International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Technical Paper

(30 April 2021)

FSTP.SS-OTA
Standardization survey for over-the-air updating in vehicles

Summary

This Technical Paper is prepared to develop a better understanding of the various efforts in organizations concerning the technology to remotely update the software of the on-board system in automobiles with the communication function as a connected car.

Based on this survey/study, there will be a clear demonstration of the importance of quickly and accurately understanding the progress in various organizations around the world including the United Nations and the efforts to accelerate the activities for practical application. The study in this field will be continued and accelerated in the future, so it is extremely important for not only Japan to continue to participate and contribute to various activities including the subject of this study in the context of international competition and cooperation but also in a global context.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Keywords

Accountability, OTA, remote vehicle software update.

Change Log

This document contains Version 1 of the ITU-T Technical Paper FSTP-SS-OTA "*Standardization survey for over-the-air updating in vehicles*" approved at the ITU-T Study Group 16 meeting held online, 19-30 April 2021.

Editor: Hideki YAMAMOTO
Oki Electric Industry Co., Ltd.
Japan

Tel: +81 48 420 7012
Fax: +81 48 420 7138
E-mail: yamamoto436@oki.com

Table of Contents

List of Tables

List of Figures

Technical Paper ITU-T FSTP.SS-OTA

Standardization survey for over-the-air updating in vehicles

1 Scope

This Technical Paper is prepared to develop a better understanding of the various efforts in organizations concerning the technology to remotely update the software of the on-board system in automobiles with the communication function as a connected car based on accountability.

2 References

Please see the Bibliography.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Technical Paper

This Technical Paper defines the following terms:

3.2.1 over the air (OTA): OTA is a synonym for wireless.

3.2.2 over the air (OTA) reprogramming: Refers to various methods of distributing new software, configuration settings, and even updating encryption keys to devices like connected car, mobile phones, set-top boxes or secure voice communication equipment.

4 Abbreviations and acronyms

This Technical Paper uses the following abbreviations and acronyms:

ACC	Adaptive Cruise Control
ACEA	European Automobile Manufacturers' Association
ADAS	Advanced Driver Assistance System
ADS	Automated Driving Systems
AES	Advanced Encryption Standard
API	Application Programming Interface
ARIB	Association of Radio Industries and Business
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Automatic Teller Machine
BSM	Basic Safety Message
CAD	Connected and Automated Driving
CAN	Controller Area Network
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CCSA	China Communications Standards Association

CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CESG	Communications Electronics Security Group
CIS	Center for Internet Security
CMAC	Cipher-based MAC
CRL	Certification Revocation List
CU	Communication Unit
DoIP	Diagnostic Communication Over Internet Protocol
DSRC	Dedicated Short Range Communication
DT	Diagnostic Tool
EATA	European Automotive Telecom Alliance
EBC	Electronic Brake Control
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECR	ECU Configuration Register
ECU	Electronic Control Unit
EVITA	E-safety Vehicle Intrusion Protected Applications
FG-VM	Focus Group on Vehicular Multimedia
FIPS	Federal Information Processing Standards
FMVSS	Federal Motor Vehicle Safety Standard
GW	Gateway
GCM	Galois/Counter Mode
GF (p)	Galois Field (prime)
HIS	The Hersteller Initiative Software
HSM	Hardware Security Module
HUD	Head Up Display
ID	Identification
IETF	Internet Engineering Task Force
IOT	Internet of Things
IS	International Standard
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
IVI	In-Vehicle Infotainment
LAN	Local Area Network
LKA	Lane Keeping Assist
LTE	Long Term Evolution

MAC	Message Authentication Code
MOU	Memorandum of Understanding
MSIP	Ministry of Science, ICT and Future Planning
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NPO	Non-Profit Organization
NPRM	Notice of Proposed Rulemaking
OBD	On Board Diagnostics
OBD-II	On Board Diagnosis II
ODD	Operational Design Domain
ODX	Open Diagnostic Exchange
OEDR	Object and Event Detection and Response
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OSI	Open Systems Interconnection
OTA	Over The Air
PC	Personal Computer
PKI	Public Key Infrastructure
POS	Point of Sales
PRNG	Pseudo Random Number Generator
PTC	Power Train Controller
RAM	Random Access Memory
ROM	Read Only Memory
SAE	Society of Automotive Engineers
SCMS	Security Credential Management System
SHE	Secure Hardware Extension
TC	Technical Committee
TCG	Trusted Computing Group
TCU	Transmission Control Unit
TIA	Telecommunications Industry Association
TOE	Target of Evaluation
TPM	Trusted Platform Module
TR	Technical Report
TRNG	True Random Number Generator
TS	Technical Specification
TSAG	Telecommunication Standardization Advisory Group
TSDSI	Telecommunications Standards Development Society, India

TTA	Telecommunications Technology Association
TTC	The Telecommunication Technology Committee
UDX	Unified Diagnostic Services
UID	User ID
URL	Uniform Resource Locator
USB	Universal Serial Bus
USDOT	United States Department of Transportation
UTC	Universal Time, Coordinated
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to X (anything)
VGP	Vehicle Gateway Platform
W3C	World Wide Web Consortium
WG	Working Group
XML	Extensible Markup Language
5GAA	5G Automotive Association
5GMF	The Fifth Generation Mobile Communication Promotion Forum

5 Introduction ([b-1])

As a connected car in the sense of connecting to a general-purpose network, one of the functions commonly required in various expected use cases is remote software update of in-vehicle systems. Although this function has different names such as reprogramming and flushing, and different processing targets, various organizations and organizations are proposing/discussing standardization. Among them are security modules including chips, use cases, security requirements, communication standards, application programming interfaces (APIs), and consideration/publication/proposal based on their operation, which are described in detail in clauses 3 to 5 of this Technical Paper. Volunteers are invited to assist in the proposal to quickly grasp, understand, and incorporate them into Japanese policies, and a Working Group on Remote Vehicle Renewal is established within the Connected Car Expert Committee. Specifically, various activities related to over-the-air (OTA) technology among remote software updates were obtained from public information, examined, and analysed from the viewpoint of in-vehicle system remote update technology, and a report is prepared.

