SIP-adus Workshop 2020

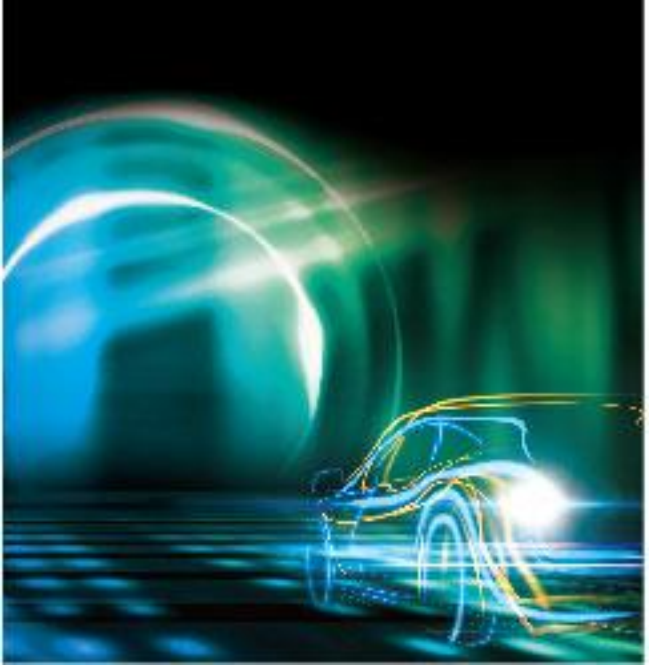
Session3：Toward realization of safe automated driving

Research for Effectiveness and Technology of Intrusion Detection Systems (IDS)

Okuyama, Ken
PwC Consulting LLC

November 10, 2020

INDEX



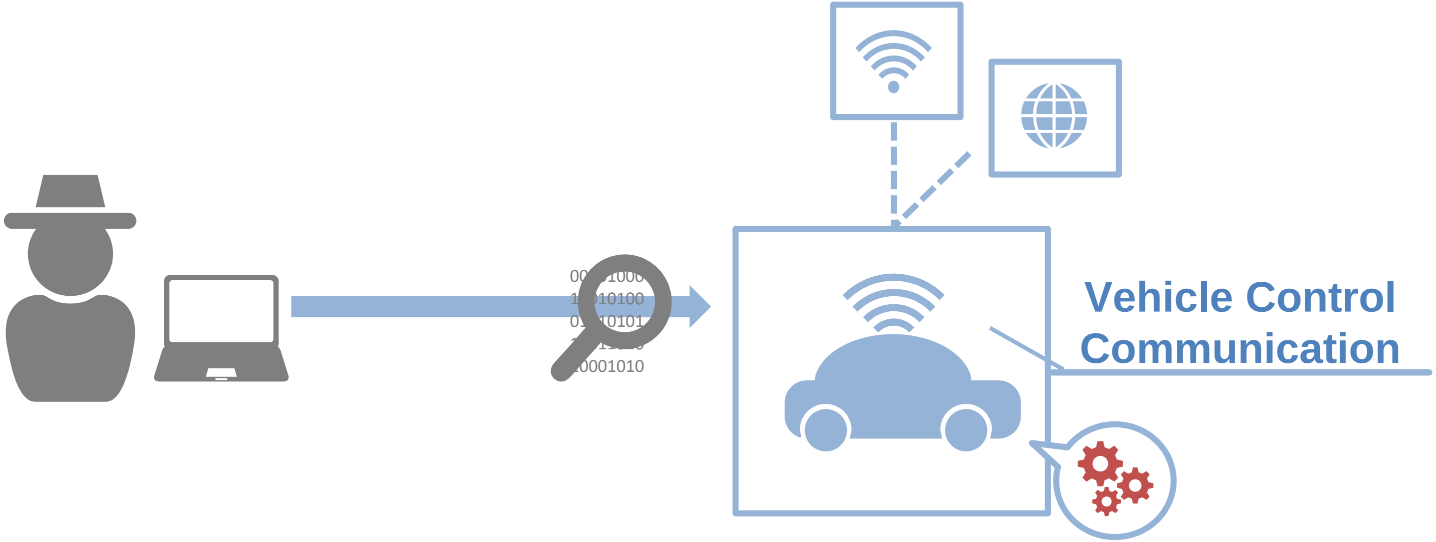
1. Background and Objectives
2. 2019 Research Summary
3. Action Plans for 2020-2021

