SIP-adus Activities Report

—Cyber Security—

Cross-Ministerial Strategic Innovation Promotion Program
Innovation of Automated Driving for Universal Services

February 14, 2017
Satoru Taniguchi, Chairperson
SIP-adus Cyber Security Sub-working group /
Toyota InfoTechnology Center Co., Ltd.

<Translated Version>

Table of contents

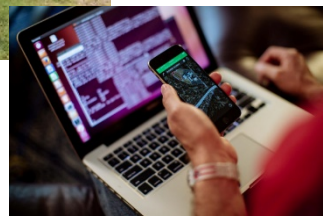
Ⅰ. Cases of cyber security attacks on vehicles

Fiat Chrysler recalls 1.4 million cars after Jeep hack

CNNMoney
@CNNMoney

フォロー

Recall Alert: Fiat Chrysler is recalling 1.4 million hackable vehicles. Check affected cars: cnnmon.ie/1OrrqGv



Ⅰ. Cases of cyber security attacks on vehicles

The Washington Post

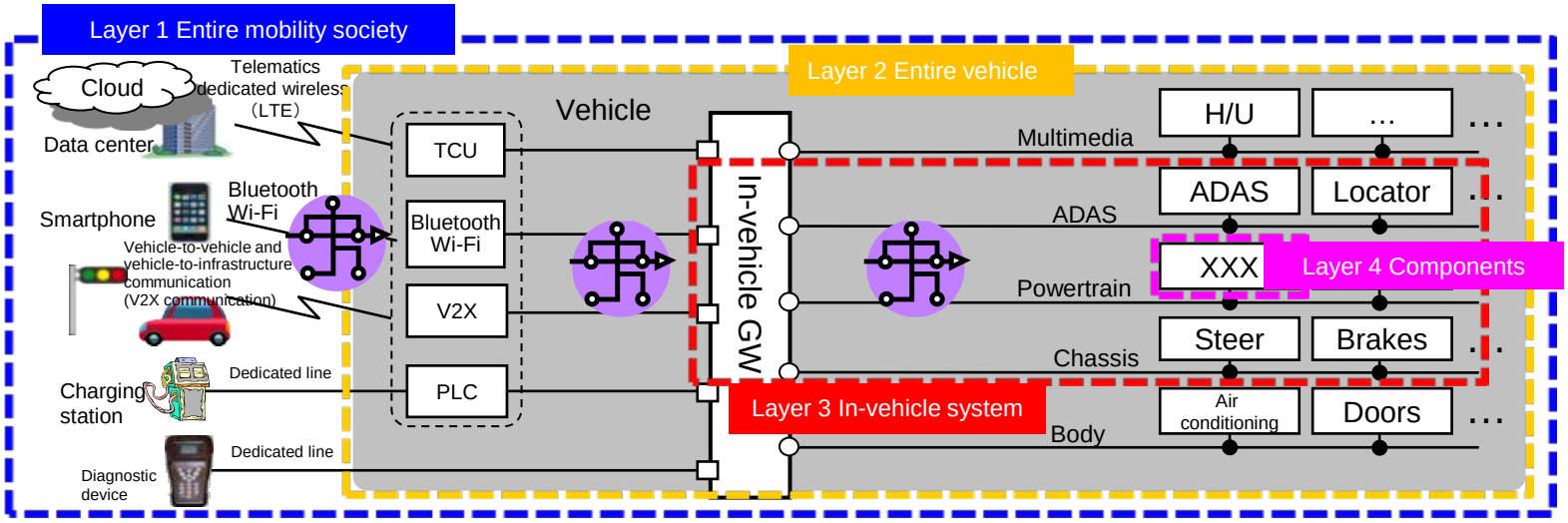
Researchers remotely hack Tesla Model S

The company said the vulnerabilities that Keen Security Lab uncovered would only be accessible under a very specific circumstance: when the vehicle's Web browser was in use and the car was connected to a malicious WiFi hotspot.