The first edition of this report is based on public information as of the end of September 2017, unless otherwise specified. After that, in light of the recent intense movements such as the publication of recommendations of [b-68] UNECE WP.29 in September 2019, volunteers were recruited again, and with the support of all concerned parties, a working group was formed to revise the report. The contents were updated as the second edition based on the information released at the end of September 2019.

This report is prepared for the purpose of developing a better understanding of the processes in various organizations on the progress of the technology to remotely update the software of the on-board system in the automobile with the communication function as a connected car. Through this survey, it is found that various studies on remote updating (software, the information they handle,) of in-vehicle systems are actively being conducted in each organization/institution. It is confirmed in this report that the security required to realize remote update is very important, and that it is important to strengthen measures against security attacks and to ensure accountability by using chips and others based on open standard specifications.

In order to promote remote updating of in-vehicle systems, the value, effectiveness and convenience in specific use cases should be officially recognized. As is widely known, the automotive industry is extremely cost-conscious. As Japan, the United States, and Europe are considering measures for automated driving and recalls that do not require the transport of the vehicle itself to the plant, remote updating of the in-vehicle system is considered to be significant. In this respect, it is very important that this revised edition shows that discussions and standardization in the United Nations, which has influence in the world, are progressing as UNECE WP.29 activities, and that it was published as a recommendation in September 2019. At the same time, it is considered to be meaningful that the value expansion of the accountable security (accountability) could be presented.

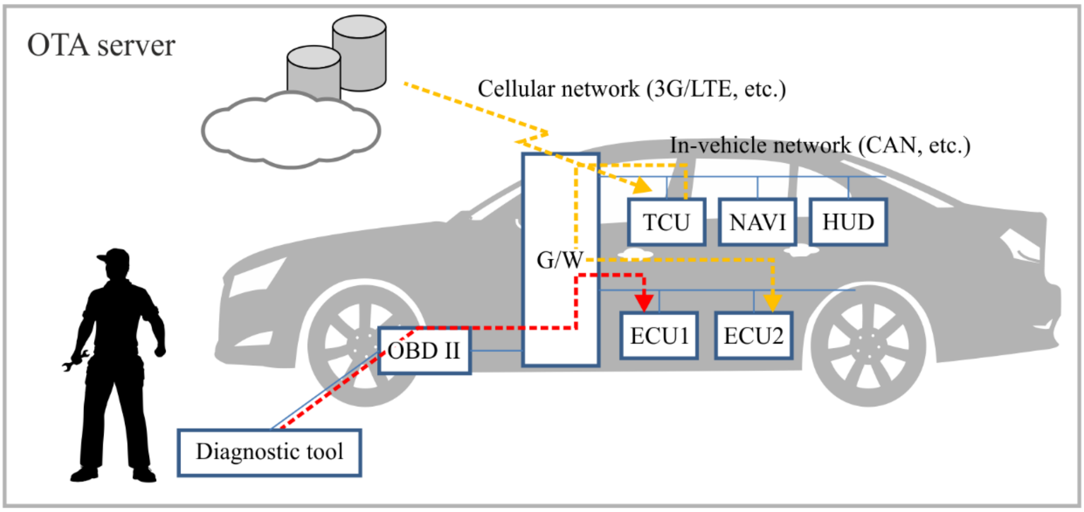
Based on this survey/study, the importance is reiterated of the need to quickly and accurately keep abreast with the developments in various organizations around the world including the United Nations and the need to accelerate the activities for practical application in Japan. The study in this field will be continued and accelerated in the future, so it is extremely important for Japan to continue to participate, contribute, and contribute to various activities including the subject of this study in the context of international competition and cooperation.

We eagerly hope that this report with the Keyword of Accountability will be of use to the concerned industry.

6 Trends in standardization of remote software updating technologies in Japan and overseas

Dozens of electronic control units (ECUs) are installed in automobiles to realize various functions such as driving control (engines, brakes, steering, etc.), advanced driver assistance system (ADAS) control (ACC, LKA, etc.), multimedia (car navigation, audio, HUD, etc.), and body control (power window, lighting control, etc.). Software is running on each ECU and these functions are realized by performing cooperative control via the on-board network. The software of each ECU mounted on an automobile is recorded in the memory of each ECU before shipment of the vehicle, and it may be updated after shipment of the vehicle in order to improve functions or to cope with malicious attacks. The software update after the vehicle shipment is called reprogramming. Reprogramming typically involves dealers and auto repair shops (hereinafter referred to as dealers, etc.). In such a case, the automobile mechanic connects the diagnostic tool by wire. However, in recent years, as Tesla and others have put it into practical use, a technology has been put into practical use to remotely update (without the assistance of a specialist) software by wirelessly connecting a vehicle to a vehicle manufacturer's server, and this technology is called remote software update (OTA reprogramming).

Although OTA reprogramming is limited to updating the ECU software (OS, Apps), it is sometimes referred to as OTA reprogramming in a broad sense, including software configuration data and map data of car navigation systems. In this Technical Paper, the broader sense of reprogramming is considered.


OTA server
Cellular network (3G/LTE, etc.)
In-vehicle network (CAN, etc.)
TCU
NAVI
HUD
G/W
ECU1
ECU2
OBD II
Diagnostic tool

FSTP.SS-OTA(21)_F6-1

(Colour convention – Red for traditional wired reprogramming, orange for OTA reprogramming)

Figure 6-1 – Reprogramming example

This Technical Paper focuses on the use cases of remote software update for automotive systems and investigated the activities of government and organizations such as academia, industry, and non-profit organizations (NPOs) worldwide. From the public information of the organization in which each member participating in this working group has knowledge, content related to the keyword "OTA Reprogramming" was selected and compiled into a common template. The results of the work are presented in clauses 7 to 9. As a result, it was possible to clarify the activities of each organization toward the realization of remote software update.

Most of the public information referred to in this Technical Paper is as of the end of September 2019, or unless otherwise specified.

