Prevention of a cybersecurity threat in a Connected & Autonomous Vehicle

beyond THE CAR

Aug.26th 2019

Hyundai Motors

HYUNDAI MOTOR GROUP

Contents

I. Paradigm Shift & Cybersecurity Threat

II. Cybersecurity Standardization

III. Issues on Autonomous Vehicles

IV. Cybersecurity in Autonomous Vehicles

V. Conclusion

Vehicle – Paradigm Shift

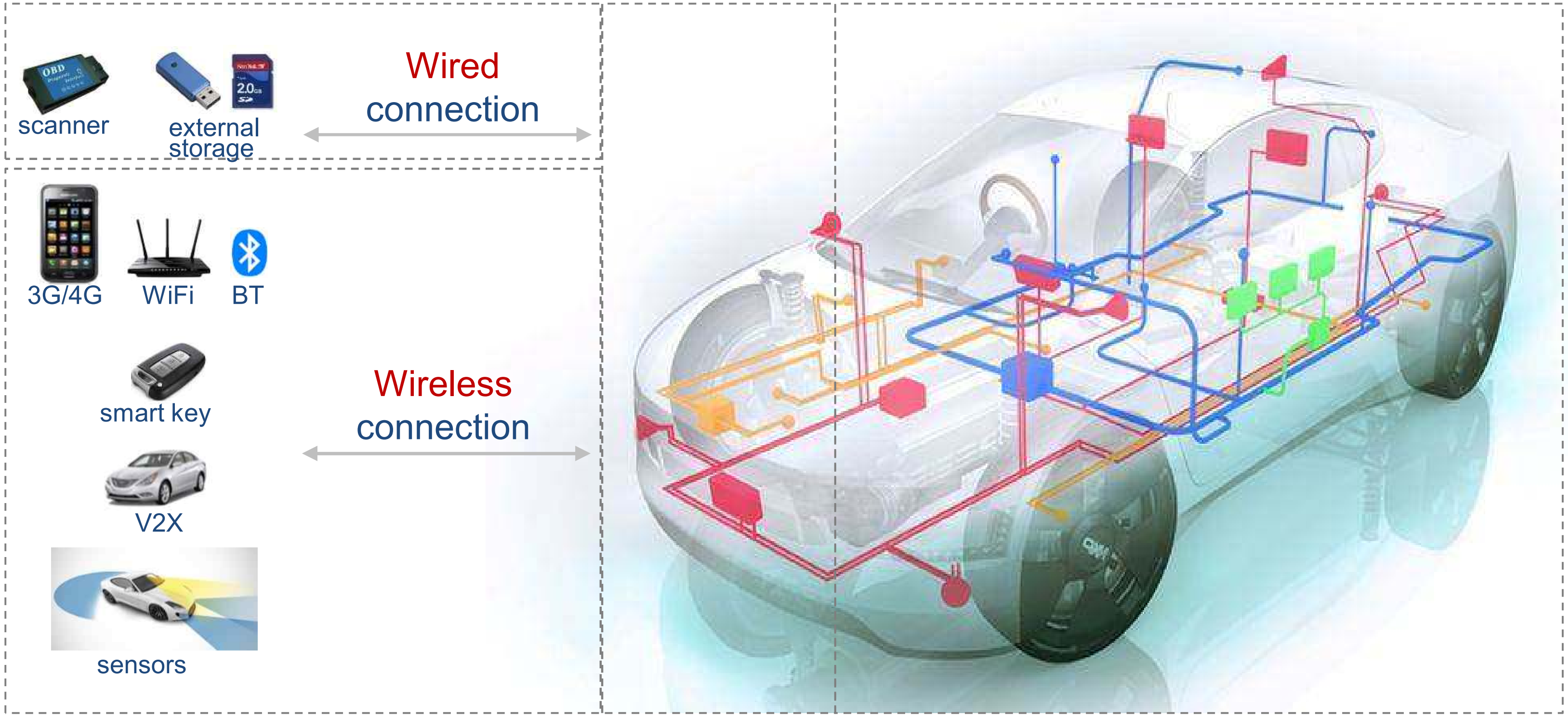
▣ A Vehicle improves a technology according to becoming an electronic system and connecting with each other

	Mechanical Systems	E/E Systems	Connected Service
Car			
Specification	• Powertrain Engine • Brake System • Steering Wheel • Chassis	• Powertrain Control Module • MDPS • TPMS • Vehicle Diagnosis System	• Telematics • Wired / Wireless network • V2X (On Board Unit) • Wi-Fi / Bluetooth

Vehicle – Attack Surface & Cybersecurity Threat

▣ An Attack Surface is enlarging according to increasing an external communication

Category



	External Communication	Interface	IVN / ECUs
Systems	• Vehicle Diagnosis System • Telematics center • Wired / Wireless network • Road side unit	• PKES • Infotainment System • OBD-II port • On Board Unit	• Central gateway • In-vehicle network - CAN, Ethernet, Lin FlexRay, MOST … • ECUs - Engine, Transmission , Brake, Airbag…

