戦略的イノベーション創造プログラム

「SIP-adus / Research of New Cyberattack Techniques and Countermeasure Technologies」

FY2022 Final Report (Summary)

PwC Consulting LLC

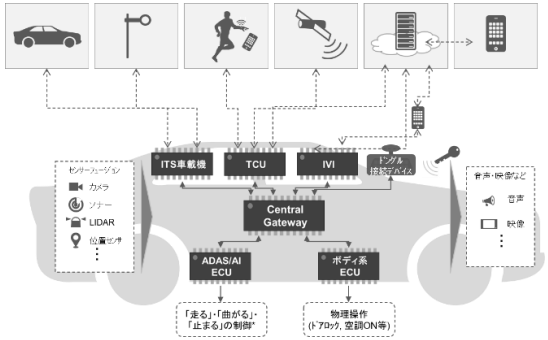
2023 Feb.

Background and Research Objective

In order to deal with changes in the security environment due to the development of automated 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?

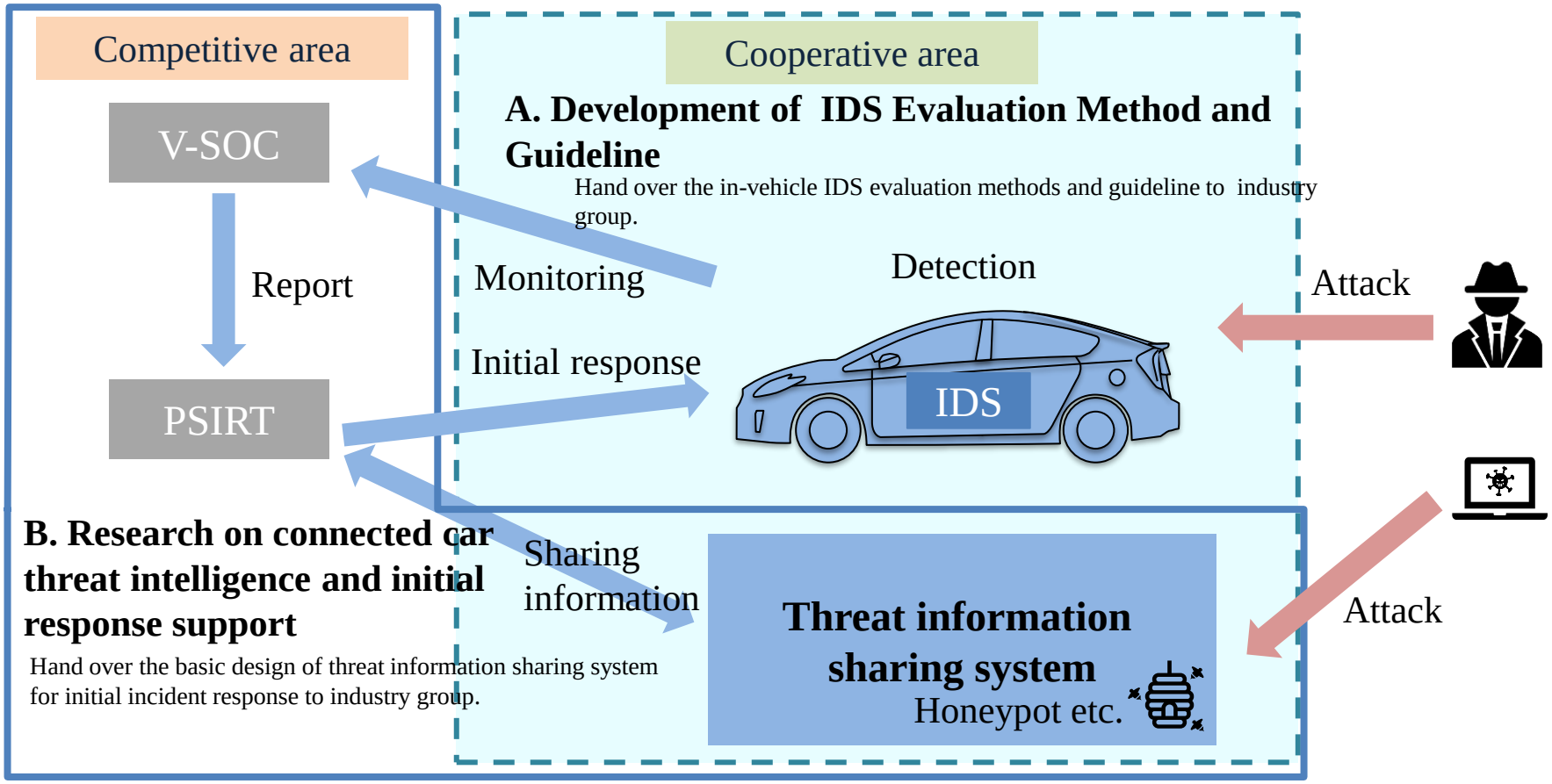
Activity B. Research on connected car threat intelligence and initial response support

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?

Research scopes

We consider in-vehicle IDS and threat intelligence sharing to be the cooperative are across the automotive industry.



a. Development of IDS Evaluation Method and Guideline

Purpose of the IDS evaluation guideline

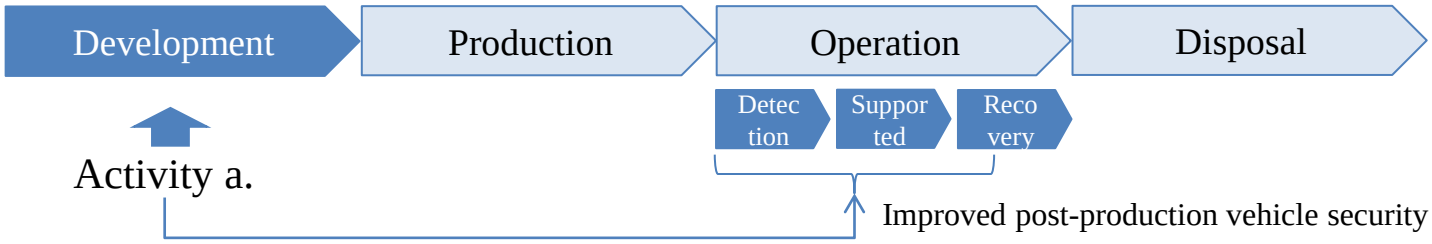
Conduct research on evaluation method for on-board IDS and develop IDS evaluation guideline which can be used during product development to contributes to the entire automotive industry in improving after production vehicle security.

Background related to post-production cybersecurity

Regulations	Industry Practices
WP29 UN-R155 sets requirements for the manufacturers to enable the vehicles to detect and respond to cyber-attacks.	Each manufacturer should specify the scope of attack to be detected as there are no existing regulations nor guidelines in this regard.

Activity a. Objectives and directions

Research IDS evaluation method for “Cyber-attack detection and vehicle recovery” and document as a “IDS evaluation guideline” to contribute to the improved cybersecurity for automotive industry.

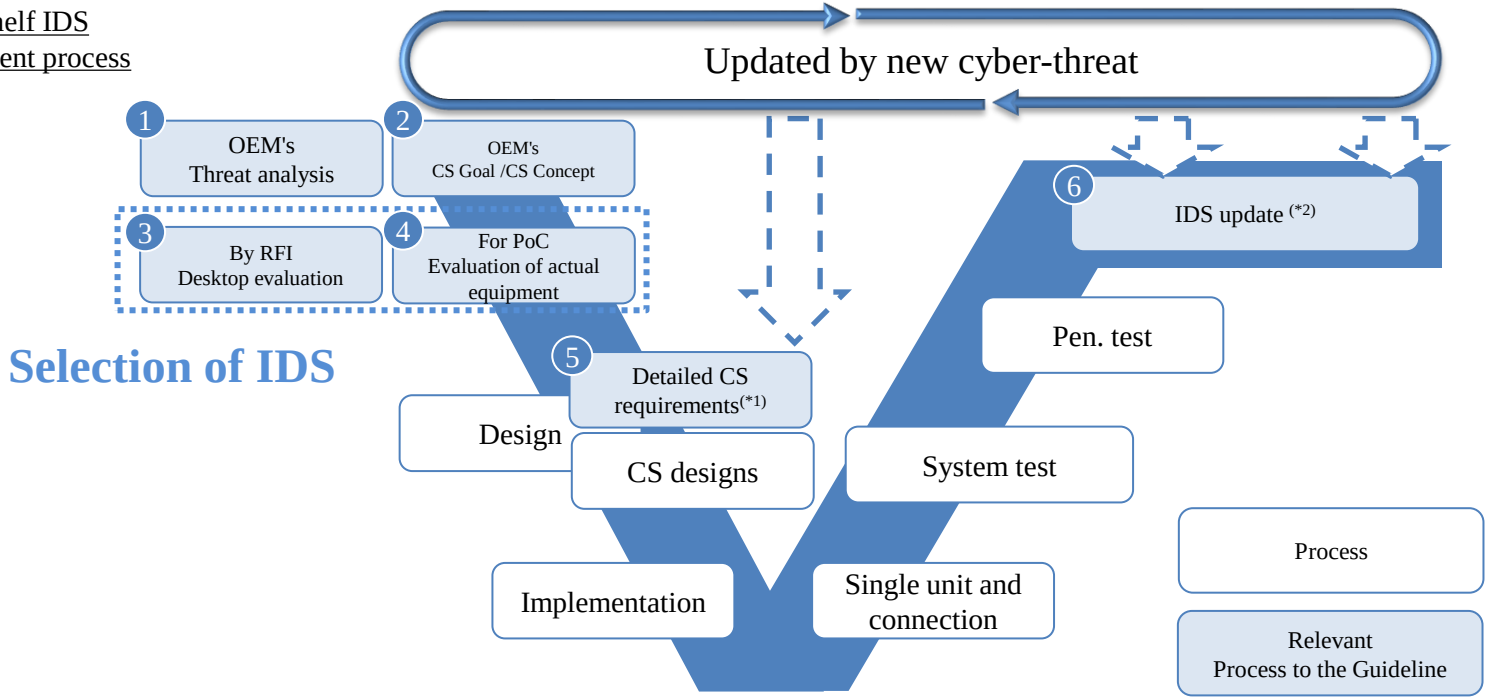


Objective of IDS assessment guideline

We assumed the case of using an off-the-shelf type IDS in which basic functions are implemented. We have developed guidelines to provide reference information for OEMs and suppliers in the selection and implementation of IDS.

Objective 1	Create the evaluation items and test procedure templates used in IDS selection process (③④)
Objective 2	Show how to create attack scenarios and derive IDS requirements in the process of OEM/ supplier's IDS (①②⑤⑥)

Off-the-Shelf IDS
Development process



(*1) Perform a risk assessment based on the functions of the vehicle and assumed vulnerabilities. Define detailed CS requirements. Applicable to refinement of cybersecurity requirements of ISO/SAE 21434.
(*2) Organize the detection capabilities required by IDS from new threats. Update IDS detection rule-definition files and programs as needed.

Approach: Scope of the IDS evaluation guidelines

As a precondition, the content of the Guideline is a requirement and assessment perspective to be considered by OEMs/ suppliers, and does not imply that the requirements listed in the Guideline must be met, and that testing must be done in the way of the Guideline.

Policy 1	Evaluate the outline at a level of detail that is comprehensive and comparable to IDS
Policy 2	Evaluate whether or not a hypothetical attack equivalent to that of a past attack can be detected and analyzed
Policy 3	Perform IDS actual machine tests in a test environment that can be easily prepared

Activity Policy: IDS Evaluation Guideline Development

Following approach will be taken to develop IDS evaluation guidelines and transfer to the industry groups.

1 Investigate Basic IDS functionality	Investigate open source information on the latest attack cases against the vehicle, and investigate and arrange the elements to be detected by the in-vehicle IDS.
2 Investigate evaluation perspectives based on the specifications	Summarize IDS evaluation perspectives as "Specification evaluation items". The output is validated/reviewed through interviews with OEMs and IDS vendors.
3 Identify basic test items/investigate method	Based on the output of [1] and OEM interviews results from [2], draft "Basic Test Case" is prepared by arranging the perspectives to be evaluated using the actual IDS at the IDS selection and verification stage.
4 IDS Evaluation	The validity of the draft of the "Basic Test Case" from [3] is verified through tests using test-bed, vehicle bench, etc. and an actual IDS, and challenges are identified.
5 Develop IDS Evaluation Guideline	The challenges identified in [4], the "basic test case" is reviewed, and the "method to identify test requirements from new threats" is identified in similar a manner as identifying the "basic test case" from the attack case.
6 Deployment for practical use	The output of [1-5] are consolidated into "IDS Evaluation Guideline" and transferred to relevant industry groups, leading to practical development and operation in the automotive industry.

Activity a. Approach (1/3)

Develop drafts of "Specification evaluation items" and "Basic test cases" based on attack information and papers on past cars, public information survey on IDS products, etc. and conduct interviews with OEMs and IDS vendors, and conduct IDS actual machine surveys to verify the validity.

1 Identify basic test items/investigate test method

Investigate open source information on the latest attack cases against the vehicle, and investigate and arrange the elements to be detected by the in-vehicle IDS.

INPUT

- Web attack information, papers
- Results of FY2019 Attack Scenario Survey and Analysis

OUTPUT

- Detection function required by IDS (security event)

2 Investigate evaluation perspectives based on the specifications

Summarize IDS evaluation perspectives as "Specification evaluation items". The output is validated/reviewed through interviews with OEMs and IDS vendors

INTPUT

- Detection function required by IDS (security event)
- Disclosure of IDS information (including results in fiscal 2019)
- OEM, IDS vendor interview

OUTPUT

- List of Specification Evaluation Items

Activity a. Approach (2/3)

Develop drafts of "Specification evaluation items" and "Basic test cases" based on attack information and papers on past cars, public information survey on IDS products, etc. and conduct interviews with OEMs and IDS vendors, and conduct IDS actual machine surveys to verify the validity.

3 Identify basic test items/investigate test method

Based on the output of [1] and OEM interviews results from [2], draft "Basic Test Case" is prepared by arranging the perspectives to be evaluated using the actual IDS at the IDS selection and verification stage.