SIP

Ⅱ. Vehicle system architecture, and cyber security countermeasure examples

There has been an increase in cases of layer 2–4 in-vehicle systems being controlled and manipulated through attacks that use layer 1 telematics and WiFi as the entry point.



Threat

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

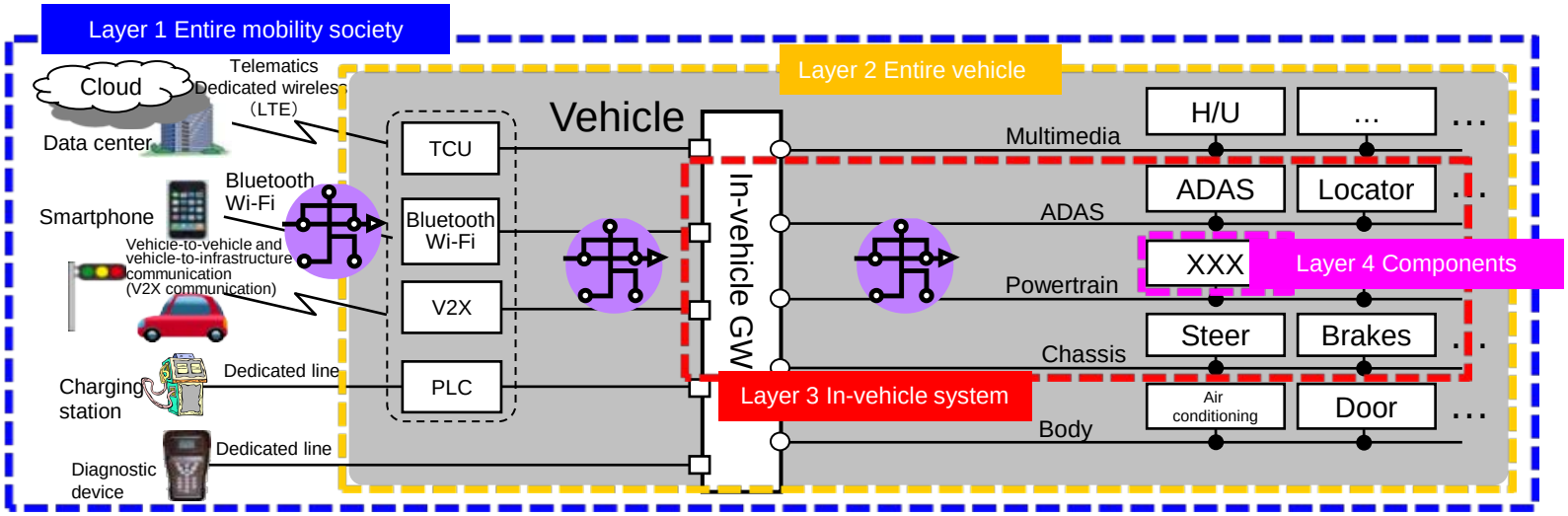
Examples of security measures

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

The countermeasures and detection technology combination at each layer ensure the vehicle system resilience. And, the system architecture is different for each OEM.

Ⅲ. Vehicle system architecture, and cyber security countermeasure examples

Conduct research targeted at vehicles' layer 2 and below with an eye toward industry and global standardization



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

"SIP Cyber-Security for Critical Infrastructure" researches data center security.