Vehicle - Attack Surface & Cybersecurity Threat

▣ A Cybersecurity Threat is coming to ours

External Communication

Interface

IVN / ECUs

Category

Wired

scanner

exte
stor

3G/4G WiFi

smart key

V2X

sensors

Systems

- Vehicle Diag
- Telematics c
- Wired / Wireless network
- Road side unit

System

- OBD-II port
- Sensors

- In-vehicle network
  - CAN, Ethernet, Lin FlexRay, MOST …

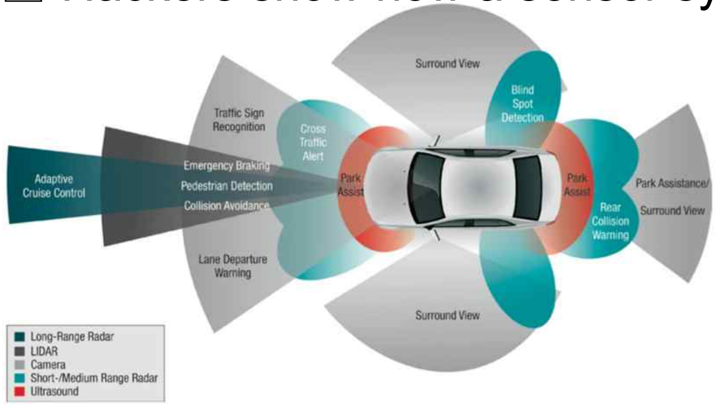
- Engine, Transmission , Brake, Airbag…

Together **We can!**

Vehicle - Autonomous Driving & Cybersecurity Threat

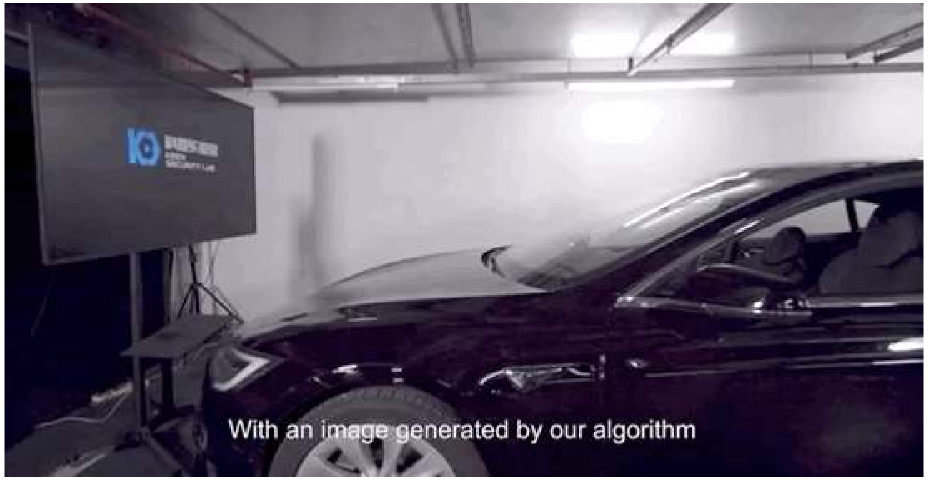
▣ An Autonomous Vehicle has a sensor system related to LIDAR and RADAR and Camera and Ultrasonic

▣ Hackers show how a sensor system can be tricked



Sensor	LIDAR	RADAR	Camera	Ultrasonic
Cost	+++	++	+	+
Size	++	+	++	+
Speed Detection	++	+++	+	+
Robust to weather	++	+++	+++	+++
Robust to day and night	+++	+++	+++	+++
Range	+++	+/++/ +++	++	+

+++ : High, ++ : Medium, + : Low



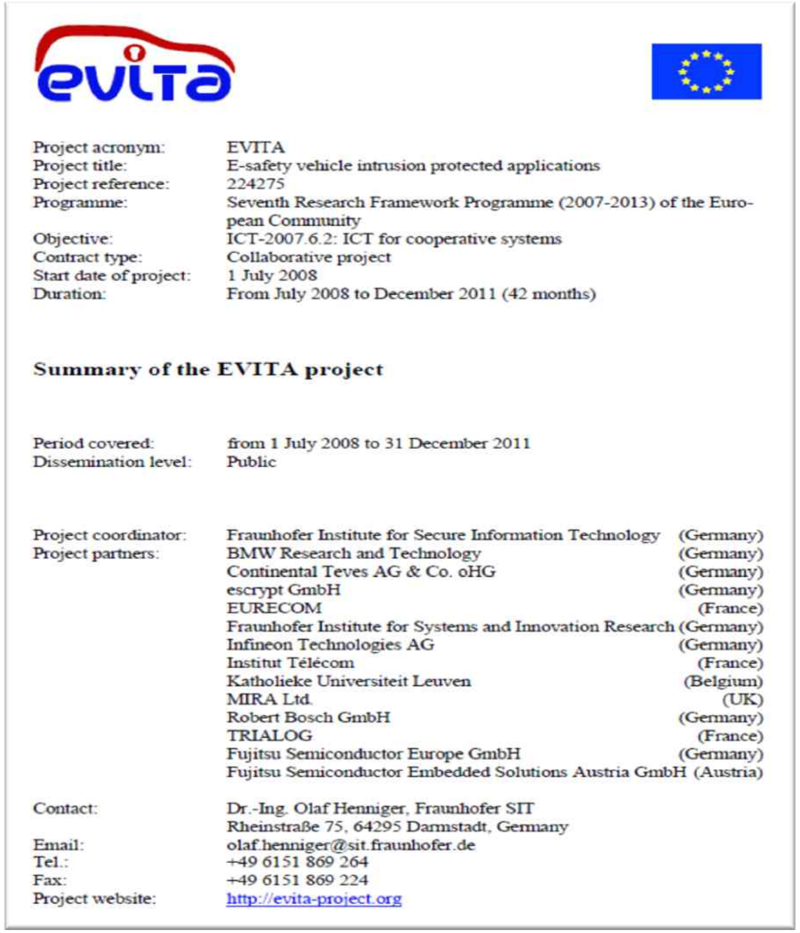
THE RESEARCHERS ARE EXPERTS, DO NOT TRY WHAT YOU ARE ABOUT TO SEE
专业安全研究行为，请勿模仿
地面干扰信息

