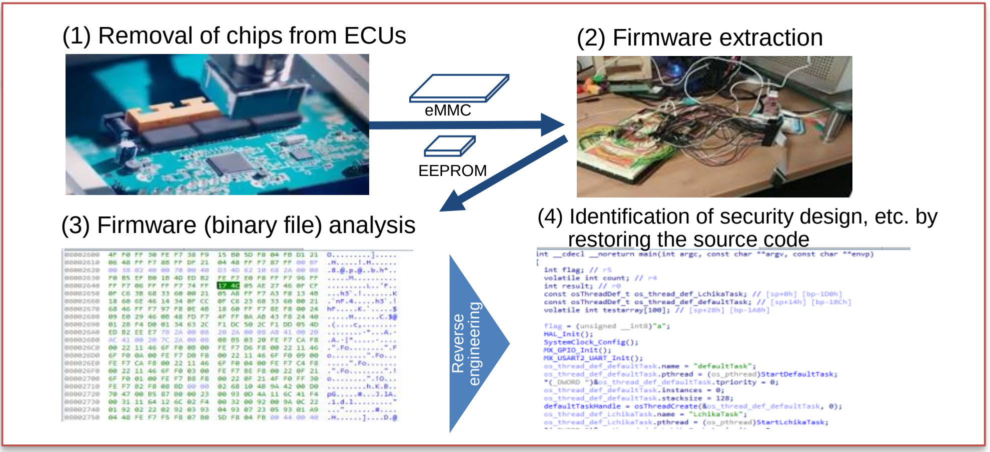
1. Reconnaissance
   - 1.1 HW investigation
   - 1.2 SW investigation

2. Intrusion
   - 2.1 Passive attacks that require user intervention
   - 2.2 Passive attacks that do not require user intervention
   - 2.3 Active attacks that exploit vulnerabilities
   - 2.4 Active attacks that utilize information obtained by intercepting communication

3. Privilege escalation
   - 3.1 Disabling a protection function
   - 3.2 Acquisition of a higher privilege level

4. Actions on objectives
   - 4.1 Information leakage
   - 4.2 Suspension of services
   - 4.3 Unauthorized operation (control system)
   - 4.4 Unauthorized operation (other than the control system)

Example of evaluation contents



(1) Removal of chips from ECUs

(2) Firmware extraction

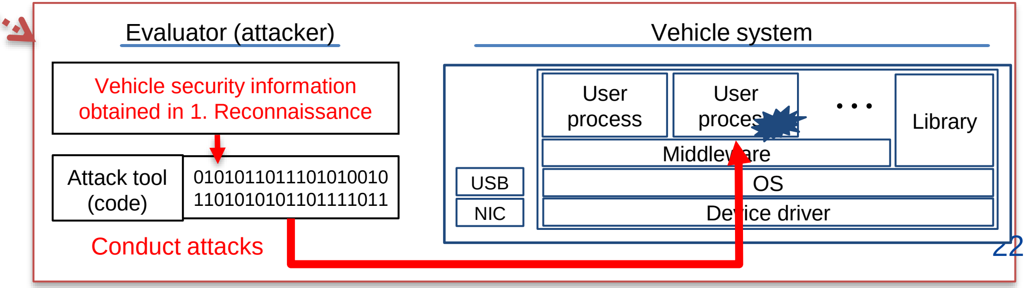
(3) Firmware (binary file) analysis

```
08002600  4F F0 FF 30 FE F7 38 F9  15 B0 5D F8 04 FB D1 21  O.........]......
08002610  06 48 FF F7 88 FF DF 21  04 48 FF F7 87 FF 00 BF  .H.....!.H.......
08002620  00 38 02 40 00 70 00 40  D3 4D 62 10 68 2A 00 08  .8.@.p.@..b.h*..
08002630  F0 B5 EF B0 18 4D ED B2  FE F7 E0 F8 FF F7 96 FF  .....M..........
08002640  FF F7 06 FF FF F7 74 FF  17 4C 05 AE 27 46 0F CF  .........L..'F..
08002650  0F C6 3B 68 33 60 00 21  05 A8 FF F7 A3 F8 13 48  ...h3`.!.......K
08002660  18 60 6E 46 14 34 0F CC  0F C6 23 68 33 60 00 21  .`nF.4.....h3`.!
08002670  68 46 FF F7 97 F8 0E 48  18 60 FF F7 8E F8 00 24  hF.....K.`.....$
08002680  09 E0 29 46 08 48 FD F7  4F FF 0A AB 43 F8 24 40  .....H......C.$@
08002690  01 28 F4 D0 01 34 63 2C  F1 DC 50 2C F1 DD 05 4D  .(....c,........
080026A0  ED B2 EE E7 78 2A 00 08  20 2A 00 08 A8 41 00 20  .........*...A.-
080026B0  AC 41 00 20 7C 2A 00 08  08 B5 03 20 FE F7 CA F8  .A.-|*......-....
080026C0  00 22 11 46 6F F0 08 00  FE F7 D6 F8 00 22 11 46  .".Fo........".F
080026D0  6F F0 0A 00 FE F7 D0 F8  00 22 11 46 6F F0 09 00  o........".Fo...
080026E0  FE F7 CA F8 00 22 11 46  6F F0 04 00 FE F7 C4 F8  .....".Fo.......
080026F0  00 22 11 46 6F F0 03 00  FE F7 BE F8 00 22 0F 21  .".Fo........".!
08002700  6F F0 01 00 FE F7 B8 F8  00 22 0F 21 4F F0 FF 30  o........".!O...
08002710  FE F7 B2 F8 08 BD 00 00  02 68 10 4B 9A 42 00 D0  .........h.K.B..
08002720  70 47 00 B5 87 B0 00 23  00 93 0D 4A 11 6C 41 F4  pG.....#...J.lA.
08002730  00 31 11 64 12 6C 02 F4  00 32 00 92 00 9A 0C 22  .1.d.l.........."
08002740  01 92 02 22 02 92 03 93  04 93 07 23 05 93 01 A9  ..."......#.....
08002750  04 48 FE F7 F5 F8 07 B0  5D F8 04 FB 00 44 00 40  .H......]....D.@
```

(4) Identification of security design, etc. by restoring the source code

```
int __cdecl __noreturn main(int argc, const char **argv, const char **envp)
{
  int flag; // r5
  volatile int count; // r4
  int result; // r0
  const osThreadDef_t os_thread_def_LchikaTask; // [sp+0h] [bp-1D0h]
  const osThreadDef_t os_thread_def_defaultTask; // [sp+14h] [bp-1BCh]
  volatile int testarray[100]; // [sp+28h] [bp-1A8h]

  flag = (unsigned __int8)"a";
  HAL_Init();
  SystemClock_Config();
  MX_GPIO_Init();
  MX_USART2_UART_Init();
  os_thread_def_defaultTask.name = "defaultTask";
  os_thread_def_defaultTask.pthread = (os_pthread)StartDefaultTask;
  *(_DWORD *)&os_thread_def_defaultTask.tpriority = 0;
  os_thread_def_defaultTask.instances = 0;
  os_thread_def_defaultTask.stacksize = 128;
  defaultTaskHandle = osThreadCreate(&os_thread_def_defaultTask, 0);
  os_thread_def_LchikaTask.name = "LchikaTask";
  os_thread_def_LchikaTask.pthread = (os_pthread)StartLchikaTask;
```