Ⅲ-1. Threat analysis

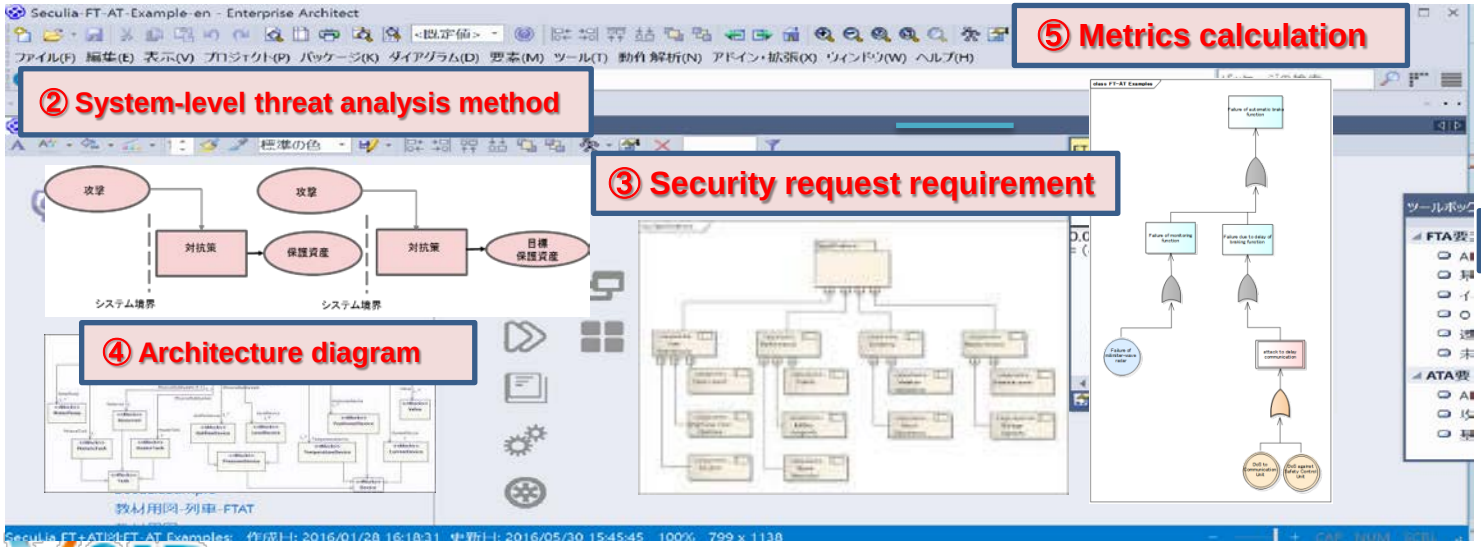
(1) Research of threat analysis methodology from cyber attacks [FY2016]

- Incorporate defense-in-depth, multi-stage attack countermeasure strategy
- Refer threat database (Auto-ISAC, NVD, etc.)
- Compatibility with JasPar analysis specification

(2) Development of integrated analysis [from FY2017]

- Tool development to integrate threat analysis and functional safety analysis.
- Development of industry standard tools collaborate with JAMA, and JasPar

[Overview of all tools (Conceptual completed diagram)]