EVITA project

- ▣ EVITA project identifies a cybersecurity requirement for a vehicle on-board network
- ▣ This project proposed an E/E Architecture and HSM class for vehicle cybersecurity

Overall

Description



evita

Project acronym:	EVITA
Project title:	E-safety vehicle intrusion protected applications
Project reference:	224275
Programme:	Seventh Research Framework Programme (2007-2013) of the European Community
Objective:	ICT-2007.6.2: ICT for cooperative systems
Contract type:	Collaborative project
Start date of project:	1 July 2008
Duration:	From July 2008 to December 2011 (42 months)

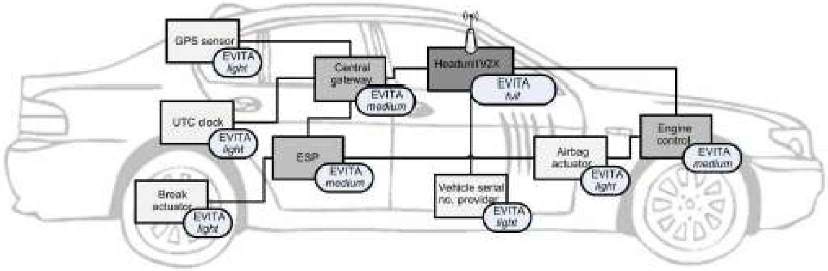
Summary of the EVITA project

Period covered:	from 1 July 2008 to 31 December 2011
Dissemination level:	Public

Project coordinator:	Fraunhofer Institute for Secure Information Technology	(Germany)
Project partners:	BMW Research and Technology	(Germany)
	Continental Teves AG & Co. oHG	(Germany)
	escrypt GmbH	(Germany)
	EURECOM	(France)
	Fraunhofer Institute for Systems and Innovation Research	(Germany)
	Infineon Technologies AG	(Germany)
	Institut Télécom	(France)
	Katholieke Universiteit Leuven	(Belgium)
	MIRA Ltd.	(UK)
	Robert Bosch GmbH	(Germany)
	TRIALOG	(France)
	Fujitsu Semiconductor Europe GmbH	(Germany)
	Fujitsu Semiconductor Embedded Solutions Austria GmbH	(Austria)

Contact:	Dr.-Ing. Olaf Henniger, Fraunhofer SIT Rheinstraße 75, 64295 Darmstadt, Germany
Email:	olaf.henniger@sit.fraunhofer.de
Tel.:	+49 6151 869 264
Fax:	+49 6151 869 224
Project website:	http://evita-project.org

Proposed Architecture



Secure on-board unit

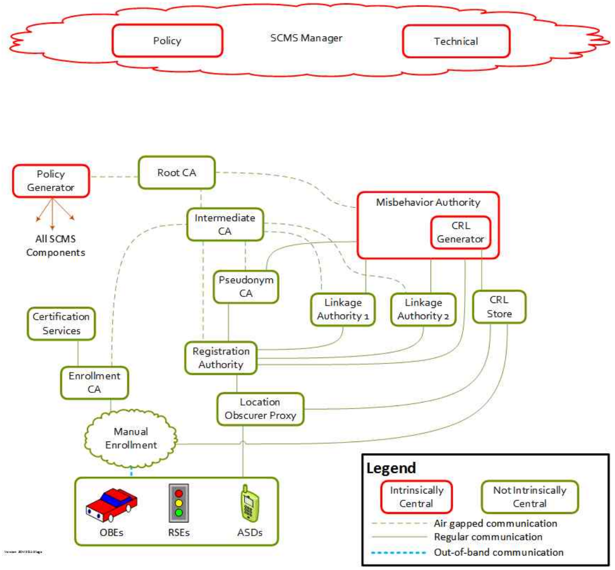
HSM	EVITA Full	EVITA Medium	EVITA Light
Internal NVM	Yes	Yes	Optional
Internal CPU	Programmable	Programmable	None
HW Crypto algo.	Asymmetric Crypto	Symmetric Crypto	Symmetric Crypto
RNG	TRNG	TRNG	PRNG
Counter	16X64bit	16X64bit	None