Evaluator (attacker)

Vehicle security information obtained in 1. Reconnaissance

Attack tool (code) | 01010110111010100010 11010101011101111011

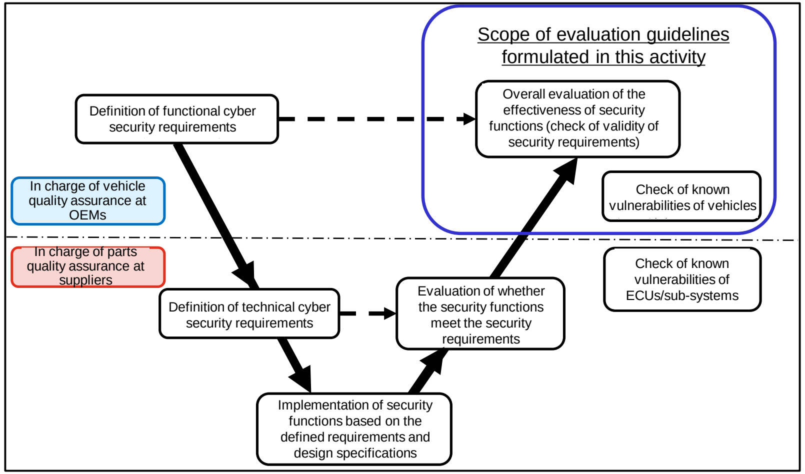
Conduct attacks

Vehicle system

Scope and Characteristics of the Guidelines

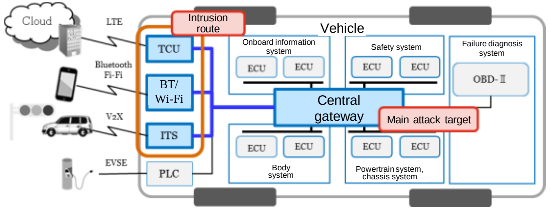
Scope

- A policy was established to create guidelines that can be used in the overall evaluation, etc. in the V-shaped model of the vehicle development based on the results of discussions with stakeholders (e.g., vehicle OEMs, JasPar) and threat analysis.

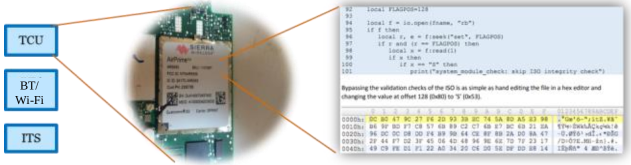

Scope of evaluation guidelines formulated in this activity
Definition of functional cyber security requirements
Overall evaluation of the effectiveness of security functions (check of validity of security requirements)
In charge of vehicle quality assurance at OEMs
Check of known vulnerabilities of vehicles
In charge of parts quality assurance at suppliers
Check of known vulnerabilities of ECUs/sub-systems
Definition of technical cyber security requirements
Evaluation of whether the security functions meet the security requirements
Implementation of security functions based on the defined requirements and design specifications

Characteristics

1. Evaluation by intrusion tests from I/F outside of vehicles from the viewpoint of real hackers (attackers)



2. The evaluation targets also include HW security countermeasures that take into account the actual attacks on vehicles.



```
local FLAGPOS=128

local f = io.open(fname, "rb")
if f then
   local r, e = f:seek("set", FLAGPOS)
   if r and (r == FLAGPOS) then
      local x = f:read(1)
      if x then
         if x == "S" then
            print("system_module_check: skip ISO integrity check")
```

Bypassing the validation checks of the ISO is as simple as hand editing the file in a hex editor and changing the value at offset 128 (0x80) to 'S' (0x53).

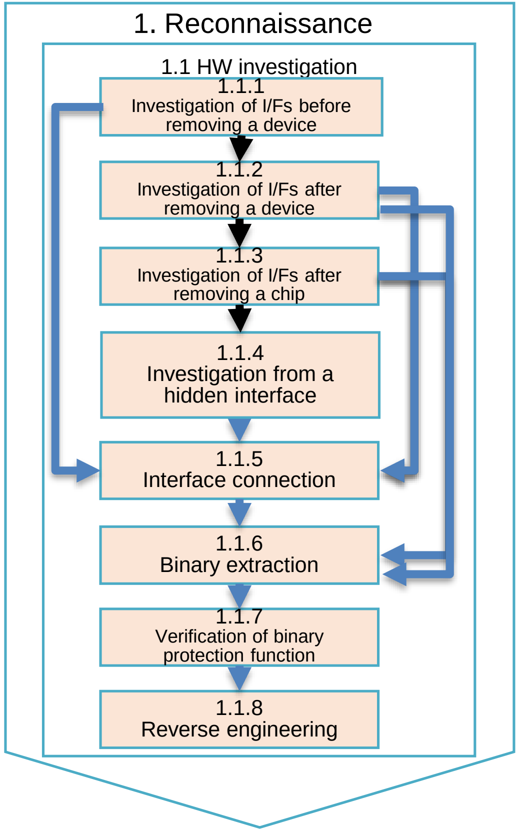
```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
0000h: DC 80 47 9C 27 F6 2D 93 3B 3C 74 5A 8D A5 E3 98
0010h: B6 9F BD F7 C8 57 6B B9 C2 C7 6B E7 BC 6B 21 EA
0020h: 96 DC 0C D8 DD F4 B9 90 64 CE 8F 8B 2A D0 8A 47
0030h: 2F 44 F7 D2 3F 45 06 4D 48 96 9E 6E 7D 7F 23 17
0040h: 49 C9 FE D1 F1 22 A0 34 20 C6 D0 5E DF DD E8 14
```

Source of Information for Guidelines (Vehicle Incidents)

The guidelines were established by profiling actual vehicle incidents in the past and incorporating techniques for reproducing them, thus helping to prevent similar vehicle incidents.