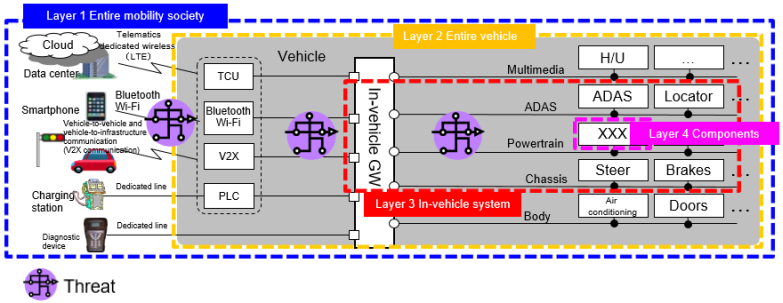


Ⅲ-2. Evaluation method

Layer 2　Entire vehicle

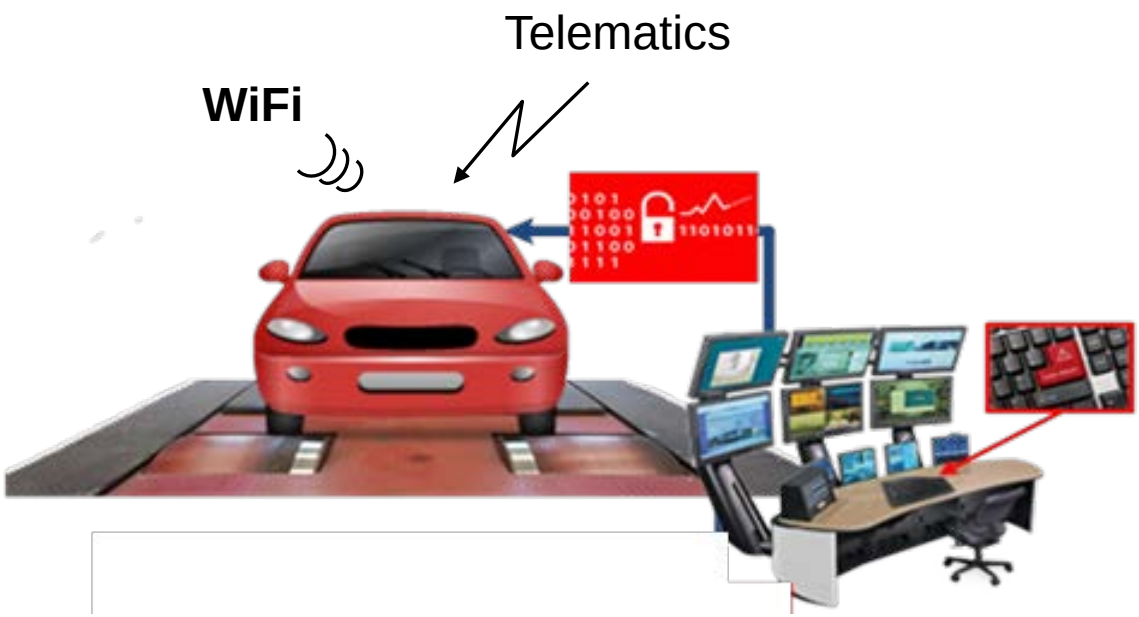
(1) Development of vehicle black box evaluation method

Confirm resilience and functional safety with WiFi and telematics as point of entry for attack



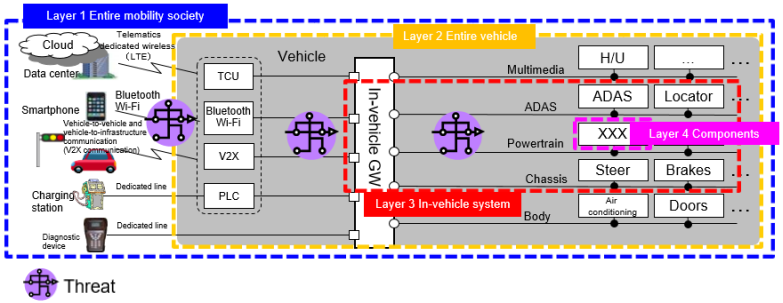
a) Sniffing
b) Port scan
c) Fuzzing
d) Penetration
e) Jamming

Large-scale field operational test from 2017
Reflection into industry standardized evaluation method
Cooperation with Auto-ISAC



Ⅲ-2. Evaluation method

Layer 3 In-vehicle system



(2) Development of evaluation method for in-vehicle communication (CAN bus)

① Using in-vehicle communication simulator, confirm
- Assumed attack method
- Communication behavior