As there are various contents in the activities and the formulation documents of the related organizations, the survey results are classified into three levels: vehicle level in clause 7, system level (communications) in clause 8, and system level (components) in clause 9. The clause for each organization provides an overview of its organization and its publications (release situation). Regarding each issue, positioning as an outline and the object were clarified first, and description contents and future prospect on the remote software update were summarized. It is classified into provisions, recommendations, guidance, specifications, technical reports, proposals, etc., and whether they are legally binding or not is described. As the objects, the following were described: Communication technology (in-vehicle LAN, in-vehicle wireless communication, etc.), update procedure, security requirement, hardware, use case (automatic driving, etc.), life cycle (operations, diagnostics, etc.), update object (applications, map data, and so on).

7 Survey by related organizations: Vehicle level

The scope of this report is a survey on trends in standards. In this clause, however, the scope of the survey is expanded to include vehicle-level standards and regulations established by UNECE, etc., and extracted requirements for remote software update (OTA reprogramming).

7.1 5GAA ([b-2] to [b-4])

7.1.1 Introduction to the organization

The 5G Automotive Association (5GAA)[1] is an international organization consisting of automobile manufacturers, semiconductor manufacturers, etc.

Its main activities include standardization for communication solutions and autonomous driving to meet social needs for connected mobility and safety. In March 2017, it signed a memorandum of understanding with EATA to collaborate on connected and self-driving solutions.[2]

7.1.2 Introduction of standards and publications

Connected cars are expected to use 5G bandwidth, but there is no mention of OTA at this time. The case for cellular vehicle to X (V2X) for safety and cooperative driving (November 2016) is presented in the link provided in the footnote[3]. It only proposes a cellular V2X that can be seamlessly deployed from 4G LTE to 5G. 5GAA Report shows superior performance of Cellular V2X vs DSRC (October 2018)[4]. The performance comparison between cellular V2X and DSRC is discussed in various execution environments. Toward fully connected vehicles: Edge computing for advanced automatic communications (December 2017)[5]. Edge computing is discussed as one of the requirements for autonomous vehicles.

Clauses 7.1.2.1 to7.1.2.3.3 outline each standard or publication mentioned in clause 7.1.2 including a description of the parts that are related to remote update.

7.1.2.1 The case for cellular V2X for safety and cooperative driving[1]

7.1.2.1.1 Summary

Issue	23 November 2016
Positioning	**Technical report** (Not legally binding) White paper
Target	**Use cases and communication technologies** ADAS and connected and automated driving (CAD)

7.1.2.1.2 Items related to remote software updates

However, in order to realize a safer autonomous vehicle (ADAS and CAD) in the future, it is necessary to shift to 5G. It needs the low latency and high bandwidth offered by 5G to connect to everything around it, not just sensors and radar. It states that cellular V2X, which is part of the 3GPP standard family, has a deployment path from 4G LTE to 5G, which is why 5GAA promotes cellular V2X.

7.1.2.1.3 Future outlook

Nothing in particular.

[1] http://5gaa.org/

[2] http://www.prnewswire.com/news-releases/5g-automotive-association-and-european-automotive-telecom-alliance-sign-a-partnership-mou-615215444.html

[3] http://5gaa.org/news/white-paper-placeholder-news-for-testing/

[4] http://5gaa.org/news/5gaa-report-shows-superior-performance-of-cellular-v2x-vs-dsrc/

[5] http://5gaa.org/news/toward-fully-connected-vehicles-edge-computing-for-advanced-automotive-communications/

7.1.2.2 5GAA Report shows superior performance of Cellular V2X vs DSRC[2]

7.1.2.2.1 Summary

Issue	30 October 2018
Positioning	**Technical report** (Not legally binding) White paper
Target	**Use cases and communication technologies** Cellular V2X and DSRC

7.1.2.2.2 Items related to remote software updates

There is no direct description of remote software updates. Here, the performance of cellular V2X and DSRC is compared in various environments such as antenna characteristics and positional relationship between the vehicle and obstacles. It is assumed that the wording of the "The Case for Cellular V2X for Safety and Cooperative Driving" published in 2016 will be examined.

The following eight tests were conducted. Consistently, cellular V2X results in better performance than DSRC.

– Lab cabled congestion control

– Lab cabled Tx and Rx tests

– Field line-of-sight (LOS) range tests

– Field non-line-of-sight (NLOS) range tests

– Lab cabled test with simulated C-channel interference

– Lab cabled near far test

– Field C-existence with Wi-Fi 80 MHz bandwidth in UNI-3

– Field C-existing of V2X with adjacent DSRC carrier

7.1.2.2.3 Future outlook

Nothing in particular.

7.1.2.3 Toward fully connected vehicles: Edge computing for advanced automatic communications

7.1.2.3.1 Summary

Issue	15 December 2017
Positioning	**Technical report** (Not legally binding) White paper
Target	**Use cases and communication technologies** Self-driving cars and edge computing

7.1.2.3.2 Items related to remote software updates

Real-time services are required between self-driving cars and cloud servers, and this paper discusses how edge computing technology can be used for real-time services, especially in the event of an accident.

V2X applications that take advantage of edge computing technologies are classified into four categories: safety, convenience, advanced driving assistance, and vulnerable road user. The other three take advantage of the real-time nature of edge computing, but convenience cites low-cost communications with original equipment manufacturer (OEM) servers as the reason.

7.1.2.3.3 Future outlook

Nothing in particular.

7.2 ACEA ([b-5] to [b-6])

7.2.1 Introduction to the organization

ACEA (European Automobile Manufacturers Association) is a trade association of European automobile manufacturers headquartered in Brussels, Belgium.

7.2.1.1 ACEA principles of automobile cybersecurity[6]

7.2.1.1.1 Summary

Issue	September 2017
Positioning	The issue itself is not legally binding.
Target	Cybersecurity of automobiles

With the increasing number of connected cars, the risk of cyber-attacks on automobiles has increased, and this document describes the following six key principles:

1) Cultivating a cybersecurity culture
2) Adapting a cybersecurity life cycle for vehicle development
3) Assessing security functions through testing phases: self-auditing and testing
4) Managing a security update policy
5) Providing incident response and recovery
6) Improving information sharing against industry actors

7.2.1.1.2 Items related to remote software updates

Items related to software update include the following.