INPUT

- Papers and guidelines (NIST SP800-94, etc.)
- Detection function required by IDS (security event)

OUTPUT

- Basic Test Case (Draft)
- Outcomes of examining the test environment

4 IDS Evaluation

The validity of the draft of the "Basic Test Case" from [3] is verified through tests using test-bed, vehicle bench, etc. and an actual IDS, and challenges are identified.

INTPUT

- Basic Test Case (Draft)

OUTPUT

- Basic test case

Activity a. Approach (3/3)

Develop drafts of "Specification evaluation items" and "Basic test cases" based on attack information and papers on past cars, public information survey on IDS products, etc. and conduct interviews with OEMs and IDS vendors, and conduct IDS actual machine surveys to verify the validity.

5 Develop IDS Evaluation Guideline

The challenges identified in [4], the "basic test case" is reviewed, and the "method to identify test requirements from new threats" is identified in similar a manner as identifying the "basic test case" from the attack case.

INPUT

- Basic test cases (including derivation methods)
- Specification evaluation items

OUTPUT

- IDS evaluation guideline (draft)

6 Deployment for practical use

The output of [1-5] are consolidated into "IDS Evaluation Guideline" and transferred to relevant industry groups, leading to practical development and operation in the automotive industry.

INTPUT

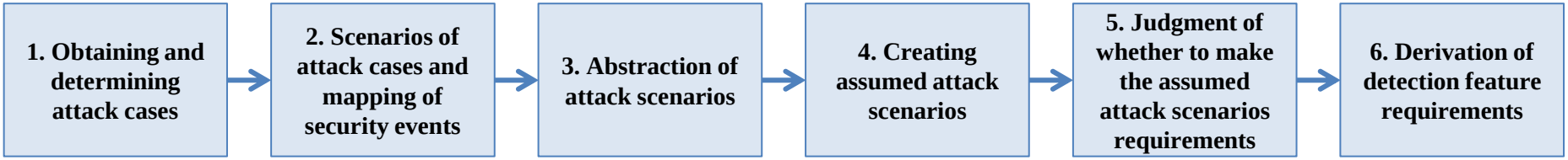
- IDS evaluation guideline (draft)

OUTPUT

- IDS evaluation guideline (First issue)

Criteria method of detect function

The method to derive the detection criterion from a certain past case was examined on 「policy 2: Evaluate whether or not a hypothetical attack equivalent to that of a priors attack can be detected and analyzed」 shown in the activity policy.



#	Overview
1	Select attack cases to be detected by obtaining attack cases.
2	Attack cases are decomposed into attack procedures for each vehicle component, requirements and objectives for establishing attacks are added, attack scenarios are created, and security events that may occur in each attack procedure are mapped.
3	Abstract attack scenarios to derive attack scenarios that are "equivalent" to attack cases.
4	Taking into account the specifications of IDS-equipped vehicles and the possibility of vulnerability, the abstraction attack scenario will be implemented in IDS-equipped vehicles, and the attack scenario that may be established in IDS-equipped vehicles will be created.
5	Consider specific actions according to the risk assessment methods and response methods defined by OEM/ supplier for the assumption attack scenario.
6	Of the security events that may occur in the in-vehicle network due to an attack, those that should be detected by IDS are selected and derived as a requirement.

Research on fundamental IDS functions (1/3)

The security conference web information and vulnerability information held by 2020 were examined, and 12 cases directly related to the vehicle were analyzed, and the security event was derived.

	Cases	Cases analyzed in detail
Web information and vulnerability information	1329	6
Research Paper	1062	6
Total	**2391**	**12**

Scope	Event	Security Event Examples
Network	Behavior of context conflicts on in-vehicle NWs	Sending control messages that do not affect basic operation at timings inconsistent with the running state, and sending valid diagnostic messages at timings inconsistent with the running state
	Attacks on the UDS protocol	Attacks on the UDS protocol
	Physical connection of fraudulent devices to the on-board NW	Connecting External Devices to OBD I/F
	Fuzzing attacks on in-vehicle NWs	Fuzzing attacks from OBD I/F
Host	Fraudulent behavior	Invoking a system call library from an unspecified process
	Illegal external communication	Communication with a source/destination outside the car that is not permitted
	Invalid file system operation	Changing Attributes of Important Files (Permissions, etc.)
	Fraudulent app installation	Installation of regulation apps
	Invalid log	Invalid system logs, application logs
	Unspecified frequency of errors	Request Processing Errors to External Public Services More Than a Certain Number of Times per Hour
	High load	High CPU and memory load conditions
	Changing the Firmware	Changing the Firmware

Research on fundamental IDS functions (2/3)

The 12 cases covered are as follows.

Information source	Attack Case Overview
USENIX Security '20 Technical Sessions	In BT/WiFi where the authentication function is defective, OBD dongle was connected, and the message which disables the remote lock was injected into the in-vehicle network, and the vehicle could be stolen. [Haohuang Wen, 2020]
Blackhat USA 2015	In FCA Jeep Cherokee, the vehicle can be remotely accessed from any terminal on the NW of Sprint, the host (OMAP) of HU/TCU can be accessed by SSH to the exposed 6667, and the FW of the CAN controller (V850) can be rewritten, and any CAN message (steering, braking, etc.) can be transmitted through the SPI. [Dr. Charlie Miller, 2015]
Vulnerability information	The buffer overflow vulnerability of the BT module of the DCU (Display Control Unit) such as Toyota Lexus is used to automatically connect to an external WiFi AP, and the firmware of the CAN controller is tampered with to override the message filtering function, and diagnostic messages can be sent to the CAN bus by connecting WiFi to the vehicle from the outside. [Lab, 2020]
Blackhat USA 2019	A command can be sent to a service waiting on the TCP port through OBD I/F or USB I/F of the HU of the BMW, a CAN message can be sent to K-CAN using TOCTOU vulnerabilities, and an ECU can be reset or a seats can be moved back and forth through the UDS message. [Zhiqiang Cai, 2019]
Blackhat USA 2019	By inserting the update management file of the crafted navigation from USB I/F of HU of BMW, and utilizing the vulnerability of the process to analyze the update management file, it was possible to reset an ECU can be reset or a seats can be moved back and forth through the UDS message. [Zhiqiang Cai, 2019]
Blackhat USA 2019	A bogus base station was installed, and the response of BMW ConnectedDrive service was rewritten, and the attacker's web server was accessed, and an ECU can be reset or a seats can be moved back and forth through the UDS message by utilizing the vulnerability of the browser, etc. [Zhiqiang Cai, 2019]
Blackhat USA 2019	A bogus base station sent a NGTP (BMW Remote Service) message for ConnectedDrive over SMS, allowing for unauthorized use of functions for remote services (such as opening doors, horns, lights, etc.). [Zhiqiang Cai, 2019]
Blackhat USA 2019	With BMW's vehicle, MITM attacks for communication between false base stations and vehicles are performed, signatures for Provisioning data are tampered with, and the buffer overflow vulnerability of TCU is utilized to reset ECU and move seat back and forth through UDS messages. [Zhiqiang Cai, 2019]
Web information	In Viper's smart alarms, a vulnerability in the servers' APIs could impersonate legitimate users and track vehicles, or shut down engines. [PARTNERS, 2019]
Vulnerability information	In Daimler Mercedes-Benz Me App, after stealing access token used between the application and the server, it can impersonate the legitimate user, log in to the server, vehicle functions (such as locking/unlocking the door that can be used through the application) can be used. [NVD, CVE-2018-18071 Detail, 2018]
Vulnerability information	Since there were only 256 combinations for Security Access, the attacker could calculate the keys and bloat the airbags. [NVD, CVE-2017-14937 Detail, 2017]

Research on fundamental IDS functions (3/3)

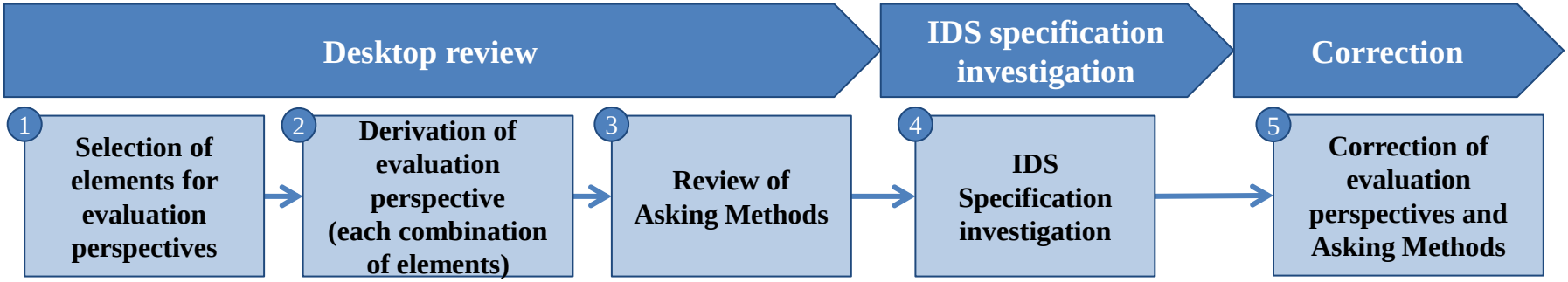
The IDS basic requirements derived from the analysis results of the cases are as follows.

※The specific basic requirements is stated only in the guidelines.

Major class	Small classification	ID
Detection Function	**No false positives**	SD-FP-1
		SD-FP-2
	Error in the data of a single message	SD-TP-1-1
		SD-TP-1-2
		SD-TP-1-3
	Transmission cycle error	SD-TP-2-1
		SD-TP-2-2
	Error in relation to previous/next message	SD-TP-3-1
		SD-TP-3-2
	Context error	SD-TP-4-1
		SD-TP-4-2
		SD-TP-4-3
		SD-TP-4-4
	Status error of in-vehicle NW	SD-TP-5-1
	Attacks on diagnostic protocols	SD-TP-6-1
		SD-TP-6-2
		SD-TP-6-3
		SD-TP-6-4
		SD-TP-6-5
		SD-TP-6-6
		SD-TP-6-7
		SD-TP-6-8
Logging Function		SL-1-1
		SL-1-2
		SL-1-3
Notification Function		SN-1-1

IDS Specification Evaluation Perspectives (1/3)

Based on "Policy 1: Evaluate the outline at a level of detail that is compprehensive and comparable to IDS“, a specification evaluation perspective was derived using the following flow.



#	Overview
1	The quality characteristics of ISO/IEC 25010 System/Software Product Quality Model, which organizes IDS's product life cycle and software quality, are selected as the perspective of evaluation.
2	Consideration an evaluation perspective on the characteristics referenced and used in each phase of the product lifecycle so that you can fully evaluate 1.
3	Create a list of questions to IDS vendors to assess whether the assessment perspective discussed in 2 is a degree of detail that can compare IDS.
4	Based on the created questions list, interviews with IDS vendors (Panasonic Corporation (Japan), ETAS Corporation (Germany), and Arilou Information Security Technologies (Israel)) are conducted to verify the validity of the specification evaluation perspectives and the content of the questions.
5	Finalization of the specification evaluation perspectives based on verification results, JASPAR, and feedback from OEMs who are assumption readers.

IDS Specification Evaluation Perspectives (2/3)

The questions to IDS vendors are as follows.

Security Function Classification	Function	Item
Basic Specifications	Form of provision	Form of offering a commercial version
		IDS provided for PoC
		Supported platforms (for SW provide)
		Product Type
	Protocol	Supported In-vehicle Network Protocols
		Supported Top CAN Protocols
		Supported Top Ethernet Protocols
	Other	Detection method
		Amount of used memory
		SOC linkage
		Communication function outside the car
Detection	Detection Settings	Necessity of DBC file
		Information required in addition to the DBC file
		Availability of setting tool
		Threshold specification parameter
	Detection	Security events to be detected
		How IDS vendors adjust detection parameters
Supported	Logging/Notification Setting Method	Logging/Notification Setting Method
	Logging	Steady-state logging items
		Logging items at detection
	Notification	Notification Items on Detection
	Detailed analysis	Availability of log analysis support tool
Recovery	Update	Update target (Physical port used)
		Update target (using OTA)

Question	Option
Select the security event to be detected.	Load condition error of in-vehicle network
	Connecting unknown external devices or sending messages
	Communication protocol error
	Operation outside the specifications of the vehicle (transmission cycle, data threshold)
	Operation that differs from the normal state of the vehicle defined in the rule (e.g., an error such as a threshold value for a change in the value)
	Operation impossible as a vehicle condition (door open during high-speed running, etc.)
	Operations that cannot be considered as the driving environment recognized by the sensor (left turn steering operation in the right curve, etc.)
	Deviation from rules for source and destination (IP, port-based)
	Others()

※ Proof of Concept. Verification the feasibility of new ideas and concepts and the effects that can be obtained from them.

IDS Specification Evaluation Perspectives (3/3)

A consideration of the answers to the question list, for the three IDS vendors (six products), is as follows.

1. Security events

Since the results of the answers were generally same for each company, each company supports the basic detection function, and it is difficult to make a big difference in the nominal specifications, so it is not possible to make a comparative evaluation of each company based on this item alone. On the other hand, part of the functional specifications, such as the type of protocol supported and the detection function of external device connection, are vendor-specific.

