

**“SIP Automated Driving System/Large Scale
Field Operational Test”, “Information
Security Field Operational Test”**

Research Summary Report

PwC Consulting LLC

February 28, 2018

Positioning of this project

Project Phase	Major Activities	Major Items	Term
STEP1 Trial Field Operational Test	Threat Analysis Research	<ul style="list-style-type: none"> • Future Common Model for the Automated Driving System • Whole picture of threat 	2017/9/28 - 2018/2/28
	Develop Evaluation Guideline Draft	<ul style="list-style-type: none"> • Evaluation Guideline Draft (First & Second draft) 	
	Information Security Evaluation Trial		
	Preparation for management of Field Operational Test (STEP2)	<ul style="list-style-type: none"> • Implementation Plan (Schedule) • Participation Protocol (Flow chart etc.) • Entry Requirements(Guideline, requirements, application form, contracts) • Entry Briefing Session Plan, material • Information Security Management Method/ structure proposal 	
STEP2 FOT	Conduct Field Operational Test and revised Evaluation Guideline	<ul style="list-style-type: none"> • Evaluation Guideline Draft (Final) 	2018/4 - 2019/2

Project Scope

Objectives and scope

Objectives:

Clarify the whole picture of threat against automated driving system including attacks from outside of the vehicle such as V2X and foster public consensus regarding security of automated driving vehicles

Scope of the research:

I. Threat Analysis Research	Research of common model for the automated driving system	<ul style="list-style-type: none">• To research the automated driving/connected car promoted by automotive manufacturers, suppliers and IT companies etc. and develop common model for the automated driving system
	Research of whole picture of threat	<ul style="list-style-type: none">• To clarify threat items, related to the common model, including attack from outside of the vehicle such as V2X• To conduct impact evaluation to each of those and identify serious threats• To reflect countermeasures to the evaluation guideline developed separately for those threats identified above

a Threat Analysis Research

The approach to identify Common model for automated driving system

自動走行システム共通モデル調査	<ul style="list-style-type: none"> 自動車メーカー、部品サプライヤ、IT企業などの自動運転・コネクテッドカーに係る取り組みをファクトベースで調査し、整理・類型化することで自動走行システム共通モデルを導出する
脅威の全体像調査	<ul style="list-style-type: none"> 自動走行システム共通モデルに基いた脅威の全体像の抽出と脅威の洗い出し、脅威の全体像の整理する 自動走行システム共通モデルに含まれる脅威に対して脅威分析を実施し、特に重大な脅威については、評価ガイドラインに対策を盛り込む

Red: Major deliverables

1 Make a list of services and functions related to automated driving system

- investigate public information of automotive manufacturers, suppliers, technology companies, etc., and make a list of services and organized functions related to automated driving/connected car

List of services and functions

Investigated companies	Services	Functions
16 automotive manufacturers	1 Driving and parking assist	<ul style="list-style-type: none"> Adaptive Cruise Control Lane Keeping Assist Cooperative Adaptive Cruise Control(V2V) Vehicle platooning Automated driving(C-ITS) ...
4 automotive suppliers		
23 technology companies	2	...

2 Assume system topology of each function

- Assume system topology of each function based on public information of automotive manufacturers, suppliers, and IT companies
- Conduct interviews with experts as well

Services	Functions
1 Driving and parking assist	<ul style="list-style-type: none"> Adaptive Cruise Control Lane Keeping Assist Cooperative Adaptive Cruise Control(V2V) Vehicle platooning Automated driving(C-ITS) ...
2

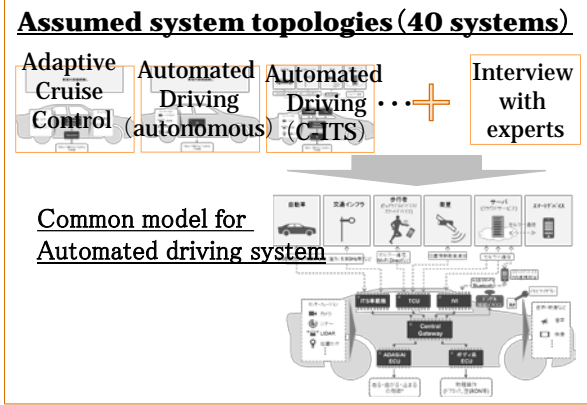
Homepage, etc.

Identify system topology

System topology of Adaptive Cruise Control

3 Identify common model for automated driving system

- Identify common model for automated driving system in this threat research by taking in to account all system topologies
- Conduct interviews with experts as well



[Input]

- Public information of 16 automotive manufacturers, 4 suppliers, and 23 technology companies

[Input]

- List of services and functions
- Public info. of major automotive manufacturers, suppliers, and tech companies
- Comments received in interviews with experts

[Input]

- System topology of each function
- Comments received in interviews with experts

[Output]

- List of services and functions related automated driving system

[Output]

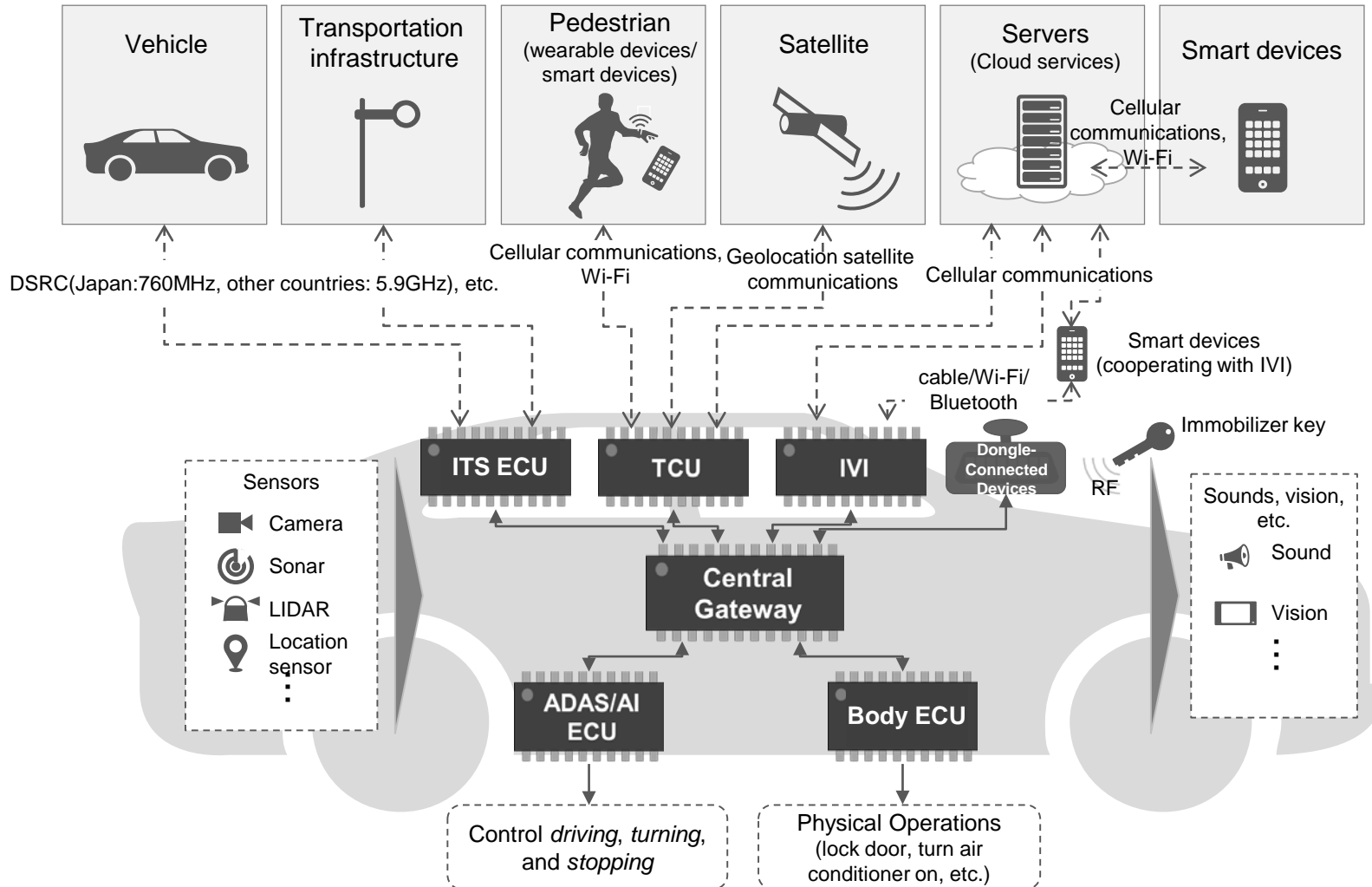
- List of system topology of each function