Incident example	Incident overview
Vulnerability of Jeep Cherokee’s Uconnect	The vehicle position is identified and the vehicle is controlled remotely by a third party. An attacker intrudes into the onboard equipment through an open port on the cellular network and falsifies the firmware of the CAN controller to enable the vehicle to be remotely controlled.
Vulnerability of BMW’s ConnectedDrive	A vehicle may be remotely controlled by a third party. The doors can be unlocked by sending a door unlock command to a vehicle from a telematics server prepared by the researchers.
Vulnerability of Tesla Model S wireless LAN	A vehicle is remotely controlled by a third party. The researchers proposed a method of directing the user to an attack site using a fake Wi-Fi spot. Attacks through the cellular network are also possible. In this case, a decoy email, etc. is used to direct the user to an attack site.
Vulnerability of Mitsubishi Outlander’s mobile app	The environment settings (e.g., air conditioning settings) are remotely controlled by a third party. The security device settings and air conditioning operation can be remotely controlled by accessing a Wi-Fi spot in the cabin.
Vulnerability of NissanConnect EV	The development settings, which are not used by general users, remain in the system. Classified information (e.g., user ID, password) can be leaked by using these settings.
Vulnerability of Nissan Leaf	The authentication system is inappropriate. The authentication mechanism is not implemented in the smartphone ⇔ server API. Other vehicles can be controlled if the last five digits of the VIN are found. * This is a vulnerability of the smartphone app. A check will be conducted to see if similar events occur between a vehicle and a server or between a vehicle and a smartphone.
Vulnerability of Subaru’s STARLINK	No expiration time is set for the security tokens which are used to authenticate smartphone devices. If security tokens are stolen, the doors could be unlocked by a third party. * This is a vulnerability of the smartphone app. A check will be conducted to see if similar events occur between a vehicle and a server or between a vehicle and a smartphone.
Vulnerability of Continental AG’s TCU	A TCU can be remotely controlled by a third party.
Vulnerability of Mazda Connect	An arbitrary code is executed from an onboard USB port. The vulnerability was used for AVN customization. * This is a local attack, but was included as an issue to evaluate resistance against reverse engineering.
Vulnerability of Honda Connect	An arbitrary code is executed from an onboard USB port. The vulnerability was used for AVN customization. * This is a local attack, but was included as an issue to evaluate resistance against reverse engineering.

1. Reconnaissance/1.1 HW investigation



1. Reconnaissance

1.1 HW investigation

1.1.1
Investigation of I/Fs before removing a device

1.1.2
Investigation of I/Fs after removing a device

1.1.3
Investigation of I/Fs after removing a chip

1.1.4
Investigation from a hidden interface

1.1.5
Interface connection

1.1.6
Binary extraction

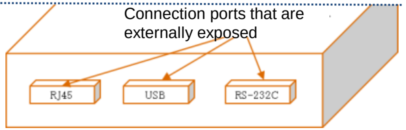
1.1.7
Verification of binary protection function

1.1.8
Reverse engineering

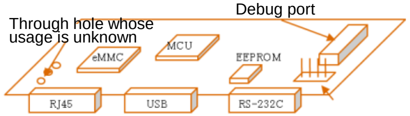
Evaluation policy

- An attacker attempts to extract data from *all the I/Fs used* by the vehicle HW (vehicle, devices, chips) *for data input/output*. When data extraction is successful, the binary file is reversed to analyze the system.

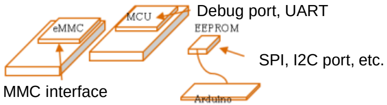
1.1.1 Target I/Fs:
RJ45, USB, RS-232C, etc.



1.1.2 Target I/Fs:
Debug port (e.g., JTAG), UART, unknown through hole



1.1.3 Target I/Fs:
Debug port, UART (pin), MMC I/F, SPI, I2C port, etc.

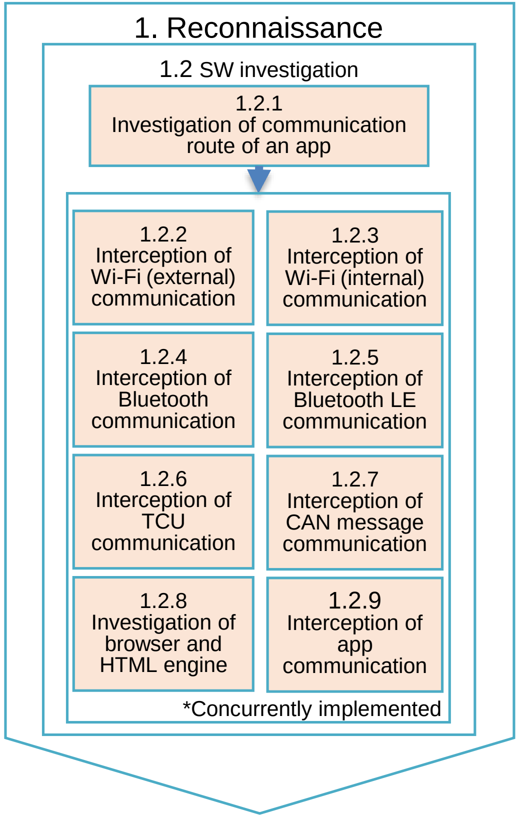


Evaluation items included other than incidents

- Techniques for extracting data from I/Fs, other than the data input/output I/Fs, in binary extraction were itemized.

e.g. Extraction by reversing the register bits using laser radiation
Extraction by scanning a semiconductor circuit using a microscope
Data extraction from secure elements and analysis

1. Reconnaissance/1.2 SW investigation



1. Reconnaissance

1.2 SW investigation

1.2.1 Investigation of communication route of an app

1.2.2 Interception of Wi-Fi (external) communication

1.2.3 Interception of Wi-Fi (internal) communication

1.2.4 Interception of Bluetooth communication

1.2.5 Interception of Bluetooth LE communication

1.2.6 Interception of TCU communication

1.2.7 Interception of CAN message communication

1.2.8 Investigation of browser and HTML engine

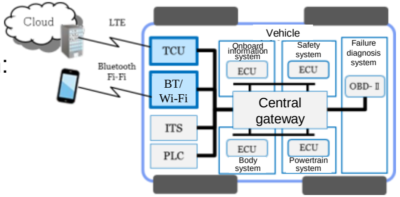
1.2.9 Interception of app communication

*Concurrently implemented

Evaluation policy

- An attacker attempts to intercept the following wireless communication (components with wireless communication functions) of the vehicle system and obtains information necessary for intrusion and spoofing.