2. Logging/notification method

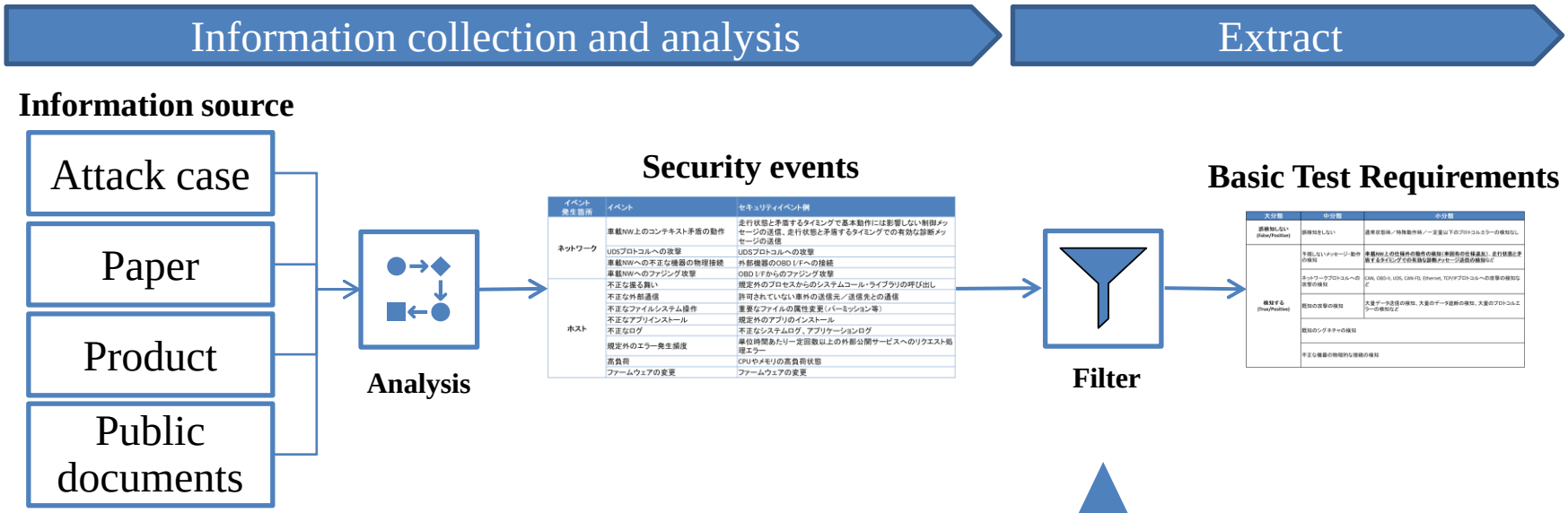
It is a prerequisite that each company is supported or can be customized, and basically customized based on OEM requirements. Therefore, by knowing the gap between the functionality required for IDS as OEM and the flexibility of the customization function, it is considered that the comparison of IDS is possible to some extent.

3. V-SOC operation services

As there are differences between vendors that exist as service menus and vendors that do not, this item is considered useful for comparison and examinations when analyzing IDS monitoring, analysis after detection, and support for response and recovery as needed are included.

Basic Test Case (1/6)

The Security events identified from the attack cases that meet certain conditions are defined as basic test requirements.



Filter conditions

1. Published in the past (2019-2021) ※1 , occurring in attacks against ※2 vehicle to which any IDS should respond, and/or;
2. It affects the basic operation (driving, steering, and braking) of the car.

※1. To take advantage of cases that have occurred in the past (see WP29 UN-R155 7 2.2.2 (f))
※2. Attacks that are considered applicable to other vehicles rather than attacks using vulnerabilities of special specifications of vehicles

Basic Test Case (2/6)

The basic test case summarizes the minimum points to be tested in the software unit test when IDS is selected or verified. The sections to be described are as follows.

Category	Item	Description
Test points	Test Case ID	Describe the ID
	Test Case Name	Describe the name of the test case
	Purpose	Describe the purpose of the test case
	SEv to be detected	Describe the SEv to be detected
	Type of attack msg to be injected	Type of attack msg injected for testing
	Prerequisites	Describe the running condition of the vehicle
	Derived Source Attack Case	Attack Case Derived from a Test Case
Test methods	Test environment	Describe either the simulation environment or the test bed environment.
	Prerequisite specifications of in-vehicle NW	Describe the specifications of vehicles equipped with IDS (vehicles equipped with IDS).
	Test Procedure	Describe the test procedure after building the test environment. Add sequential numbers (1., 2., and so on) to each viewpoint.
	Expected value	Describe the expected value of the test result <Hope Detection Test Case (SD-FT-*, SD-TP-*)> The guideline specifies that these information will be output to the IDS detection log. Number of detection: Number of detected Detection bus: bus detected by IDS as SEv (see next slide) Detection Type: Detection Type (see next slide) Reason for detection: Reason for detection (see next slide) Message to be detected
Remarks		Describe the precautions for implementation of the evaluation.

Basic Test Case (3/6)

The definitions of the expected values (detection bus, type, and reason) of the basic test case items listed on all slides are as follows.

Detection bus definition

Possible Values	Description
I	Information bus
C	Control bus
D	Diagnostic bus

Detection Type Definition

Detection Type	Description
Specific	Detect specific messages
Range	Detect specific time intervals

Detection reason definition

Reason for detection	Description
Incorrect ID	Invalid ID
Range	Range of incorrect data
Cycle	Illegal transmission cycle
Variation	Amount of change in incorrect data
Order	Fraudulent transmission order
Amount	Amount of fraudulent messages
Diag UDS	UDS protocol violation
Diag OBD	OBD protocol violation
Diag DoCAN	DoCAN protocol violation
Diag Err	Receiving error responses (including negative responses)

Basic Test Case (4/6)

An example of a fundamental test case is shown below.

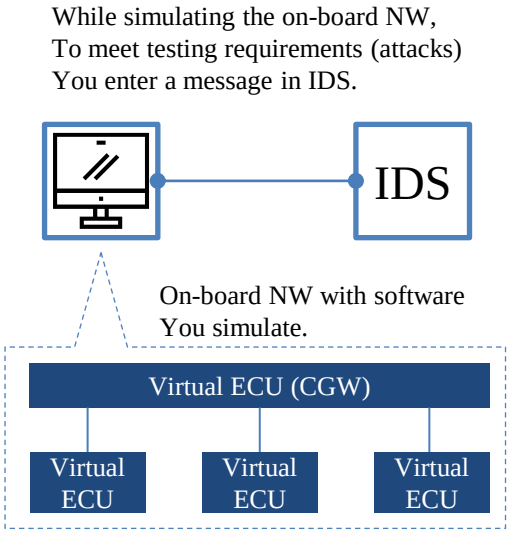
Category	Item	Content
Test points	**Test Case ID**	SD-TP-1-2
	Test Case Name	Detecting the extent of illegal data by injecting the PT/chassis msg, body system msg
	Purpose	Verify that messages that violate a defined range of signal values are detected.
	SEv to be detected	Range of incorrect data
	Type of attack msg to be injected	PT/Chassis msg, Body System msg
	Prerequisites	Driving condition: Constant velocity driving
	Derived Source Attack Case	OBD2dongle/Wen(USENIX'20)-2 Jeep Cherokee(BH USA 2015)
Test methods	**Test environment**	Simulation environment
	Prerequisite specifications of in-vehicle NW	Vehicle speeds should not exceed between 0 km/h and 140 km/h.
	Test Procedure	1. The logging data of the control system bus of the actual vehicle is injected into the control system bus of CANoe from [Replay Block]. 2. A total of three messages of 141, 142, and 143 Km/h in <Vehicle Speed> are injected to CANoe control system bus at any timing, one message at a time from [i-Generator] (by pressing the key set at the injection timing). 3. Confirming that the log as expected is output in the IDS detection log.
	Expected value	Number of detection messages: 3 Detection bus: C Detection Type: Specific Reason for detection: Range Detection messages: {attack msg}
Remarks		

Basic Test Case (5/6)

Assumption test environments can be broadly divided into the following three categories. Among them, since the cost of the vehicle (bench) environment is larger than the simulation environment and the test bed environment in the test environment construction, this paper examines it on the assumption that it is carried out in either of the latter two.

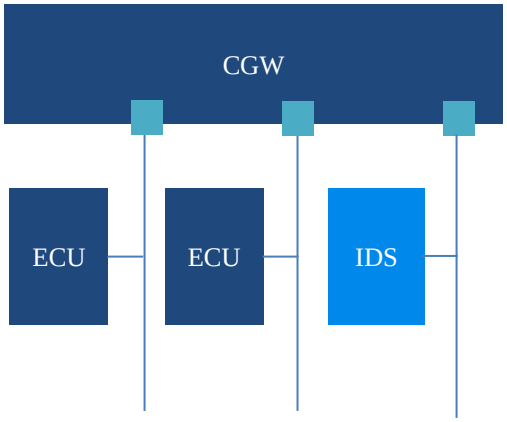
Simulated environment

A test environment that does not use an actual ECU. The in-vehicle network is reproduced on the software.



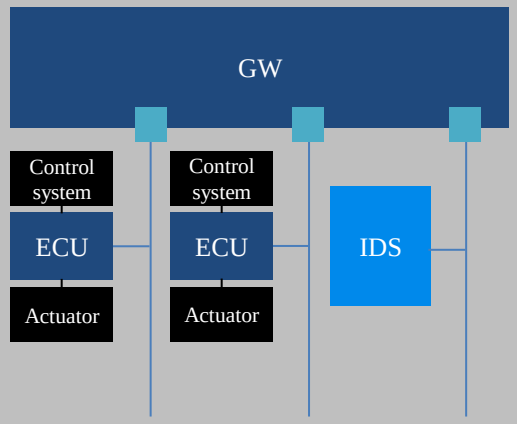
Test bed environment

An environment constructed with the minimum necessary hardware that meets the test requirements.



Vehicle (bench) environment

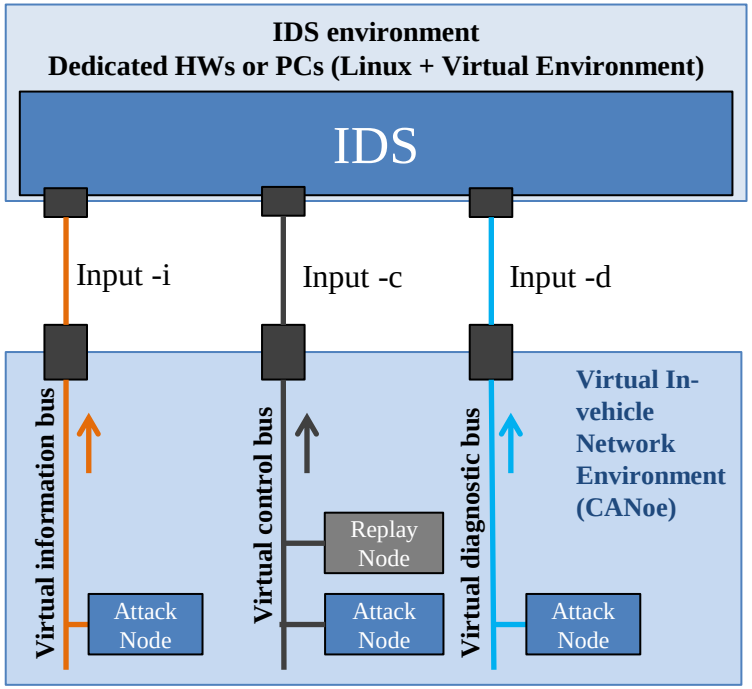
An environment in which an input device equivalent to an actual vehicle, an ECU, and an actuator are connected.



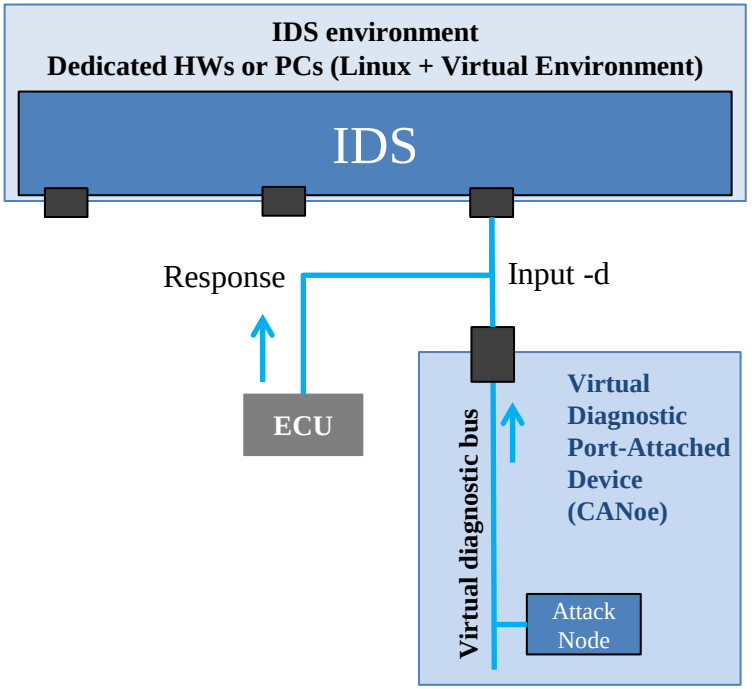
Basic Test Case (6/6)

The basic configuration assuming the basic test case is as follows.

Simulation environment

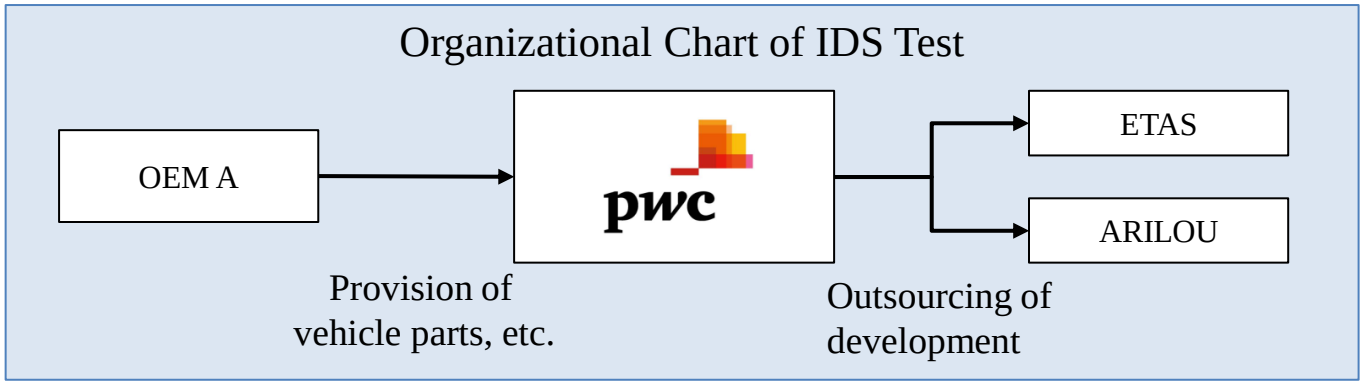


Test bed environment



Verifying Test Cases with IDS Actual Machine Test (1/5)

The IDS actual machine test is not intended to evaluate IDS, but to verify the validity of the basic test case. The implementation system and contract form of the actual machine test are shown below.