1

Background and Objectives

Background

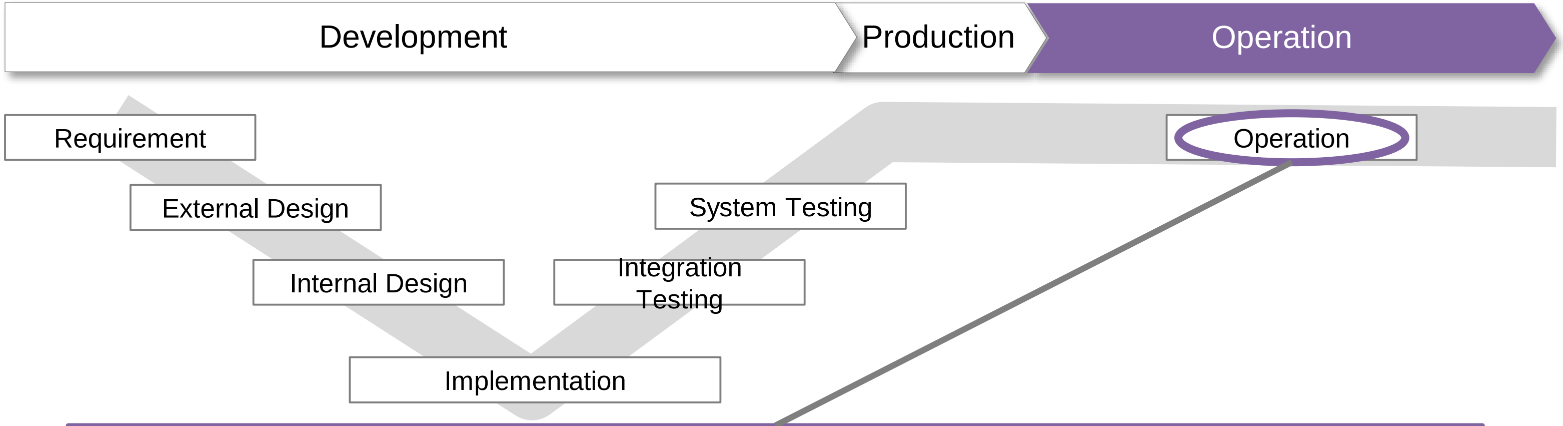
- New cyber attack methods for vehicle cyber security are continuously reported at international conferences
- As cars are connected to the outside world, they are exposed to many security threats. There have been published demonstrations of taking away vehicle control, etc.



Vehicle Control Communication

Intrusion detection systems against cyber-attacks

◆ Detection Technology as a countermeasure against new cyber attacks



- Mechanisms to detect and monitor cyber-attacks during vehicle operations
- Intrusion detection systems (IDS) against cyber-attacks on vehicles are in the spotlight as a methods for a countermeasure against new cyber-attack

We have selected the research on new cyber-attack trends and intrusion detection systems (IDS) as a countermeasure for the attacks.

SIP

2

2019 Research Summary

Activity Summary

Purpose

In response to changes in the environment surrounding vehicle cyber security, an investigation into new cyber attack techniques and the corresponding countermeasures will be performed

Information Collection

Conduct a survey of the following three areas

Investigate trends in attacks on vehicles	Perform surveys regarding trends in cyber security measures such as IDS	Study of IDS evaluation methods Verification based on the results of the basic evaluation
✓ Using vehicle attack data (FY2017-2019) create scenarios and perform risk assessment ✓ Analyze attack trends and prioritize (also used for IDS evaluation)	✓ Organize security technologies and products, primarily IDS for vehicles ✓ Based on a separate product survey, organize technical product classifications to assist in evaluating IDS devices	✓ Organize evaluation methods based on IT industry standards and the latest in-vehicle Cyber Security regulations ✓ Investigate IDS evaluation methods based on actual IDS products and verify evaluation methods

Attack Trends in Vehicles – Overview of Investigation

1. Collect information on attack methods from vehicle security cases

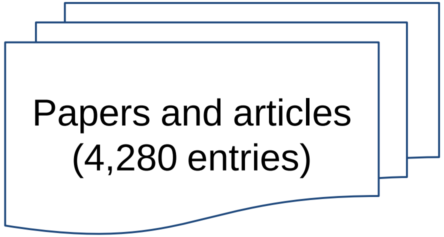
2. Analyze new attack methods

3. Conduct risk assessment for derived attack methods

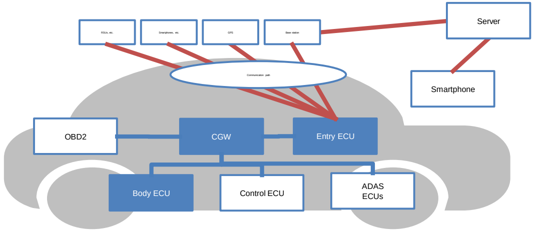
[Attack Case Investigation]
<u>Identify vehicle cyber-attack cases to determine targets for further analysis</u>

[Attack Scenarios]
<u>Organize into common scenario structure to enable comparison between the cases</u>

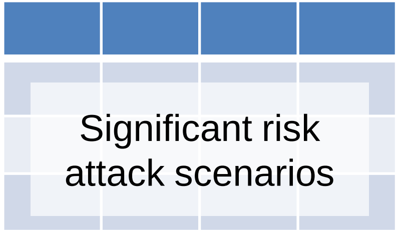
[Risk Analysis]
<u>Evaluate and compare attack scenarios derived from the case studies</u>



Papers and articles
(4,280 entries)



Target attack scenarios
(105 entries)