Hardware Security Module

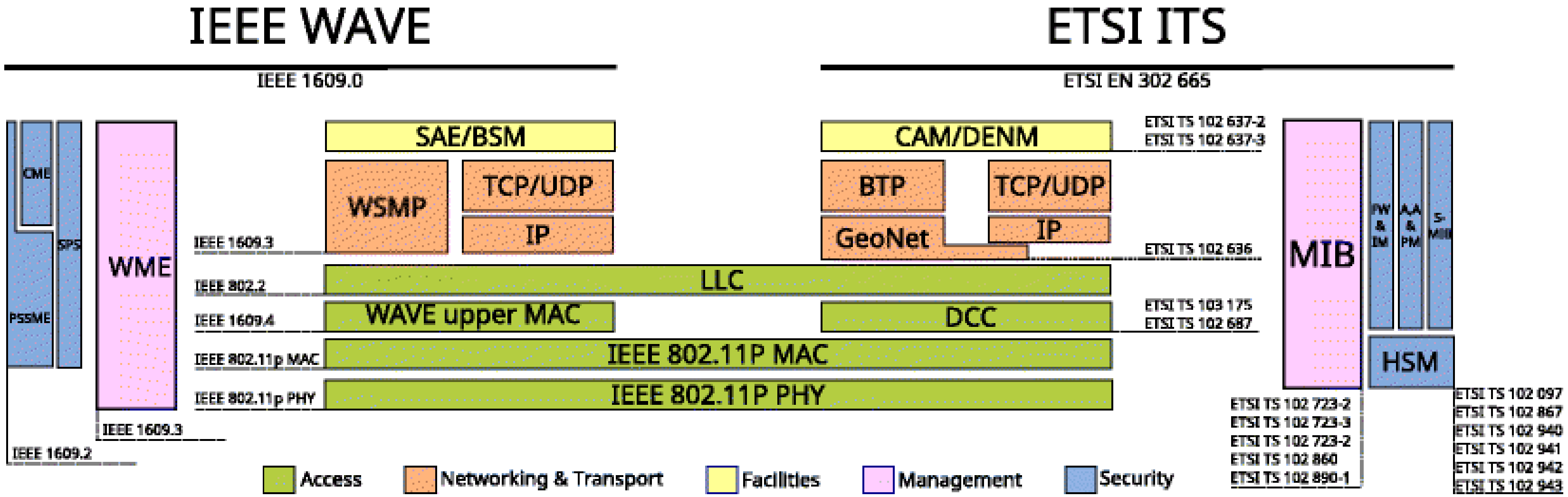
V2X security – Security Credential Management System

▣ V2X security defines a specification for a secure communication

SCMS



V2X Standardiza-tion



ITU-T SG17 Q13 Standardization

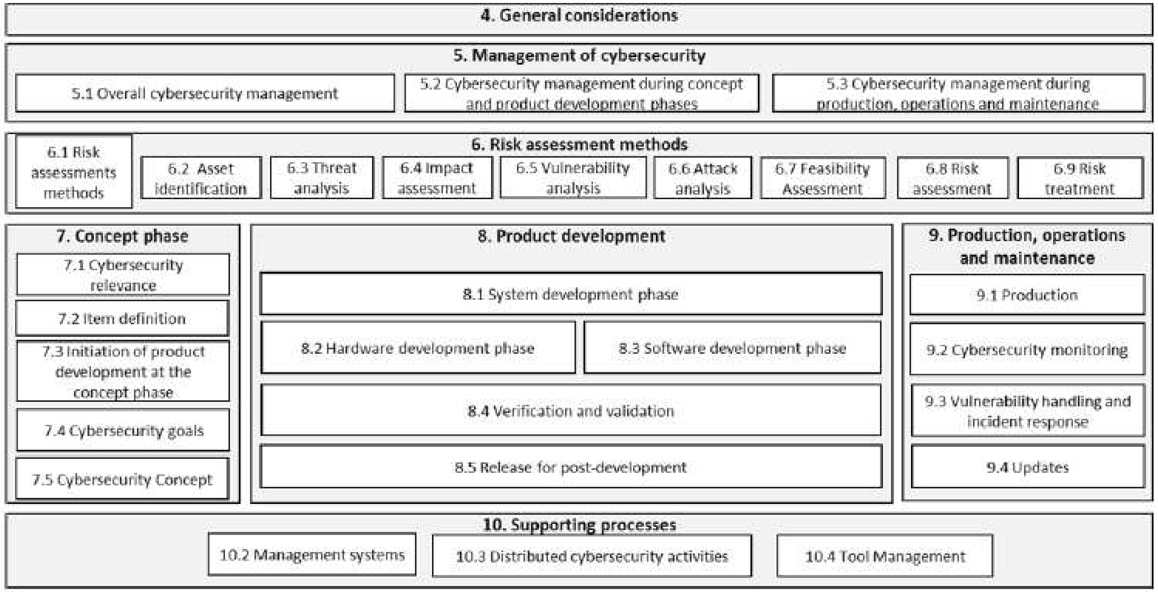
▣ ITU-T SG 17 Q13 standardization is developing a vehicle cybersecurity solution

Standards Number	Keyword	Description	Schedule (due to)
X.1373	Secure OTA	Secure software update capability for intelligent transportation system communication devices	September 2020
X.itssec4	Intrusion Detection System	Methodologies for intrusion detection system on in-vehicle systems	??
X.itssec2	V2X Security	Security guidelines for V2X communication systems	??
X.itssec3	External Devices Security	Security requirements for vehicle accessible external devices	??
X.stcv	Security Threats	security threats in connected vehicles	March 2019
X.mdcv	Misbehavior Detection (Security-related)	security-related misbehavior detection mechanism based on big data analysis for connected vehicles	December 2020

ISO/SAE 21434 : Road Vehicles Cybersecurity Engineering

▣ ISO/SAE 21434 helps to keep a secure vehicle by removing a cybersecurity vulnerability

▣ ISO/SAE 21434 considers not only a cybersecurity but also a safety



4. General considerations

5. Management of cybersecurity
- 5.1 Overall cybersecurity management
- 5.2 Cybersecurity management during concept and product development phases
- 5.3 Cybersecurity management during production, operations and maintenance

6.1 Risk assessments methods

6. Risk assessment methods
- 6.2 Asset identification
- 6.3 Threat analysis
- 6.4 Impact assessment
- 6.5 Vulnerability analysis
- 6.6 Attack analysis
- 6.7 Feasibility Assessment
- 6.8 Risk assessment
- 6.9 Risk treatment