Verifying Test Cases with IDS Actual Machine Test (2/5)

The basic test case is a baseline from the evaluation point of view, and some of the test methods and expected values need to be adjusted according to the specifications of the target vehicle (ECU) and IDS. In the actual machine test, the test method and the required specifications for IDS were adjusted based on the specifications of the ECU and IDS provided.

Contents of the test method adjusted based on the vehicle (ECU) specifications

1. Threshold of the signal value to be used in the test
2. Preconditions for permitting specific values of the signal values used in the test (definition of the context in which a specific signal value is permitted)
3. Maximum allowable periodic disruption of messages used in the test (10%)
4. Maximum bus load for each bus (95%)

Policy for coordinating and implementing test methods based on IDS specifications

a. Test cases that can be tested with reference to other test cases are excluded.
b. Test cases related to functions (remote functions, etc.) that are not used in the vehicle in the actual machine test are excluded.
c. Functions that are considered not difficult to implement (they can be developed as required at a cost that is not too high), such as the output of the cumulative number of detection occurrences, are excluded.
d. If the base IDS is able to detect SEv, but it does not detect the expected value of the test case (detection count, detection reason), and if it requires more than a certain cost to detect it as expected, it should be excluded or IDS requirements should be adjusted (whether it actually operates as expected when PoC are used with OEM, or when it is mounted on a mass-production vehicle depends on the coordination with the IDS vendor).

Verifying Test Cases with IDS Actual Machine Test (3/5)

Among the target items excluded, *a to c are test cases that are excluded based on the adjustment and implementation policy of the test method based on the IDS specification defined in the previous slide. *1-3 are test cases that are excluded based on the specifications of the Base IDS and discussions with vendors. The reasons for this are described on the following slide.

Major class	Small classification	Test Case ID	ETAS	ARILOU
Detection function	No false positives	SD-FP-1	○	○
		SD-FP-2	Not applicable (*a)	Not applicable (*a)
	1. Error in the data of a single message	SD-TP-1-1	○	○
		SD-TP-1-2	Adjustment (specification of msg)	Not applicable (*1)
		SD-TP-1-3	Adjustment (prerequisites)	Adjustment (Detection target msg is output only to the payload.)
	2. Transmission cycle error	SD-TP-2-1	○	Adjustment (detection count)
		SD-TP-2-2	○	Adjustment (detection count)
	3. Error in relation to previous/next message	SD-TP-3-1	Adjustment (specification of msg)	Not applicable (*1)
		SD-TP-3-2	Not applicable (*a)	Not applicable (*a)
	4. Context error	SD-TP-4-1	Adjustment (detection target msg)	○
		SD-TP-4-2	○	Adjustment (detection target msg)
		SD-TP-4-3	Not applicable (*b)	Not applicable (*b)
		SD-TP-4-4	Adjustment (prerequisites)	○
	5. Status error of in-vehicle NW	SD-TP-5-1	○	○
	6. Attacks on diagnostic protocols	SD-TP-6-1	Adjustment (prerequisites)	○
		SD-TP-6-2	Adjustment (prerequisites)	Adjustment (Detection reason)
		SD-TP-6-3	Not applicable (*2)	Adjustment (Detection reason)
		SD-TP-6-4	○	○
		SD-TP-6-5	Not applicable (*a)	Not applicable (*a)
		SD-TP-6-6	○	○
		SD-TP-6-7	○	○
		SD-TP-6-8	○	○
Logging Function		SL-1-1	○	○
		SL-1-2	Not applicable (*c)	Not applicable (*c)
		SL-1-3	Not applicable (*c)	Not applicable (*c)
Notification function		SN-1-1	○	Not applicable (*3)

Verifying Test Cases with IDS Actual Machine Test (4/5)

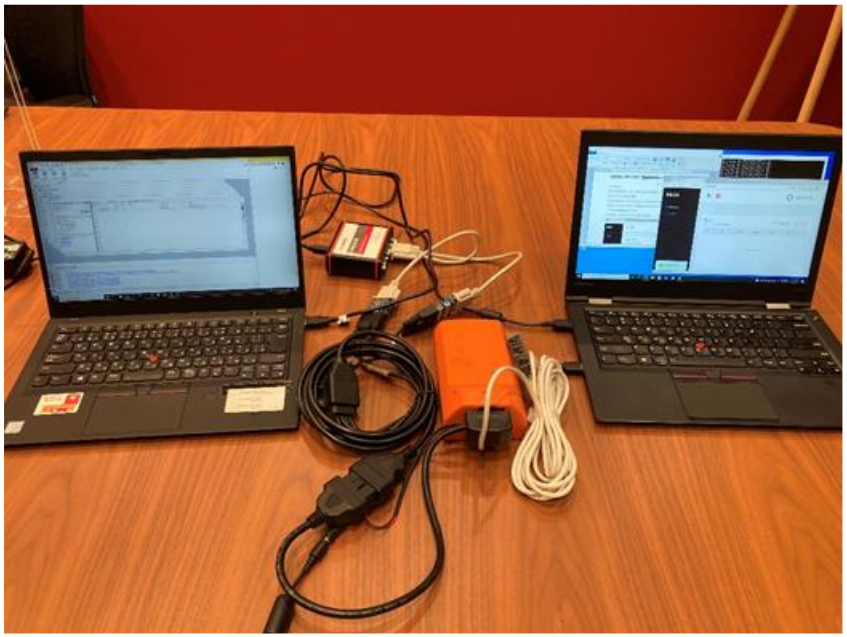
Reasons for exclusion from the Base IDS specification (previous slide*1 to 3) are shown below.

Comment number	Reasons for Exclusion
(*1)	ETAS/ARILOU's IDS customizes the system for OEMs. However, in order to shorten the development period, the IDS actual machine test has a minimum specification that outputs only one high-priority detection reason (e.g. "illegal transmission period") when a periodic transmission message is injected. On the other hand, the original expected value was to output all the corresponding detection reasons for the attack message (e.g. "illegal transmission cycle" and "invalid data range" as detection reasons). This time, the test cases that had the above effects were excluded, and the attack message to be injected was set to "not periodically send" in the target of the detection rule, etc. were adjusted.
(*2)	ETAS's base IDS does not support sequencing or stateful detection rules, so some test cases were excluded.
(*3)	IDS of ARILOU can be output to other CAN buses for IdsR module of AUTOSAR, for example, but this time, the message transmission function to the on-board network was omitted in order to shorten the development man-hour. For this reason, test cases related to the notification function were excluded.

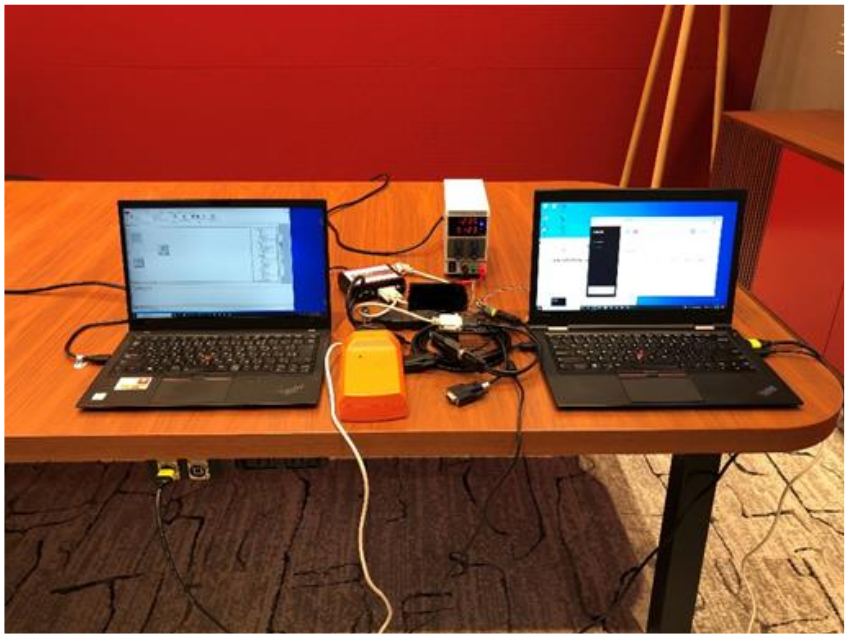
Verifying Test Cases with IDS Actual Machine Test (5/5)

The IDS actual machine test environment was constructed based on the basic configuration which was assumed when the basic test case was examined, and it was confirmed that the procedure shown in all test cases targeted for the test could be carried out as expected. The actual architecture of the IDS-based verification by “Arilou Information Security Technologies” is shown below.

Simulation environment



Test bed environment



Activities for Social Implementation

We had 8 meetings with Jaspar. The guidelines have already been transferred to JASPAR in 2022.

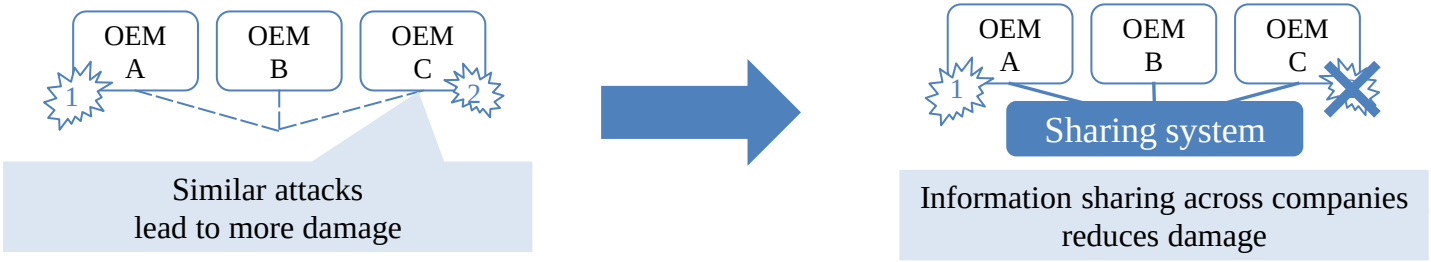
Meeting Name	Date	Agenda
1st Technical Review Meeting	October 9, 2020	• Explanation of activity a.
2nd Technical Review Meeting	December 18, 2020	• Effectiveness of operations • Counseling regarding equipment provision
3rd Technical Review Meeting	April 14, 2021	• Usage Scenes of IDS Development Process Verification and Assumed Basic Test Cases • Scope of the fundamental test case
4th Technical Review Meeting	June 28, 2021	• Basic Test Case Test Perspective
5th Technical Review Meeting	July 29, 2021	• Basic Test Case Test Method
6th Technical Review Meeting	October 5, 2021	• Specification evaluation point of view
7th Technical Review Meeting	November 18, 2021	• Explanation of the purpose of activity a. (again)
8th Technical Review Meeting	February 10, 2022	• Explaining comments from OEMs that challenges in launching IDS development • Verifying schedule to transfer

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

Research objective

The purpose is to investigate the basic specifications of information sharing systems and information collection methods, and to contribute to the improvement of security response capabilities in the automobile industry.

✓ <u>Advantage of information sharing system</u>



#	Theme	Outputs		For social implementation
B	Threat information sharing	Basic specifications for information sharing system	Hand over to	J-Auto-ISAC
	Proactive information collecting	Guideline for proactive information collecting		J-Auto-ISAC

We established 2 outputs and hand them over to J-Auto-ISAC for social implementation.

Outputs details

In activity b, we established “Basic specifications for information sharing system ” and “Guideline for proactive information collecting”.
We handed them over to J-Auto-ISAC for social implementation.

Outputs	Purpose and reader
Basic specifications for information sharing system	purpose: Propose an information sharing system what will improve the cyber security capabilities of the automotive industry. Reader will be… • Organizations who promotes information sharing and analysis about automotive security • OEMs and Suppliers involved in information sharing activities.
Guideline for proactive information collecting	purpose: Propose how to collect threat information proactively. This guideline can be used as a reference when OEMs, suppliers. Reader will be… • Industry groups, OEMs and suppliers who want to proactively collect information about attacks on vehicle systems

Activity Policy: Activity b. Research Approach

Following approach will be taken to develop “Basic specifications for information sharing system” and “Guideline for proactive information collecting”, and transfer to the industry groups.

Basic specifications for information sharing system					
1. Basic research We research what is Threat Intelligence, and how is it utilized for countermeasures.	**2. Examine methods** The method to apply method of threat information gathering in IT sector is examined.	**3. Examine system specifications** Information sharing system “To-Be” is formulated and system specification is examined.	**4. Formulation system specifications** Formulation the specifications and verification the applicability of elemental technologies to automotive field.	**5. Development the basic specifications** Based on [2] to [4], the basic specifications are summarized.	**6. for social implementation** Handover the Output created in [5] to related industry groups.

Guideline for proactive information collecting					
1. Basic research We research how do you gather and analyze information to form threat intelligence.	**2. Examine methods** The method to apply method of threat information gathering in IT sector is examined.	**3. Experiment collecting method** Based on [2], we conduct experiments and evaluate the effectiveness of the information gathering method.	**4. Extension collecting method** Evaluate the effectiveness of the information gathering method for the extended method of [3] and other methods.	**5. Development the Guideline** Continuing the experiment in [4] and summarizing it as a guide based on the experiment and [2] to [4].	**6. for social implementation** Handover the Output created in [5] to related industry groups.

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

◆Basic specifications for information sharing system

Examination of basic specifications

Initial response in this activity refers to activities that prevent incidents through information gathering during normal times and response activities after an incident occurs.