[Output]

- The common model for automated driving system for the threat analysis research**

Common model for automated driving system (Early 2020's)

The common model for automated driving system for the threat analysis research



*Since the topology of control functions related to steering, brakes, engines, etc. does not directly affect the threat analysis result, abstracted these

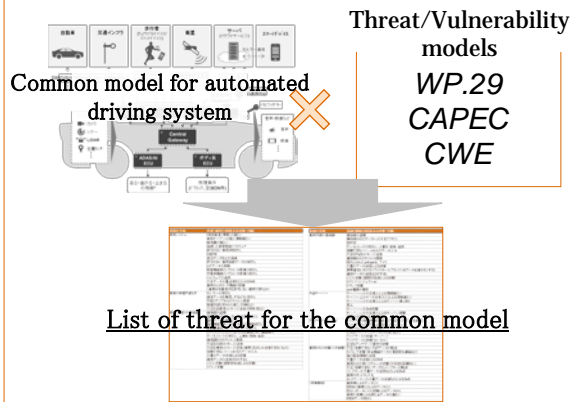
The approach to identify whole picture of threat

自動走行システム共通モデル調査	<ul style="list-style-type: none"> 自動車メーカー、部品サプライヤ、IT企業などの自動運転・コネクテッドカーに係る取り組みをファクトベースで調査し、整理・類型化することで自動走行システム共通モデルを導出する
脅威の全体像調査	<ul style="list-style-type: none"> 自動走行システム共通モデルに係る、V2X等車外からの攻撃を含む脅威を洗い出し、脅威の全体像の整理する 自動走行システム共通モデルに含まれる脅威に対して脅威分析を実施し、特に重大な脅威については、評価ガイドラインに対策を盛りこむ

Red: Major deliverables

4 Make a list of threat for the common model

- Apply *Threat Matrix* created by WP.29, threat/vulnerability models to the common model, and make a list of threat for the common model

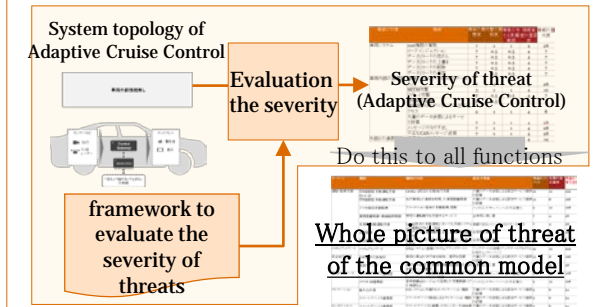


[Input]
 • Common model for automated driving system
 • Threat models(WP.29 Threat Matrix, CAPEC)
 • Vulnerability models(CWE)

[Output]
 • List of threat for the common model

5 Identify whole picture of threat for the common model

- Develop a framework to evaluate the severity of threats combination with the list of threat for the common model and indicators for evaluating the severity of threats
- Apply the framework to system of each function and evaluate the severity of the threat of it
- Do this to all functions and identify a whole picture of threat for the common model

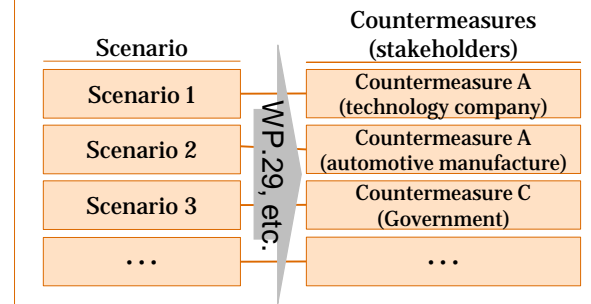


[Input]
 • List of threat for the common model
 • Indicators for evaluating the severity of threats(WP.29, CRSS)
 • System topology of each function

[Output]
 • **Whole picture of threat of the common model**

6 Investigation of countermeasure against serious threats

- Identify important countermeasures and clarify stakeholders taking responsibilities, based on serious threats for the common model
- In addition, reflect countermeasures, if necessary, in information security evaluation guideline



[Input]
 • Whole picture of threat of the common model
 • Security countermeasures developed in WP.29

[Output]
 • **Research results on countermeasures against threats of the common model for the automated**

Whole picture of threat for the common model

Below are threats scored level II or higher, of the common model.

Whole picture of threat for the common model

Level of threat	Level I (Caution)	Level II (Warning)	Level III (Critical)
Score	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

Services		Functions			Threat	Magnitude of threat	Probability of attack	Threat Severity		
Category		Category	Content							
1	Driving and parking assist	1-3	Adaptive Cruise Control(V2V)	Function to control inter-vehicle distance with preceding vehicle by cooperating with ITS	Accepting information from an unreliable or untrusted source	2.8	1.6	4.4		
					Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	4.2	1.6	6.7		
		1-4	Vehicle platooning(V2V)	Function to follow the leading car automatically by communicating with the leading car (Function for commercial vehicle such as trucks)	Accepting information from an unreliable or untrusted source	2.8	1.6	4.4		
					Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	4.2	1.6	6.7		
		1-5	Automated driving(C-ITS)	Function to perform all driving tasks on behalf of humans by cooperating with ITS	Accepting information from an unreliable or untrusted source	2.8	2.4	6.7		
					Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	4.2	2.4	10.0		
		1-9	Automated parking(Cooperative Smart device)	Function to perform automated parking remotely by giving operation instructions of the vehicle via an application installed on the smart device	Attack on back-end server stops it functioning	1.8	2.4	4.3		
					Accepting information from an unreliable or untrusted source	2.8	2.4	6.7		
		2	Safety driving assist	2-2	Pedestrian detection(V2P)	Function to avoid a collision with pedestrian by communicating with a smart device owned by a pedestrian and detecting a pedestrian near the vehicle	Accepting information from an unreliable or untrusted source	2.8	1.6	4.4
							Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	4.2	1.6	6.7
4	Software update	4-1	OTA	Function to update software of ECU using wireless communication	Compromise of over the air software update procedures	4.2	2.4	10.0		
					The software is manipulated before the update process	3.6	1.2	4.3		