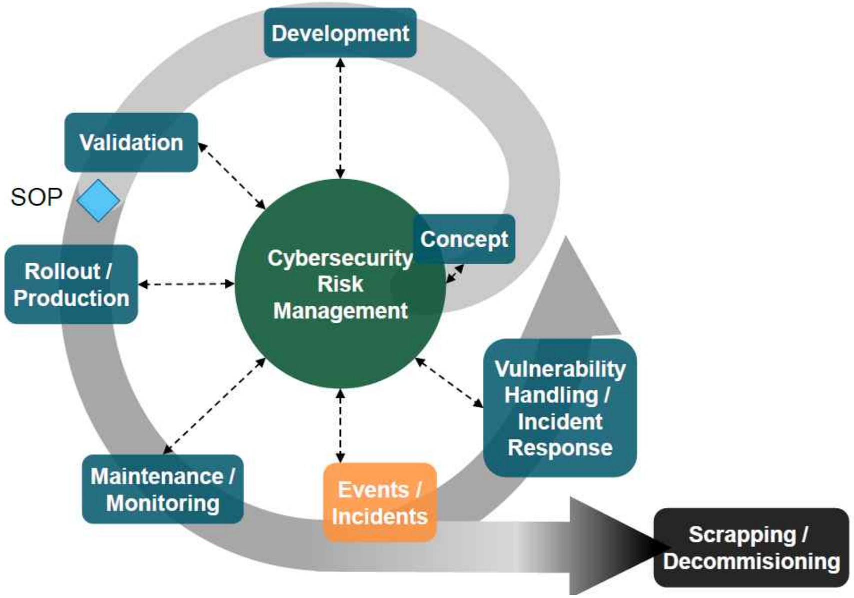
7. Concept phase
- 7.1 Cybersecurity relevance
- 7.2 Item definition
- 7.3 Initiation of product development at the concept phase
- 7.4 Cybersecurity goals
- 7.5 Cybersecurity Concept

8. Product development
- 8.1 System development phase
- 8.2 Hardware development phase
- 8.3 Software development phase
- 8.4 Verification and validation
- 8.5 Release for post-development

9. Production, operations and maintenance
- 9.1 Production
- 9.2 Cybersecurity monitoring
- 9.3 Vulnerability handling and incident response
- 9.4 Updates