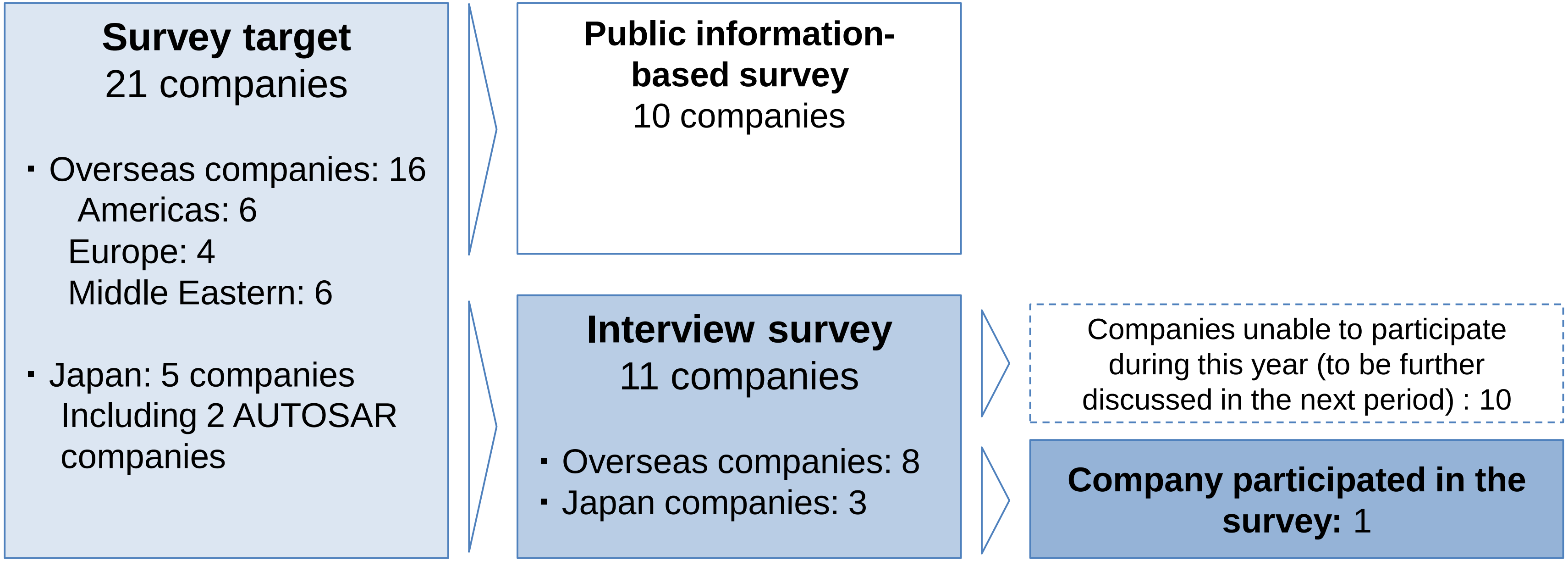
Significant risk attack scenarios

Risk assessment results for the attack Scenarios

IDS Trends Survey

◆ Survey of IDS vendors through interviews

Security Vendor/Supplier (written/interviewed)



Survey target
21 companies

- Overseas companies: 16
  - Americas: 6
  - Europe: 4
  - Middle Eastern: 6
- Japan: 5 companies
  Including 2 AUTOSAR companies

Public information-based survey
10 companies

Interview survey
11 companies

- Overseas companies: 8
- Japan companies: 3

Companies unable to participate during this year (to be further discussed in the next period) : 10