Whole picture of threat for the common model

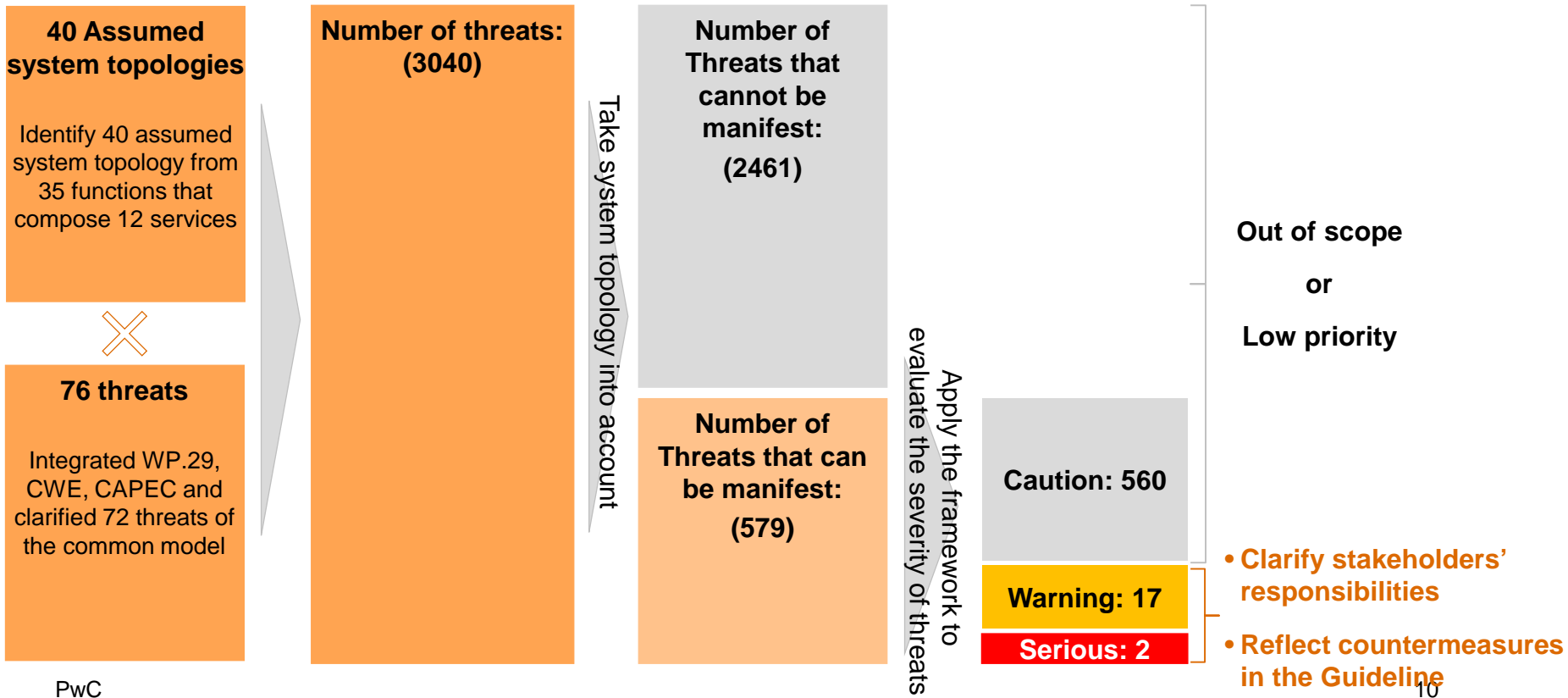
Below are threats scored level II or higher, of the common model.

Whole picture of threat for the common model

					Level of threat				
					Level I (Caution)	Level II (Warning)	Level III (Critical)		
					Score	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0	
Services		Functions			Threat	Magnitude of threat	Probability of attack	Threat Severity	
Category		Category	Content						
5	Failure detection	5-1	Failure detection	Function to predict and detect failures by using self-diagnosis function provided by itself	Attack on back-end server stops it functioning	1.8	2.4	4.3	
8	Vehicle remote control	8-1	Lock/unlock doors remotely	Function to control the locking / unlocking of the door of a remotely in cooperation with a smart device or the like	Attack on back-end server stops it functioning	1.8	2.4	4.3	
		8-3	Power charge control	Function to control charging status, such as charge rate, charge stop, etc., remotely in cooperation with a smart device	Attack on back-end server stops it functioning	1.8	2.4	4.3	
		8-4	Power charge control (collaborating with cloud-based AI service)	Function to control charging status, such as charge rate, charge stop, etc., remotely in collaborating with cloud-based AI service	Attack on back-end server stops it functioning	1.8	2.4	4.3	
		8-5	Air conditioner control	Function to control air conditioner remotely in cooperation with a smart device	Attack on back-end server stops it functioning	1.8	2.4	4.3	
		8-6	Air conditioner control (collaborating with cloud-based AI service)	Function to control air conditioner remotely in collaborating with cloud-based AI service	Attack on back-end server stops it functioning	1.8	2.4	4.3	
		8-7	Engine restart/steering lock release prohibition	Function to prohibit engine restart/ steering lock release based on owner's request	Attack on back-end server stops it functioning	1.8	2.4	4.3	

The approach to identify whole picture of threat(Summary)

- Based on all the systems related to the common model, identify threats that can be manifest, and clarify threats to be handled preferentially by using the severity evaluation framework
- Against the identified threats, clarify the responsible stakeholders of countermeasures and reflect threats that need countermeasures in the evaluation guideline



Threats and countermeasures that should be concerned by stakeholders

01

**Automotive
manufacturers**

- Automotive manufacturers need to take countermeasures against threats such as "Sending a large number of garbage data to vehicle information system" to ITS cooperative type automated driving function.
- We've added items to the guideline on serious threats that automotive manufacturers should work through, and we are hoping that countermeasures will be taken by evaluating them based on these in the future.

02

**Technology
companies**

- IT service providers need to take countermeasures against threats such as "Compromise of over the air software update procedures" to OTA function
- These countermeasures are mainly required for information systems such as servers, and these are out of the scope of this project.
- Meanwhile, these countermeasures are considered in "SIP/Cyber-Security for Critical Infrastructure", cooperative efforts will be required in the future.

03

**The Government,
etc.**

- The government, etc. need to take countermeasures against threats such as "Sending a large number of garbage data to vehicle information system" to ITSs cooperating with vehicles.
- Countermeasures to these threats in cooperated with the automated driving system are currently not developed, and it is necessary to consider security measures for the future spread.

04

**Device
manufacturers**

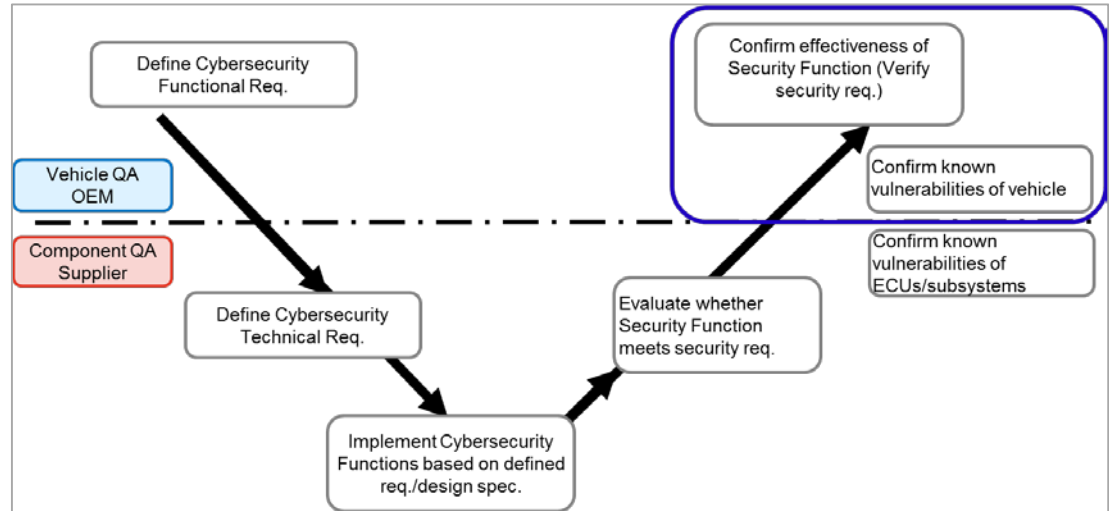
- Wearable device and smart device manufacturers need to take countermeasures against threats such as "Sending a large number of garbage data to vehicle information system" to V2P-devices it providing.
- Countermeasures to these threats in cooperated with the automated driving system are currently not developed, and it is necessary to consider security measures for the future spread.