Target communication:
- TCU (3G/4G)
- Wi-Fi
- Bluetooth

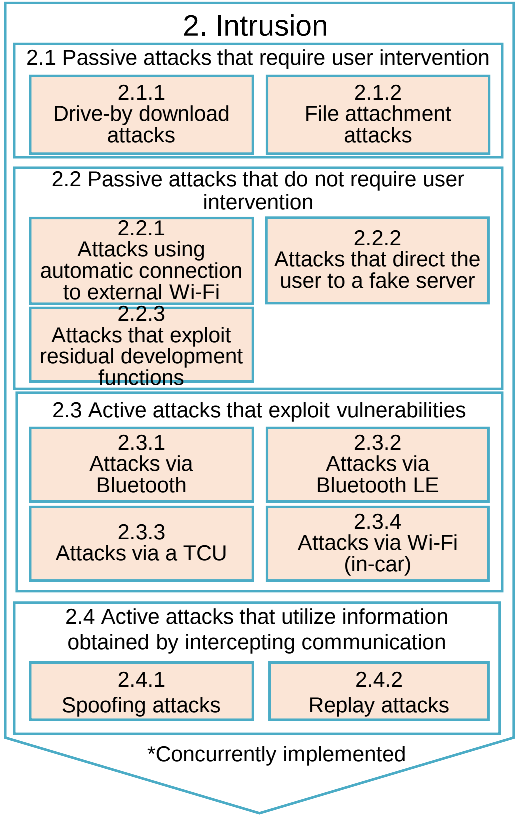


- An attacker attempts to intercept the transmitted/ received data of all the apps that use the wireless I/Fs above and obtains information necessary for intrusion and spoofing.

Evaluation items included other than incidents

- There were Bluetooth-related incidents in the vehicle component systems such as Bosch’s Bluetooth dongle. The details were itemized.

2. Intrusion



2. Intrusion

2.1 Passive attacks that require user intervention

- 2.1.1 Drive-by download attacks
- 2.1.2 File attachment attacks

2.2 Passive attacks that do not require user intervention

- 2.2.1 Attacks using automatic connection to external Wi-Fi
- 2.2.2 Attacks that direct the user to a fake server
- 2.2.3 Attacks that exploit residual development functions

2.3 Active attacks that exploit vulnerabilities

- 2.3.1 Attacks via Bluetooth
- 2.3.2 Attacks via Bluetooth LE
- 2.3.3 Attacks via a TCU
- 2.3.4 Attacks via Wi-Fi (in-car)

2.4 Active attacks that utilize information obtained by intercepting communication

- 2.4.1 Spoofing attacks
- 2.4.2 Replay attacks

*Concurrently implemented

Evaluation policy

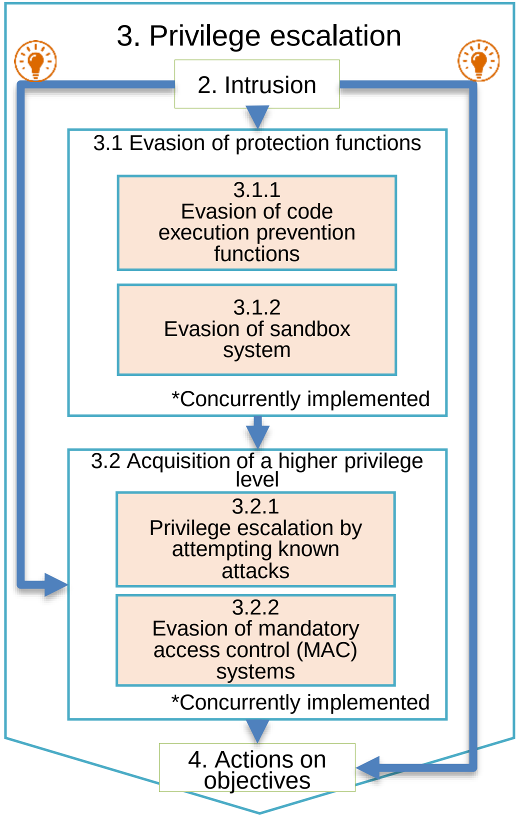
- An attacker attempts attacks via wireless I/Fs until a system console becomes available (intrusion).
- The attack patterns were classified based on the "vehicle NW access condition" and "occupant involvement" that affect the method of attacks.

Occupant involvement / NW access	Attacks that require the occupant's intervention (tricking a user)	Automated attacks that do not require the occupant's intervention (tricking a device)
No direct connection to a vehicle from the external NW (external response only)	Attacks that depend on the occupant's operation to start execution of an attack program Evaluation item 2.1	Change the target that is automatically accessed by the system based on the intention of an attacker Evaluation item 2.2
Direct access to a vehicle is possible from the external NW	(N/A)	Attacks that exploit vulnerabilities of various I/Fs (Evaluation item 2.3) Attacks that use information derived from intercepted communication (Evaluation item 2.4)

Evaluation items included other than incidents

- There were Bluetooth-related incidents in the vehicle component systems such as Bosch's Bluetooth dongle. The details were itemized.
- It was judged that advanced persistent threats should be considered because there are many attacks on IT security and significant damage is caused. Thus, the file attachment attacks and attacks that direct the user to a fake server were itemized.

3. Privilege escalation


3. Privilege escalation
2. Intrusion
3.1 Evasion of protection functions
3.1.1
Evasion of code execution prevention functions
3.1.2
Evasion of sandbox system
*Concurrently implemented
3.2 Acquisition of a higher privilege level
3.2.1
Privilege escalation by attempting known attacks
3.2.2
Evasion of mandatory access control (MAC) systems
*Concurrently implemented
4. Actions on objectives

Evaluation policy

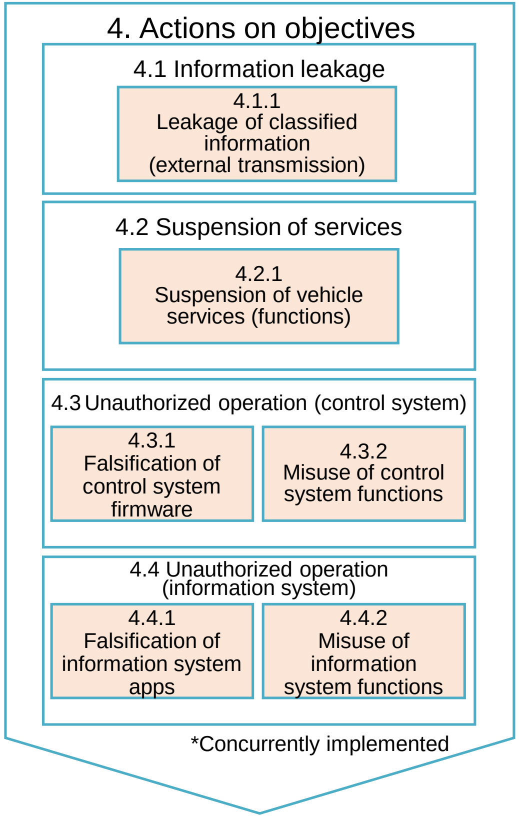
- An attacker attempts measures to evade the applicable cause depending on the error status when arbitrary code execution fails.
- The status and cause of failure of arbitrary code execution are as follows.

Status of failure	Evaluation items	Cause of failure	Example of defense system
Cannot be executed	3.1.1	No code in the intended position	ASLR
		Located in a segment where code execution is prohibited	DEP, Nxbit
Denied access to an attack target	3.1.2	Code execution in a controlled area	Sandbox
Suspension of execution	3.2.1	Lack of execution authority	General access control
	3.2.2	Suspension by mandatory access control	SELinux

Evaluation items included other than incidents

- Considering the jailbreaking of IoT products (smart devices in particular), the problems were itemized because similar problems are likely to occur in vehicle security in the future.