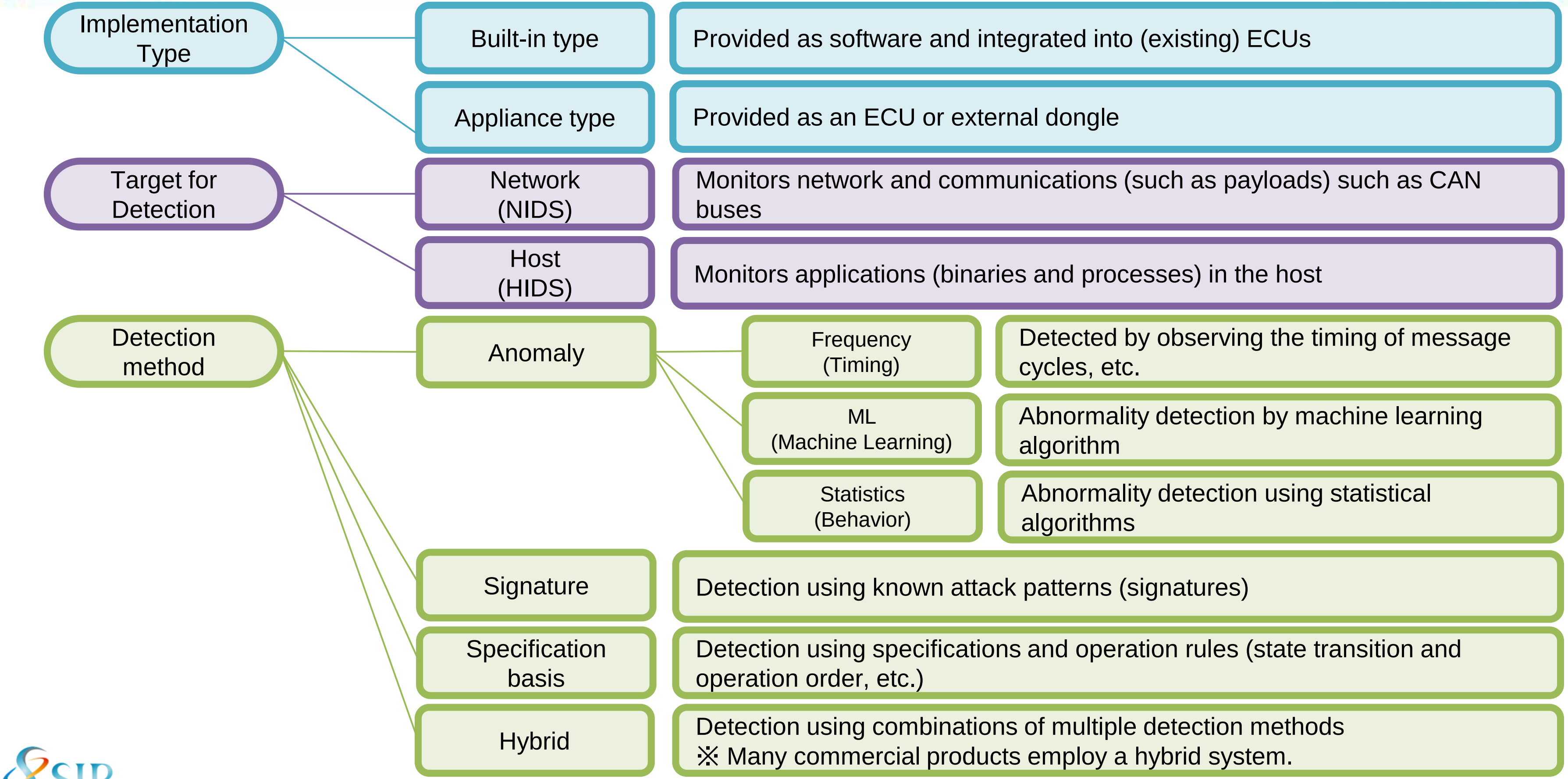
Company participated in the survey: 1

Survey target (strategy Long list)

Survey target (adjustment)

Participation in basic evaluation using actual equipment (ID provided)

Defense Technology Research

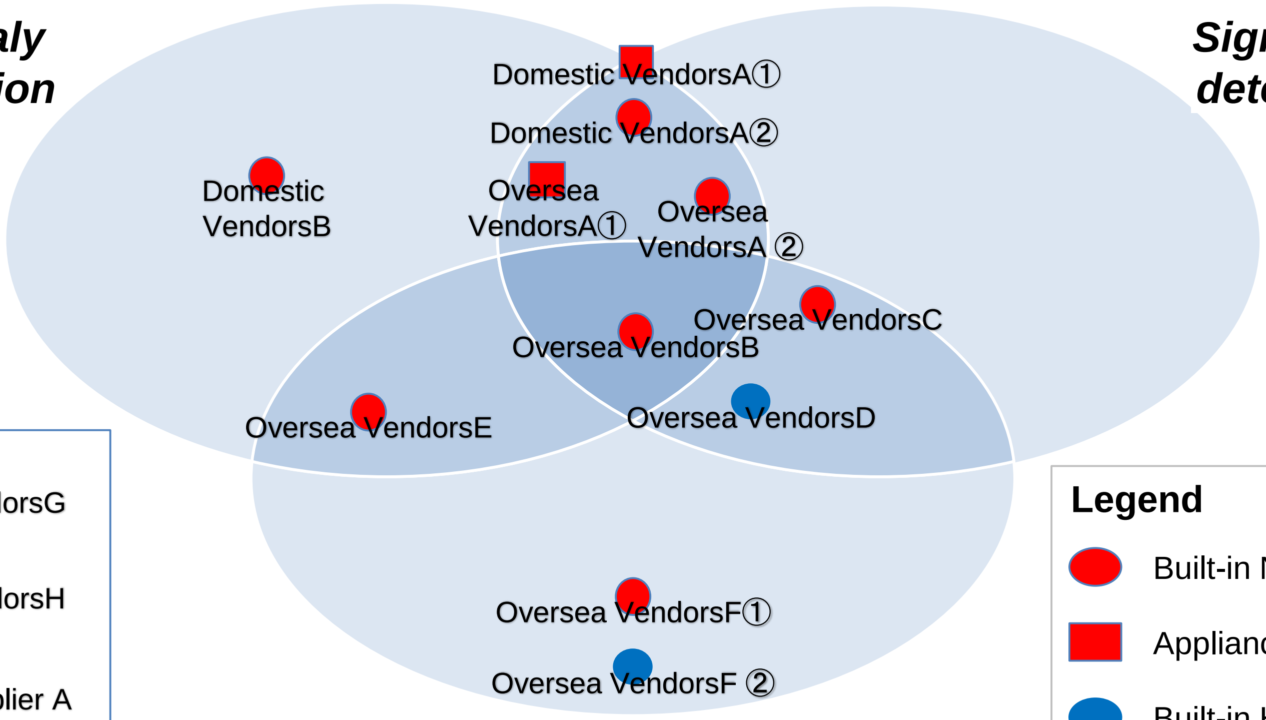


Implementation Type	Built-in type		Provided as software and integrated into (existing) ECUs
	Appliance type		Provided as an ECU or external dongle
Target for Detection	Network (NIDS)		Monitors network and communications (such as payloads) such as CAN buses
	Host (HIDS)		Monitors applications (binaries and processes) in the host
Detection method	Anomaly	Frequency (Timing)	Detected by observing the timing of message cycles, etc.
		ML (Machine Learning)	Abnormality detection by machine learning algorithm
		Statistics (Behavior)	Abnormality detection using statistical algorithms
	Signature		Detection using known attack patterns (signatures)
	Specification basis		Detection using specifications and operation rules (state transition and operation order, etc.)
	Hybrid		Detection using combinations of multiple detection methods ※ Many commercial products employ a hybrid system.