Overview and scope of Evaluation Guideline

Scope

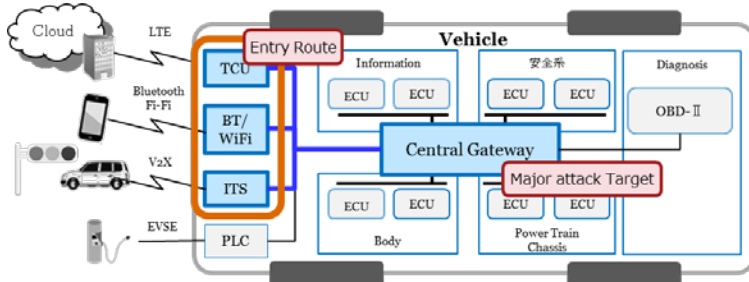
- Developed directing towards contributing to comprehensive evaluation in V model of the vehicle development process based on the results of discussion with stakeholders such as OEMs, JasPar etc.

Scope of the guideline

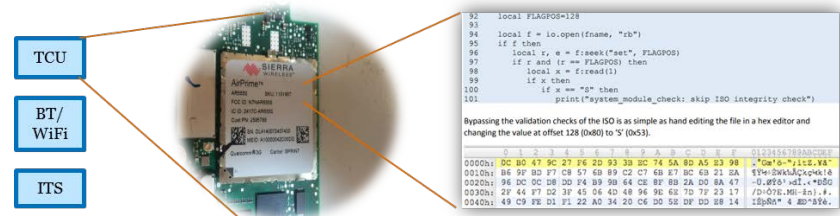


Characteristics of evaluation method

- Evaluation by intrusion test from vehicle's external I/F from actual hacker(attacker)'s viewpoint

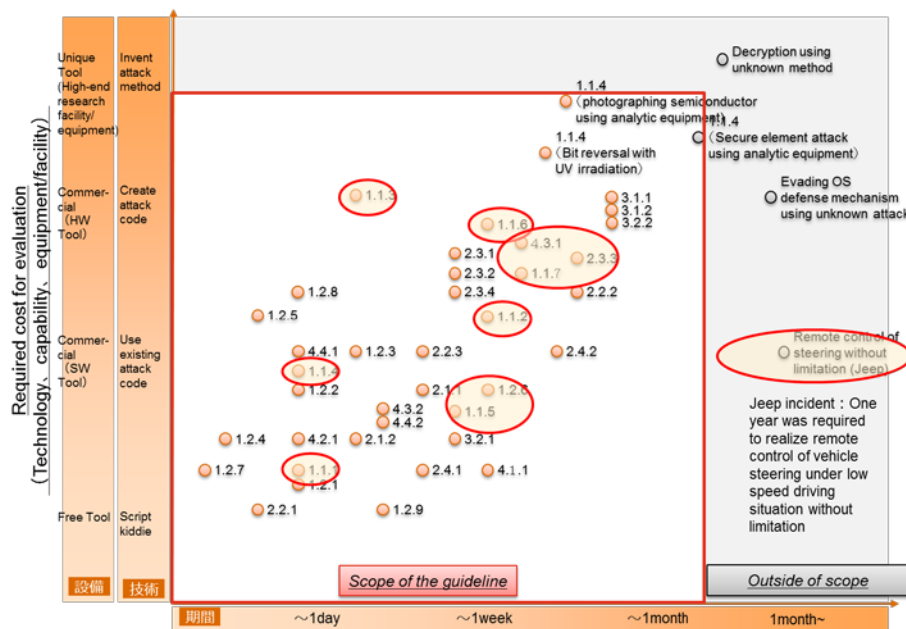
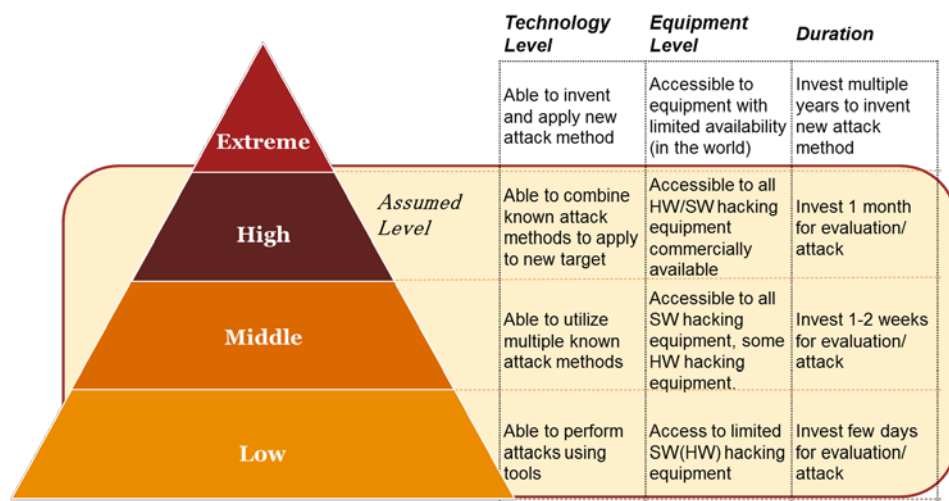


- Evaluate HW security functions taking into consideration actual attacks to vehicles



Evaluation Guideline - Evaluation Items

Through analyzing attacker profile, evaluation items cover cases when attackers have highly advanced technical capabilities, equipment and/or facilities to prevent actual vehicle security incidents.



Evaluation level assumed in the guideline
 Evaluation level is set taking into consideration technical capabilities and equipment/facility of actual attackers.

Evaluation level and items matrix
 Include advanced attack (evaluation) such as HW evaluation.
 Possibility of outsourcing by items basis is also considered.

