Symposium on The Future Networked Car

(Geneva, Switzerland, 5 March 2015)

Security issues related to the future Networked Car

Koji Nakao
Distinguished Researcher,
Network Security Research Institute, NICT
Information Security Fellow, KDDI

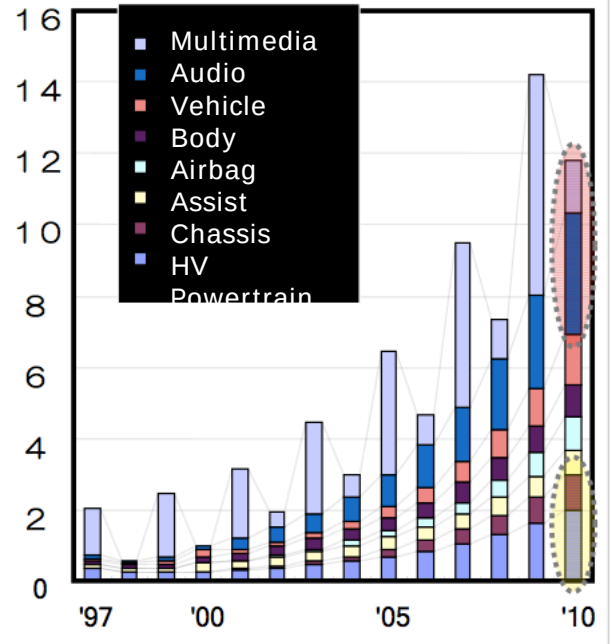
Agenda

- Background
- Framework of ITS security for standards
- On going work for secure software remote update (ITU-T X.itssec-1 (draft))
- Utilization of light-weight crypto
- V2V Communication Verification Project in Japan

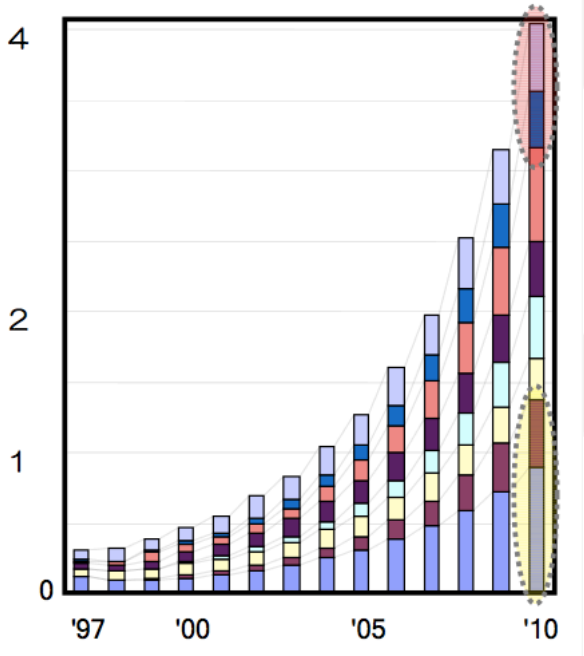
Increase in Automotive Electronics

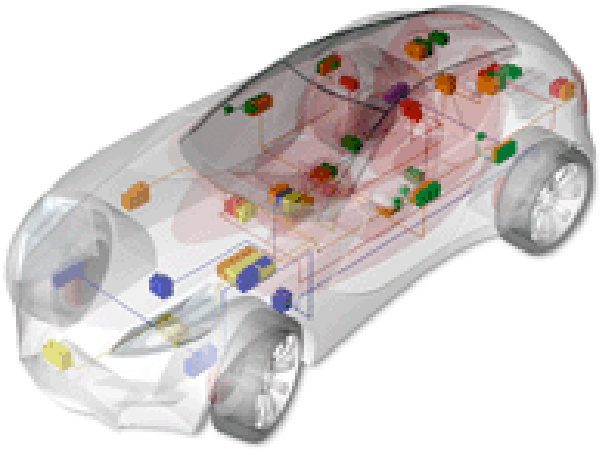
50%	100	100 million	5	2miles
Proportion of electronic components of car production costs	Number of ECUs in luxury models	Number of lines of car software	Number of networks in the car (average)	Length of cable in the car