Results of Research on Defense Technology

Anomaly detection

Signature detection



🟥 Domestic VendorsA①

🔴 Domestic VendorsA②

🔴 Domestic VendorsB

🟥 Oversea VendorsA①

🔴 Oversea VendorsA ②

🔴 Oversea VendorsC

🔴 Oversea VendorsB

🔴 Oversea VendorsE

🔵 Oversea VendorsD

🔴 Oversea VendorsF①

🔵 Oversea VendorsF ②

Specification-based detection

🔴 Oversea VendorsG

🔴 Oversea VendorsH

🔴 Domestic supplier A

Detection method not disclosed

Legend

🔴 Built-in NIDS

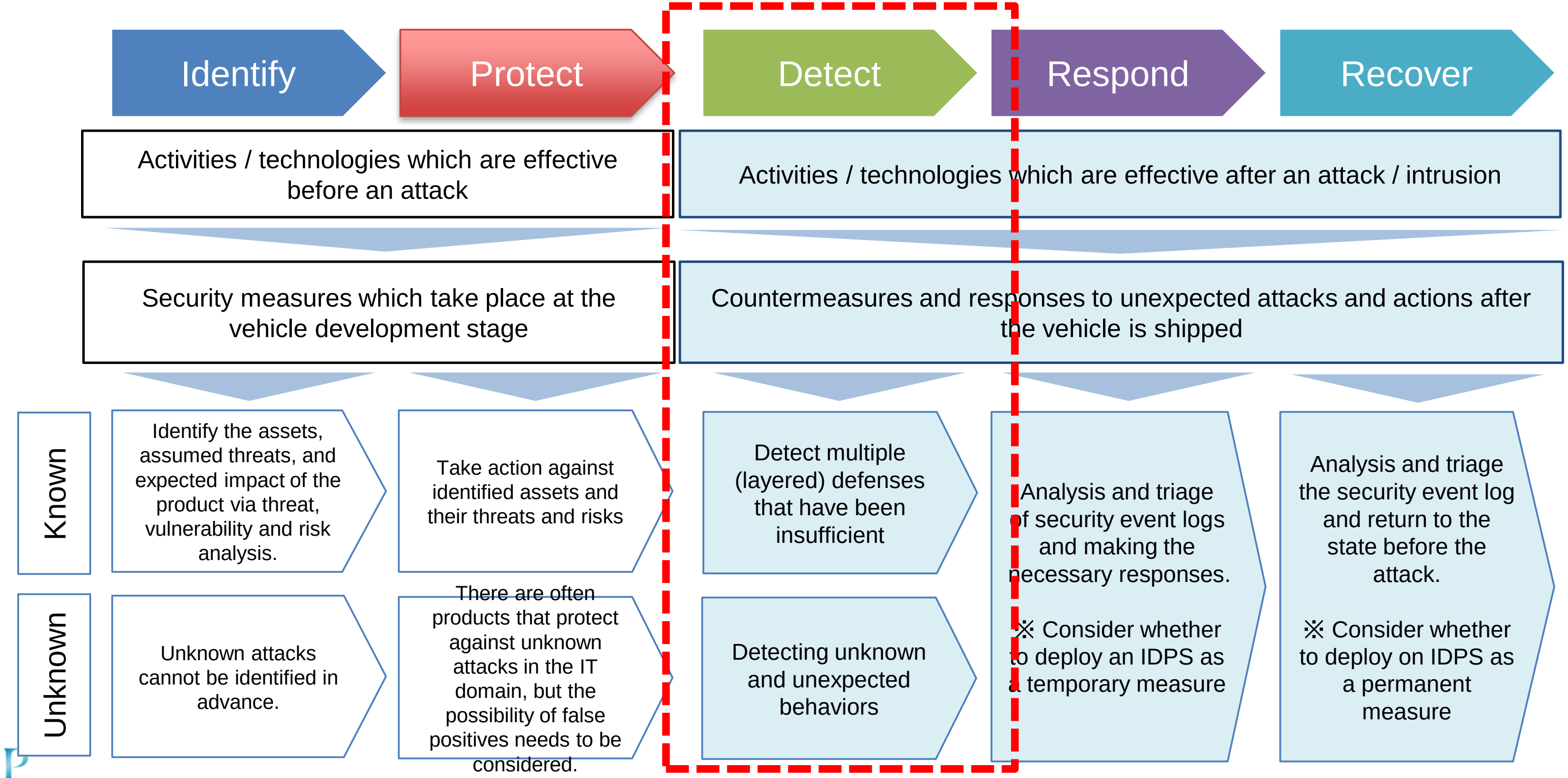
🟥 Appliance NIDS

🔵 Built-in HIDS

🟦 Appliance HIDS

IDS Evaluation Methodology and Verification Survey

- We’ve surveyed how to evaluate IDS in terms of known and unknown attacks.