4. Actions on objectives



4. Actions on objectives

4.1 Information leakage

4.1.1
Leakage of classified information
(external transmission)

4.2 Suspension of services

4.2.1
Suspension of vehicle services (functions)

4.3 Unauthorized operation (control system)

4.3.1
Falsification of control system firmware

4.3.2
Misuse of control system functions

4.4 Unauthorized operation (information system)

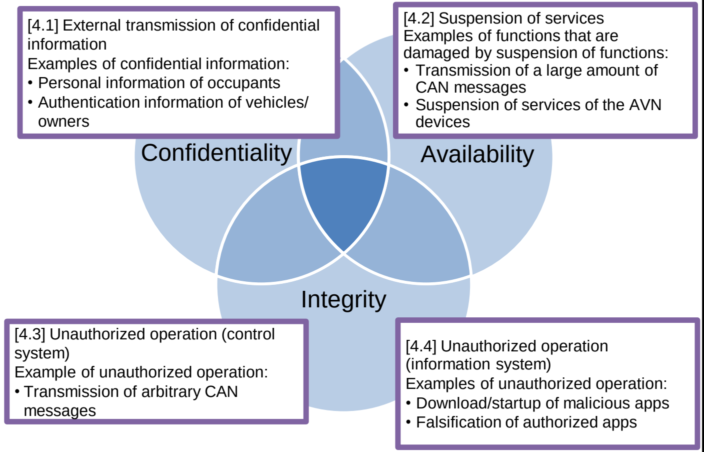
4.4.1
Falsification of information system apps

4.4.2
Misuse of information system functions

*Concurrently implemented

Evaluation policy

- Execution of attacks that cause damage to a system from the viewpoint of security characteristics (CIA: confidentiality, integrity, and availability)



[4.1] External transmission of confidential information
Examples of confidential information:
- Personal information of occupants
- Authentication information of vehicles/ owners

[4.2] Suspension of services
Examples of functions that are damaged by suspension of functions:
- Transmission of a large amount of CAN messages
- Suspension of services of the AVN devices

[4.3] Unauthorized operation (control system)
Example of unauthorized operation:
- Transmission of arbitrary CAN messages

[4.4] Unauthorized operation (information system)
Examples of unauthorized operation:
- Download/startup of malicious apps
- Falsification of authorized apps

Evaluation items included other than incidents

- N/A
(In known vehicle incidents, attacks were launched on confidentiality, integrity, and availability.)

3

(3)

SIP-adus Initiatives

Verification of the guidelines through FOTs with OEMs in Japan

Verification of the Guidelines through FOTs with OEMs in Japan

Objective: Apply the formulated guidelines to actual systems for verification and improvement

Check the importance of evaluations on actual systems through FOTs

Number of participating OEMs	In FY2017, an FOT was conducted (on a trial basis) with the **participation of one OEM** in Japan. In FY2018, an FOT was conducted with the **participation of four OEMs** in Japan.
Results	The information security evaluation guidelines were finalized based on verification and improvement through FOTs. **FOT results reported** (1) Evaluation of the content/items of FOTs by participants (2) Establishment of the evaluation process through FOTs (3) Improvement of the evaluation guidelines through FOTs

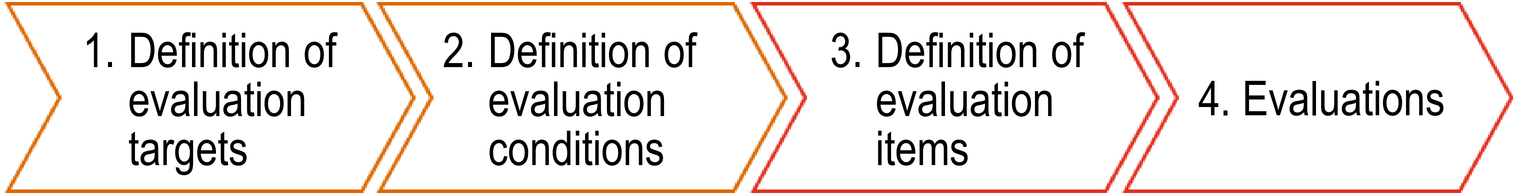
Result (1) Evaluation of the Content of FOTs by Participating Companies

Evaluation item	Content
Establishment of evaluation techniques (formulation of evaluation guidelines)	• Techniques that help ensure a certain level of security quality • Techniques that help improve the uniformity of penetration tests that are highly dependent on personal skills
FOTs using vehicles systems	• Activities that contribute to verifying the validity of the evaluation guidelines • Verification using multiple vehicles is preferred.
Future initiatives	• The studies on countermeasures against identified problems, etc. are still dependent on evaluators. There is room for improvement. • Guidelines should be available not only in the overall evaluation in the latter half of the V-shaped development model but also in the upstream processes such as design.

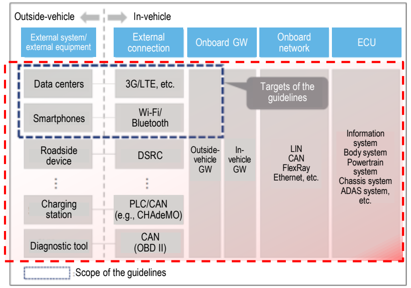
Result (2) Establishment of the Evaluation Process

Define the standard evaluation process for vehicle system security evaluation (penetration test) through FOTs and establish a technique that can be used for assessment.

Defined evaluation process



1. Definition of evaluation targets
2. Definition of evaluation conditions
3. Definition of evaluation items
4. Evaluations



Outside-vehicle ⇐ ⇒ In-vehicle

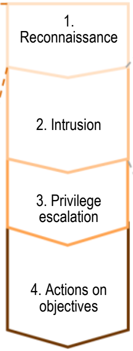
External system/ external equipment	External connection	Onboard GW		Onboard network	ECU
Data centers	3G/LTE, etc.	Outside-vehicle GW	In-vehicle GW	LIN CAN FlexRay Ethernet, etc.	Information system Body system Powertrain system Chassis system ADAS system, etc.
Smartphones	Wi-Fi/ Bluetooth				
Roadside device	DSRC				
⋮	⋮				
Charging station	PLC/CAN (e.g., CHAdeMO)				
Diagnostic tool	CAN (OBD II)				

Targets of the guidelines

Scope of the guidelines

Reconnaissance skills

Category	Skills
HW reverse engineering	Basic knowledge about HW such as MCU and ISP
	UART/JTAG pin scanning techniques
	Flash memory dumping techniques
Binary analysis	Reverse engineering
	Source code analysis techniques
	Antivirus software evasion techniques
Network analysis	Wi-Fi protocol analysis
	Bluetooth protocol analysis
	Knowledge about TCP/IP protocol stack
Management	Provision of information to downstream processes