Software Development Volume



Software Development Cost

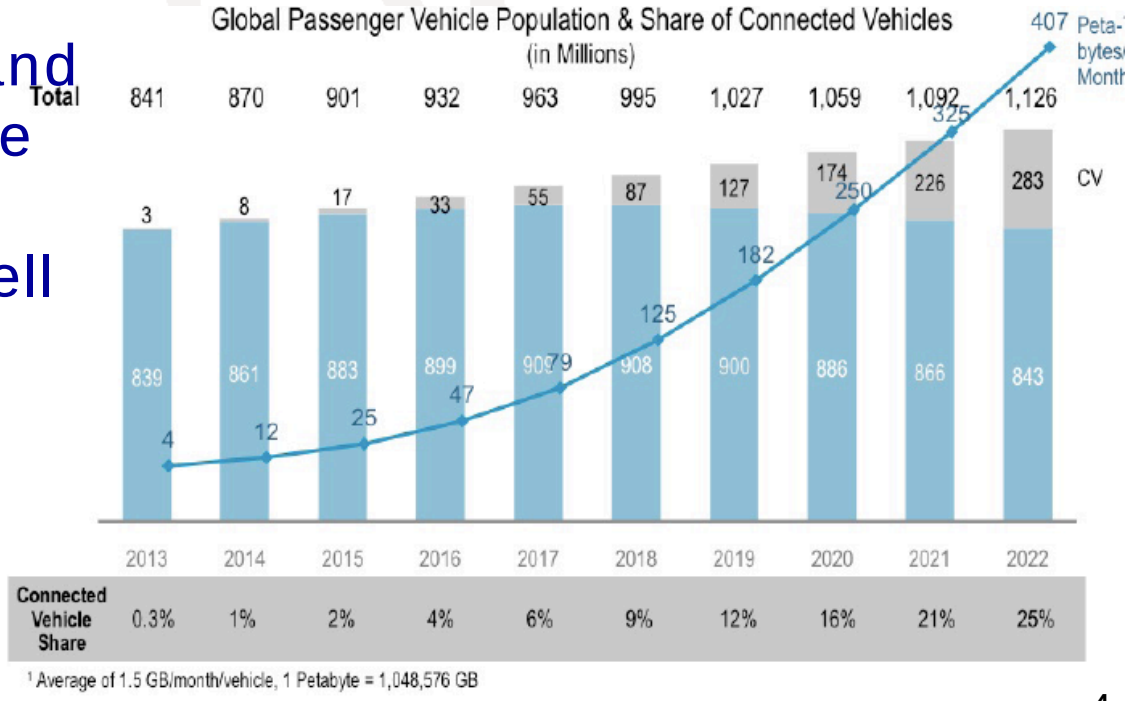




ECU: Electronic Control Unit

Connected Vehicles

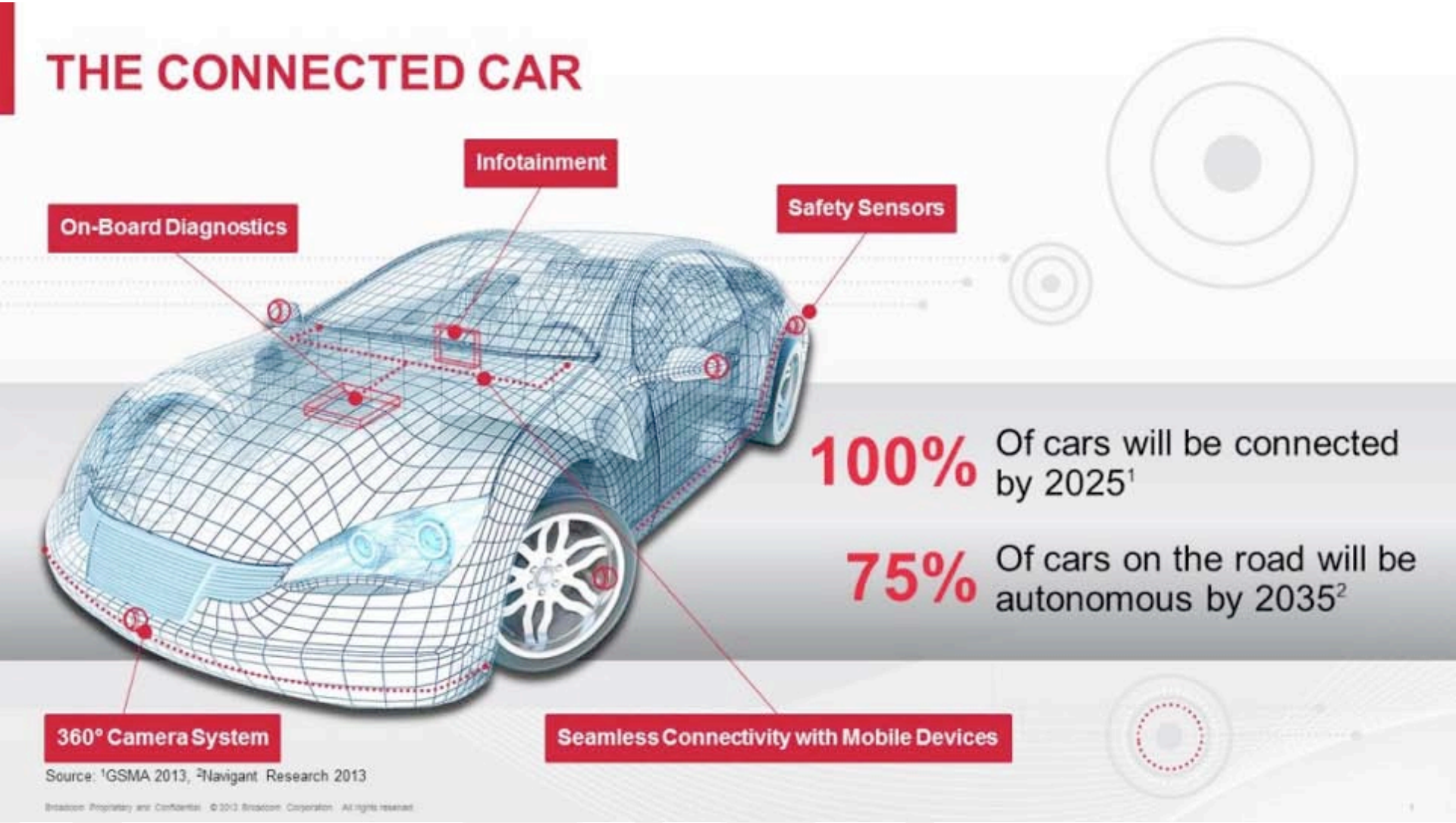
- Internet connection (LTE, 3G, Wi-Fi, Bluetooth ...)
  - via customer's smartphone, SIM embedded in the vehicle, etc.
- Autonomous car
  - Control engines and brakes based on the info from roadside infrastructure as well as car-mounted sensors, cameras, and radars



[1] Average of 1.5 GB/month/vehicle, 1 Petabyte = 1,048,576 GB

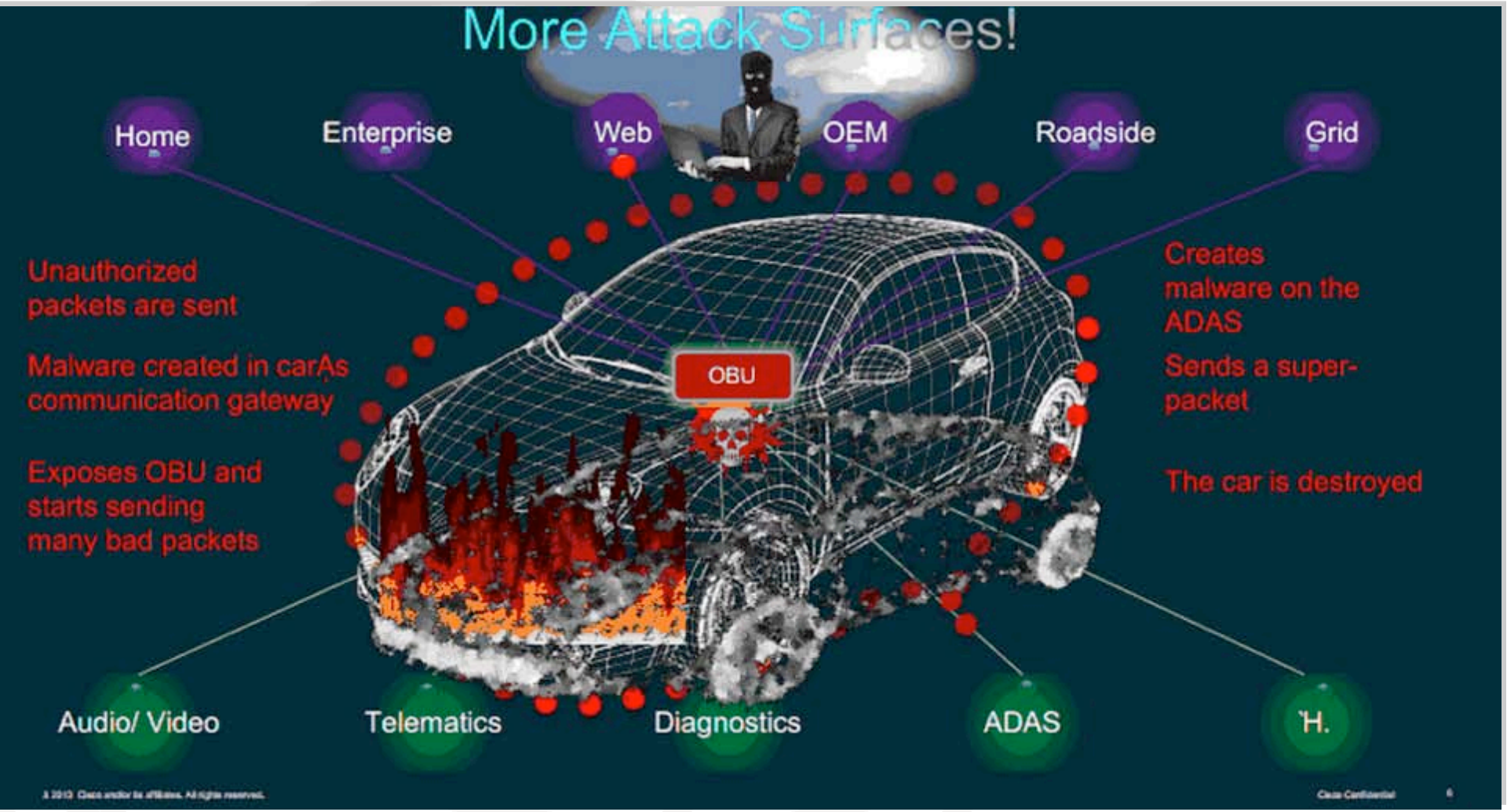
Sources: Cisco IBSG, 2011, based on data from U.S. Department of Transportation, iSupply, McKinsey & Company

The Connected Car



http://johndayautomotivelectronics.com/top-five-technologies-enabling-the-connected-car/

More Attack Surfaces!



http://gigaom.com/2013/08/06/ciscos-remedy-for-connected-car-security-treat-the-car-like-an-enterprise/

Framework of ITS standards (not authorized in ITU-T)

Architecture of a series of standards (General issues)

Reference Architecture/Model

ITS Ref. Model

Terminologies

Common Terms for ITS

Service Models (def) and Requirements

V2V, V2I, V2N

Service Requirements

Service/Protocol Specifications

e.g. Software Remote Update

Mechanisms and Algorithms

e.g. Encryption, Message Processing

Architecture of a series of standards (Security issues)

Reference Architecture/Model

ITS Ref. Model

Terminologies

Common Terms for ITS

Service Models (def) and Requirements

Security Guideline

Security Requirements

Service/Protocol Specifications

e.g. Secure Software Remote Update (X.itssec-1)

Mechanisms and Algorithms

e.g. Encryption, Mac, Authentication..