Evaluation Guideline – Evaluation Scope

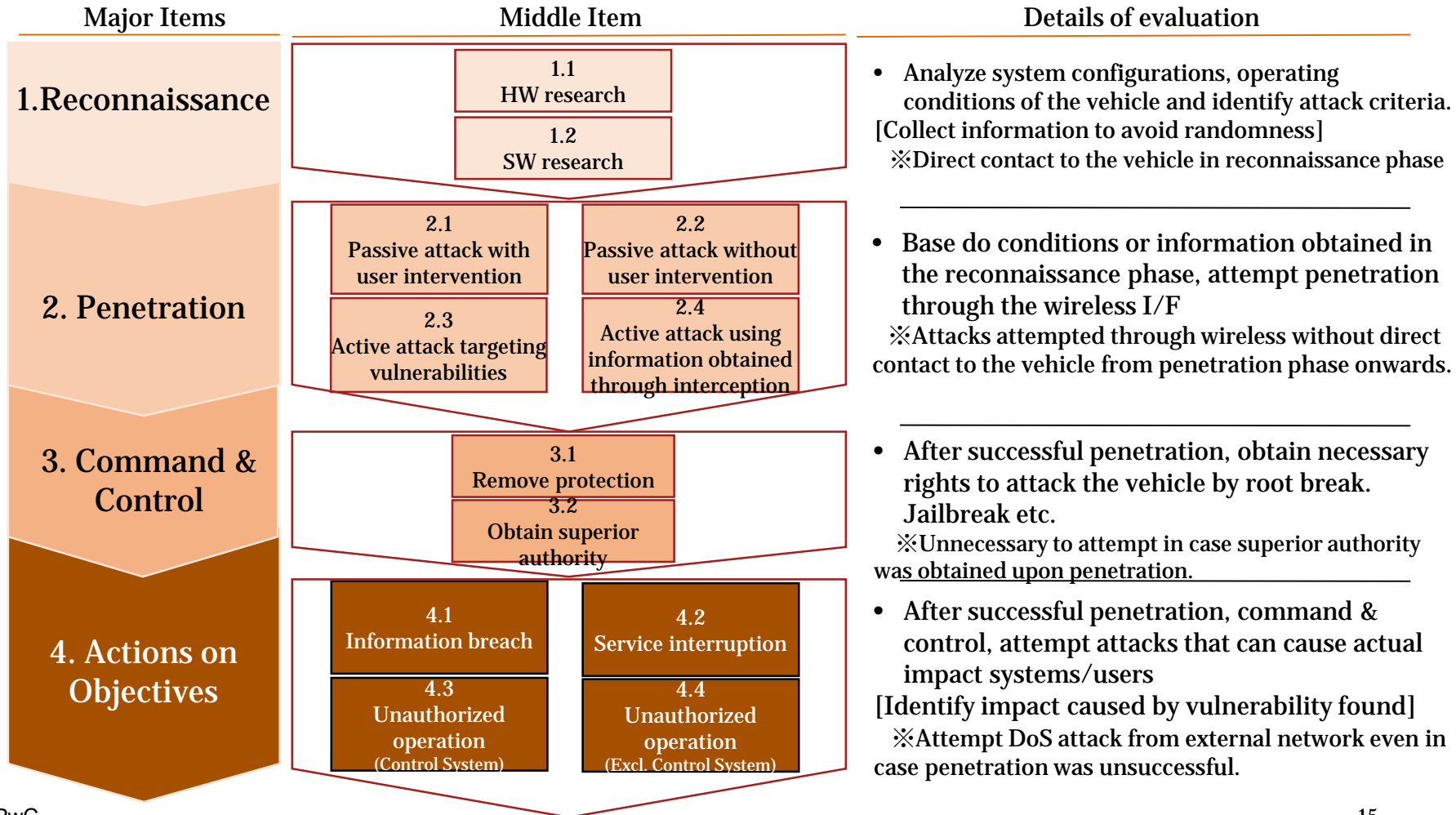
This guideline profiles following examples of vehicle incidents/vulnerabilities and method to reproduce each attack performed are documented in the guideline. This will prevent occurrence of vehicle security incidents similar to the following.

Incident	Incident overview
Jeep: Cherokee uConnect Vulnerability	Vulnerability which may allow third party to remotely locate or control the vehicle. Intrusion to vehicle system via open port in cellular network to tamper CAN controller firmware to remotely control the vehicle.
BMW: ConnectedDrive Vulnerability	Vulnerability which may allow third party to remotely control the vehicle. Unlocking the door by sending command to the vehicle from telematics server operated by security researcher.
Tesla: ModelS Wireless LAN Vulnerability	Vulnerability which may allow third party to remotely control the vehicle. Researcher presented method to mislead the target to attacking site. Attack through cellular network was also possible using decoy mail to mislead user to attacking site.
Mitsubishi: Outlander Mobile app. Vulnerability	Vulnerability which may allow third party to remotely control vehicle air-conditioning etc. Remotely control security alarm setting or air conditioning by accessing Wi-Fi spot within the vehicle.
Nissan: Nissan Connect EV Vulnerability	Possible breach of confidential information such as user ID, password by misusing setting for product development purpose not meant to be used by the general users unintendedly remained.
Nissan: Leaf Vulnerability	Defect in authentication method (no authentication between smartphone and server API) enables vehicle control by finding out lower 5 digits of the VIN number. *Vulnerability of smartphone app. but confirm if the same could occur between vehicle vs serve or vehicle vs smartphone.
SUBARU: StarLink Vulnerability	No validity for security token used for smartphone device authentication allowing third party to unlock the door in case the token was obtained. *Vulnerability of smartphone app. but confirm if same could occur between vehicle Vs serve or vehicle vs smartphone.
Continental AG: TCU Vulnerability	Vulnerability which may allow third part y to remotely control TCU.
Mazda: Mazda Connect Vulnerability	Vulnerability which may allow executing any codes from USB port in the vehicle. Used for AVN customization. * Although a local attack, selected as evaluation point for anti-reverse engineering performance.
Honda: Honda Connect Vulnerability	Vulnerability which may allow executing any codes from USB port in the vehicle. Used for AVN customization. * Although a local attack, selected as evaluation point for anti-reverse engineering performance.

Information Security Evaluation Guideline

List of items(Major, medium)

Systemize evaluation methods, items based on actual attack process of hackers



International Standardization Process

Cooperate with P-members of Technical Committee/Sectional Committee to ensure to reflect vehicle information security technologies promoted by Japan to WD/CD/DIS

WD created by WG by the experts assigned by the secretary

Obtain approval based on defined criteria. If the criteria can be fulfilled, register as FDIS

*Approval by voting



Creation/revision of standard proposed from secretary of member countries, Technical Committee(TC), Sectional Committee(SC) etc.

Secretary to promote discussion on CD based on opinions from P-members and revise if necessary
✕In case technical issues cannot be solved, committee can issue as TS

Approved as international standard (In case disapproved, either submit revised proposal, issue as TS or discard)