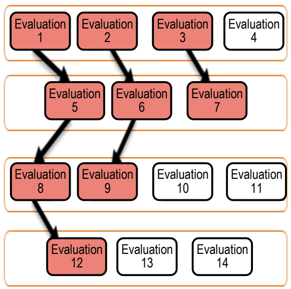


1. Reconnaissance
2. Intrusion
3. Privilege escalation
4. Actions on objectives

Intrusion skills

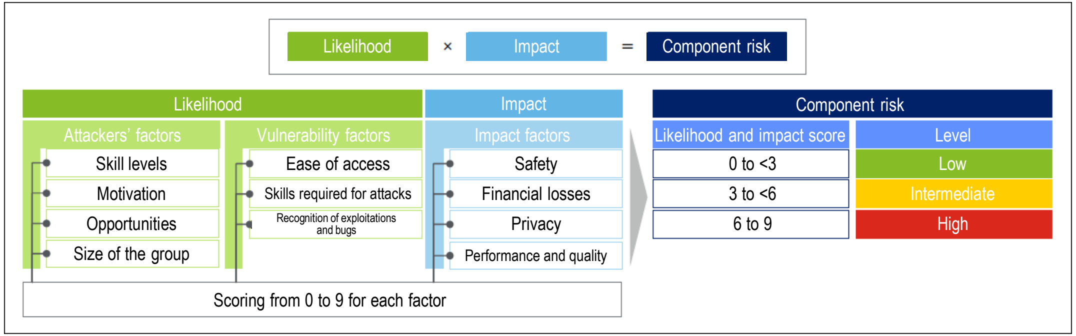
Category	Skills
Intrusion	Reverse engineering
	Identification and exploitation of vulnerabilities
	Wi-Fi/Bluetooth/TCP/IP protocol analysis
Privilege escalation	Memory security (DEP, ASLR) and evasion techniques
	MAC (mandatory access control) and evasion techniques
	Falsification detection techniques (e.g., secure boot) and evasion techniques
Actions on objectives	Knowledge about the CAN protocol
	Techniques to use DoS tools
	Understanding of HW configuration

Approach of a penetration test (image)



Process 1. Selection of Evaluation Targets

Analyze the risks of the overall vehicle system and peripheral systems, identify I/Fs and components whose risks of attacks are high, and select and define evaluation targets based on this technique



Likelihood × Impact = Component risk

Likelihood

Attackers' factors
- Skill levels
- Motivation
- Opportunities
- Size of the group

Vulnerability factors
- Ease of access
- Skills required for attacks
- Recognition of exploitations and bugs

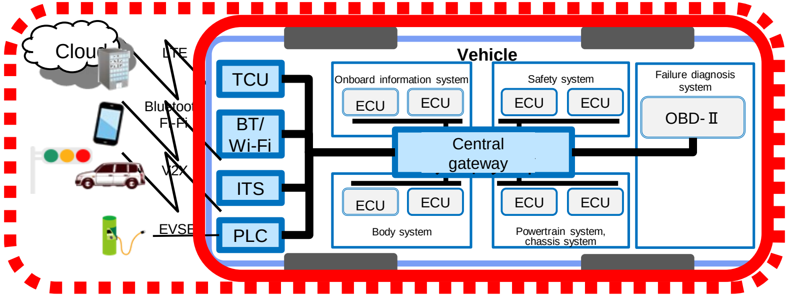
Impact

Impact factors
- Safety
- Financial losses
- Privacy
- Performance and quality

Scoring from 0 to 9 for each factor

Component risk

Likelihood and impact score	Level
0 to <3	Low
3 to <6	Intermediate
6 to 9	High



Process 2. Definition of Evaluation Conditions

Evaluation conditions	**Details of the conditions**
Evaluators' skills	• Define the skills required for evaluation, and conduct a check by evaluators/ administrators in advance
Man-hours for evaluation	• (In this FOT) Assign two persons for the standard evaluation period of two months in total (40 business days), and make evaluations using the man-hours
Evaluation environment (vehicles)	• Check the feasible evaluation environment based on the actually available equipment

Evaluation results

Evaluation criteria	Reconnaissance phase: Evaluations were made by evaluators with the skills above for the specified period. Reconnaissance was unsuccessful. The safety of the target and the grounds for safety were confirmed. Intrusion phase: Evaluations were made by evaluators with the skills above for the specified period. Intrusion was unsuccessful via all the I/Fs.

[Reference] Overview of “Evaluators’ Skills”

Reconnaissance skills

Category	Skills	Overview
HW analysis	Surface analysis	Analyze the configuration of a printed wiring board based on the knowledge about hardware, and search/identify debugging ports and external communication ports
	Processing	Delaminate and re-solder a flash memory, etc. soldered on a printed wiring board, and process a printed wiring board as necessary
	Binary extraction from data I/O ports	Extract and write data from a flash memory delaminated from a printed wiring board using tools, etc. or from an external communication port
	Binary extraction from debugging ports	Extract data from the identified debugging ports above
Binary analysis	File system analysis	Analyze data extracted from a flash memory, and analyze and identify the data structure of the file system, etc.
	Software architecture analysis	Analyze a group of files extracted from the file system, and analyze and identify software architecture such as the OS and library
	Binary code analysis	Analyze respective identified files such as program files, and analyze and identify their design and implementation
	Source code analysis	Decompile binary codes using various tools, and analyze and identify their design and implementation at the source code level
	Evasion of protection functions	Analyze and evade protection functions implemented in software such as data encryption, obfuscation, and encoding
Network analysis	Analysis of Wi-Fi communication	Intercept and analyze Wi-Fi communication
	Analysis of Bluetooth/Bluetooth LE communication	Intercept and analyze Bluetooth and Bluetooth LE communication
	Analysis of cellular communication	Intercept and analyze cellular communication
	Analysis of TCP/IP communication	Intercept and analyze TCP/IP communication
Management	Provision of information to downstream processes	Manage the information analyzed and identified in the reconnaissance process above, and provide such information to the downstream phase/ensure linkage

[Reference] Overview of “Evaluators’ Skills”