On going work for software remote update (ITU-T X.itssec-1 (draft) by SG 17)

Works related to Remote Update in other SDOs

- ISO TC204 24102-2
  - ITS TC204 24102 series focuses on ITS station management
  - Part 2 (24102-2) discusses about remote maintenance of ITS-SCU (station communication unit)
  - It does not include remote maintenance of devices on vehicle
  - Provided by ETSI TC ITS below

- ETSI TC ITS
  - Provides 20 standards regarding ITS that include ITS infrastructure, communication protocol, etc.,
  - Collaborating with EVITA, PRESERVE for a structured standardization
    - EVITA: an FP7 project to develop security mechanisms for on-board devices
    - PRESERVE: an incoming project of EVITA which aims to develop and experiment an HSM based V2X communication technology
  - SG17 needs to survey activities in ETSI TC ITS regarding standardization of secure software update

Introduction of draft Rec. X.itssec-1 “Scope”

Functionality of Head Unit

- ! Status check of ECUs
- ! Log collection
- ! In-car diagnosis function

Functionality of Server

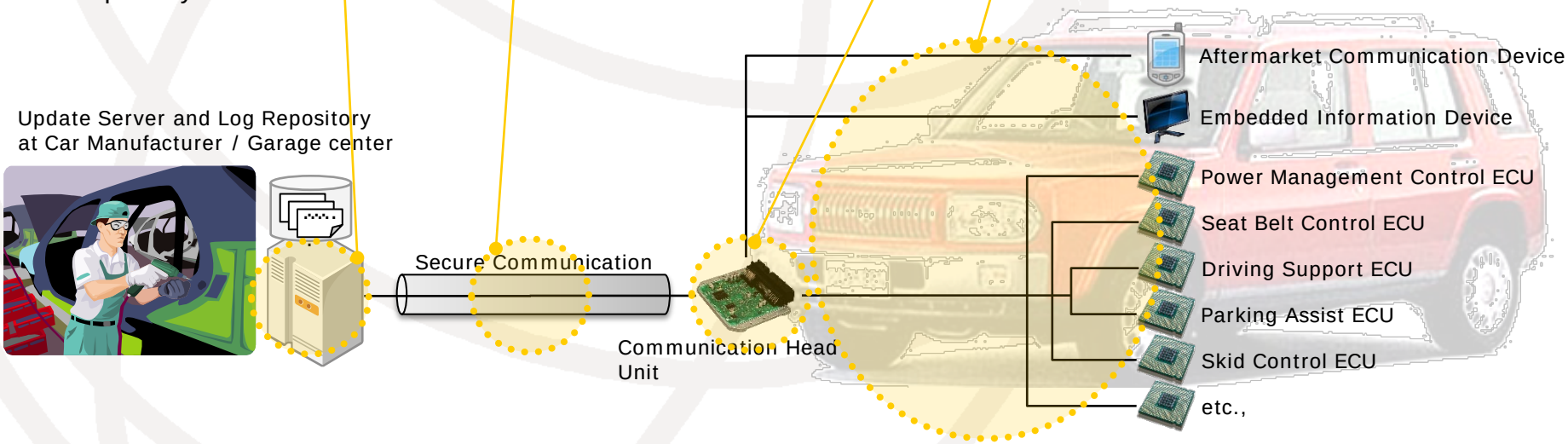
- ! Stored Data Definition
  - ✓ Auth info
  - ✓ Log Audit
  - ✓ With considerations of privacy concerns

Communication protocol

- ! Between Car and Manufacturer / Garage
- ! Encryption
- ! Authentication

Diagnosis of on-board devices

- ! Status check of ECUs
- ! Log collection
- ! Verification of update module

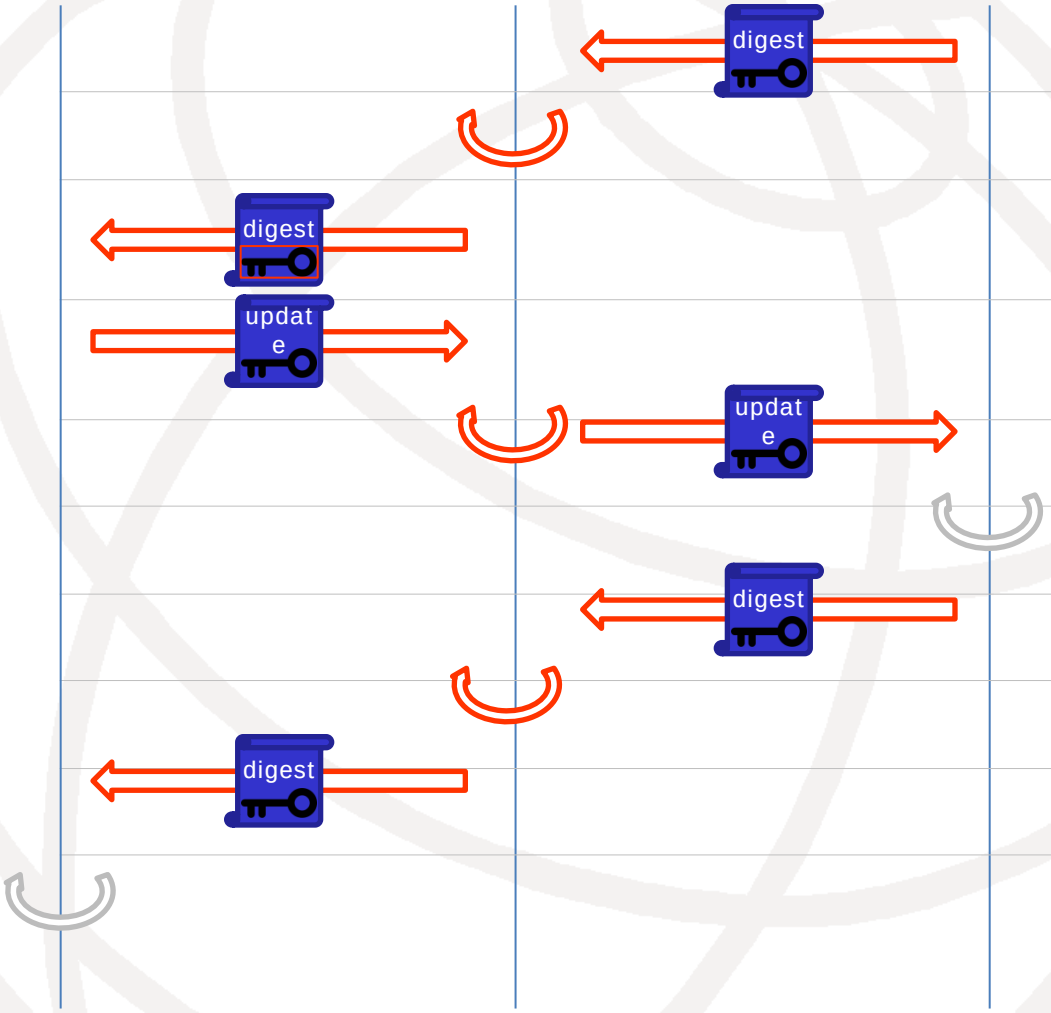


Example: data flow of remote update

Update Server and Log Repository
at Car Manufacturer / Garage center

Communication Head Unit

ECU



1. ECU generates a digest of its SW with its own secret key and sends it to the head unit
2. Head unit verifies the digest
3. Head unit merges collected digest and resigns it with its own secret key, then sends it to the manufacturer center
4. The center determines an update program, signs it with own secret key, sends it to the head unit.
5. Head unit verifies the update program and transmits it to ECU
6. ECU applies the update program by itself
7. Again, ECU generates a digest, sign it and sends it to the head unit for verification
8. Head unit verifies the digest
9. Head unit resigns the digest with own secret key, and sends it to the center
10. The center determines whether SW update process is successful or not. After the process has done successfully, the center stores the update log into own DB.