(1) Adapting a cybersecurity life cycle for vehicle development

This clause refers to secure ECUs, secure network communication, secure E/E architecture, and secure extended vehicles, and refers to the following three items for secure extended vehicles.

- Secure internet and back-end communication
- Secure remote fleet management systems (FMS) and remote diagnostics
- Secure over-the-air software updates

This clause also mentions security logs, communication protection, control keys and access, user data protection, identification/authentication/authorization as security functions, and explains security logs and controls keys and access as follows:

- *Security logs: Security events should be logged when required. Access to the security logs are documented and protected from disclosure to unauthorized users. Furthermore, when required, security logs should be sent off-board, through a secure channel, for safe storage.*

Control keys and access: Keys are managed safely, and the use of a trusted infrastructure (public key infrastructure) is enriched.

[6] http://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf

(2) Managing a security update policy

This clause refers to the preparation of security update functions as necessary for cyber threats, and OTA is described below:

– *In any case, while secure over-the-air updates seem may for many components, the need for physical updates might be present in the years to come in a number of cases.*

7.2.1.1.3 Future outlook

Although the publication itself is not legally binding, it states that ACEA is used for recommendations to ENISA, UNECE/WP.29, Auto-ISAC, etc. It also refers to ACEA member companies for further discussion in ISO/SAE 21434[7].

7.3 SAE ([b-7] to [b-18])

7.3.1 Introduction to the organization

SAE International[7] is a non-profit organization whose members are engineers and specialists in the aircraft, passenger car, commercial vehicle, and other industries.

The main activity is the establishment of standards by the technical committee. The organization also supports educational programs such as A World In Motion and Collegiate Design Series.

The Board of Directors is a global organization with more than 128,000 members and is composed of people from various fields.

7.3.2 Introduction of standards and publications

Here, the activities of SAE on OTA are introduced.

Firmware Update Over The Air (FOTA) for Automotive Industry (August 2007)[8]

– In addition to the cost of updating the software due to the recall, the company also says that the time it takes to disable a vehicle by bringing it to a dealer is a problem.

NOTE – OTA is sometimes called FOTA, but it is basically used in the same sense.

Over the Air Software Update Realization within Generic Modules with Microcontrollers Using External Serial FLASH (March 2017)[9]

– As another method for reducing the processing time of software update, an installation in which an external serial flash memory is added to each ECU has been introduced. In this method, each ECU can operate in a local memory during a download to an external serial flash memory so that the vehicle can continue to be used.

Analysis of Software Update in Connected Vehicles (April 2014)[10]

– Examples include 3G/4G modems, Wi-Fi, and OTA with smartphones (Bluetooth or USB tethering), all of which are proven in the telecom industry. At the same time, this paper conducts a questionnaire survey in North America. For each use case, the advantages and disadvantages of the requirements are shown, and the OTA readiness of each OEM is shown.

OTA flashing: the challenges and solutions (January 2016)[11]

[7] http://www.sae.org/

[8] https://www.sae.org/publications/technical-papers/content/2007-01-3523/

[9] https://www.sae.org/publications/technical-papers/content/2017-01-1613/

[10] https://www.sae.org/publications/technical-papers/content/2014-01-0256/

[11] https://www.sae.org/news/2016/01/ota-reflashing-the-challenges-and-solutions

– With the success of Tesla, the problems are being sorted out. Problems include the processing time for remote software updates, the need for integration checks after software updates, and the memory required for rollback.

Feasibility Study for a Secure and Seamless Integration of Over the Air Software Update Capability in an Advanced Board Net Architecture (April 2016)[12]

– Unlike the telecom industry, remote software updates in the automotive industry require a secure and seamless implementation. The feasibility of software updates for this requirement has been investigated and reported.

Safe and Secure Software Updates Over The Air for Electronic Brake Control Systems (September 2016)[13].

– If the target of the remote software update is the electronic brake control (EBC) system, the security measures should be expanded. As examples, the security architecture by TPM of HSM and TCG of SHE and EVITA is introduced.

OTA updating bringing benefits, challenges (August 2016)[14]

– It is shown that remote software updates can be used not only to provide software patches but also to add functionality.

Improvement of the Resilience of a Cyber-Physical Remote Diagnostic Communication System against Cyber Attacks (April 2019)[15]

– It analyses the vulnerability of cyber physical systems for remote diagnosis and remote update to cyber attacks and describes how to improve resilience.

System Engineering for Automated Software Update of Automotive Electronics (April 2018)[16]

– This paper discusses the update architecture of the automobile domain in comparison with the update of personal computer (PC), etc. Stable interface design for updates is important, and it shows how to measure its effectiveness.

Measures to Prevent Unauthorized Access to the In-Vehicle E/E System, Due to the Security Vulnerability of a Remote Diagnostic Tester (March 2017)[17]

– It discusses its vulnerability in the architecture of remote diagnostics. It then describes an architecture for enhanced security.

Over-the-air (OTA) programming allows remote software updates: Over-the-air affair (February 2019)[18]

– Remote updates can be used for maintenance as well as adding new features, according to the report. There is also a mention of the 5G update.

OTA will drive cybersecurity programs (April 2018)[19]

– It states that the hardware and software design of Internet-connected vehicles must take cybersecurity into account.

[12] https://www.sae.org/publications/technical-papers/content/2016-01-0056/

[13] https://www.sae.org/publications/technical-papers/content/2016-01-1948/

[14] https://www.sae.org/news/2016/08/ota-updating-brings-benefits-challenges

[15] https://www.sae.org/publications/technical-papers/content/2019-01-0112/

[16] https://www.sae.org/publications/technical-papers/content/2018-01-0750/

[17] https://www.sae.org/publications/technical-papers/content/2017-01-1689/

[18] https://www.sae.org/news/2019/02/over-the-air-remote-programming

[19] https://www.sae.org/news/2018/04/ota-will-drive-cybersecurity-programs

Clauses 7.3.2.1 to 7.3.2.12.3 outline each of them and the parts related to remote update are described.