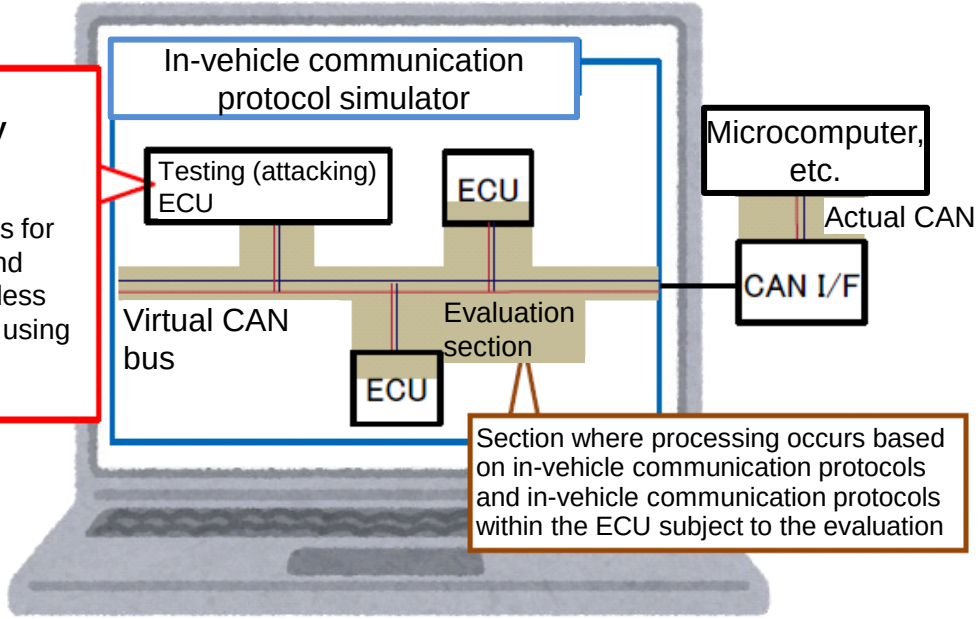
[Create evaluation database]

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

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

Evaluation (attack) method example

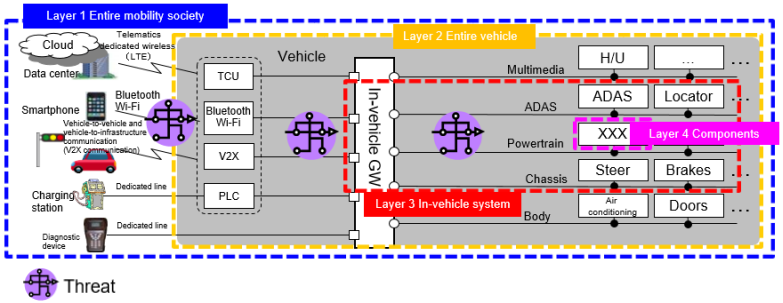
DoS attack / high frequency transmission (specific node)
Monitor transmitted messages for ECU subject to evaluation, and send same CAN-ID/meaningless data messages to virtual bus using shortest cycle for simulator specification