Requirements for the secure software update

- Functions requirements to be provided
  - ✓ Remote diagnosis of software modules of on-board devices
  - ✓ Digest based software verification at center
  - ✓ Secure delivery and application of update modules
  - ✓ Log audit at center

  → Apply digital signature or MAC mechanism using HSM

- Limitations inherent to ITS environment
  - Characteristics of ITS communication environment
    - High latency, low bandwidth, frequent disconnection, etc.,
  - Non-continuous operation of vehicles
    - disconnections due to frequent stop and start of engines
    - a long durations with no connection (e.g., long summer vacation)
  - Low computational power of ECU and HSM

Security Considerations for Software Remote Update

Functionality of Head Unit

- ! Status check of ECUs
- ! Log collection

Functionality of Server

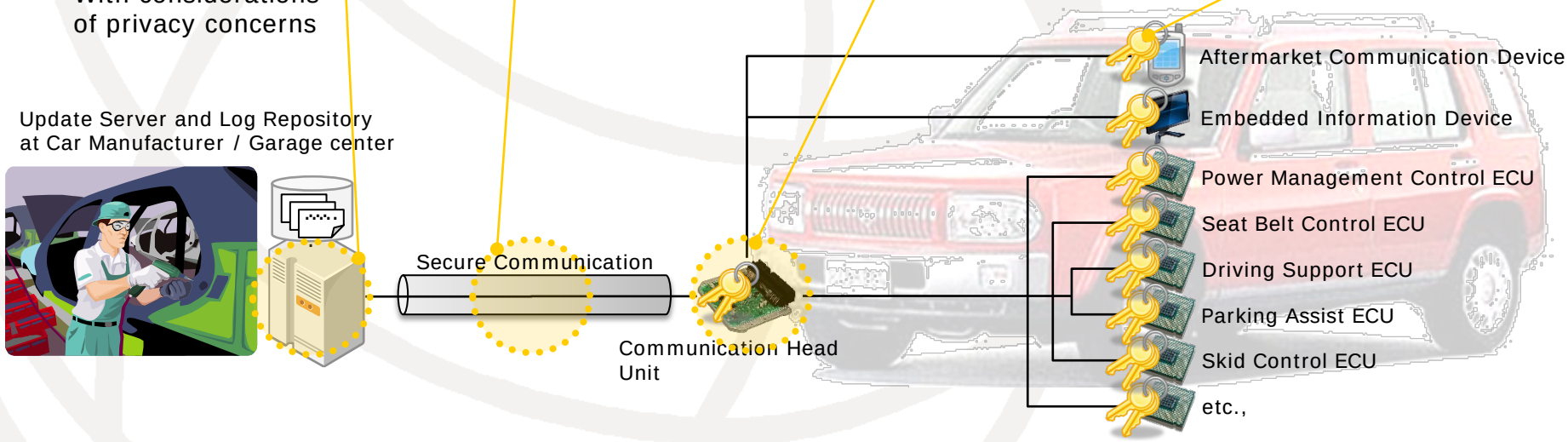
- ! Definition of Stored Data
  - ✓ Auth info
  - ✓ Log Audit
  - ✓ With considerations of privacy concerns

Communication protocol

- ! HTTPs with client auth
- ! TNC (RFC5792/5793)
- ! IPsec, VPN, etc.,

Hardware Security Module (HSM)

- ! HSM as a trust anchor
  - ✓ HSM (EVITA)
  - ✓ TPM (TCG)
  - ✓ SHE (HIS)



Structure of the Recommendation(draft)

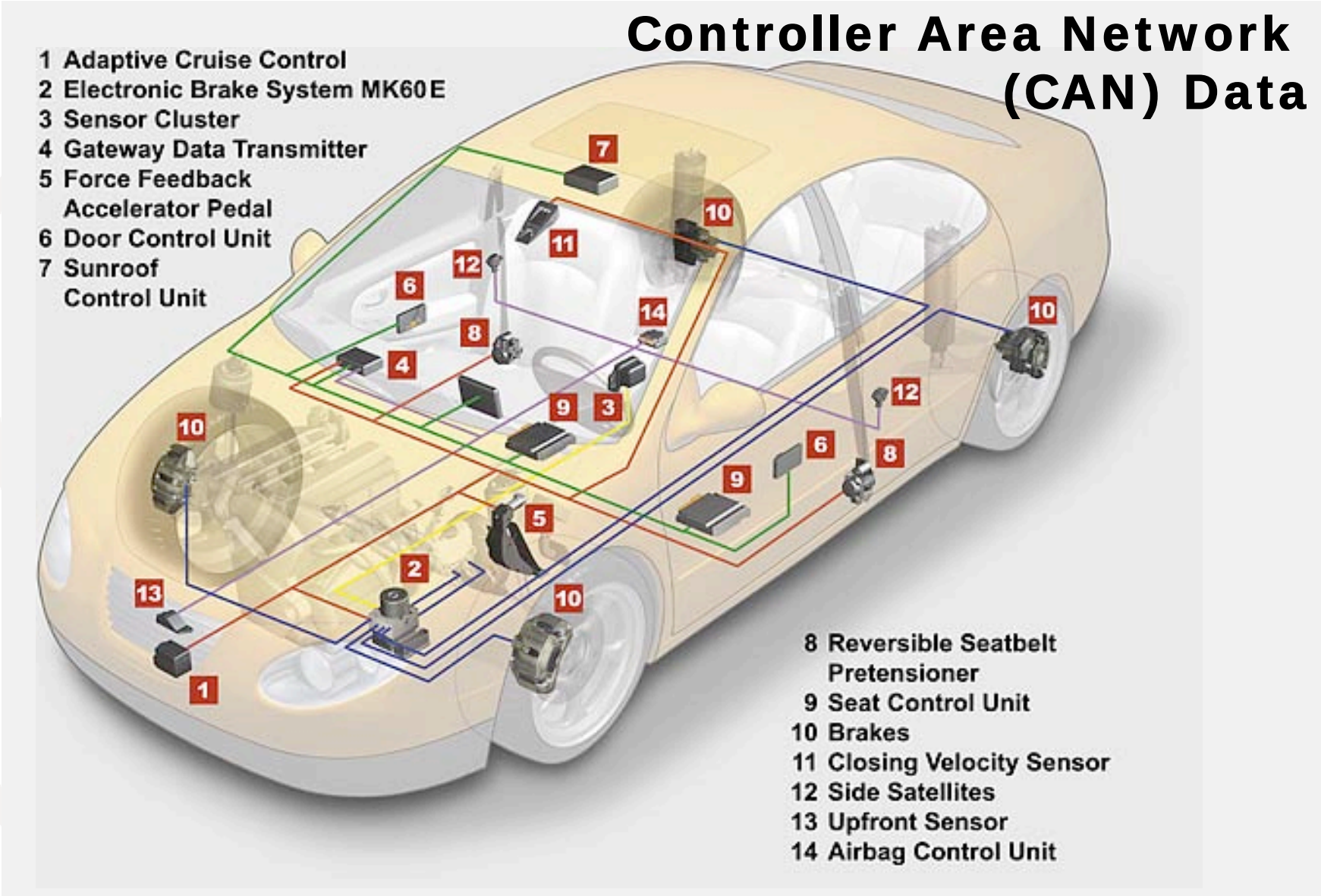
6. Basic model of remote software update
    1. Definition of components for secure software update in the ITS environment
        1. ECU
        2. Communication head unit
        3. Center server
    2. Basic mechanism
7. Threats and Risk Analysis
8. Functional requirements for the secure software update
    1. Remote diagnosis of software modules
    2. Digest based software verification
    3. Secure delivery and application of update modules
    4. Log auditing
9. Model and procedure of secure software update
    1. System model
    2. Data flow of remote software update
10. Functional specifications for components on the ITS environment
    1. In-car communication devices
    2. Communication head unit
    3. Center server
11. Practical use cases