7.3.2.1 Firmware update over the air (FOTA) for automotive industry

7.3.2.1.1 Summary

Issue	5 August 2007
Positioning	**Technical report** (Not legally binding)
Target	**Communication technologies, update procedures, use cases** Maintenance, repair, and service operation

7.3.2.1.2 Items related to remote software updates

At this point, the telecom industry was already using OTA technology for remote software updates. Assuming the method is applied to the automotive industry, several use cases are analysed, and the benefits and challenges are described. However, this report is based on the case from 2001 to 2005.

(1) Security cost

– One of the reasons for the percentage of warranty costs paid by OEMs relative to product sales is software-related recalls. As a solution to this problem, the company says that using OTA technology to update remote software not only reduces the cost of coverage, but also has customer benefits, such as not having to bring a vehicle to a dealer for every recall.

(2) Software update use cases

– There are three use cases for software updates: recall, periodic inspection, and claims. Software updates include cable-based (wire) and over-the-air updates.

7.3.2.1.3 Future outlook

Nothing in particular.

7.3.2.2 Over the air software update realization within generic modules with microcontrollers using external serial FLASH

7.3.2.2.1 Summary

Issue	28 March 2017
Positioning	**Technical report** (Not legally binding)
Target	**Update procedure** Process design

7.3.2.2.2 Items related to remote software updates

An advantage of software update through an on board diagnostics (OBD) interface at a dealer or the like is that the processing time of the software update is not visible to the user. This is because only the total time of various other services performed in the factory is visible. However, the user cannot use the vehicle during that time.

Similarly, if the update data is downloaded to the external serial flash memory, the time is not specified to the user. In the meantime, the user's vehicle can operate. This paper provides an example implementation.

Bottlenecks in the traditional way:

– The update data downloaded to the central storage is distributed to each ECU, but not all ECUs can be distributed simultaneously. Delivery takes place over the CAN bus from the OBD port, but the transfer rate is not fast. During this time, the vehicle cannot operate, so this becomes an issue.

A/B swap:

– A memory required for each ECU is prepared in two pages of A and B, and update data are transferred to the memory B. Since the ECU is executed by the memory A during this time, the vehicle can be operated. When the completion of the update is confirmed, the ECU restarts after swapping from memory A to memory B.

Serial flash memory:

– Serial flash memory is easily available and inexpensive to add to each ECU. Since the ECU is executed in the local memory, the update data can be transferred to the serial flash memory in parallel with its execution. In addition, there is an advantage that various ECUs can be updated simultaneously. This paper gives a concrete example of this implementation. This implementation also refers to memory implementation for rollback in case of update failure.

7.3.2.2.3 Future outlook

Nothing in particular.

7.3.2.3 Analysis of software update in connected vehicles

7.3.2.3.1 Summary

Issue	1 April 2014
Positioning	**Technical report** (Not legally binding)
Target	**Communication technologies, use cases, and update procedures** Embedded software and electronic controls

7.3.2.3.2 Items related to remote software updates

It categorizes use cases by means of communication (3G/4G, Wi-Fi, Bluetooth, USB tethering) in an OTA update to show the advantages and disadvantages to the requirements. These OTA updates have been shown to be a proven method for the telecom industry.

The requirements shown here are secure communication, high-speed communication, communication cost, presence or absence of an additional device, area restriction of wireless communication, memory for rollback, and propriety of forced update. The report demonstrates how the current OEMs (Tesla, Chevy Volt, Mercedes, Chrysler, Audi, Toyota) are using the OTA update in North America.

The latter half of the report shows the results of interviews with users of various ages in North America about their level of interest and expectations regarding in-vehicle software updates.

7.3.2.3.3 Future outlook

Nothing in particular.

7.3.2.4 OTA reflashing: The challenges and solutions

7.3.2.4.1 Summary

Issue	21 January 2016
Positioning	**Article** (Not legally binding)
Target	**Use case** Human factors and safety

7.3.2.4.2 Items related to remote software updates

This paper describes problems and solutions in OTA reprogramming (referred to here as flashing) of flash memory.

Reprogramming processing time

– Tesla estimates 45 minutes and more than 1 day for reprogramming at dealerships. The problem lies in data bandwidth, which could be solved by using Wi-Fi or cellular networks.

Intermodule integration

– After the remote software update, an integration check between the modules connected to the in-vehicle CAN is required. The objective is to ascertain which modules have been updated, what impact those updates will have, and a rollback feature in case the installation fails.

7.3.2.4.3 Future outlook

Nothing in particular.

7.3.2.5 Feasibility study for a secure and seamless integration of over the air software update capability in an advanced board net architecture

7.3.2.5.1 Summary

Issue	5 April 2016
Positioning	**Technical report** (Not legally binding)
Target	**Update procedure, hardware, security** Architecture, electronic control unit, and cybersecurity

7.3.2.5.2 Items related to remote software updates

Compared to the cellular industry, OTA in the automotive industry has unique challenges, including ensuring safety. From the viewpoint of the driver, the following three points are listed as requirements.

– OTA must withstand malicious attacks

– OTA must be quick and not hamper vehicle availability

– The safety of the vehicle in operation must be ensured

It examines the feasibility of these requirements and provides specific examples of update flows, security architectures, etc.

7.3.2.5.3 Future outlook

Nothing in particular.

7.3.2.6 Safe and secure software updates over the air for electronic brake control systems

7.3.2.6.1 Summary

Issue	18 September 2016
Positioning	**Technical report** (Not legally binding)
Target	**Use case** Electronic brake control

7.3.2.6.2 Items related to remote software updates

When applying OTA in an EBC system:

– Ensure vehicle safety and security

– Ensure vehicle availability

It is explained by showing examples that it is necessary to consider the following two points.