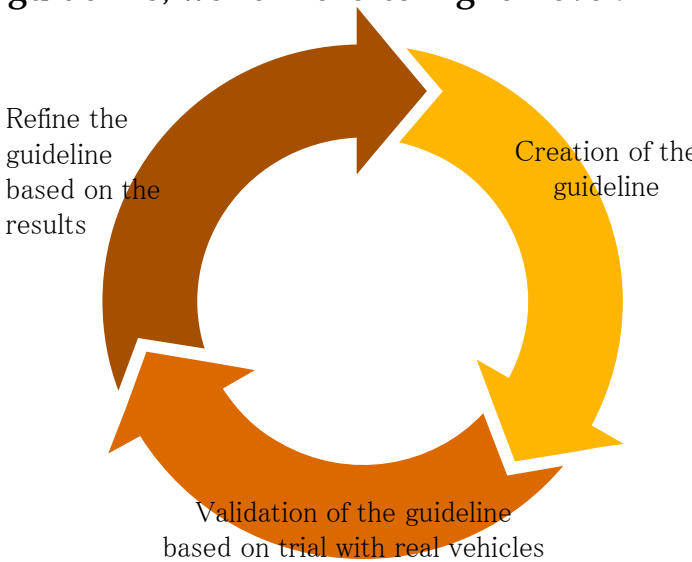


Within 36 months

JISC, ISO standardization process

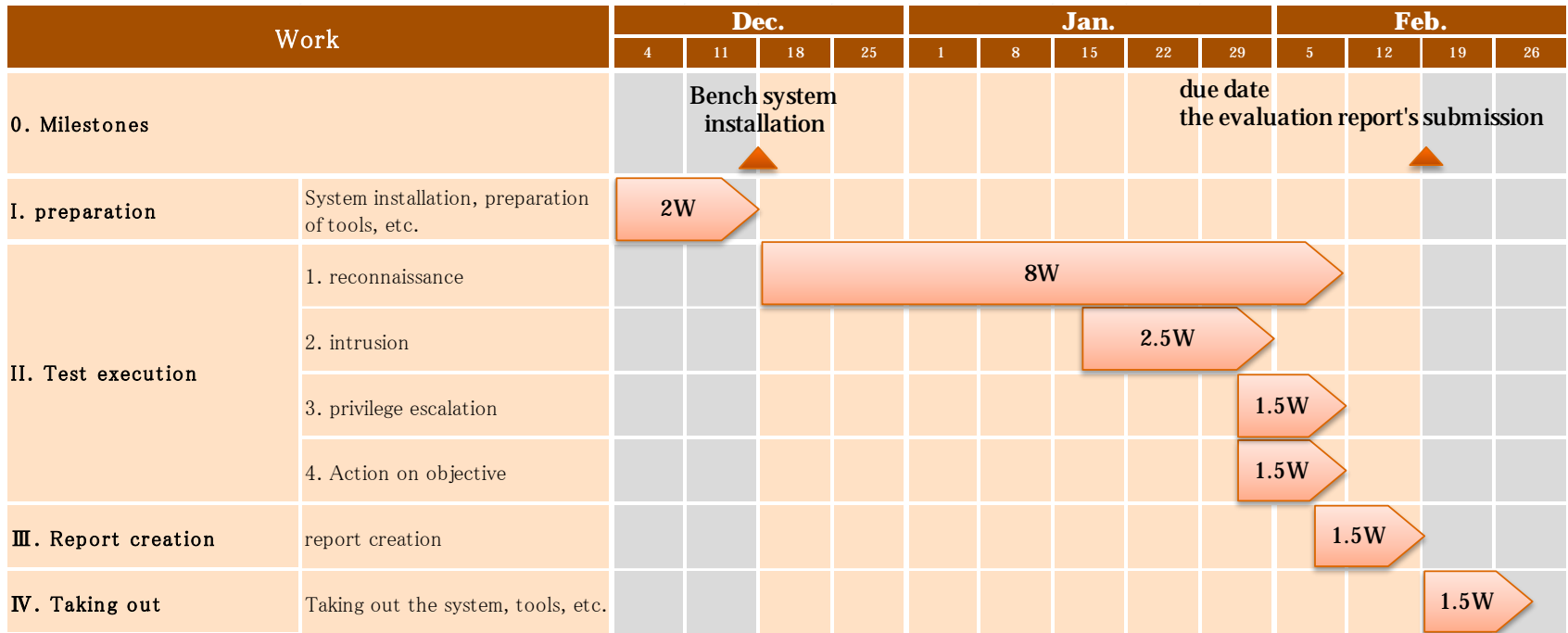
Objective of the trial

The trial’s objective is to evaluate the validation of the guideline, and give suggestion for improvement to vehicle providers.

Validation of the guideline	Feedback to vehicle providers
<p>Comply with the items of the evaluation guideline, evaluate the validation of the contents by executing the trial to the real vehicles. At the same time, by reflecting the evaluation results in the guideline, we refine it to higher level.</p> 	<p>From the hackers perspective, investigate vulnerabilities that could come out factors of security threats related to the test machine. If we detect items which need improvement, we will give OEMs with advice for improvement</p> <p style="text-align: center;"><u>OEMs’ Merits</u></p> <ol style="list-style-type: none"> 1. HW/SW hacking trials delivered by sophisticated white hackers, clarify possible damage 2. Provide procedures that hackers actually attack to target vehicles in detail, and make it possible for OEM engineers to reproduce the procedures 3. Provide better measures from the both development costs and security quality based on the actual damage

Schedule of the trail

From the installation of the bench system to submit the evaluation reports, the evaluation period was almost eight weeks including the year-end/new-year's holiday. In the reconnaissance phase, seven weeks were spent to obtain the firmware. Meanwhile, due to time constraints, work related to privilege escalation and action on objective was carried out partly.



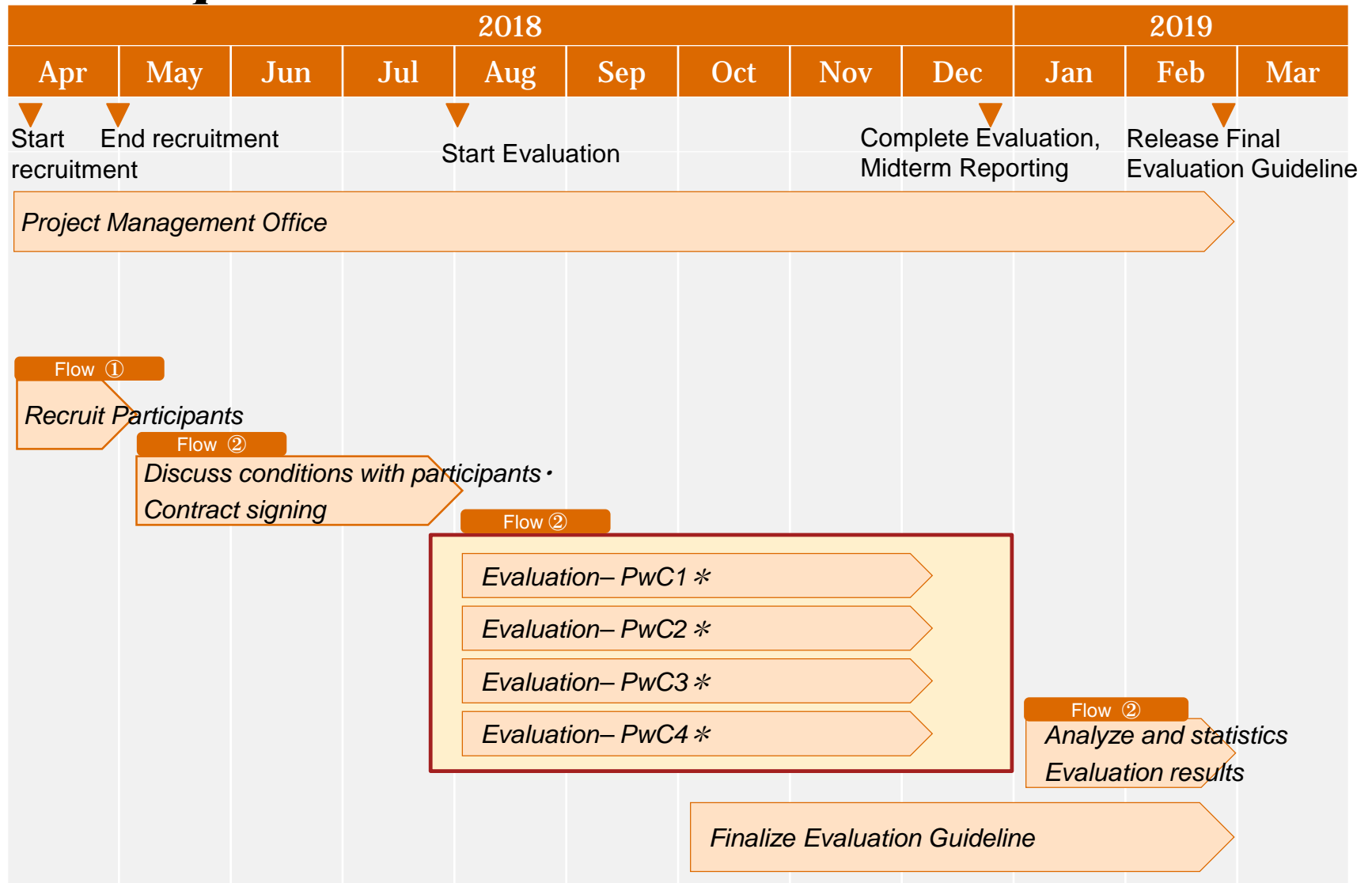
The format of the trial's report

The results of this trial reported with the following format.