10. Supporting processes
- 10.2 Management systems
- 10.3 Distributed cybersecurity activities
- 10.4 Tool Management

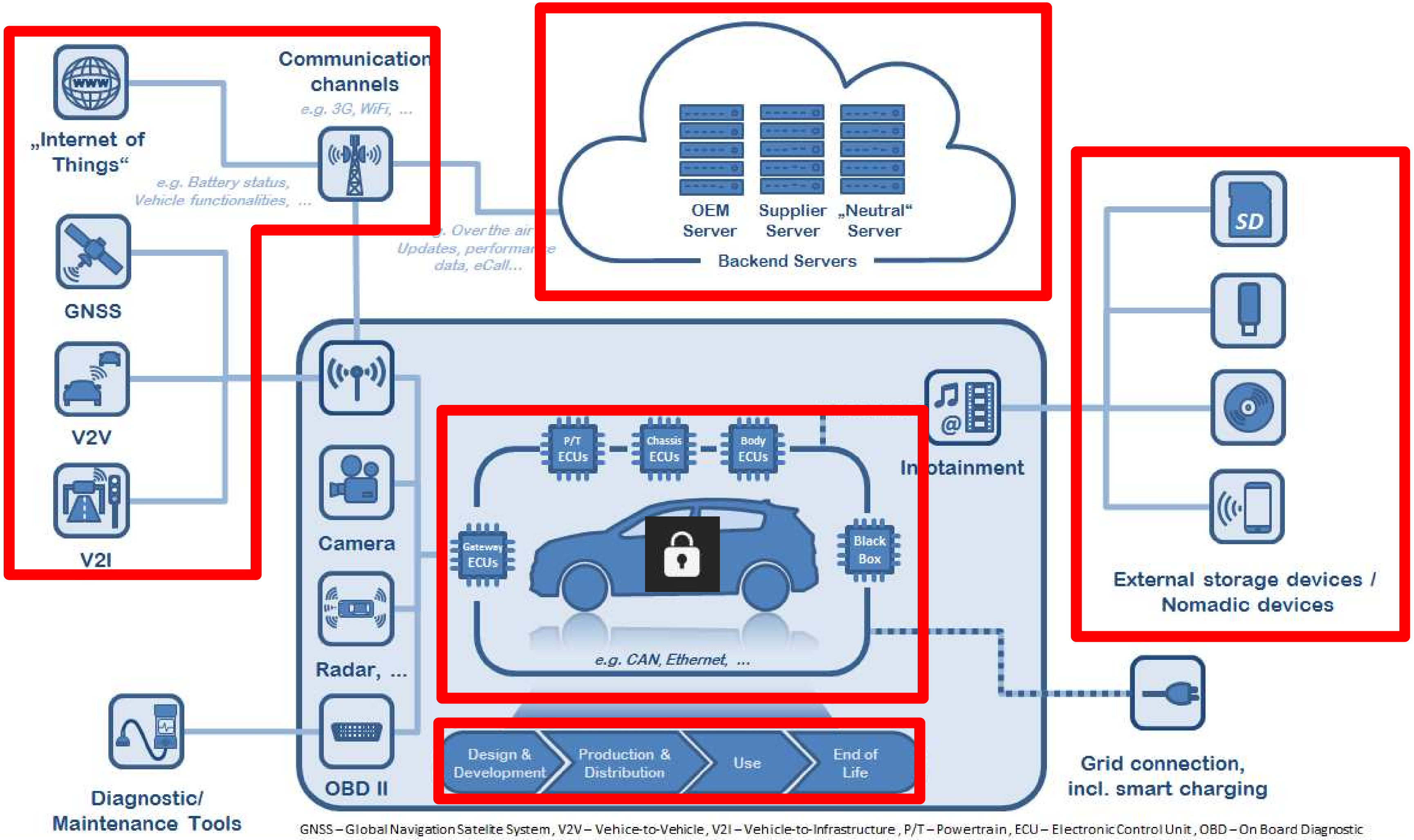
ISO/SAE 21434 overview


Development
Validation
SOP
Concept
Cybersecurity Risk Management
Rollout / Production
Vulnerability Handling / Incident Response
Maintenance / Monitoring
Events / Incidents
Scrapping / Decommisioning

Cybersecurity lifecycle

Vehicle Cybersecurity Solution

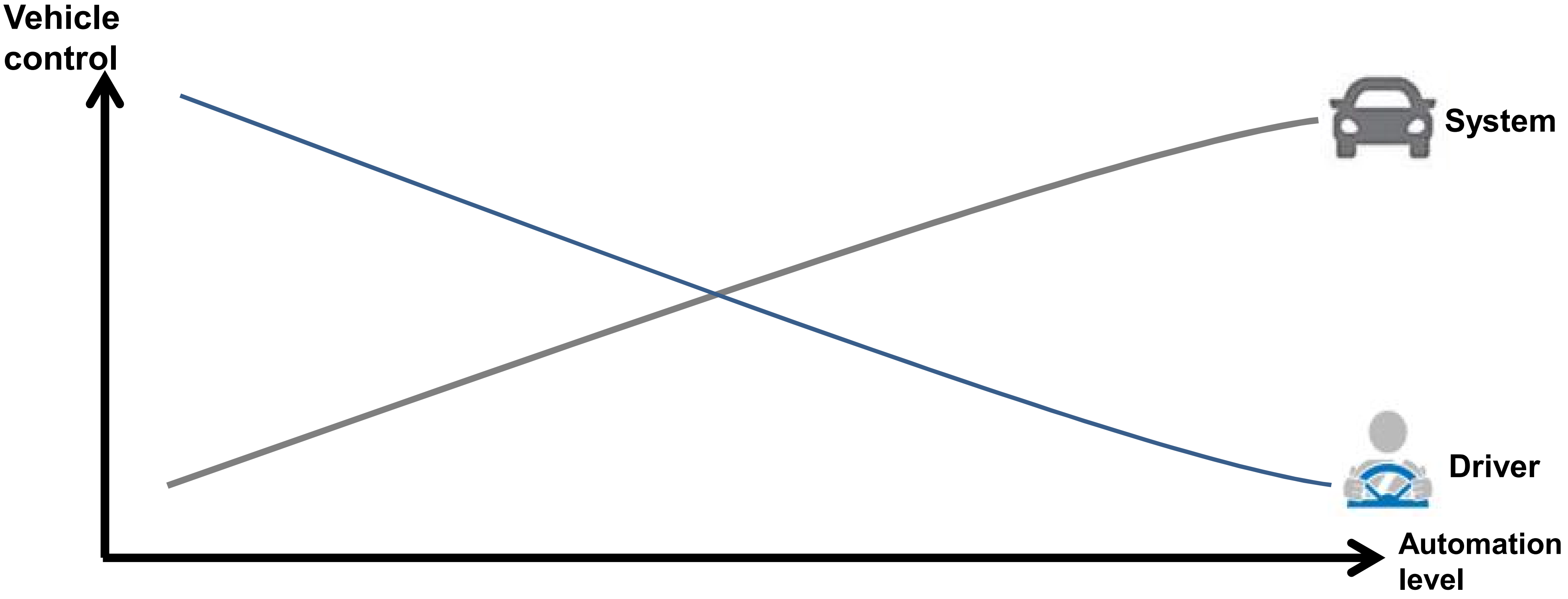
- ▣ A Standardization researches IDS, HSM, Secure OTA and V2X Security
- ▣ Vehicle Cybersecurity Solutions apply form a server to ECU for a security and safety



GNSS – Global Navigation Satelite System, V2V – Vehice-to-Vehicle, V2I – Vehicle-to-Infrastructure, P/T – Powertrain, ECU – Electronic Control Unit, OBD – On Board Diagnostic

Issues on Autonomous Vehicles

- ▣ Due to inherit danger of road vehicle, we need low latency connection with control system
- ▣ High & Full Automation Vehicle controls the vehicle dominant over human driver