Conclusions and Recommendations

- Introduced **Secure Remote Update** ;
- It is under development in ITU-T SG 17 as a Recommendation **X.itssec-1**;
- The Recommendation should be a **neutral content** without introducing some specific methods;
- **Collaboration with automotive industry** is necessary including with EU and US
- The goal of the Recommendation should be **a practical reference / guide for implementing secure remote update for software in the vehicle.**

Utilization of light-weight crypto

Much data to be protected(1)



http://www.aa1car.com/library/can_systems.htm

Much data to be protected(2)

V2X Communication Data

http://telematicswire.net/connected-cars-and-smart-homes-coherence-of-a-convergence-platform/

Lightweight Cryptography

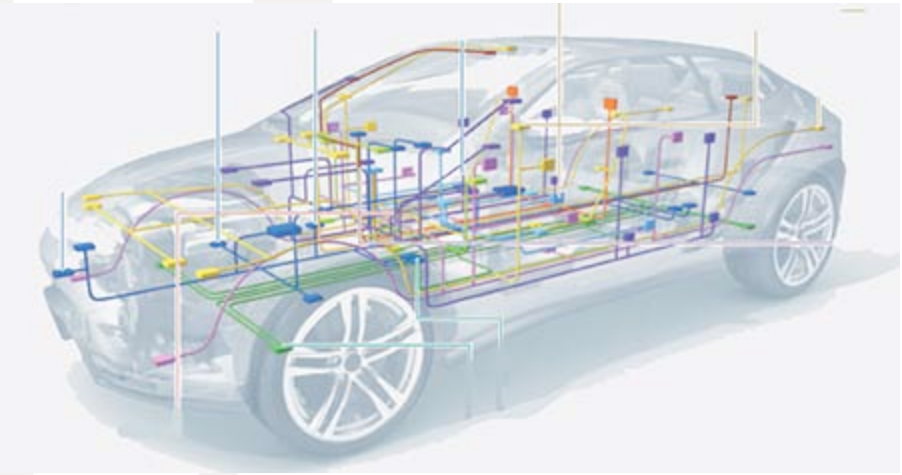
- "Cryptography tailored for implementation in constrained environments" [ISO/IEC 29192-1]
  - Constraints: chip area, energy consumption, power, memory, communication bandwidth, execution time, etc.
  - Applications: RFID tags, sensors, health-care/medical devices, low-energy applications, low-latency applications, ...
  - **Suitable for Internet of Things!**

Lightweight Cryptography

- R&D
  - EU ECRYPT-I (2004-2007), ECRYPT-II (2008-2013)
    - European Network of Excellence for Cryptology funded within ICT Programme of the European Commission's FP6, FP7
  - Japan CRYPTREC (2013-)
- Standardization
  - ISO/IEC 29192
    - Lightweight Cryptography, in ISO/IEC JTC SC27 WG2 since 2009

Why Lightweight Cryptography for Vehicles? (1)

- A modern vehicle contains 50 to 100 or more electronic control units (ECUs).
  - collection of embedded constrained devices
- CAN bus data field is (only) 32 bits.

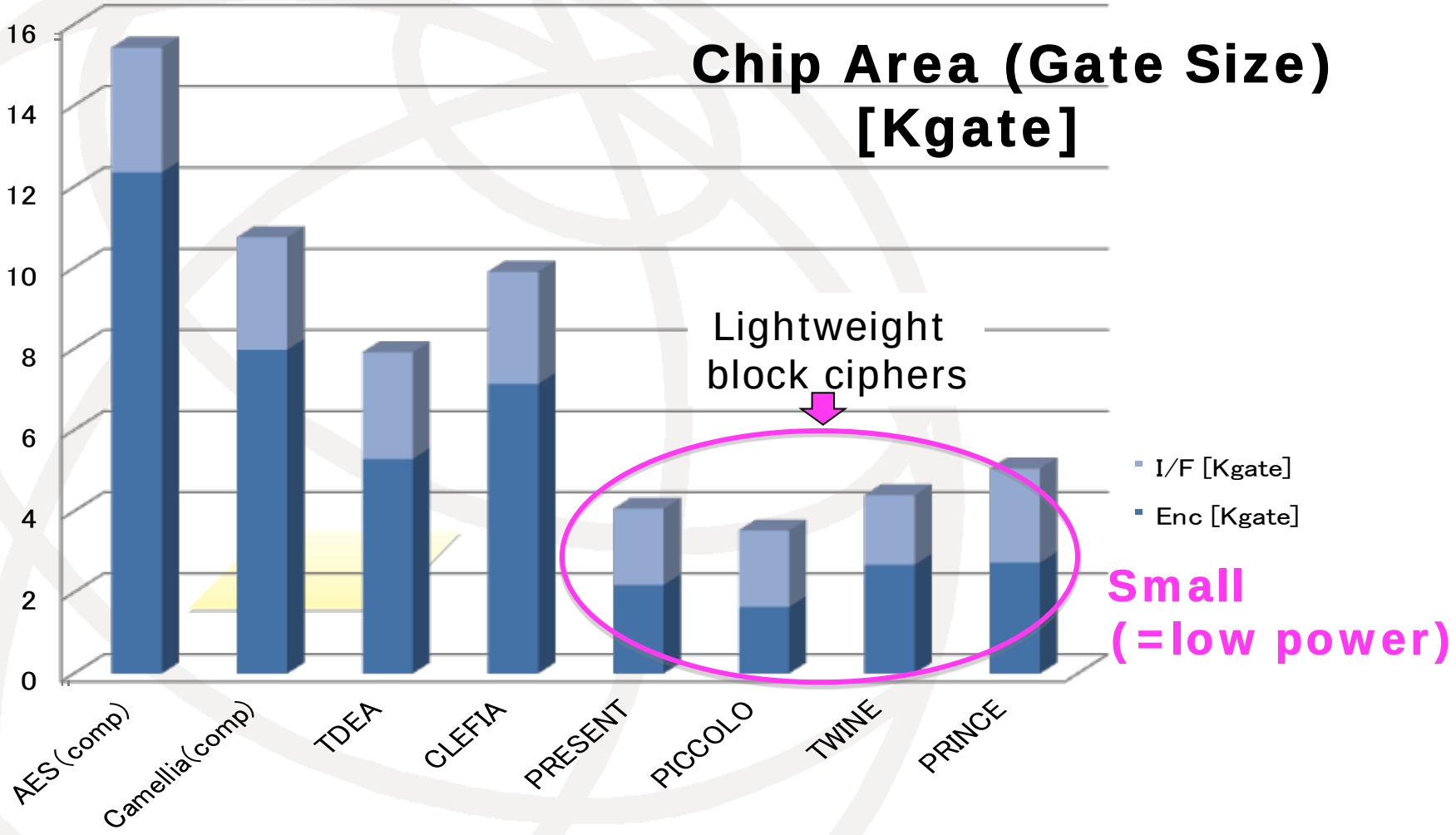


http://www.digikey.jp/ja/articles/techzone/2014/jul/what-engineers-need-to-know-when-selecting-an-automotive-qualified-mcu-for-vehicle-applications

Why Lightweight Cryptography for Vehicles? (2)

	AES	Lightweight block ciphers
Properties		
Block Size	128 bits	64 bits
Key Size	128/192/256 bits	80-128 bits
Key Schedule		Light (Simple)
S-box	8 x 8	4 x 4
Hardware Implementation		
Gate Size (ASIC)	3-10 Kgate	< 3 Kgate
latency		< 20ns within 10Kgates
Software Implementation (on microcontrollers)		
ROM (Enc+Dec)	1KB	< 200B