The former, security, means protecting vehicles from malicious attacks. To do this, a firewall must be installed to protect the encryption key and the memory that stores the key. The system using TPM and HSM is mentioned as a concrete implementation example.

During the update, the vehicle needs to be stopped for safety reasons. During this time, the EBC system is down. This affects the availability of the latter. An example of an implementation that reduces this downtime while extending safety measures is shown in the following three steps.

- Analysis of in-vehicle network configuration and data flow
- Example of implementing a security function on an in-vehicle network
- Implementation options to reduce EBC system downtime

7.3.2.6.3 Future outlook

Nothing in particular.

7.3.2.7 OTA updating bringing benefits, challenges

7.3.2.7.1 Summary

Issue	14 August 2016
Positioning	**Article** (Not legally binding)
Target	**Update target, update procedure** Parts and components

7.3.2.7.2 Items related to remote software updates

Similar to the article on OTA flashing (21 January 2016), the report suggests that using Wi-Fi to lower communications costs may be an option and that integration checks are necessary. Unlike this Technical Paper, it does not limit its focus to flash memory, but instead broadly describes the benefits and challenges of OTA.

- Reprogramming has the potential to be used not only for patches but also for adding functionality.
- Require extra memory for rollback.
- OEMs must collect data on vehicle components.

7.3.2.7.3 Future outlook

Nothing in particular.

7.3.2.8 Improvement of the resilience of a cyber-physical remote diagnostic communication system against cyber attacks

7.3.2.8.1 Summary

Issue	2 April 2019
Positioning	**Technical report** (Not legally binding)
Target	**Communications technology, security, and use cases** Remote diagnostics, cyberattack resilience

7.3.2.8.2 Items related to remote software updates

It analyses vulnerabilities to cyber attacks during remote diagnostics and explores ways to improve resilience. Remote diagnostics are cloud-based, and OTA firmware updates are one of the key features of cloud-based services.

It introduces a central gateway system to counter cyber attacks and a remote diagnosis system using it. However, while several papers, guidelines, and standards have been released by the SAE on cyber security, it is known that cyber security is a moving target. Not only wireless but also wired communication methods and data encryption methods are described as examples.

7.3.2.8.3 Future outlook

Nothing in particular.

7.3.2.9 System engineering for automated software update of automotive electronics

7.3.2.9.1 Summary

Issue	3 April 2018
Positioning	**Technical report** (Not legally binding)
Target	**Communication technologies, update procedures, use cases** Update system architecture and requirements

7.3.2.9.2 Items related to remote software updates

Regarding the method of software update, the conventional method and the method used for personal devices such as PCs are compared and analysed, and requirements for the update system are described. Although wired communication and wireless communication are mentioned as communication technologies, OTA is considered as one of remote update technologies.

Even in the present state, the communication cost becomes a problem, because the transfer capacity of map data of the navigation is large. Also, the update method used for personal devices is not directly applicable to automobiles because of the limited resources of the automobile and the long life cycle compared to PCs and the like. As requirements for software update systems for automobiles, nine points such as safety, communication security and bandwidth, and man-machine interface for automatic update are listed.

7.3.2.9.3 Future outlook

Nothing in particular.

7.3.2.10 Measures to prevent unauthorized access to the in-vehicle e/e system, due to the security vulnerability of a remote diagnostic tester

7.3.2.10.1 Summary

Issue	28 March 2017
Positioning	**Technical report** (Not legally binding)
Target	**Communications technology, security, and use cases** Remote diagnostic system

7.3.2.10.2 Items related to remote software updates

The conventional on-site (in the factory) diagnosis has shifted to remote diagnosis, where OTA is described as a technique for obtaining diagnostic data and updating ECU firmware. There is also mention of in-vehicle communication protocols, which discuss the architecture and security issues of remote diagnostic systems.

7.3.2.10.3 Future outlook

Nothing in particular.

7.3.2.11 OTA programming allows remote software updates: Over-the-air affair

7.3.2.11.1 Summary

Issue	21 February 2019
Positioning	**Article** (Not legally binding)
Target	**Communication technologies, update procedures, use cases** Maintenance, add features, 5G

7.3.2.11.2 Items related to remote software updates

For maintenance, it is necessary to update specific parameters and obtain engine performance reports, and OTA technology is required. In particular, 5G OTA can improve update latency with high speed, high reliability, and large capacity. The update technology based on the difference between the old and new firmware contributes not only to the ECU but also to the improvement of the automatic operation function.

7.3.2.11.3 Future outlook

Nothing in particular.

7.3.2.12 OTA will drive cybersecurity programs

7.3.2.12.1 Summary

Issue	16 April 2018
Positioning	**Article** (Not legally binding)
Target	**Communication technology and security** Countering cybersecurity

7.3.2.12.2 Items related to remote software updates

Here is what the authors think about the threat and current state of connected cars:

– *Connected cars are part of the Internet of things, and they are threatened by the Internet. As attackers launch new attacks against the Internet, OTA updates of the software are essential to counter cybersecurity. Traditional dealer updates do not work. At present, each manufacturer relies on its own method, and the object is limited to infotainment at first, but standardization is necessary in the future.*

7.3.2.12.3 Future outlook

Nothing in particular.

7.4 UNECE WP.29 GRVA TFCS ([b-19] to [b-22])

7.4.1 Introduction to the organization

The World Forum for Harmonization of Automobile Standards (WP.29), one of the activities under the auspices of the United Nations, establishes and amends regulations based on the Agreement, and manages and administers the Agreement[20]. There are two Agreements, that is, the 1958 Agreement (UN Agreement on Mutual Recognition of Type-Approvals for Vehicles) and the 1998 Agreement (United Nations Global Technical Regulations on Vehicles).

European countries, Japan, the United States, Canada, Australia, South Africa, China, South Korea, and other countries are participating in WP.29. Other non-governmental organizations that have participated include OICA (International Automobile Manufacturers Association), IMMA

[20] https://www.mlit.go.jp/common/000036077.pdf

(International Motorcycle Association), ISO (International Standards Association), and CLEPA (Society of Automotive Engineers of Japan). Japan has been a member since 1977.