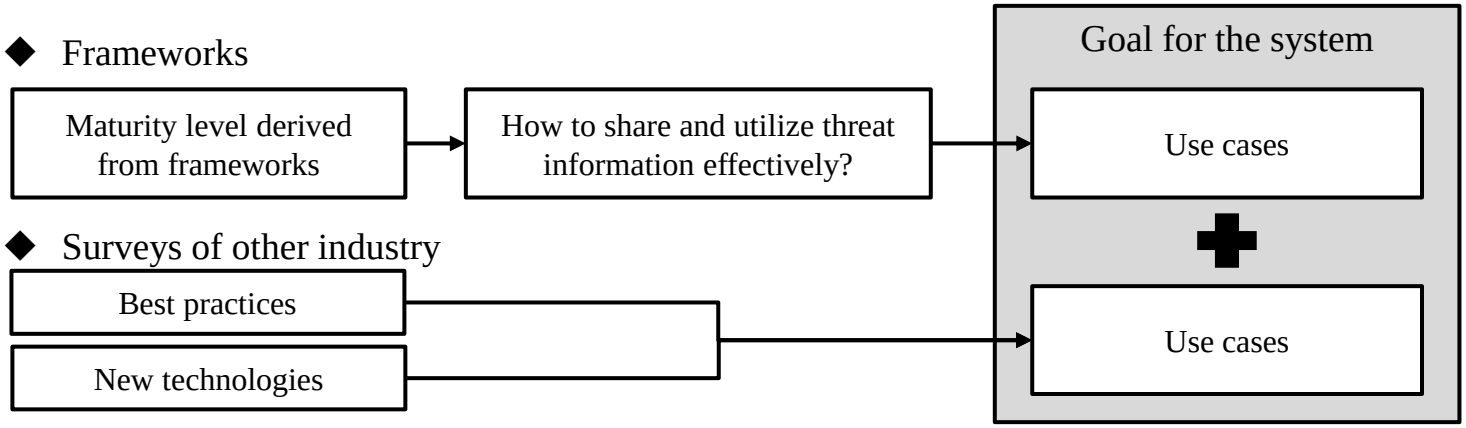
Phase		Description
Preventive measures	Identification	Identify threats and vulnerabilities related to owned cars and systems through information gathering
	Defense	Take appropriate security measures against identified threats and vulnerabilities
Countermeasures for incidents	Detection	Monitoring the vehicle system and detecting events
	Response	Respond to incidents that have occurred
	Recovery	Recover incidents that have occurred and take permanent measures

Scope of the Initial response in this project

What should an information sharing system “To-Be”

We expressed "To-Be" by use case. Use cases are derived from frameworks and best practices of other industry.

Approach for formulation of the “To Be”



CMM for Handling threat information

Lv.	Description
4 Adaptive	The company is aware of cyber security risks related to its products or owned systems as well as its supply chain, and collects threat information timely. Threat information is utilized by the company and its stakeholders for incident prevention and post-incident management, and the method is formulated and regularly reviewed.

*https://www.ipa.go.jp/security/publications/nist/index.html
*https://www.acq.osd.mil/cmmc/about-us.html

Examples: Use cases

Some examples of use cases are derived from frameworks and best practices of other industry are shown as follows.

Examples of Use cases from frameworks

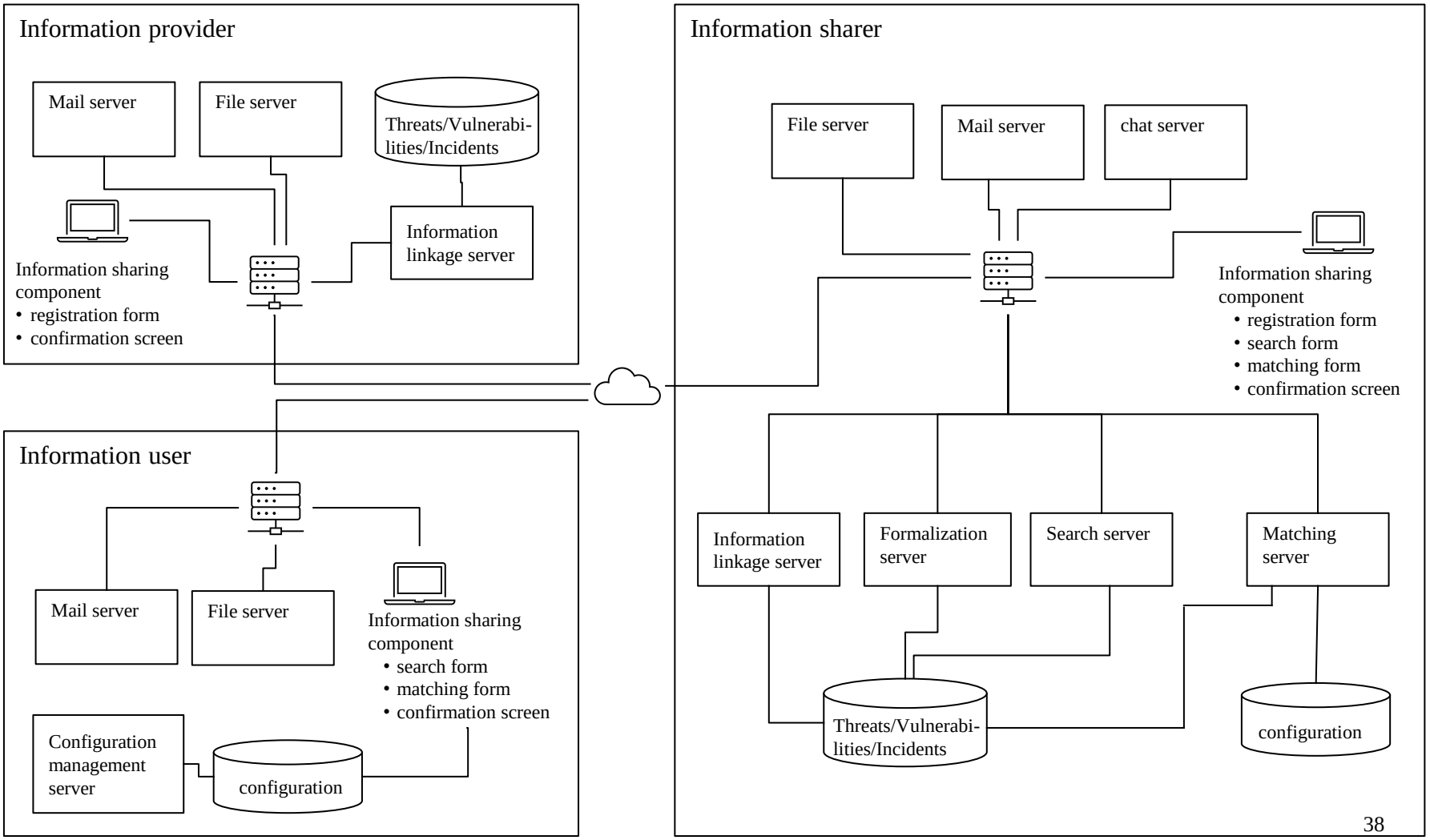
Activity goal (classification)	Use cases
information sharing	Information users analyze unformatted information group (threat information, vulnerability information, incident information) and then grasp risks from information related to their company.
	Information sharers organize and formalize unformatted incident information as threat information and vulnerability information. Information users grasp risks from information related to their own companies.
information utilization	Information sharers search for related countermeasure information based on formalized information group (threat information, vulnerability information), and information users apply the countermeasure.
	Information sharers search for related countermeasure information based on unformatted information group (threat information, vulnerability information, incident information, countermeasure information), and information users apply the countermeasures.
process automation	Information users formalize and associate their own product information with related product/part information.
	Information providers formalize information group (vulnerability information, countermeasure information), and information users compare whether it is related to the company's product and grasps the necessary countermeasures.

Example of Use cases from surveys of other industry

Use cases
Anonymization of the source of information is possible when the information provider provides the information.
Information sharers provide information users with background information and sources, as well as indicators of information group (threat information, vulnerability information, incident information) to the extent possible.
Information sharing among information users and within some information user groups.
Information providers can set the range of information sharing.

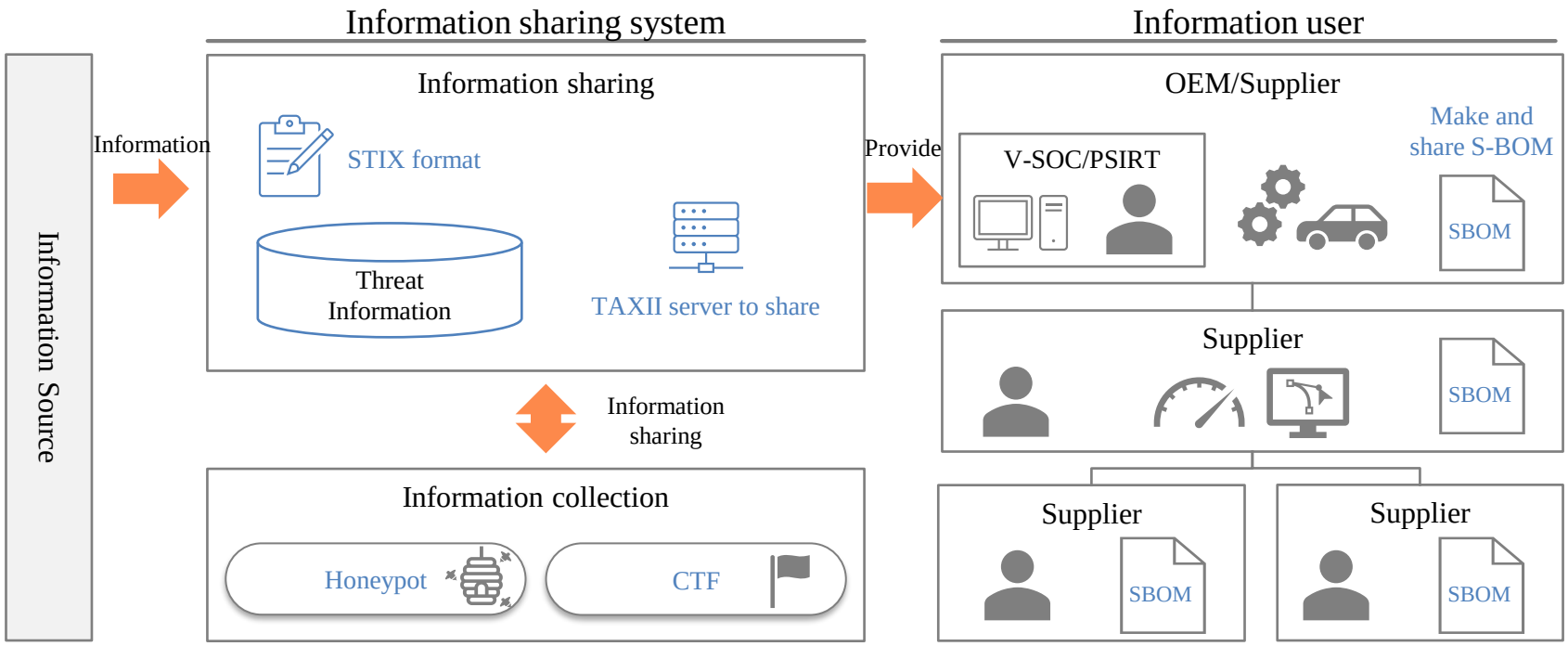
Schematic image of the sharing system

The basic specifications of the information sharing system are derived from the viewpoints of information providers, information sharers, and information users.



PoC: Information sharing system

We focused on STIX, TAXII, and S-BOM as candidate technologies to realize an information sharing system. We verified whether these technologies can be applied to the automobile industry.



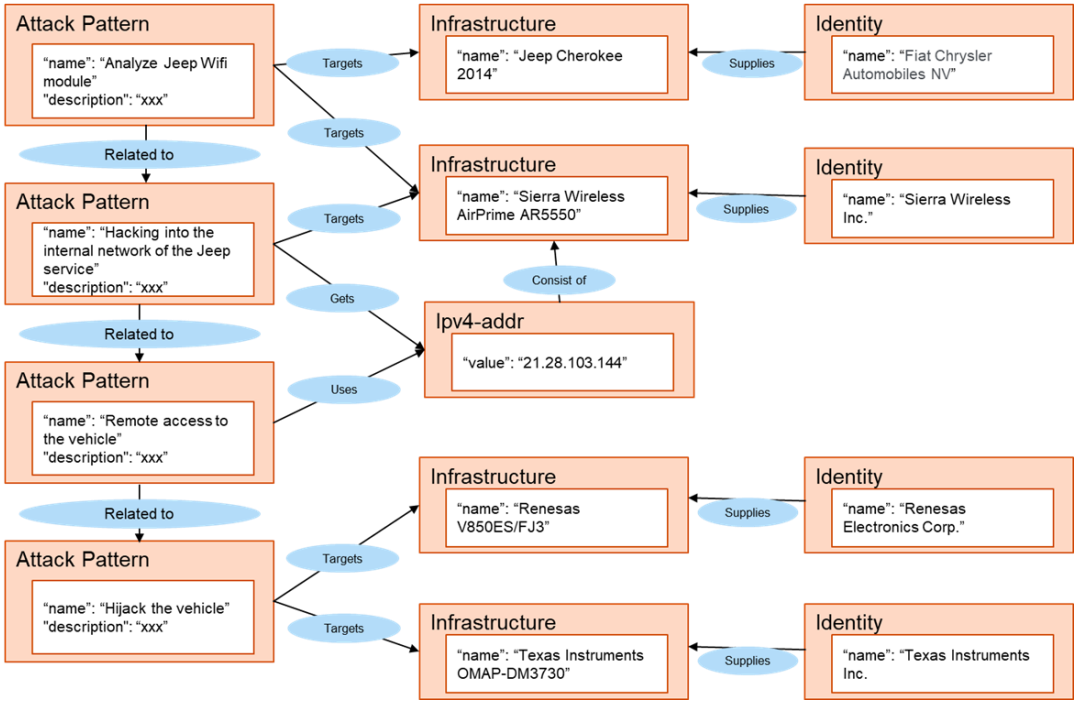
- STIX : Can STIX be applied to the description of threat information about automobiles?
- TAXII : Can the specifications set this time be realized using the functions of TAXII?
- SPDS-Lite(S-BOM) : Confirm whether it is possible to use the component list described in SPDL-Lite for the threat information described in STIX.

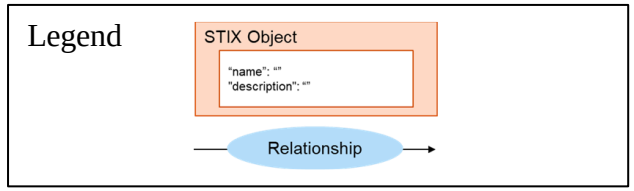
PoC: STIX

Threat-information from reported incidents was attempted to be described in STIX format. Consequently, though it is able to apply STIX in the reported cases, STIX can be used more efficiently by standardizing description rules.