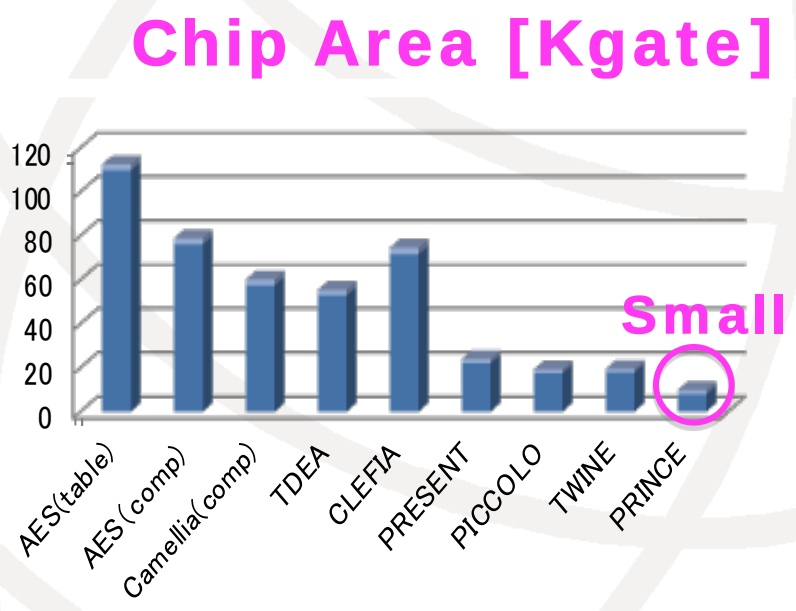
Why Lightweight Cryptography for Vehicles? (3)

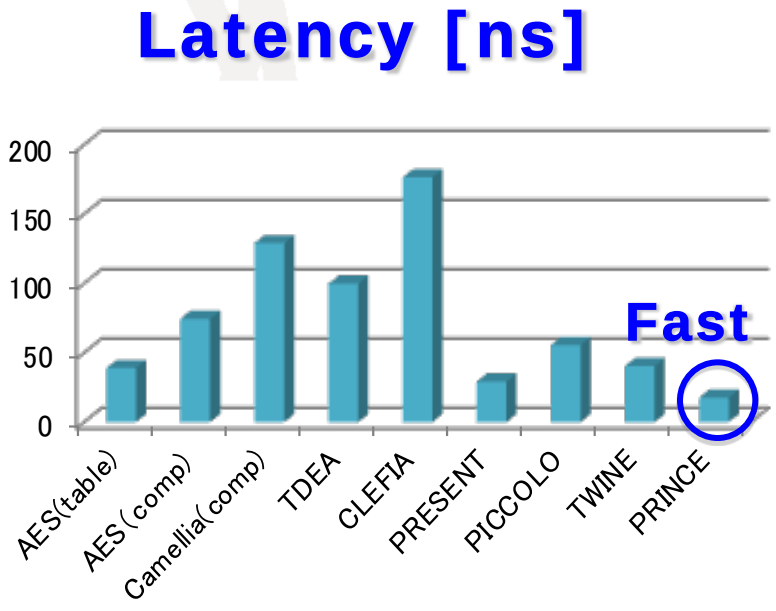


Suzuki, Sugawara, Saeki, “On Hardware Implementation of Lightweight /Low-Latency Cryptography”, SCIS2014

Low Latency

- Real-time response is crucial in Advanced Driver Assistance Systems (ADAS).
- AES can't achieve encryption in dozens of nano-seconds within dozens of kgates.





Conclusions and Recommendations

- Introduced **lightweight cryptography**
- Suitable for **constrained devices**, the connected cars and ITS security.
- Some lightweight algorithms are mature and standardized in ISO/IEC.
- It's high time to standardize **practical standards for connected cars and ITS security** in ITU-T.
- Collaboration with automotive industry is necessary.

豊田通商株式会社
TOYOTA TSUSHO CORPORATION

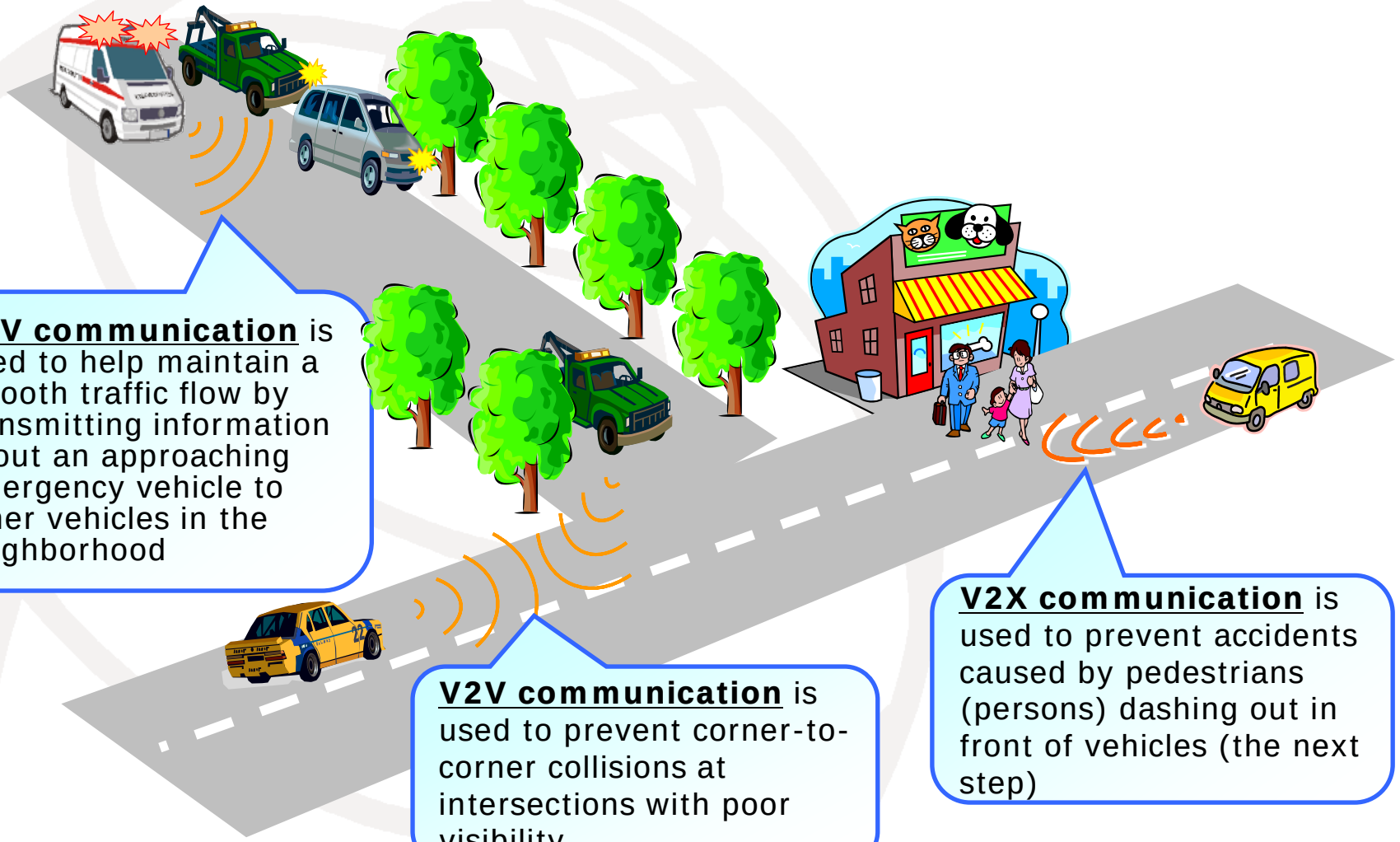
ICT for Next Generation ITS
―MIC ITS Project Result Presentation―

V2V Communication Verification Project

<Subcontracted investigation of communication technologies toward the establishment of next-generation ITS>