From Japan, members of the Ministry of Land, Infrastructure, Transport and Tourism participate in promoting international harmonization of standards and mutual recognition of certification for automobiles with a view to promoting the spread of safe and environmentally friendly automobiles.

At the end of 2016, the Task Force on Cybersecurity and OTA for Self-Driving Cars (TFCS) was established by the Subcommittee on Self-Driving Cars (GRVA), which was established under the umbrella of WP.29.

7.4.2 Introduction of standards and publications

As of September 2019, GRVA, the parent committee of the TFCS, published the following documents mentioned in clause 7.4.2.1.

7.4.2.1 Items related to remote software updates

As of the end of September 2017, a draft of "Recommendation of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD on Software Updates" has been prepared and the following content has been mentioned.

- Reference model
- Type approval process for software updates
- Additional software update requirements (including securing the update process)
- Software id number and its use

In September 2019, WP.29 TFCS will complete a document consisting of cyber security proposals and software update proposals. Cybersecurity proposals consist of guidance and draft standards for manufacturers, and software update proposals consist of guidance, draft standards 1 (basic part), and draft standards 2 (provisions on software version control associated with other UN regulations).

7.4.2.2 Future outlook

In WP.29, the output of the TFCS was submitted at GRBA-04 in September 2019 and for approval at the WP.29 meeting in March 2020 at the earliest. It is scheduled to take effect six months after approval.

Each country promotes the enactment of the law in accordance with the above. Japan has been promoting domestic standardization based on the draft of the UN WP.29 standards and has established the following requirements.

- Capability requirements of the manufacturer
- System requirements of the manufacturer
- Vehicle requirements

The development of national laws and regulations (Article 99, paragraph 3 of the Road Trucking Vehicle Act (specific alteration)) related to the implementation of the software update (include some cyber security requirements) was completed on 24 May 2019. The enforcement will be within one year and five months.

After publication of the original paper in October 2019, the UN press release of the updated version was published on 25 June 2020. (https://www.unece.org/info/media/presscurrent-press-h/transport/2020/un-regulations-on-cybersecurity-and-software-updates-to-pave-the-way-for-mass-roll-out-of-connected-vehicles/doc.html).

The Regulation text is available at: https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.

7.5 U.S. DOT/NHTSA ([b-23] to [b-29])

7.5.1 Introduction to the organization

The U.S. DOT and NHTSA are government agencies of the United States of America.

– U.S. Department of Transportation

– NHTSA: National Highway Traffic Safety Administration

Under the U.S. DOT umbrella, NHTSA issues laws, regulations and guidelines related to the installation and performance of vehicles for safety (safety) and notifies and manages the progress of recalls. From the viewpoint of safety, V2X and autonomous driving are promoted, and guidelines and policies based on laws and regulations are issued and opinions are sought.

The U.S. DOT is also conducting demonstration tests of V2X at several locations in the United States.

7.5.2 Introduction of standards and publications

The following are the major publications issued by NHTSA that may be related to remote software updates.

Automated Driving Systems 2.0 (September 2017)[21]

– Updated and replaced Federal automated vehicles policy issued in September 2016

Cybersecurity Best Practices for Modern Vehicles (October 2016)[22]

– Federal Motor Vehicle Safety Standards; vehicle to vehicle (V2V) Communications notice of proposed rulemaking (NPRM) (December 2016)[23, 24]

– This NPRM is related to V2V communication and message format, and does not directly target remote software update, but it is introduced because there is a description on remote software update as a software update means.

Hereinafter, the outline of each of them and the parts related to remote update are described.

7.5.2.1 Automated Driving Systems 2.0

[21] https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[22] https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf

[23] http://www.safercar.gov/v2v/pdf/V2V%20NPRM_Web_Version.pdf

[24] https://www.gpo.gov/fdsys/pkg/FR-2017-01-12/pdf/2016-31059.pdf

7.5.2.1.1 Summary

Issue	September 2017	 Automated Driving Systems 2.0
Positioning	**Specifications** Guidance This document is a voluntary guidance and is not mandatory. Public comment available at launch[25] (Until 14 November 2017). Regular updates are planned to keep pace with the technology's evolution.	
Target	**Use case (automatic operation)** Automated driving systems (ADS) ADS used in vehicles corresponding to levels 3 to 5 in the definition of SAE	

To introduce this paper, the figure which is the front page figure of this original paper, is used to provide a visual image for specialists as well as for usual readers to directly make an association to the content in this paper.

In the United States, where 94% of crashes are caused by human factors, expectations are high that the introduction of autonomous driving systems (hereinafter referred to as ADS) will reduce the number of crashes. In addition to safety purposes, it is also expected that there will be more opportunities for people with disabilities, the elderly, and those who cannot afford to own a car, and that transportation efficiency will be improved to save energy and reduce environmental pollution.

This book can be broadly divided into two parts:

(1) Voluntary Guidance

(2) Technical Assistance to States

Part (2) is related to policies and regulations by state governments. In the following, only the summarization of part (1) is performed.

The voluntary guidance lists the following 12 safety factors (safety elements) for ADS:

(1) System safety

– To develop highly safe products in accordance with development processes conforming to various standards (ISO, etc.). With regard to the development process, notes are provided, especially for software development.

(2) Operational design domain

– For each ADS, assumed operating conditions (ODD) shall be defined, and the ADS shall be designed to operate appropriately under the ODD.

– ODD includes the conditions under which ADS are used (operating speed, daytime/night time operation, etc.) and each ADS must be tested for proper operation under assumed conditions.

(3) Object and event detection and response (OEDR)

– Under the defined ODD, the OEDR function of the ADS needs to detect objects that can affect the safe operation of the ADS, such as other vehicles, pedestrians, and animals, and select appropriate operations.

(4) Fall back (minimal risk condition)

[25] https://www.federalregister.gov/documents/2017/09/15/2017-19637/automated-driving-systems-a-vision-for-safety#

– When the operating environment is different from the assumed ODD, or when ADS does not operate normally due to system failure, appropriate measures (stop, etc.) shall be taken according to the situation at that time.