#	Target vehicle type	Overview
1	Cherokee (Jeep)	It is reported that the ECU firmware can be rewritten through the cellular telephone network, and BCM such as the vehicle's steering, air conditioner, stereo, etc. can be operated illegally for the driving vehicle. (2015)

STIX Objects and Relations





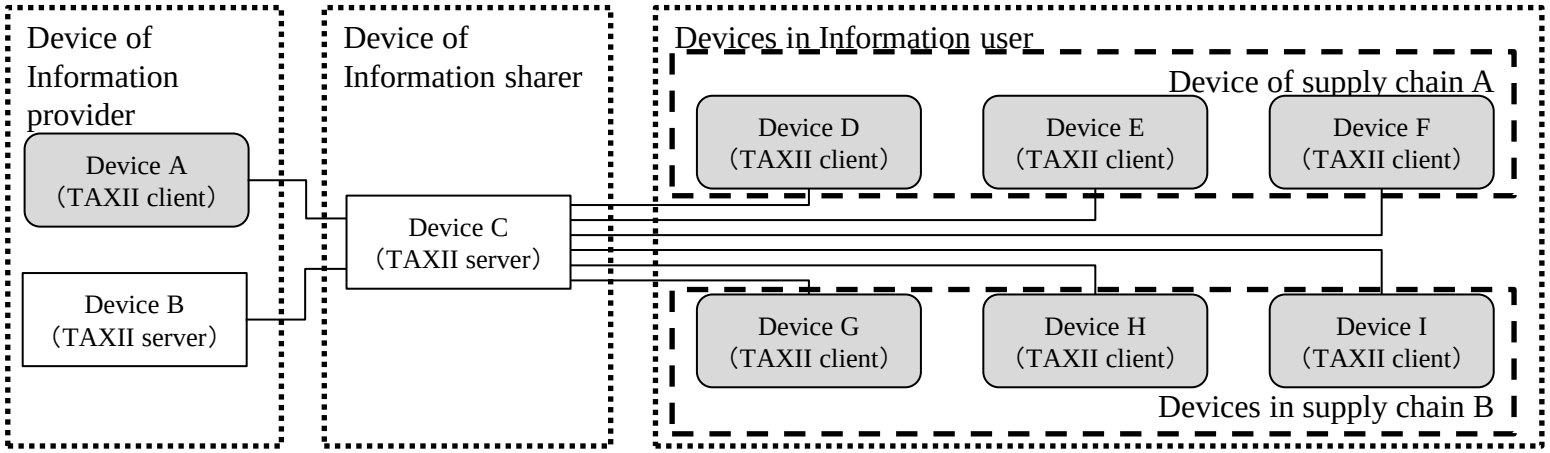
Approach;

1. Search for automobile attack incidents reports
2. Analyze the reports to obtain threat information
3. Make the threat information into STIX Object
4. Use "relationship" attribute to describe relations between objects

PoC: TAXII

We constructed a PoC environment and confirmed whether the information sharing method defined in the specifications can be realized. With the current TAXII version 2.1, it is difficult to complete information sharing with TAXII alone, and it is expected that it will be used in combination with other IT technologies.

PoC System



Examples of PoC test cases

No	information sharing method	test case
1	Information sharing to the entire industry	Information sharing from device C to devices D, E, F, G, H, and I
2	Information sharing to specific groups within supply chain A	After saving information from device D to device C, share information only to devices E and F
3	Information sharing to specific individual company within supply chain A	After saving information from device D to device C, share information only to device E

PoC: SPDX-Lite(S-BOM)

Confirm whether it is possible to use the component list described in SPDL-Lite for the threat information described in STIX. Since the threat information may not include the software name and version name, it can be used efficiently by including the device name and manufacturer in the S-BOM.

Prepared component information

Item	OEM name	HW	SW package	component package	Wi-fi supplier	HW	SW package	component package	processor supplier	HW	SW package	component package	ECU supplier	HW	SW package	component package
content	OEM-A	Hardware_A	Software_A-1	Software_A-1-1	Supplier-B	Hardware_B	Software_B-1	Software_B-1-1	Supplier-C	Hardware_C	Software_C-1	Software_C-1-1	Supplier-D	Hardware_D	Software_D-1	Software_D-1-1

Compare SPDX-Lite with STIX

No		1	2	3	4	5	6	7	8	9	10	11	12
STIX	Item	identity	attack-pattern			ipv4-addr	infrastructure			-	-	-	-
	content	Jeep Cherokee	Air Prime AR5550	V850 controller	OMAP chip	21.28.103.144	Sierra Wireless AirPrime AR5550	Renesas V850 processor	Texas Instruments OMAP-DM3730 system	-	-	-	-
S-BOM	Item	-	-	-	-	-	Creator- Organization			DocumentName			
	content	-	-	-	-	-	Supplier-B	Supplier-C	Supplier-D	Software_A-1	Software_B-1	Software_C-1	Software_D-1

Summary

We hope that cyber security in the automobile industry will be improved by referring to the basic specifications created in this research study.
Followings show some options to utilize our outputs.

- Information sharing activities will be further improved by developing an information sharing system based on the specifications and operating it continuously.

- The specifications will help OEMs/Suppliers to cultivate further understanding of technology trends in foreign countries and other industries.

- Promote security research on the connected service side, which each company independently investigates and responds to, across the industry.

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

◆Guideline for proactive information collecting

Threat information collecting method

The purpose of this study is to establish a threat information method in the automotive industry. We experimented whether it is possible to collect automobile threat information using Playground and Honeypot, which are already used in the IT field.

Purpose	• Establishing methods for gathering and accumulation threat information in the car domain.
What-If	• In the IT field, various methods have been tested and operated to actively collect threat information on the trends of cyber attackers, attack methods, etc., and they are useful for the construction of cyber intelligence. • In the connected system, the threat information can be collected by the same technique, and cyber intelligence can be constructed. 
Gathering information	• Cyber Attacker Properties (Indicators such as IP Address and URL) • Attack operandi (TTPs of attack codes, malware, etc. attempted)
Approach	• Attack patterns on connected systems are organized, and the possibility of collecting threat information in connected systems is evaluated through actual observation experiments using the threat information collection method in the IT field.

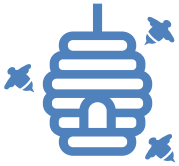
Expectation on Playground and Honeypot

The expectation of honeypot and CTF 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:



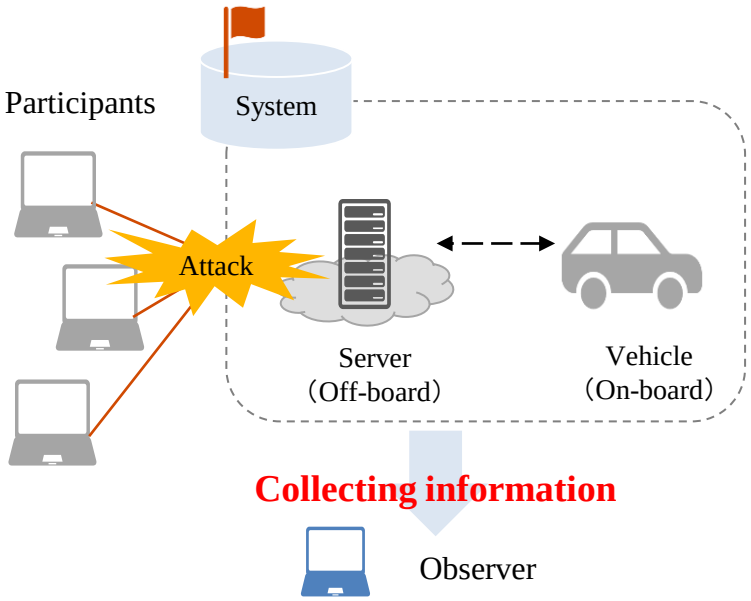
- Are there actually connected cars being accessed from the internet?
- Are there any devices that have been accidentally exposed to the internet?

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

Purpose: Playground

The purpose is to investigate what kind of cyberattacks are conducted against connected vehicles. Investigate the attacker's motivation (attack purpose) and behavior such as access and details.

Purpose	We want to know… Attack, Activity, Behavior
Plan	• Targeting vehicle control, acquisition of vehicle information, etc., the participant will attempt to attack the target system. • Obtain knowledge for quick detection of attacks based on observations of attackers' attack techniques and methods, etc.

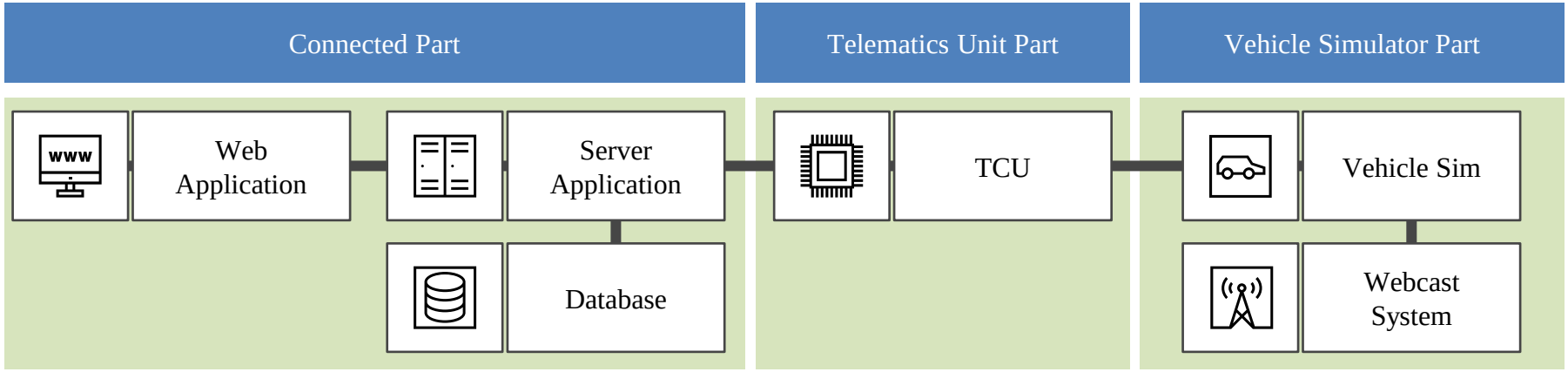


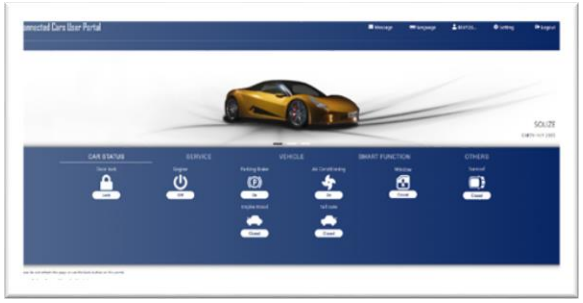
Advantages for playground

- Able to know attacker’s motivation and attack procedures.
- Trace attacker’s behavior by checking logs.
- Improve cyber-security measures based on the collected information.

System configuration of Playground Platform

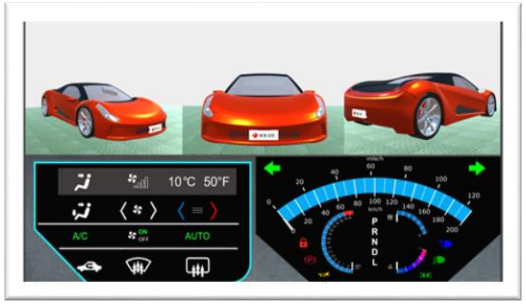
We built a platform that replicates/mimics the vehicle, connected services (servers and user portals or apps) to hold a CTF with the goal of “Hijack the car”
The platform is a cyber attack verification system consisting of a connected server, telematics unit, and vehicle simulator.





User Application
(Owner’s portal)

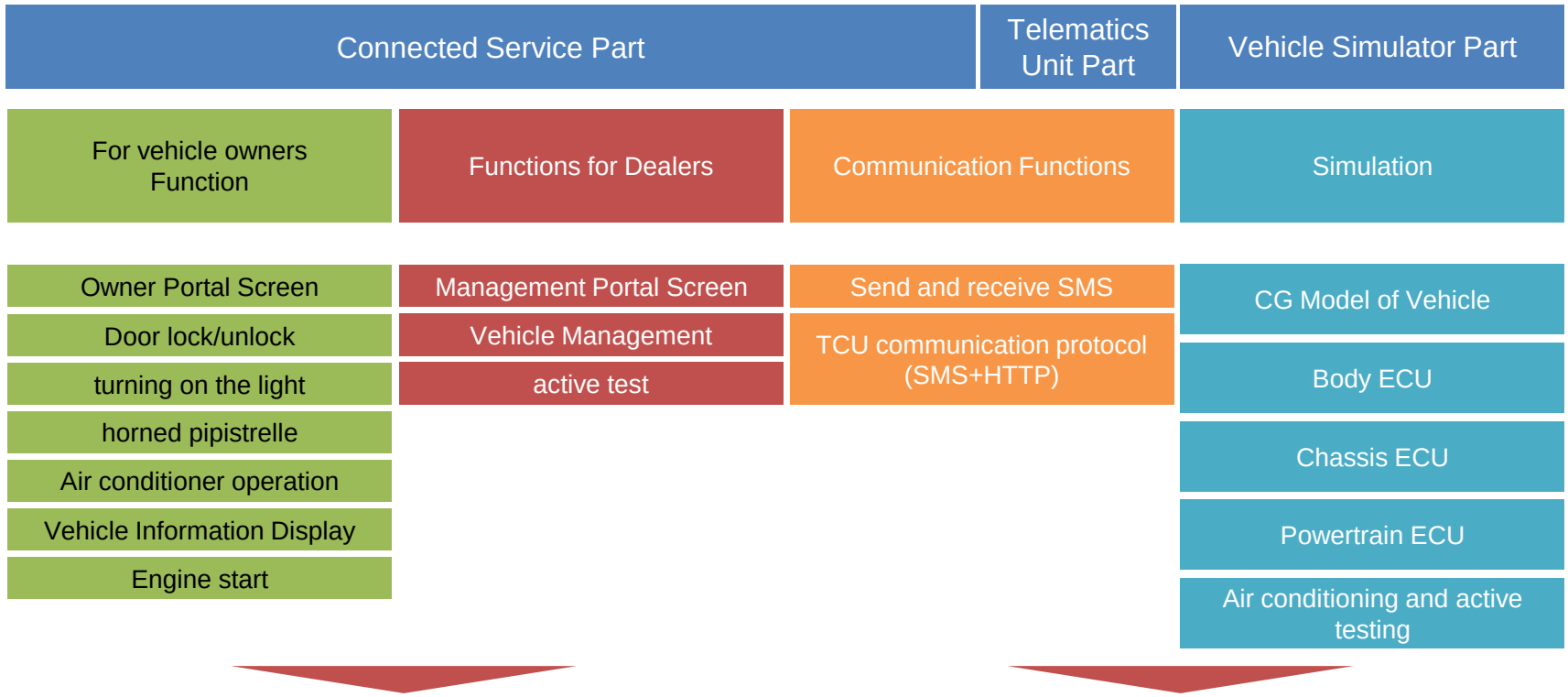
TCU
(Rpi, SIM, Dongle)