Item of the guideline	Fill in section number of items described in the evaluation guideline
Result of the evaluation	Fill in the contents of the result of the evaluation
Risk	Fill in the degree of risk of items according to the criteria on the right
Contents of the evaluation	Fill in contents to be confirmed by the evaluation
Procedures of the evaluation	Fill in procedures of the evaluation in detail
Possible risks	If problems discovered, fill in possible risks and damage
Condition of attack successful	If problems discovered, fill in the condition of the attack successful
Improvements	If problems discovered, fill in improvements to protect the attack

Risk	Criteria's definition
High	If the discovered vulnerability is not modified on the target system, highly urgent security violation could occur without advanced technology or high cost, and it is possible to give critical effect on business operation(such as recall, business suspension, etc.). Immediate implementation of countermeasures for vulnerabilities should be undertaken.
Medium	If the discovered vulnerability is not modified on the target system, urgent security violation could occur without a certain level of technology or cost, and it is possible to give huge effect on business operation(significant reduction of business performance, etc.). It is recommended to implement countermeasures for vulnerabilities as necessary.
Low	There is no immediate security impact on matters found in the target system, however it is expected to improve security at a certain level by implementing countermeasures. It is recommended to implement countermeasures for the vulnerabilities in the future.
Info	It is an item that may have some influence on matters found in the target system. It is recommended to consider pros and cons of countermeasures.

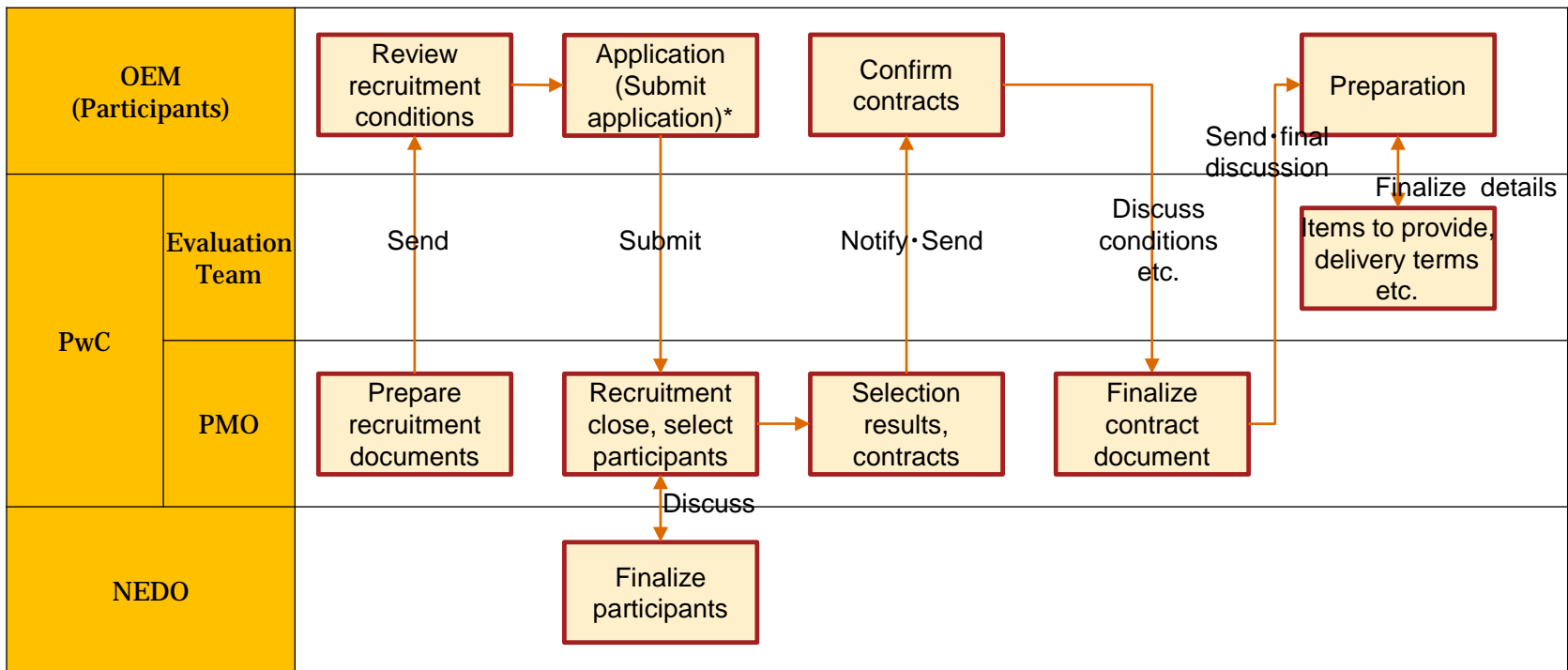
Field Operational Test Schedule Overview



PwC * Two months evaluation period for each participants. Period will be agreed in prior to the start of evaluation.

Implementation Flow①: Participants Recruitment

Implementation flow of participants recruitment and prior arrangements are planned as shown below.