	Identify	Protect	Detect	Respond	Recover
	Activities / technologies which are effective before an attack		Activities / technologies which are effective after an attack / intrusion		
	Security measures which take place at the vehicle development stage		Countermeasures and responses to unexpected attacks and actions after the vehicle is shipped		
Known	Identify the assets, assumed threats, and expected impact of the product via threat, vulnerability and risk analysis.	Take action against identified assets and their threats and risks	Detect multiple (layered) defenses that have been insufficient	Analysis and triage of security event logs and making the necessary responses. ※ Consider whether to deploy an IDPS as a temporary measure	Analysis and triage the security event log and return to the state before the attack. ※ Consider whether to deploy on IDPS as a permanent measure
Unknown	Unknown attacks cannot be identified in advance.	There are often products that protect against unknown attacks in the IT domain, but the possibility of false positives needs to be considered.	Detecting unknown and unexpected behaviors		

Evaluation Form of Actual Machines (Equipment Used)

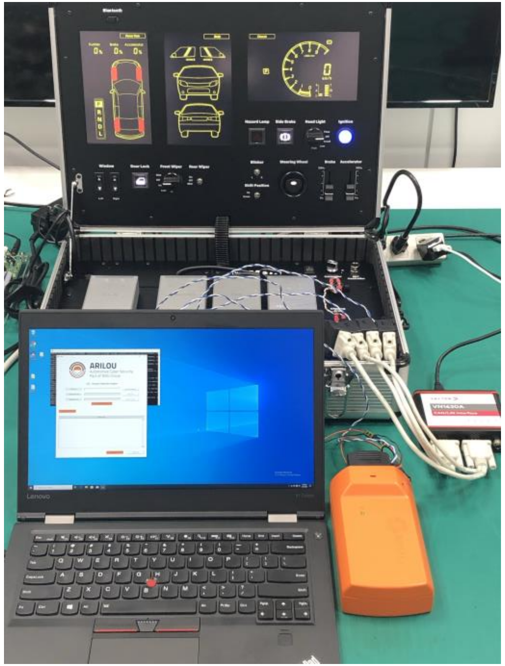


Fig1. IDSs provided by Arilou are connected to PASTA and running.
addition to IDS (Fig3), both companies also provided monitoring environments.

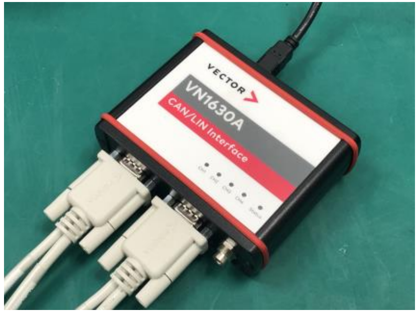


Fig2. Vector VN1630A + CANPiggy × 2
The above is controlled by CANoe.

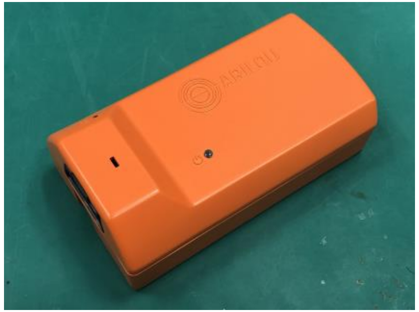


Fig3. IDS provided by Arilou

Evaluation results (on test-bed)

◆ Method

- False positives and negatives are checked by inputting attack messages (or stopping the relay) using the results of the attack trend survey and cross-checking them with the detection log of the IDS side.

ID	Item	Test result (corresponding detection log)	Attack counts entered from CANoe	Number of messages detected by IDS	Correct answer rate for the number of attacks
4-1	Steady-state measurement	OK	0	0	0% (no false positive)
4-2	Message injection (random message)	OK	1000	1000	100%
	Message injection (ID zero)	OK	1000	1000	100%
	Message injection (bit flip)	OK	1000	1000	100%
	Message injection (ECU reset/software reset by UDS)	OK	2	2	100%
	Message injection (ECU reset/key off on reset by UDS)	OK	2	2	100%
	Message injection (ECU reset/hardware reset by UDS)	OK	2	2	100%
	Message replacement by the middle man	OK	1000	1000	100%
	Message replacement by the middle (Bit Flip)	OK	1000	1000	100%
	Interim message relay stop	OK	400	389	97%
4-3	Installing a man-in-the-middle ECU	N/A	N/A	N/A	N/A
4-4	Message Injection (vulnerability attack)	OK	1	1	100%
	Man-in-the-middle message-based vulnerability attack (broadcast)	OK	1	1	100%
4-5	Message injection (error frame)	OK	1000	0	100%

◆ Results and Discussion

- Able to detect attack messages, except for message stopping by MITM attack
- Detection of message cycle may be a false positive
- There is a configurable threshold that can be changed to avoid
- etc.