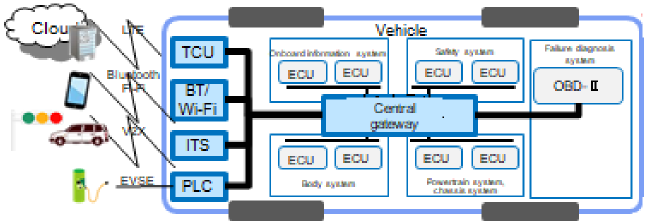
Intrusion skills

Category	Skills	Overview
Intrusion	Threat analysis	Analyze and identify an attack surface which is considered as the starting point of intrusion based on the results of the reconnaissance phase
	Binary code analysis	Analyze respective files such as program files that serve as an attack surface based on the threat analysis results, and analyze and identify their design and implementation
	Identification and exploitation of vulnerabilities	Identify vulnerabilities that are available for intrusion concurrently with the binary code analysis or based on the results of binary code analysis, and exploit such vulnerabilities by creating attack codes, etc.
Privilege escalation	Evasion of vulnerability mitigation technologies	Analyze and evade vulnerability mitigation technologies such as data execution prevention and address space layout randomization
	Evasion of safety measures	Analyze and evade safety measures specific to a product (e.g., restriction on operation conditions, throttling)
	Evasion of mandatory access control systems	Analyze and evade mandatory access control systems such as SELinux
	Evasion of falsification detection systems	Analyze and evade falsification detection and integrity verification systems such as secure boot
Actions on objectives	Analysis of onboard network	Analyze and identify the overall configuration of the onboard network (e.g., layout of the central gateway and various ECUs)
	Analysis of CAN communication	Intercept, analyze, and retransmit CAN communication based on the results of network analysis
	Verification and reproduction of attacks	Verify and reproduce attacks that exploit vulnerabilities based on the results of the reconnaissance and intrusion processes above

Process 3. Definition of Evaluation Items

Select evaluation items that should be conducted from the (existing) security evaluation items and determine the sequence of these items based on the results of risk evaluation and condition check.

Evaluation targets



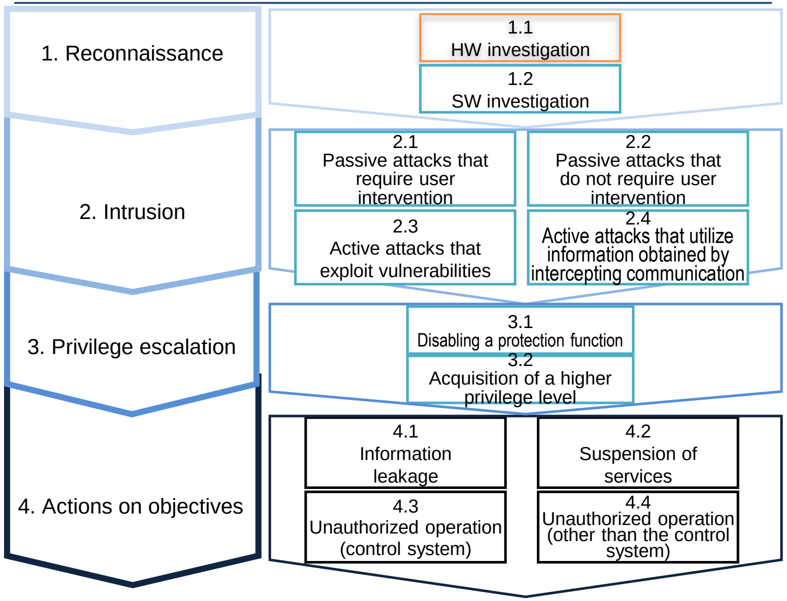
Evaluation conditions

Evaluators’ skills

Man-hours for evaluation

Evaluation environment (vehicles)

Items of evaluation guidelines



1. Reconnaissance

1.1 HW investigation

1.2 SW investigation

2. Intrusion

2.1 Passive attacks that require user intervention

2.2 Passive attacks that do not require user intervention

2.3 Active attacks that exploit vulnerabilities

2.4 Active attacks that utilize information obtained by intercepting communication

3. Privilege escalation

3.1 Disabling a protection function

3.2 Acquisition of a higher privilege level

4. Actions on objectives

4.1 Information leakage

4.2 Suspension of services

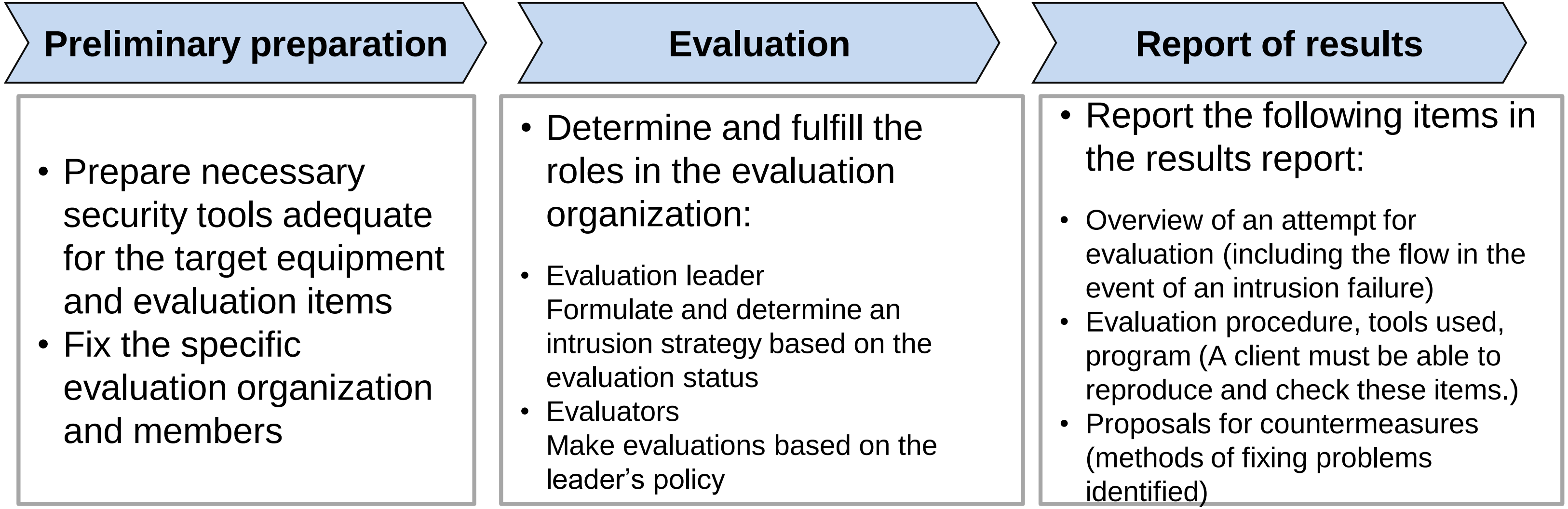
4.3 Unauthorized operation (control system)

4.4 Unauthorized operation (other than the control system)

Process 4. Evaluations

Make evaluations based on the defined evaluation items. Organize evaluations in consideration of the characteristics of the penetration test, and specify items that should be indicated in the evaluation results.