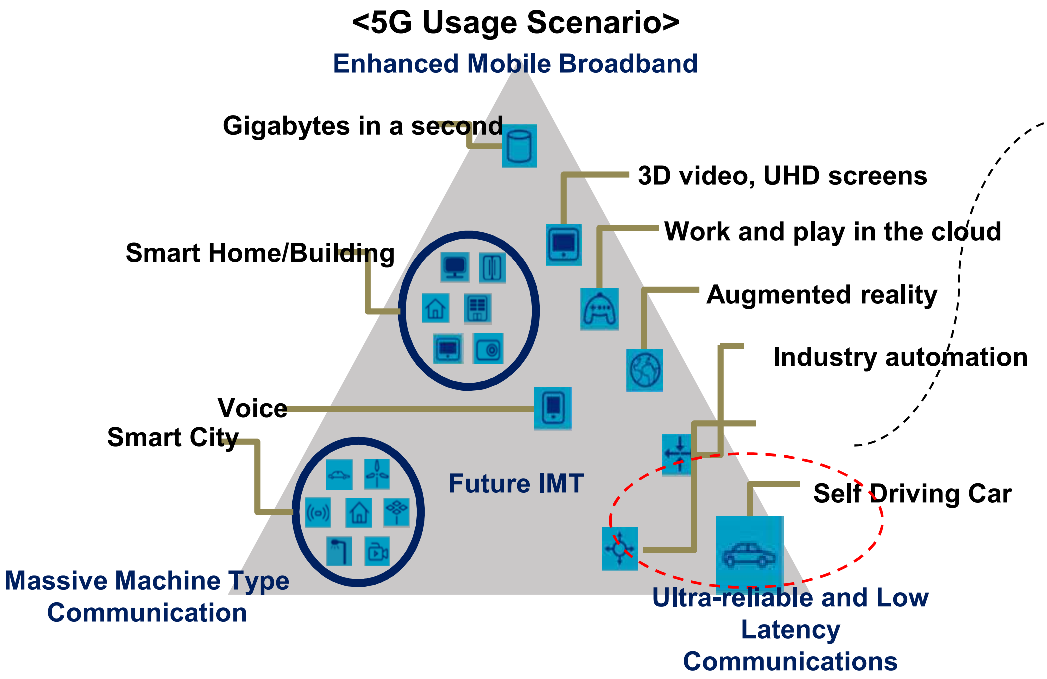
Issues on Autonomous Vehicles

▣ 영상

Cybersecurity in Autonomous Vehicle – 5G network

▣ An Autonomous Vehicle's requirement meets data latency within 1 ms

▣ High & Full Automation Vehicle requires ultra-reliable and low latency communications



Source : 5G use cases and requirements, NOKIA

TS 22.186 Requirement for autonomous driving

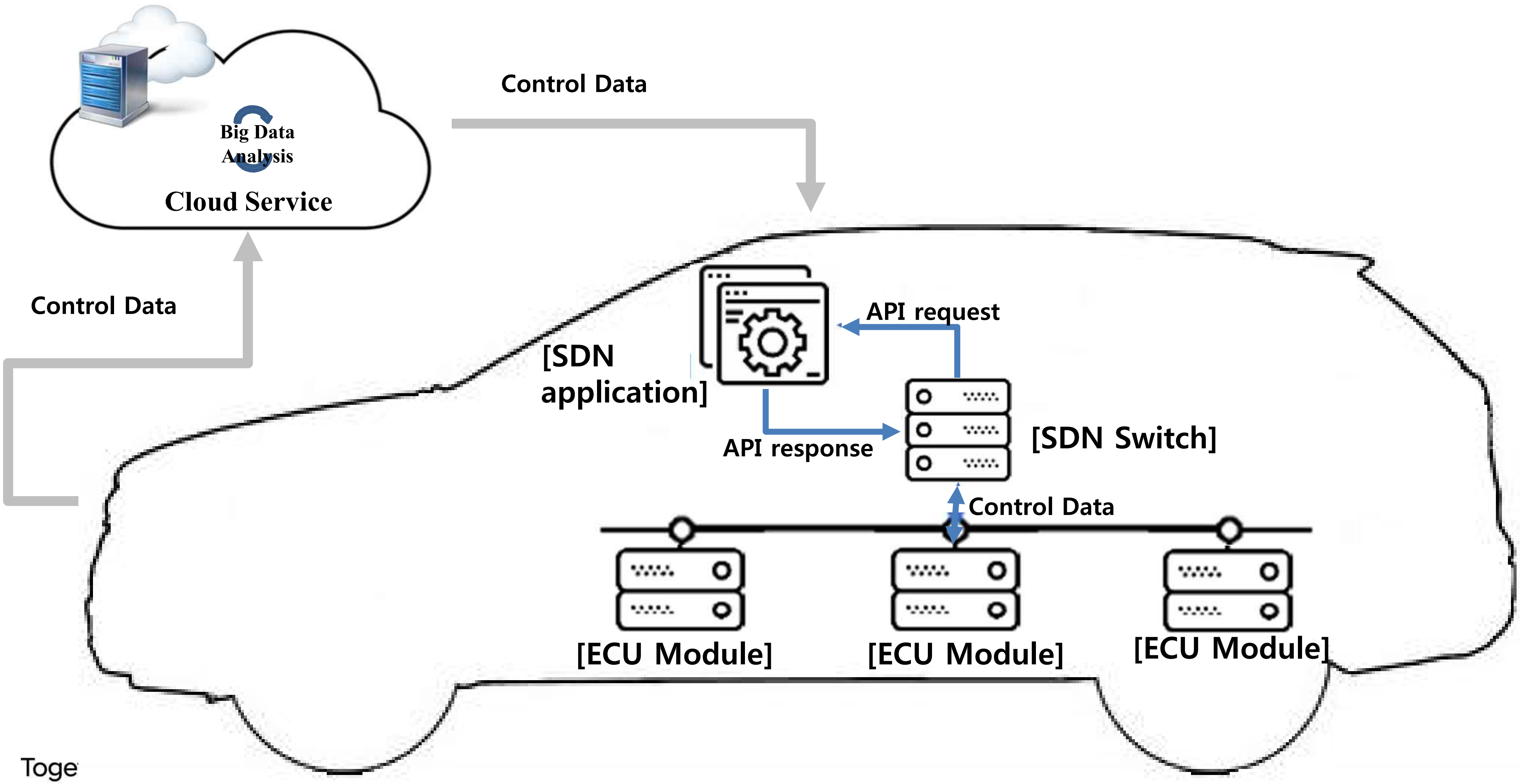
Service	Required Latency (ms)	Data Rate (Mbps)
Platooning	10	65
Advanced driving	3	53
Extended sensors	3	1000
Remote driving	5	UL:25 DL:1