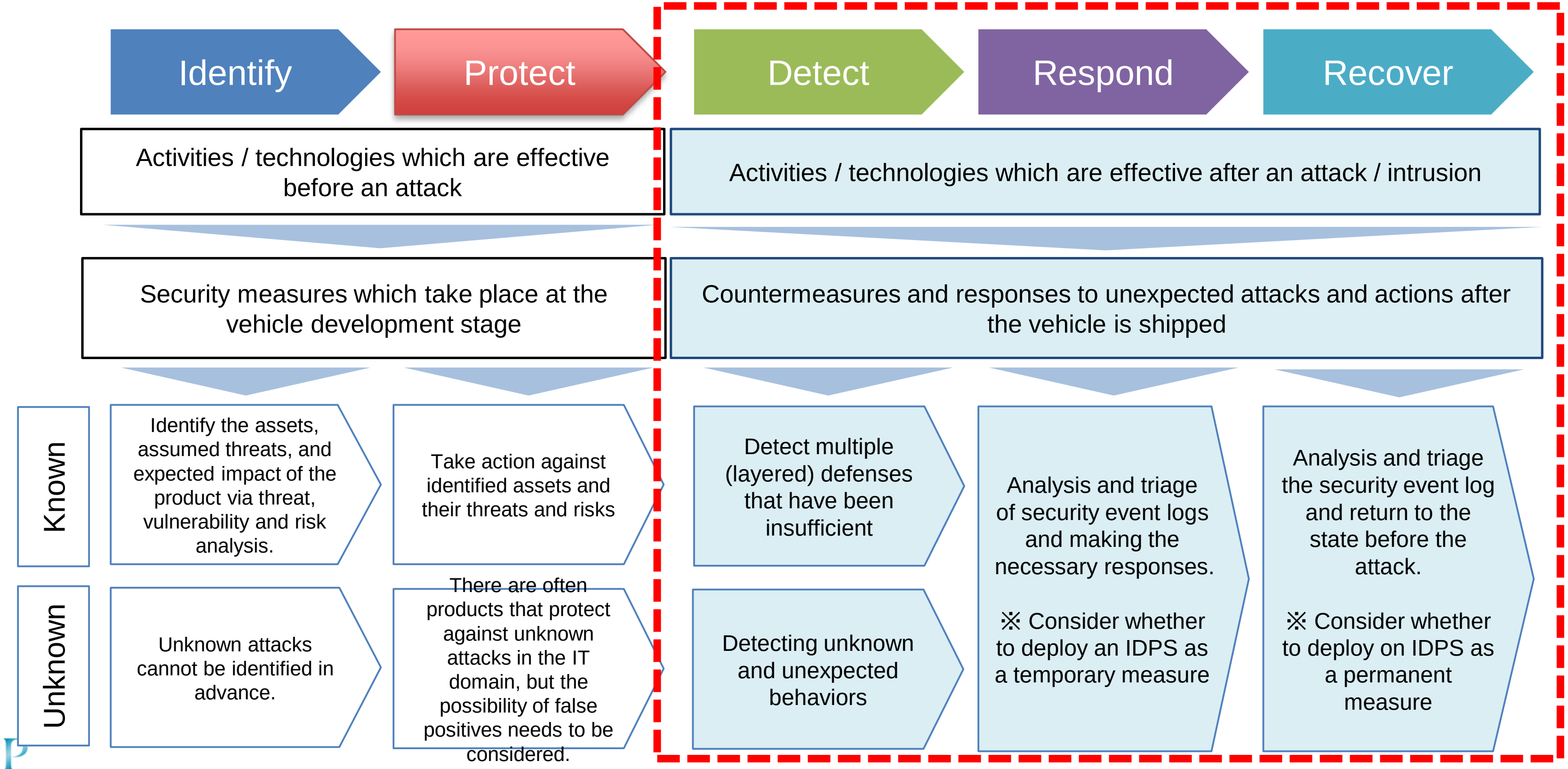
- Flexibility in how security events are detected
- On the other hand, decisions based on the manufacturer's security policy to detect or not detect, and items specific to the vehicle model are also needed

3

Action Plans for 2020-2021

Research on response and recovery using IDS

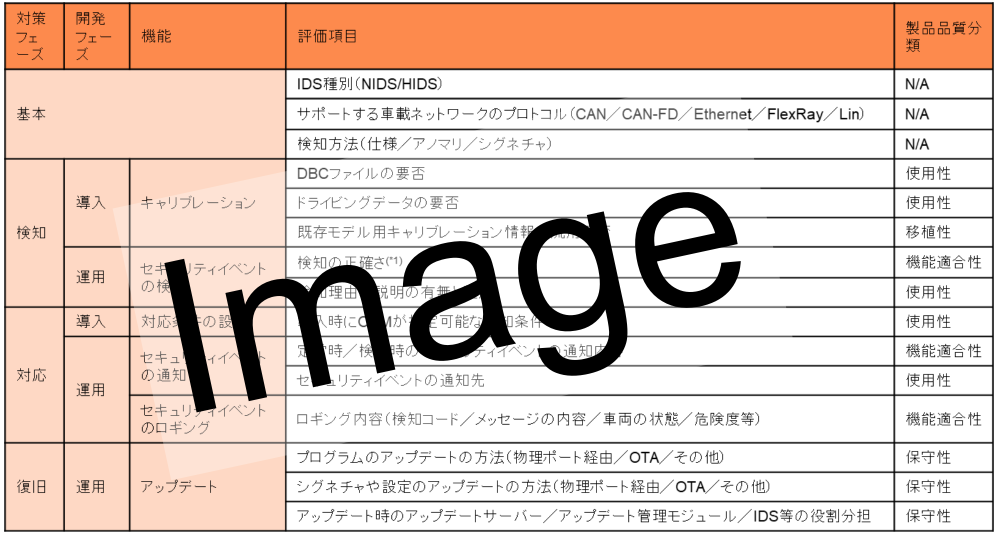
- Expanding the scope to include response and recovery



	Identify	Protect	Detect	Respond	Recover
	Activities / technologies which are effective before an attack		Activities / technologies which are effective after an attack / intrusion		
	Security measures which take place at the vehicle development stage		Countermeasures and responses to unexpected attacks and actions after the vehicle is shipped		
Known	Identify the assets, assumed threats, and expected impact of the product via threat, vulnerability and risk analysis.	Take action against identified assets and their threats and risks	Detect multiple (layered) defenses that have been insufficient	Analysis and triage of security event logs and making the necessary responses. ※ Consider whether to deploy an IDPS as a temporary measure	Analysis and triage the security event log and return to the state before the attack. ※ Consider whether to deploy on IDPS as a permanent measure
Unknown	Unknown attacks cannot be identified in advance.	There are often products that protect against unknown attacks in the IT domain, but the possibility of false positives needs to be considered.	Detecting unknown and unexpected behaviors		

Development and validation of the IDS evaluation guidelines

- We will study evaluation methods for IDS and related systems with the scope of not only detection but also response and recovery, and verify the validity of the methods by verifying them with actual machines.