Vehicle and dashboard

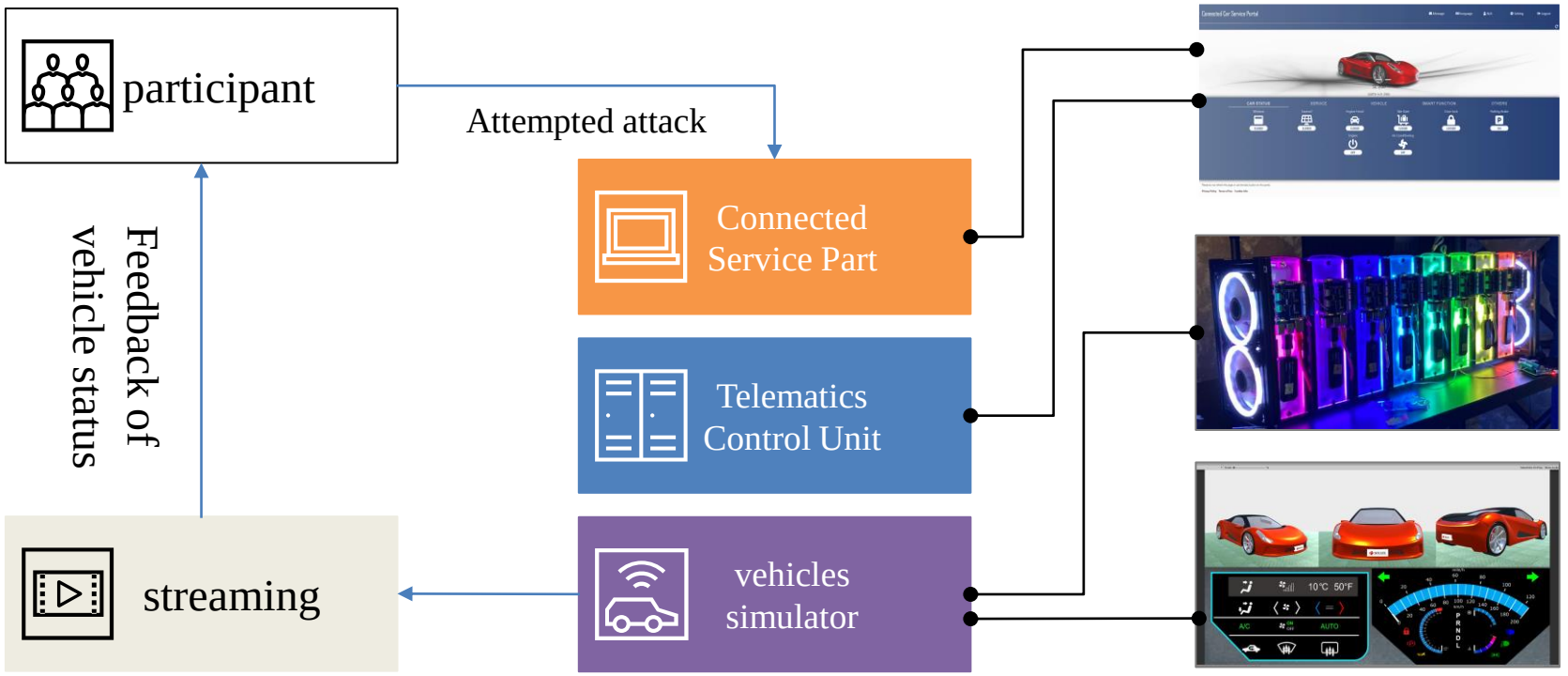
Platform Features

The platform implements the following main features as connected functions
Users can operate the vehicle (simulator) via connected services.



Overall picture of Playground

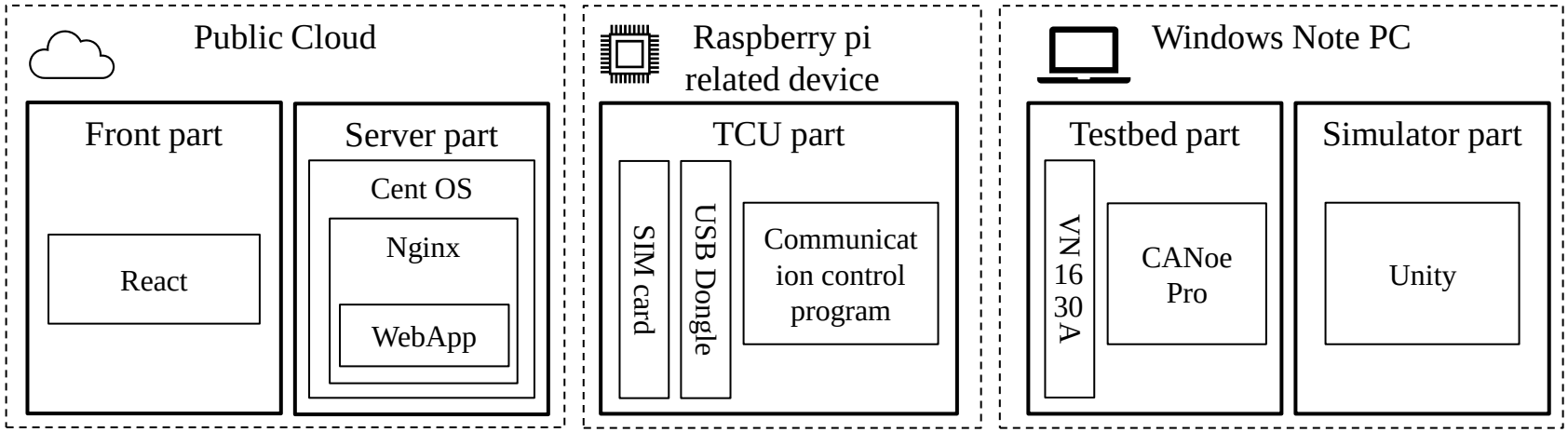
Observation and analysis of car attacks by white hat hackers via connected services during the contest will contribute to the elucidation of the characteristics and behavioral traits of these attacks.



Playground results

In our playground, we defined "web application", "server" and "TCU" as the attack surface for the vehicle, and investigated the motivation and attack method.

Playground system architecture



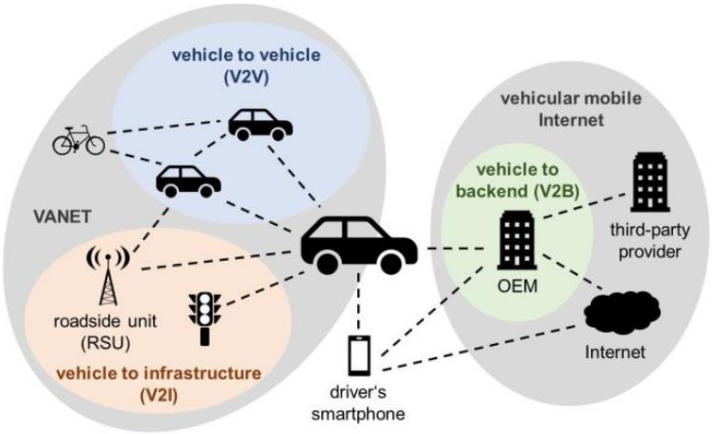
Examples of revealed motivations and attacks

Component	Motivation	Tried attacks
WebApp	• API survey • Analyze login process and APIs	• Analyze downloaded JavaScript
Server	• Analyze overall picture of WebApp and the usage of APIs	• WebApp code analysis
TCU	• Compromise TCU	• Survey on buffer overflows and USE-AFTER-FREE vulnerabilities

Purpose: Honeypot

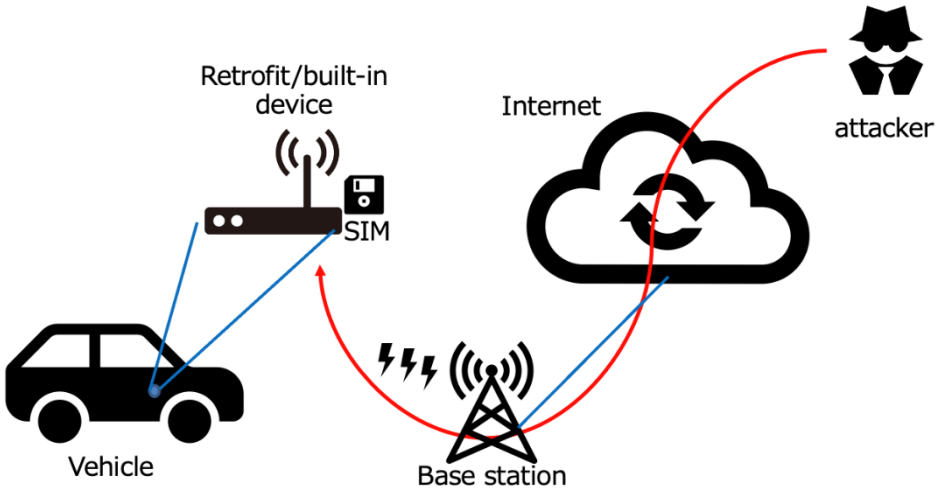
The purpose of Honeypot is to observe “what kind of cyber attacks are received from the Internet against vehicle-mounted devices such as routers and gateways which devices are exposed to the internet.”

Background



As car become more automated and connected, security issues on vehicles are changing.

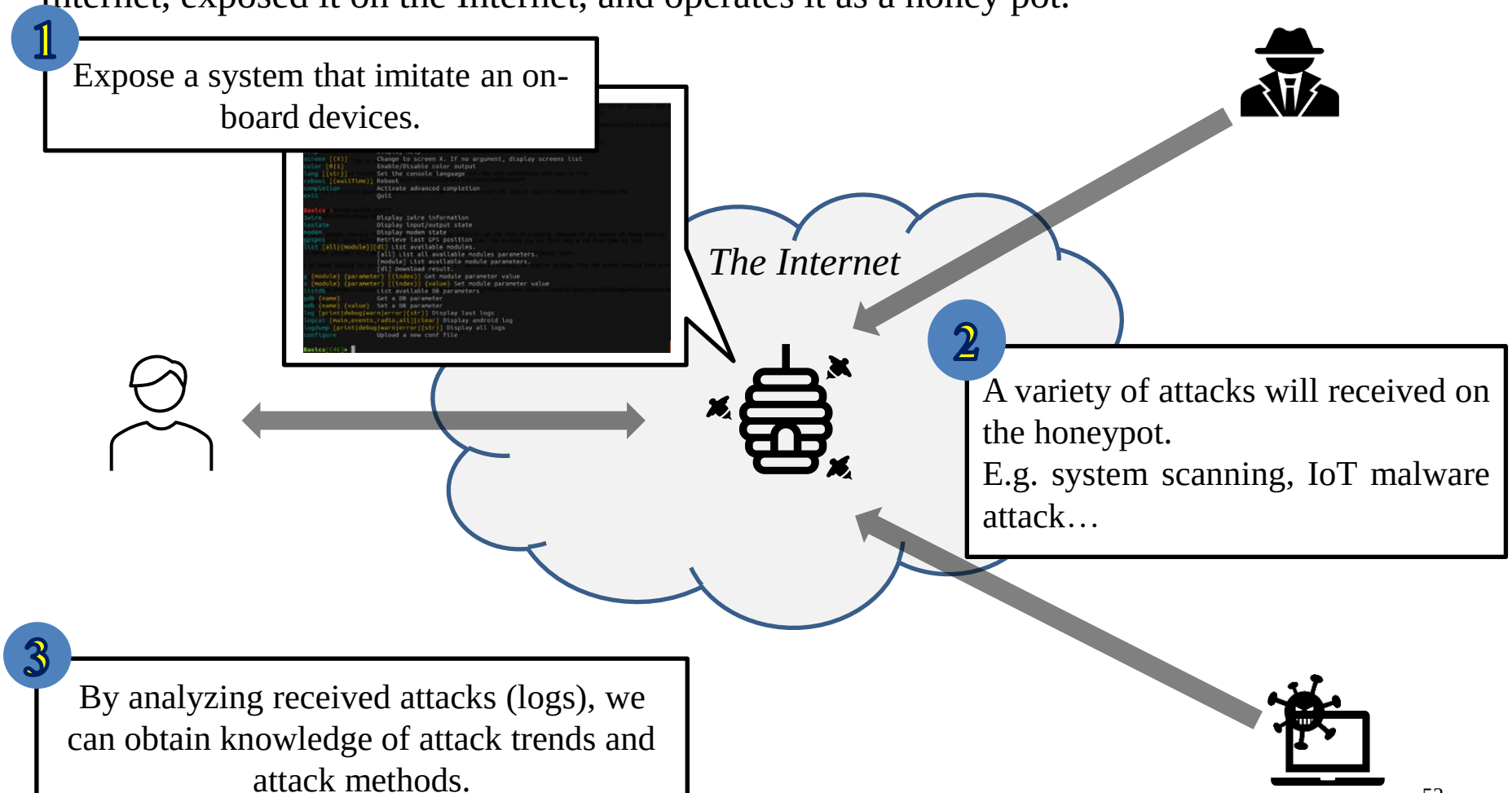
Purpose of Honeypot



Our scope of Honeypot is direct attacks on on-board devices received from the internet.