Flow chart for conducting a penetration test



Preliminary preparation

- Prepare necessary security tools adequate for the target equipment and evaluation items
- Fix the specific evaluation organization and members

Evaluation

- Determine and fulfill the roles in the evaluation organization:

- Evaluation leader
  Formulate and determine an intrusion strategy based on the evaluation status
- Evaluators
  Make evaluations based on the leader's policy

Report of results

- Report the following items in the results report:

- Overview of an attempt for evaluation (including the flow in the event of an intrusion failure)
- Evaluation procedure, tools used, program (A client must be able to reproduce and check these items.)
- Proposals for countermeasures (methods of fixing problems identified)

Result (3) Improvement of Guidelines through Implementation of FOTs

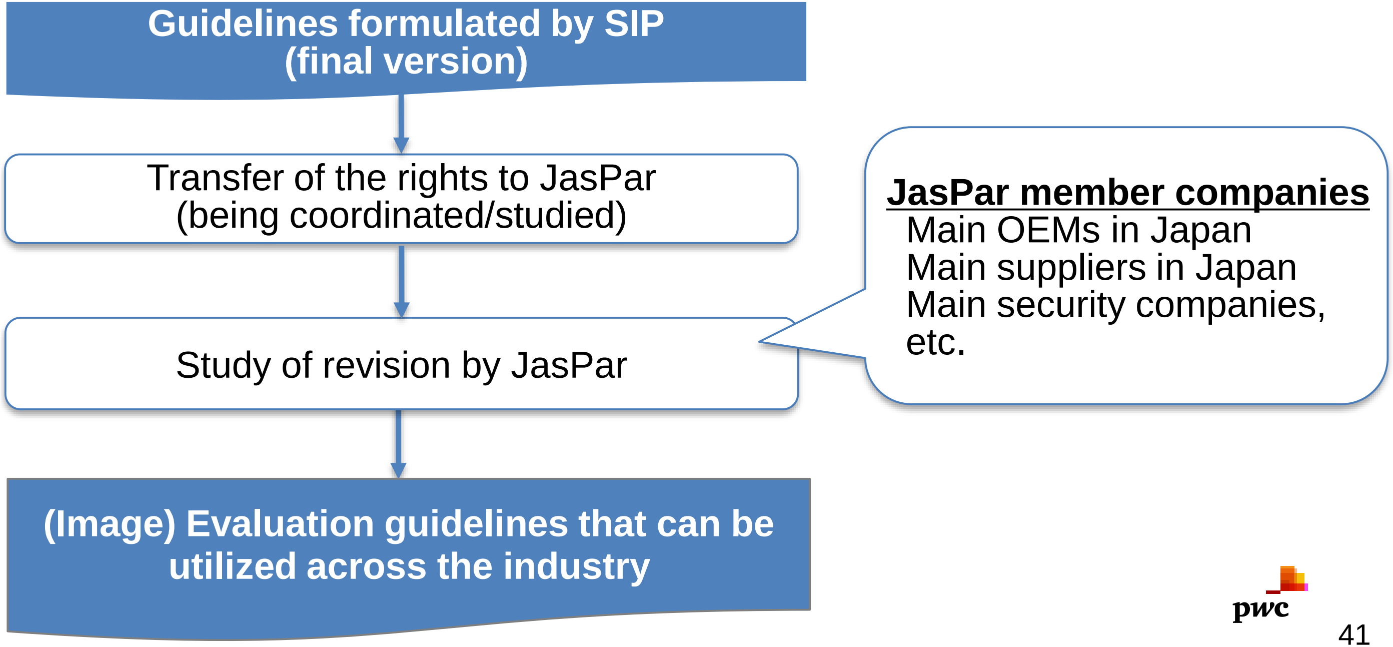
It is currently planned to make improvements for 19 evaluation items in the FOT of this fiscal year.

***Items in the boxes with thick lines are particularly important for evaluation.**

Item number in the guidelines	Details	Reason
1.1.1 Investigation of I/Fs before removing a device	Evaluation item updated: “1.1.1.1 Check of USB port connection”	Review of the details by evaluators based on the evaluation results
	Evaluation item added: “1.1.1.4 Check of an SD card”	Review of the details by evaluators based on the evaluation results
1.1.3 Investigation of I/Fs after removing a chip	Evaluation content updated: “1.1.3.2 Investigation of a flash memory chip”	Description updated by the evaluators
1.1.5 Interface connection	Evaluation content updated: “1.1.5.5 Acquisition of console by binary falsification”	Description updated by the evaluators
1.1.6 Binary extraction	Evaluation content updated: “1.1.6.1 Binary extraction from UART (with the OS started)”	Description updated by the evaluators
	Evaluation content updated: “1.1.6.3 Binary extraction from UART (with the bootloader started)”	Description updated by the evaluators
	Evaluation content updated: “1.1.6.5 Binary extraction from a flash memory”	Description updated by the evaluators
1.1.7 Verification of binary protection function	**Evaluation item added: “1.1.7.8 Investigation of obfuscation”**	**Feedback from the FOT reflected**
1.1.8 Reverse engineering	**Evaluation item added: “1.1.8.2 Selection of targets”**	**Feedback from the FOT reflected**
1.2.6 Interception of TCU communication	Evaluation item updated: “1.2.6.1 Investigation of modems”	Review of the details by evaluators based on the evaluation results
	Evaluation item added: “1.2.6.2 Interception of TCU-IVI communication”	Review of the details by evaluators based on the evaluation results
1.2.8 Interception of CAN message communication	Evaluation technique updated: “1.2.8.1 Installation of CAN message capture tools”	Description updated by the evaluators
2.3.4 Attacks via Wi-Fi (in-car)	Evaluation technique updated: “2.3.4.1 Log in from a public port”	Description updated by the evaluators
	Evaluation technique updated: “2.3.4.3 Analysis of the API source code”	Description updated by the evaluators
3.1.2 Evasion of discretionary access control (DAC)	Evaluation technique updated: “3.1.2.2 Evasion of check of arbitrary access control”	Review of the details by evaluators based on the evaluation results
3.1.3 Evasion of safety functions	Intermediate evaluation category added	Review of the details by evaluators based on the evaluation results
3.2.1 Evasion of functions to prevent privilege escalation	Evaluation technique updated: “3.2.1.1 Check of privilege escalation prevention functions”	Review of the details by evaluators based on the evaluation results
	Evaluation technique updated: “3.2.2.2 Evasion of mandatory access control”	Review of the details by evaluators based on the evaluation results
3.3.1 Evasion of secure boot	**Intermediate evaluation category added**	**Review of the details by evaluators based on the evaluation results**

Future Initiatives to Utilize the Guidelines

At the closing of SIP-adus (1st Phase), the rights of the guidelines will be transferred to JasPar, an organization that formulates the technology standards for vehicle security, for utilization and future management of the guidelines in the auto industry. Discussions have been held to spread the use of the guidelines.



Guidelines formulated by SIP (final version)

Transfer of the rights to JasPar (being coordinated/studied)

Study of revision by JasPar

JasPar member companies

Main OEMs in Japan
Main suppliers in Japan
Main security companies, etc.

(Image) Evaluation guidelines that can be utilized across the industry

Thank you