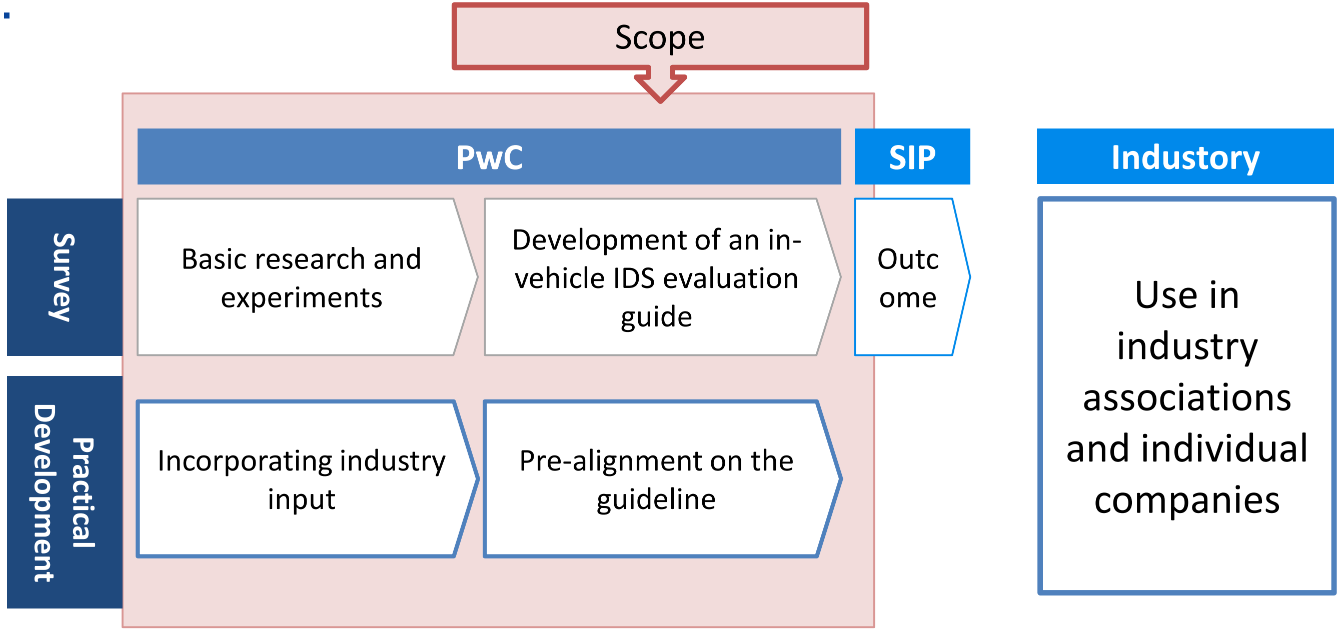
対策フェーズ	開発フェーズ	機能	評価項目	製品品質分類
基本			IDS種別（NIDS/HIDS）	N/A
			サポートする車載ネットワークのプロトコル（CAN／CAN-FD／Ethernet／FlexRay／Lin）	N/A
			検知方法（仕様／アノマリ／シグネチャ）	N/A
検知	導入	キャリブレーション	DBCファイルの要否	使用性
			ドライビングデータの要否	使用性
			既存モデル用キャリブレーション情報[illegible]	移植性
	運用	セキュ[illegible]リティイベント の検[illegible]	検知の正確さ(*1)	機能適合性
			[illegible]知理由[illegible]説明の有無[illegible]	使用性
対応	導入	対応[illegible]件の設[illegible]	[illegible]入時にC[illegible]Mが[illegible]定可能な[illegible]知条件	使用性
	運用	セキュ[illegible]ィイベント の通知	定[illegible]時／検[illegible]時の[illegible]ティイベント[illegible]通知内[illegible]	機能適合性
			セ[illegible]ュリティイベントの通知先	使用性
		セキュリ[illegible]イベント のロギング	ロギング内容（検知コード／メッセージの内容／車両の状態／危険度等）	機能適合性
復旧	運用	アップデート	プログラムのアップデートの方法（物理ポート経由／OTA／その他）	保守性
			シグネチャや設定のアップデートの方法（物理ポート経由／OTA／その他）	保守性
			アップデート時のアップデートサーバー／アップデート管理モジュール／IDS等の役割分担	保守性

↔

Evaluation and feedback of results

Forming a common understanding w/ industry

- Harmonize in advance with stakeholders on the target requirements of the output IDS Evaluation Guide and the IDS evaluation methods to be described, with the ultimate goal of using them in practice as an exit strategy.



Scope

PwC

SIP

Industory

Survey

Basic research and experiments

Development of an in-vehicle IDS evaluation guide

Outcome

Practical Development

Incorporating industry input

Pre-alignment on the guideline

Use in industry associations and individual companies

Thank you