Toyota Tsusho Corporation

Objective of V2V communication



V2V communication is used to help maintain a smooth traffic flow by transmitting information about an approaching emergency vehicle to other vehicles in the neighborhood

V2V communication is used to prevent corner-to-corner collisions at intersections with poor visibility

V2X communication is used to prevent accidents caused by pedestrians (persons) dashing out in front of vehicles (the next step)

Identified services expected to be commercialized in early stage

Viewpoint of identification

- Previous examination
- Target market
- Competing service
- Similar services overseas
- ⋮

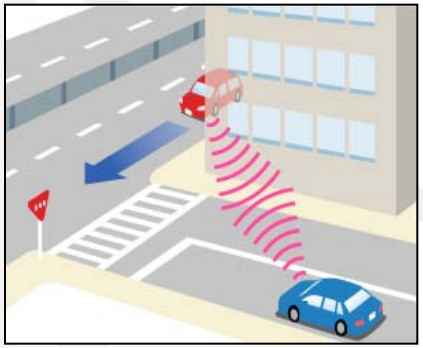
Identification of Services

- Support for preventing collisions during right turns
- Support for preventing accidents during left turns
- Support for preventing corner-to-corner collisions at intersections with poor visibility
- Support for recognizing approaching emergency vehicles
- ⋮

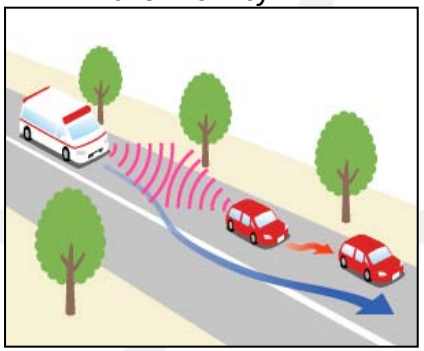
System definition, Result evaluation

Message Set Examination

Collision prevention support



Support in recognizing vehicles in the vicinity



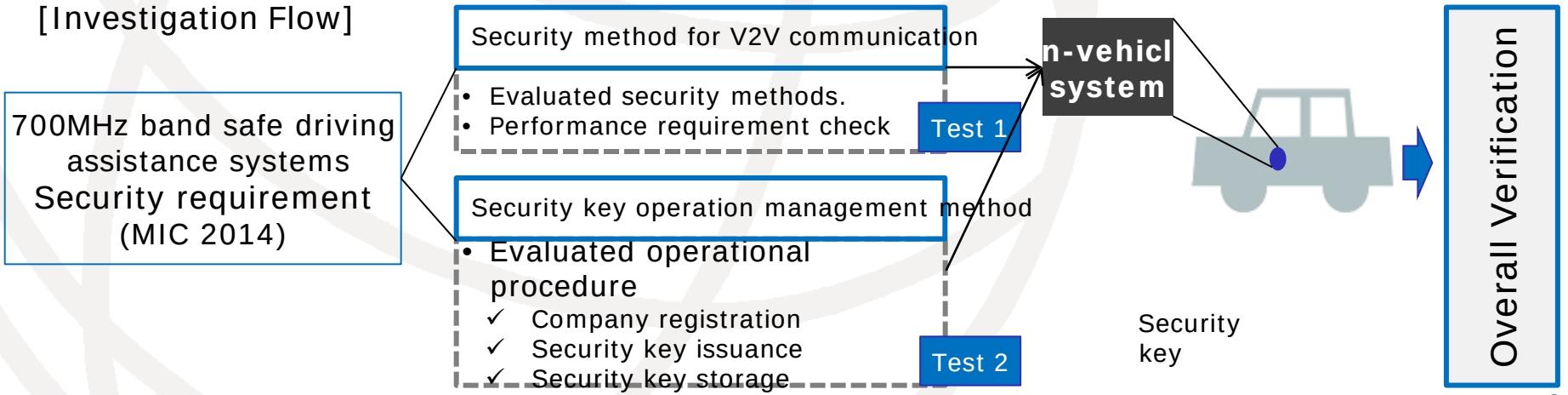
Identified services expected to be commercialized in early stage.

Security Evaluation(1)

[Security evaluation scope]

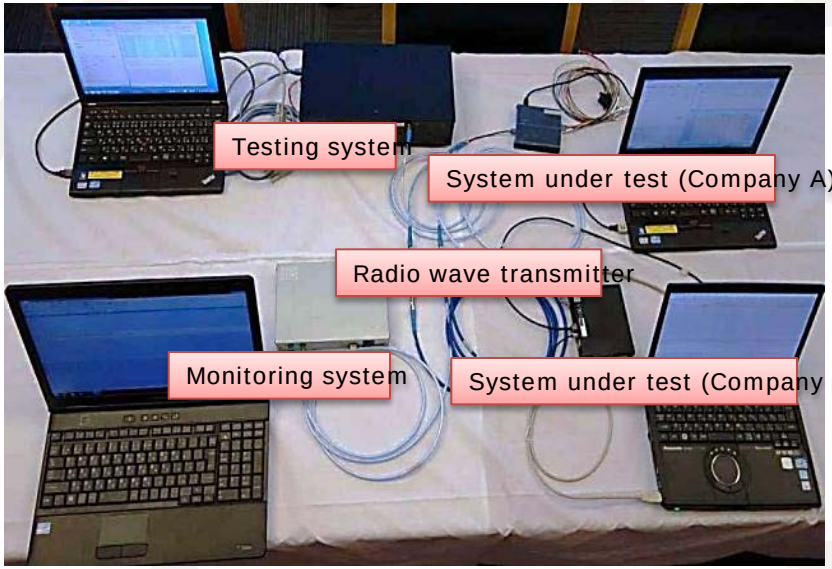
Phase	Startup phase	Popularization phase	Expansion phase
Trends in safe driving assistance systems	Start of safe driving assistance systems based on V2V communication	Start of safe driving assistance systems based on V2I communication An increase in the number of in-vehicle systems could potentially encourage more disruptions or attempts to gain unauthorized access	Start of safe driving assistance systems based on V2X communication
Security items to be considered in each phase	• **Security method for V2V communication** • **Security key operation management method**	• **Security method for V2I communication** • **Framework for maintaining security** • **Security update method** • **Abnormality detection method**	• **Security method for V2X communication**

[Investigation Flow]

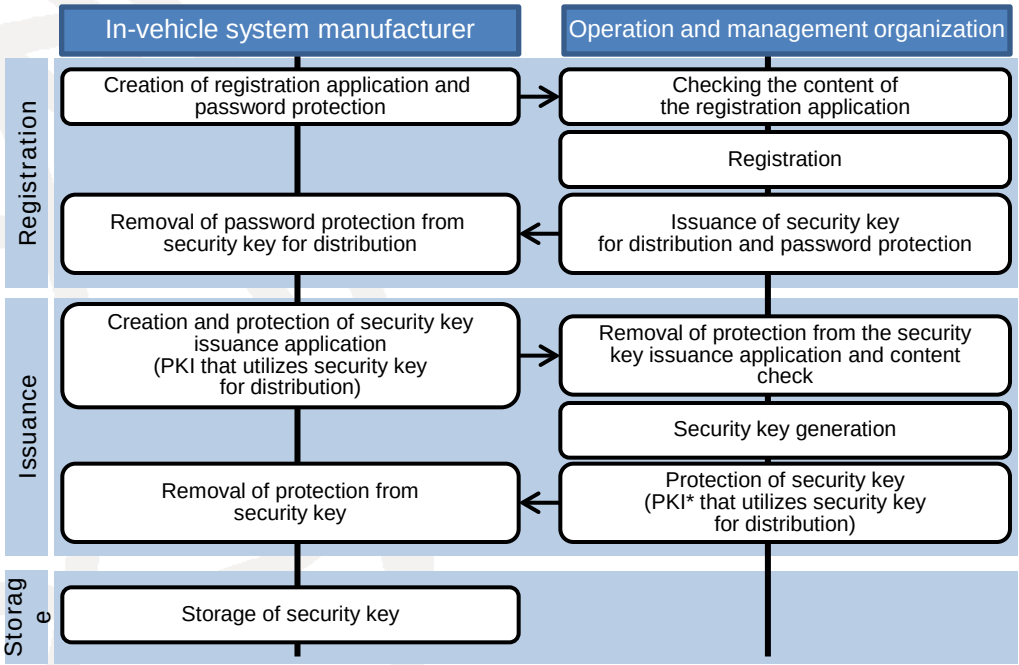


Security Evaluation(2)

[Test 1] Security method for V2V communication



[Test 2] Security operation management method



*PKI: Public Key Infrastructure

This process checks whether an in-vehicle system can send messages without any problem while also receiving messages from other in-vehicle systems in a simulated environment in which many vehicles are present.