Ⅲ-2. Evaluation method

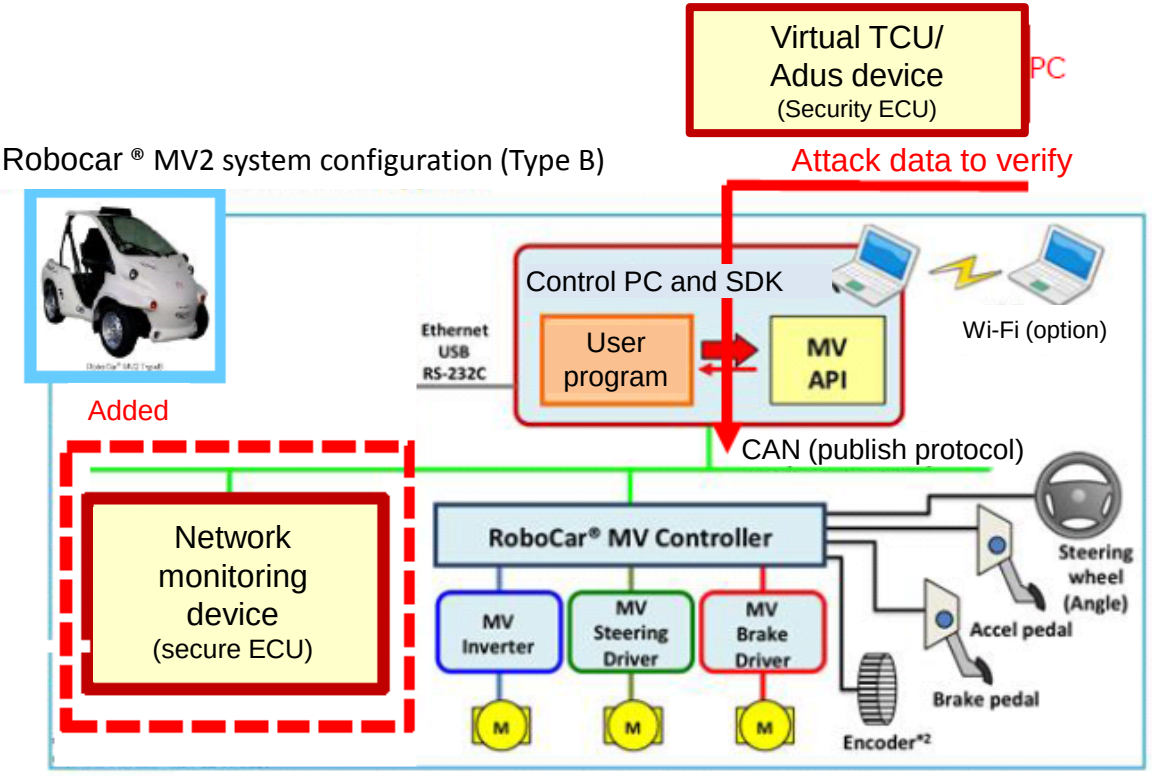
Level 3 In-vehicle system

(2) Development of evaluation method for in-vehicle communication (CAN bus)



- ② Intrusion detection guidelines
  - ・CAN message cycle disturbance
  - ・CAN message cycle omission, etc.

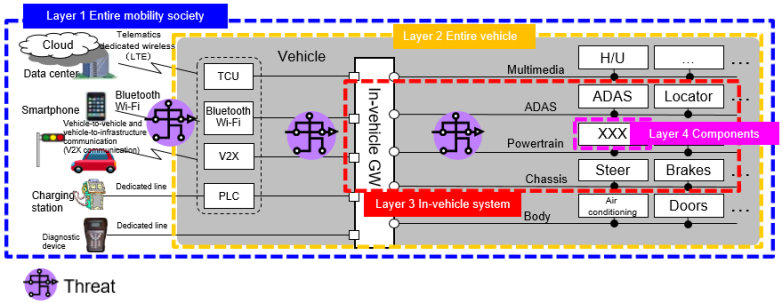
Robocar ® MV2 system configuration (Type B)



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

Ⅲ-2. Evaluation method

Layer 4 Components



(3) Development of evaluation method for key distribution and reprogramming Certification

Research the appropriate/standard durability levels for the reprograming corresponding to the each in-vehicle computer (ECU) security risk

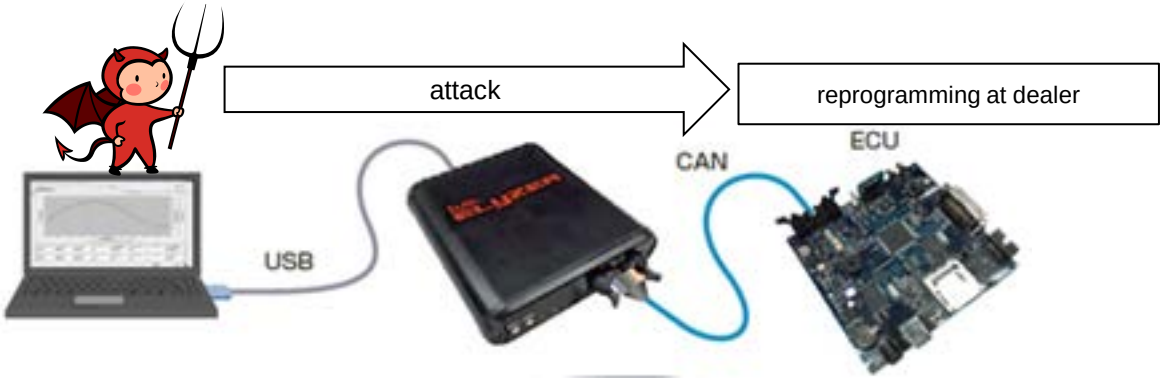
- Cryptogram algorithms
- Random bit number, Entropy