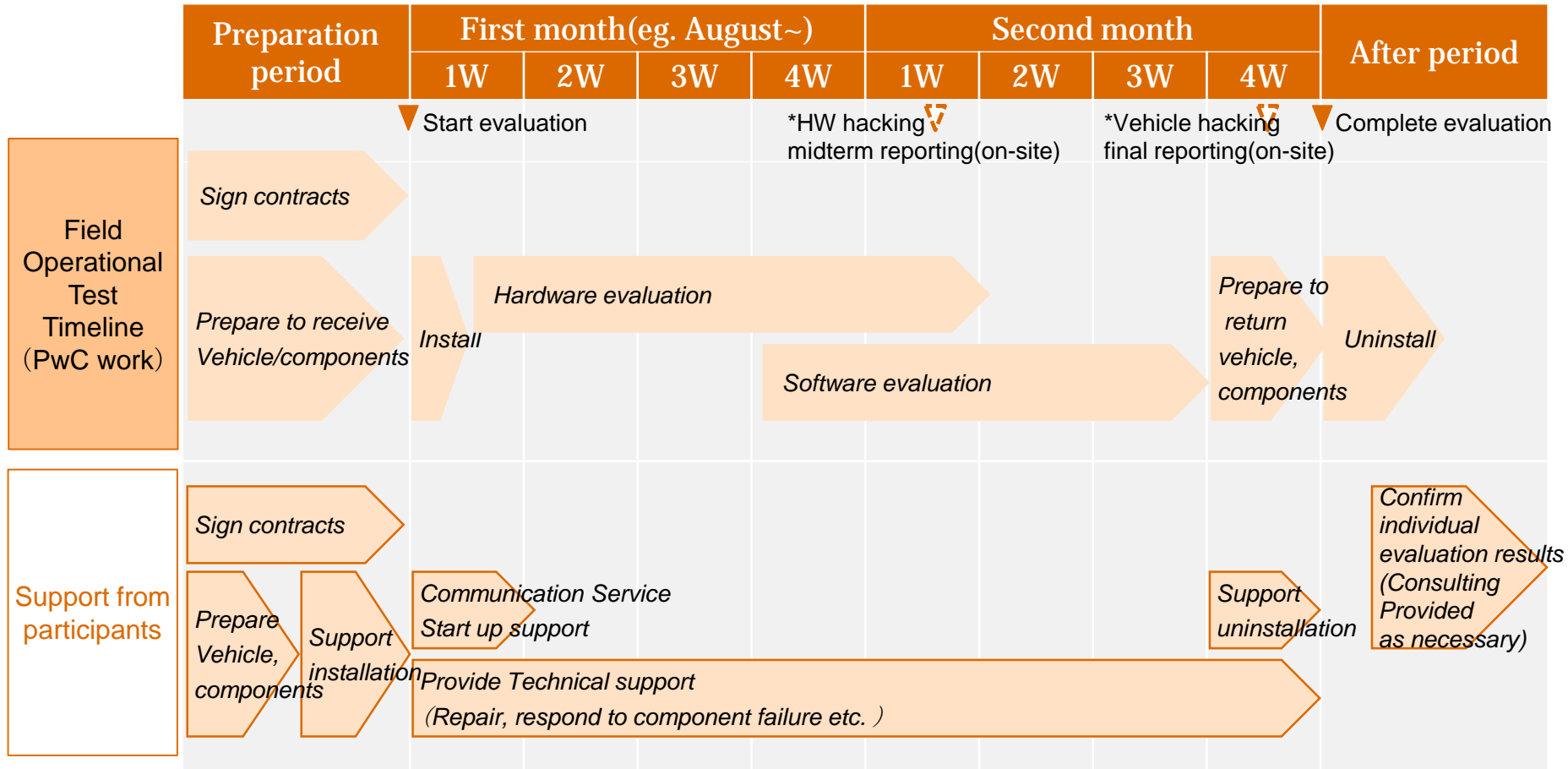


* Briefing session will be held in case requested from candidate OEM.

d Preparation for Management of Field Operational Test

Required support from the participants and timeline

After signing contracts related to the Field Operational Test (18/8~) participants are required to provide necessary support following the project timeline.



*Midterm/final reporting (on-site) is not included in the plan but they can be scheduled in case requested by the participants. Location and details will be arranged in prior to the visit.

d Preparation for Management of Field Operational Test

Items to be provided by the participants(1/2)

We require participants to provide following items during the period of Field Operational Test (planned duration, 4 months)

No.	Item	Qty	Conditions, details	Required
1	Vehicle* (Commercial vehicle, test vehicle are also acceptable)	1	<ul style="list-style-type: none"> • Able to connect to telematics services (including test environment) <p>【Note】 Vehicle will be used for testing highly critical evaluation results.</p>	<input type="radio"/>
2	Information System ECU	3 sets	<ul style="list-style-type: none"> • Able to connect to telematics services (including test environment) • Includes communication component such as TCU, AVN etc. • Include communication component with functions for cellular network, Wi-Fi, BT etc. 	<input type="radio"/>
3	GatewayECU		<ul style="list-style-type: none"> • Directly connecting to information system ECU 	<input type="radio"/>
4	Antenna		1 sets	<ul style="list-style-type: none"> • GPS, cellular network etc.
5	Interfaces inside the vehicle	<ul style="list-style-type: none"> • Interface general users can use inside the vehicle (Display, mike, USB port, touch pad etc. 		<input type="radio"/>
6	Information system wire harness	<ul style="list-style-type: none"> • Connecters attached to each end (unprocessed condition acceptable) 		<input type="radio"/>
7	Connector PIN diagram for each ECU	1 set	<ul style="list-style-type: none"> • Able to identify which PIN connects to power as well as voltage. 	<input type="radio"/>
8	Wiring Diagram	1 set	<ul style="list-style-type: none"> • Include information system ECUs and GateWayECUs 	<input type="radio"/>

* Vehicle bench (system connecting necessary components) can be provided instead of vehicle as long as it operates wireless communication functions such as Wi-Fi, BT, telematics etc. same as vehicles.

d Preparation for Management of Field Operational Test

Items to be provided by the participants(1/2)

We require participants to provide following items during the period of Field Operational Test (planned duration, 4 months)

No.	Item	Qty	Conditions/Details	Required
9	Telematics Service Accounts	4 (for all vehicle + component sets)	<ul style="list-style-type: none">• Able to use all telematics services accessible by general users (including test environment)	<input type="radio"/>
10	Telematics Service Server	—	<ul style="list-style-type: none">• Operate server during the field operation test period which can be connected from the vehicle or communication component using above accounts <p>【Note】</p> <ul style="list-style-type: none">• Both production/test environment are acceptable however below will be performed against the server:<ol style="list-style-type: none">1.Use of services provided to general users2.Research server information that can be obtained from outside (host name, certificate, port number etc.)• Anything that may effect telematics service operation will not be performed	<input type="radio"/>
11	Manuals	1 (each)	<ul style="list-style-type: none">• All manuals obtainable by general users such as vehicle manual, service manual etc.	

d *Preparation for Management of Field Operational Test*

Support required from the participants

No.	Timing	Item	Period	Details
1	Before starting Evaluation (Assuming by end of July)	Sign contracts* • Contract regarding FOT (lease contract) - Includes acceptance for vehicle/component hacking** • NDA • Communication service agreement etc.	-	• Internal arrangements and preparations etc. towards contract signing.
2		Arrangement for conditions for items to be provided	-	• Discuss items to provide, deliver and other conditions necessary
3		Prepare vehicle/components	-	• Prepare vehicle/components of conditions for the test as well as preparation for its delivery.
4	Upon starting Evaluation	Support for installing vehicle/components	-	• Provide necessary information for transportation, installation of the vehicle/components
5		Support for initial connection of communication service	1 week	• Support for connecting to communication service etc.
6	During Evaluation	Provide technical support	Approx. 2 months	• Support for repairing initial failure or failure unrelated to the test
7	After Evaluation	Support for returning vehicles/components	-	• Provide information regarding transportation, uninstallation of the vehicle/components
8		Confirm and provide feedback on Individual Evaluation Report	-	• Confirm individual vehicle evaluation report and provide feedback to PwC (optional)

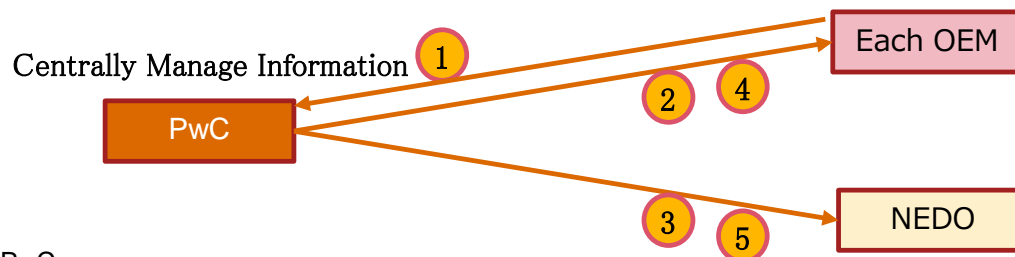
* We wish to discuss types and/or details of the contracts after May including used of document template/format convenient for each participants.

** Acceptance for hacking may also be included in terms and conditions of participation

Confidential information and scope of disclosure

Scope of disclosure for confidential information obtained from the participants and through the field operational test will be restricted as shown below.

Category	Item	Details	Provider /Creator	Scope of disclosure		
				Vehicle Provider	NEDO	Public Disclosure
Subject	1. Vehicle / Components	Vehicles and components subject for evaluation	Each OEM	○ (PwC)	✘	✘
Procedure	2. Individual Evaluation procedure	Summarize and share individual evaluation procedure as necessary	PwC	○	✘	✘
	3. Evaluation Guideline (Final)	Evaluation guideline reflecting the result of field operational test	PwC	○	○	○
Result	4. Vehicle Evaluation Reports (Individual)	Evaluation results summary report including technology and equipment used. (Highly confidential as it may include vulnerability information)	PwC	○	✘	✘
	5. Statistics of Evaluation Results	Results modified to enable disclosure	PwC	○	○	○





© 2018 PwC Consulting LLC., PwC Cyber Services LLC. All rights reserved.

PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.