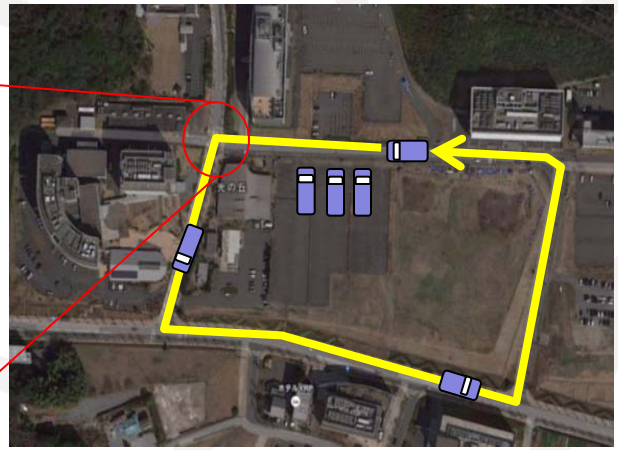
Evaluated operation management methods and carried out verification that assumed an actual operation.

Overall Verification – Test Description

Test course (simulated street at JARI)

Satellite photo: ©2015 Google

Public road (YRP: Yokosuka City)

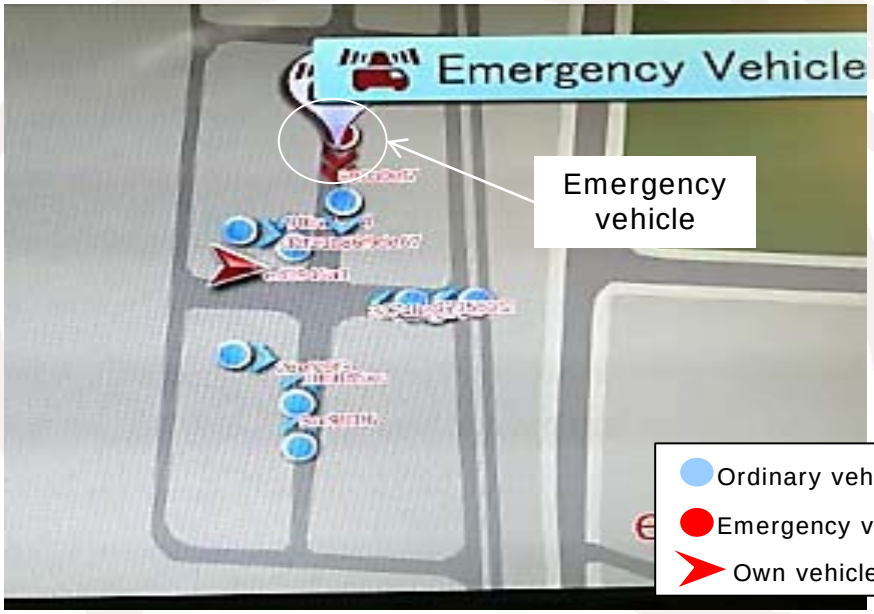


Satellite photo: ©2015 Google

Overall Verification– Test Result

[Security functions verification]

Human Machine Interface (HMI) example Provided by Pioneer Corp.



Map：Copyright（C） INCREMENT P CORP.

(Left) Identified as an emergency vehicle
(Right) Fake emergency vehicle, which is originating the message that imitate an emergency vehicle, is identified as a general vehicle by the security functions.

- Realized V2V communication by the in-vehicle system that implements the security functions.
- Identified the emergency vehicle by the security functions.

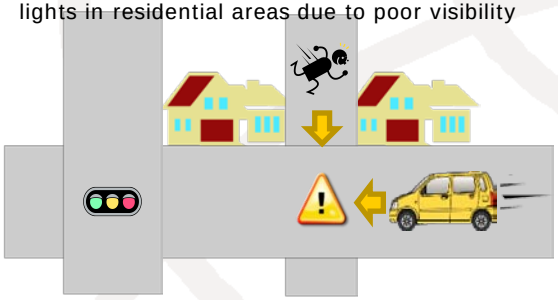
Examination of V2P Communication Systems (near future Targets)

Accident example collection and cause analysis

Accident scenarios determined from collected data and analysis results

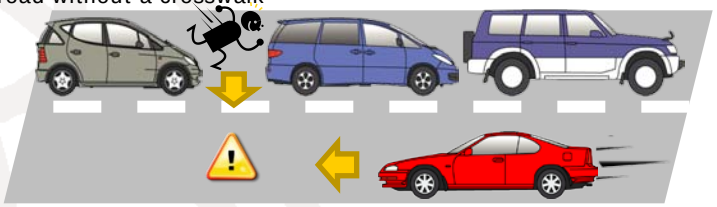
Case 1: Collision with cross traffic in intersection (seniors/children, bicyclists)

→ Accidents that occur in narrow intersections without traffic lights in residential areas due to poor visibility



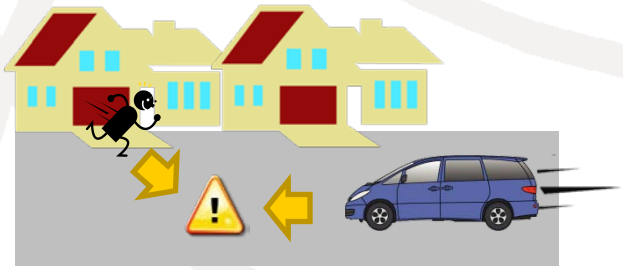
Case 2: Pedestrian crossing right in front of or behind a vehicle on single-lane roads with poor visibility (seniors/children)

→ Accidents that occur when a pedestrian (or bicyclist) dashes out from between parked cars or cars stopped due to traffic congestion in order to cross a two-lane road without a crosswalk



Case 3: Pedestrian dashing out on a single-lane road with poor visibility (children, pedestrians)

→ Accidents that occur when a child (pedestrian) dashes out of a house, store, or vacant lot without checking for safety



Case 4: Turning right or left on a single-lane road without a dedicated bike lane (bicyclists)

→ Accidents that occur when a bicyclist tries to turn right (left) without checking for safety

* Includes accidents that occur when a bicyclist swerves toward the middle of the road to avoid a parked car.

Priority targets

Who: Seniors (65 years or older), children (12 years or younger), and bicyclists

Where: Intersections on residential streets and single-lane roads with poor visibility

How: Crossing outside crosswalks (during right/left turn in the case of bicyclists)

Summary

- Standardization of Recommendation X.itssec-1 (Secure Remote Update)
  - Need to collaborate with SDOs (ISO: TC204, ETSI: ETSI TC ITS Working Group Security (WG5)) and EVITA, PRESERVE. TCG…
  - This Recommendation should be a neutral content without introducing some specific methods for providing a practical reference/guide for implementing secure remote update for software in the vehicle.
- Light-Weight Encryption for ITS
  - Light-Weight is suitable for constrained devices, the connected cars and ITS security.
  - It's high time to standardize practical standards for connected cars and ITS security in ITU-T.
- At the next SG17 meeting in April 2015, framework of standards for ITS will be discussed in connection with the work in SG 16.