[Assessment methodology]

① Evaluation of actual device attack by testing board

② Key management research for other industries (*)

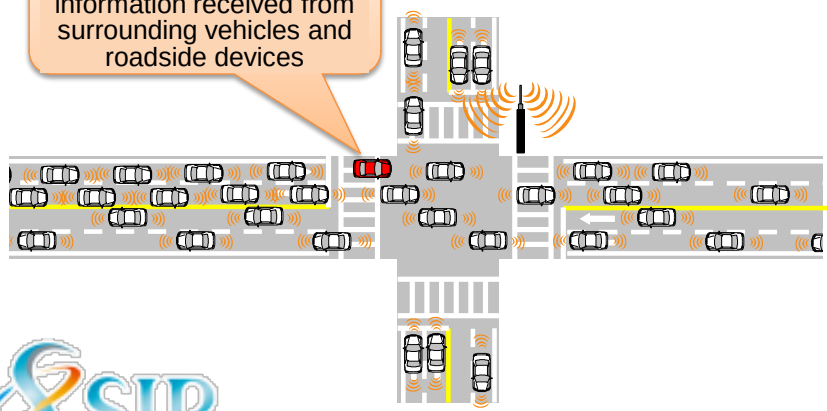
(*) Bank ATMs, credit card payment terminals, smart meters



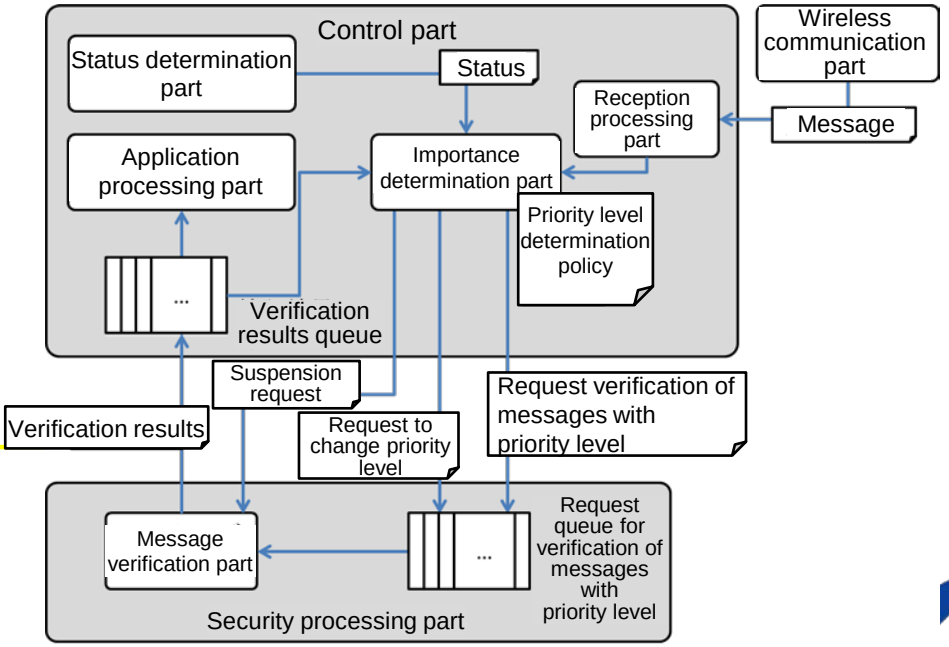
Ⅲ-3. V2X signature validation

[Background]	Secure real-time communication at time of V2X becomes common
[Research]	Simplification of message signature verification process in V2X communication
[Target]	1,000 messages/sec

Using a message verification method with priority levels, complete performance target.
- Confirm evaluation on actual devices
- Try standardization proposals, for ISO/TC204/WG16



Message verification method with priority levels



Ⅳ. Four-year plan

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

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

END

Thank you for your attention.