구분	WAVE	LTE (Rel.15)	5G (Rel.16)
Data Rate	>54Mbps	>300Mhps	>20Gbps
Latency	~10ms	20~30ms	~1ms
Coverage	250~300m	Approx. several km	Approx. several km
Mobility	>200km/h	>160km/h	>500km/h

Cybersecurity in Autonomous Vehicle – SDN in-vehicle network

▣ An Autonomous Vehicle needs to take a reliable and real-time control by system

▣ A Software Defined Network provides a flexibility, reliability and low-latency

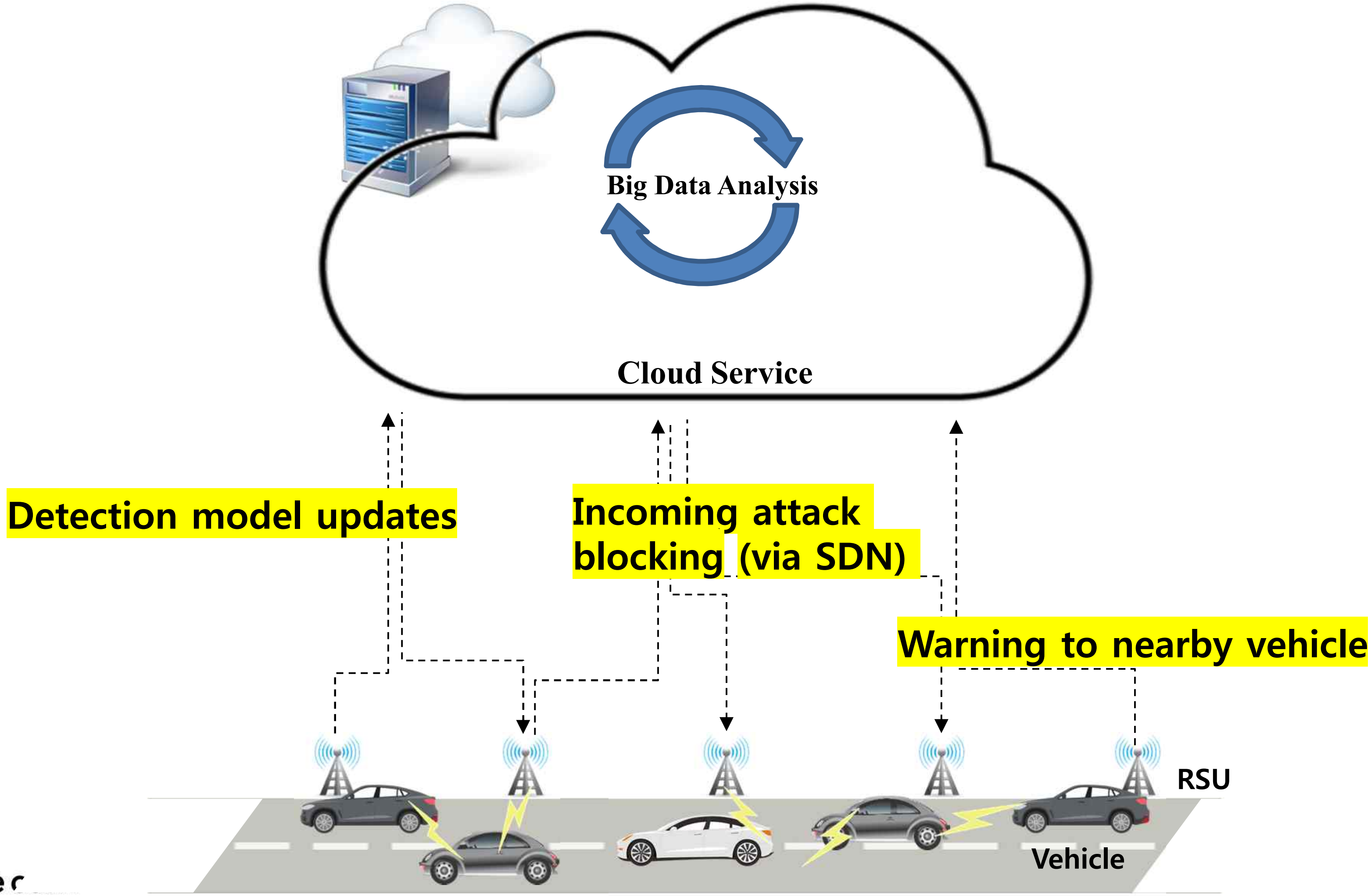


Toge

Intrusion Response System for autonomous vehicle

▣ '5G and SDN' based IRS is optimal solution to block cyber attacks in autonomous vehicles

- allowing real-time intrusion response from inside and outside attacks
- quick propagation of warning message in a wide area through 5G Network.



Conclusion

- ✓ Paradigm Shift in the Automotive Industry
- ✓ Increased Cybersecurity Threats
- ✓ Standardization for cybersecurity
- ✓ Cybersecurity Issues in an Autonomous Vehicle
- ✓ A Cybersecurity Solution in an Autonomous Vehicle