Vehicular Honeypot

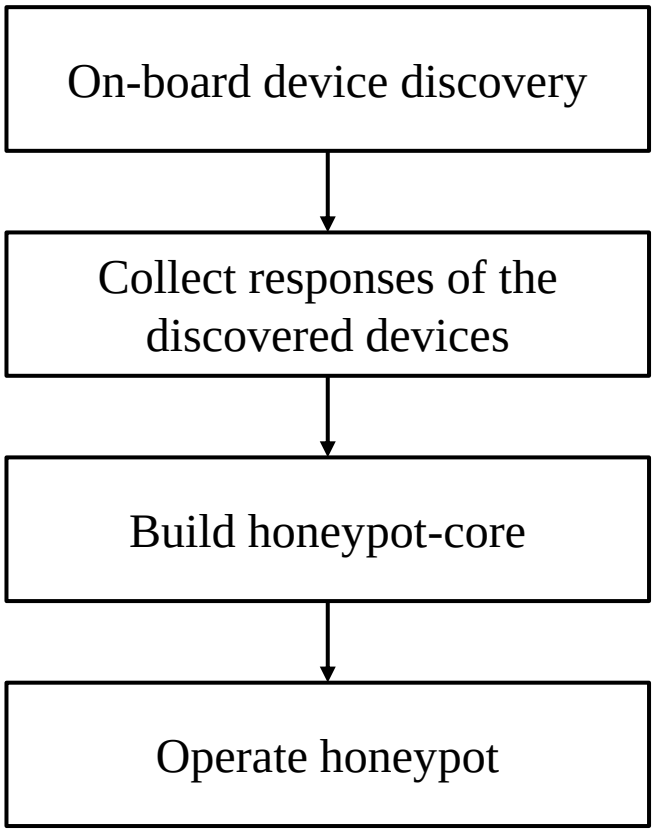
The point of vehicular honeypot is to attract attackers and obtain insights and knowledge of attack trends and attack methods.
Therefore, a system that imitates an on-board device that can be accessed from the Internet, exposed it on the Internet, and operates it as a honey pot.



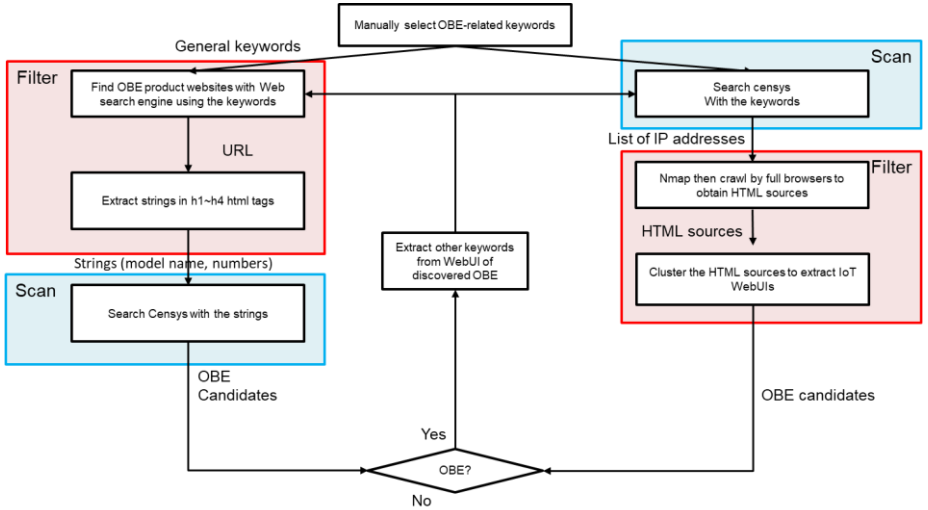
Honeypot building process

We prepared honeypot by the following 4 steps. We have 2 approaches to discover on-board devices.

Honeypot building process



Device discovery



2 approaches for device discovery

- Search the search engine (google) with keywords related to cars, and collect the name, model, and model number of in - vehicle equipment. Then, use obtained information to search on Censys.
- Firstly, search on Censys with keywords related to the cars. After the clustering, using web search to identify whether the devices are car-related devices or not.

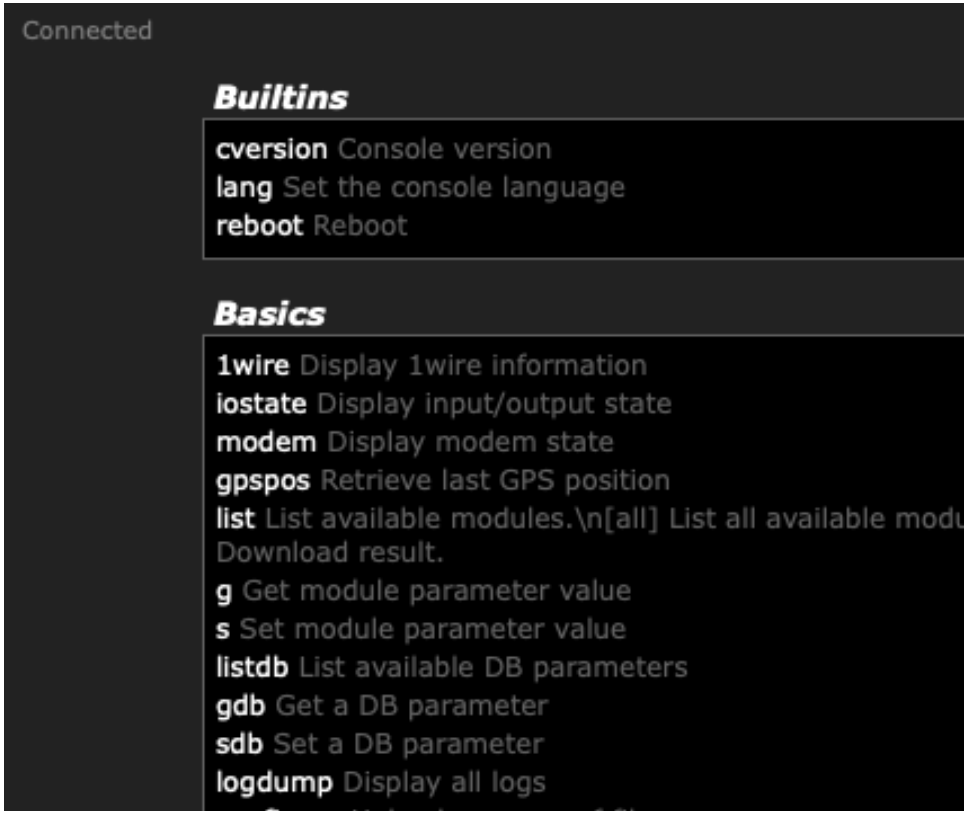
Example of discovered on-board devices

Discovery of on-board device revealed that some devices were vulnerably exposed on the Internet.

An example of discovered on-board device

22/tcp OpenSSH5.1
23/tcp telnet
80/tcp http

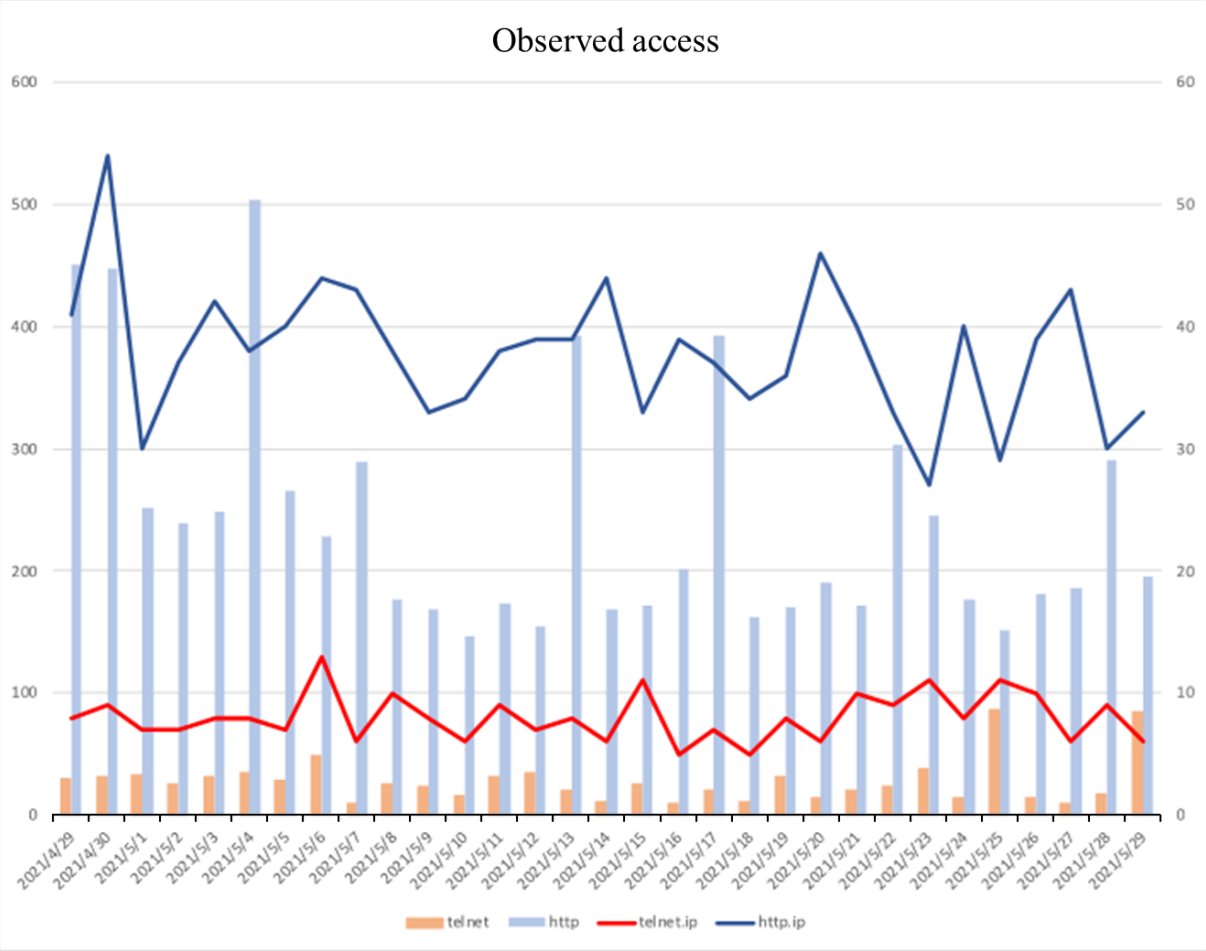
No-authentication



Jose Carlos Norte. Hacking industrial vehicles from the internet: http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html （reference 2023.02.22）

Result of honeypot observation

Although the attacks clearly targeted on-board devices were not observed, many attacks aimed at various vulnerabilities in network services were observed.
On-board devices could have those vulnerabilities, and as a result, it was confirmed that they could be attacked that would affect the operation of in -vehicle aircraft.



Summary

We hope that cyber security in the automobile industry will be improved by referring to the basic guideline established in this research study.
Followings show some options to utilize our outputs.

- In order to efficiently analyze logs obtained from the playground and honey pot, it is recommended to utilize tools such as SIEM.
- The guideline will help OEMs/Suppliers to cultivate further understanding of technology trends about collecting threat information proactively.
- In addition to collecting information, we will promote research on how to analyze the collected information.

Activities for Social Implementation

We had 5 meetings with J-Auto-ISAC. Our outputs, the Specification and the guideline will have transferred to J-Auto-ISAC in 2023.

Outputs	Hand over to	Future work
Basic specifications for information sharing system	J-Auto-ISAC	• J-Auto-ISAC will improving information sharing activities based on the Specification. • In order to cooperate with domestic and foreign organizations such as US-Auto-ISAC, we need to consider structuring threat information. • Continue to have touch points with US-Auto-ISAC and other organizations to catch the latest technical trends.
Guideline for proactive information collecting	J-Auto-ISAC	• J-AUTO-ISAC will collects threat information proactively with reference to the guideline • One option is that the guide will be disclosed to the members in order to help OEMs and suppliers to collect threat information.

Collaborations with German partner

Trends in Automated Driving Security Development Assistance in Germany

In Germany, the Federal Department of Education and Research (BMBF) is leading the security research and development support for connected cars (automated driving), and at least four projects are currently in progress. The projects are in collaboration with SecForCARs.

R&D support requirements in Germany		
The following outcomes needs to be included at minimum: • Methods for protecting vehicles and infrastructures from cyber-attacks • Methods for verifying vehicle security		
#	**Project Name**	**Activity theme**
1	SATiSFy (Implement of safety functions in an automated driving vehicle)	Evaluation of individual components (sensors, etc.) and their mutual interactions related to automated driving
2	**SecForCARs (Security of Connected Automated Vehicles)**	**Research and Evaluation of Methods and Tools for Securing Communication to Vehicles**
3	SecVI (Security Architecture of Communication Network for Vehicles)	Developing a Robust, low-complexity network architecture for vehicles
4	VITAF	Ensuring the reliability of the automated driving How cyber-attacks are Detected and Responded Immediately Developing a mechanism to avoid impacts on safe operation even in the event of cyber-attacks Vehicle data protection (e.g. masking)

https://www.forschung-it-sicherheit-kommunikationssysteme.de/foerderung/bekanntmachungen/it-sicherheit-und-autonomes-fahren

Japan-Germany Collaboration Workshop

Five JAPAN-Germany collaboration workshops are planned, and as of April 2022, the third workshop has been held.

Time and location	Meeting	Agenda
2021/7 Online	WS1	• Threat intelligence and Vehicular honeypots • Concept and demonstration for integrated OTA software update • IDS management concept for distributed IDS
2021/12 Online	WS2	• Threat intelligence and Vehicular honeypots • Security Composition for Automotive System of Systems • Platform and Hardware Security
2022/4 Online	WS3	• Threat information sharing system • Discovery of exposed automotive devices • Crypto Hardware security
2022/10 Hybrid @Kyoto	WS4	• Incorporating Threat Intelligence into Automotive Trust Models • Model-based Security-Testing: Yet another Pentest? • Threat information sharing and vehicular honeypot
2023/1 Hybrid @Kokura	WS5	• Threat information sharing and proactive information collecting for connected cars • Enhancing Automotive Security with Hardware Trust Anchors • Automotive Security Future challenges and approaches

This report documents the results of Cross-ministerial Strategic Innovation Promotion Program (SIP) Phase 2/Automated Driving for Universal Services (SIP-adus, NEDO management number: JPNP18012) that was implemented by the Cabinet Office and was served by the New Energy and Industrial Technology Development Organization (NEDO) as a secretariat.