(5) Validation methods

– It indicates that the ADS should be checked to see if it works as expected, based on simulations, tests on trucks and public roads. The test may be conducted by an entity such as a car manufacturer or a component manufacturer, or by an independent third party.

(6) Human machine interface

– To accurately convey messages such as the state of automatic driving and the cancellation of automatic driving in an emergency.

(7) Vehicle cybersecurity

– Robust design that takes cybersecurity into account.

– Guidance and best practices from NIST, NHTSA, SAE, and Auto-ISAC are encouraged to be considered and adopted.

(8) Crashworthy

– ADS, including unmanned vehicles, should meet NHTSA impact resistance standards, regardless of autonomous driving levels.

(9) Post-crash ADS behaviour

– When resuming automatic operation after being involved in a collision accident, record the process. If important safety parts fail, the operation shall not be resumed.

(10) Data recording

– To record and share various events in order to investigate the causes of defects and consider countermeasures.

(11) Consumer education and training

– Thoroughly educate employees, dealers, and customers about ADS.

(12) Federal, state and local laws

– Appropriate logs should be maintained to ensure compliance with state laws.

– In situations where safety is required, humans may temporarily violate state law, but ADS is also required to be able to safely handle predictable events. The ADS also needs to be updated to accommodate future changes to state laws.

Compared with the positioning of the first edition of this document, which is the federal automated vehicles policy issued in September 2016, the following items are omitted. However, this does not mean that there is no longer a need for consideration, and it is said that further discussion is necessary[26]。

– Privacy

– Ethical considerations

– Registration and sharing

7.5.2.1.2 Items related to remote software updates

According to the Federal Automated Vehicles Policy published in September 2016, safety assessments should be submitted in advance of any changes to the autonomous driving function or degraded mode operation due to remote software updates.

However, this version does not mention remote software updates.

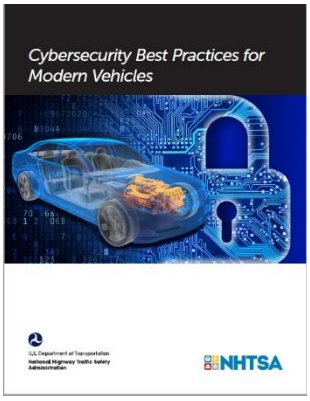
[26] https://www.nhtsa.gov/manufacturers/automated-vehicles-manufacturers

7.5.2.1.3 Future outlook

It should be updated regularly to reflect technological advances and changes in the environment.

7.5.2.2 Cybersecurity best practices for modern vehicles

7.5.2.2.1 Summary

Issue	October 2016	 Cybersecurity best practices for modern vehicles
Positioning	**Guidance** (Not legally binding) It is expected to be referred to when examining the cybersecurity of automobiles. Although this document itself is not binding or regulated, purpose notes that the National Traffic and Motor Vehicle Safety Act (amended) requires designs to take into account the risks posed by cyber security vulnerabilities.	
Target	**Lifecycle** All cars Documents for individuals and organizations related to the vehicle body and equipment, including vehicles, in-vehicle systems, and software, covering the entire life cycle of the vehicle	

To introduce this paper, the figure which is the front page figure of this original paper, is used to provide a visual image for specialists as well as for usual readers to directly make an association with the content in this paper.

NIST's Cyber Security Framework[27] and recommends a design approach based on the five elements of "Identify, defend, detect, respond, recover". Information sharing using Auto-ISAC is also recommended.

At the moment, the Federal Motor Vehicle Safety Standard does not cover security measures, but the revised National Traffic and Motor Vehicle Safety Act states that unwarranted security risks from potential security vulnerabilities should be avoided and calls for increased security efforts.

The top priority of the U.S. DOT is cyber security measures to prevent the leakage of safety and personal information. NHTSA is actively conducting cyber security investigations of vehicles and is considering strengthening cyber security in a broad range of areas involving relevant parties.

Recent NHTSA activities include the recall of approximately 1.5 million vehicles (Recall Campaign Number 15 V 461000), the submission to Congress of reports on safety measures including security measures (January 2016), the Advisory Council on Security (January 2016), the conclusion of contracts with 18 automobile manufacturers on next-generation safety policies including security measures, and the issuance of the "NHTSA Federal Automated Vehicles Policy" (September 2016).

Automobile-related manufacturers and other industry partners are also engaged in activities related to automobile security, such as the creation and publication of the J 3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (January 2016), a guidebook on automobile cybersecurity measures prepared by the SAE (Alliance of Automobile Manufacturers), the establishment of Auto-ISAC (late 2015), and the establishment of a framework for examining best practices related to security established by two trade associations (Alliance of Automobile Manufacturers and Global Automakers).

[27] https://www.nist.gov/cyberframework

NHTSA supports these activities and complements existing voluntary security standards, policies, best practices and lessons learned, and publishes this document as a resource for future industry activities.

The auto industry should adhere to the cybersecurity framework (issued by NIST), which consists of five key functions: Identify, Protect, Detect, Respond, and Recover, as a comprehensive and systematic approach to implementing layered security measures.

NHTSA also recommends that IT security standards such as ISO/IEC 27000[27] and centre for Internet security (CIS) best practices be considered (CIS CSC). This is to reduce security risks in vehicle development, dealer and service environments and supply chains.

7.5.2.2.2 Items related to remote software updates

Although not limited to a remote software update, it is required to design a means and a method for quickly recovering in the event of an incident (5.1 Layered approach).

Also, regarding software update, it mentions access restriction to debug mode and development mode, key management, and diagnosis access restriction. There were no details.

In many cases, firmware breaches are breakthroughs that can lead to vulnerability detection or end-to-end security attacks, and developers of firmware software should use tools that support secure coding and security measures during the development process.

In many systems, all external flash memory is encrypted to prevent unauthorized data recovery and firmware analysis. Since the firmware may be acquired at the time of updating, it is said that measures should be taken to prevent a third party from acquiring the unencrypted firmware (6.7.4 Control access to firmware).

It also reduces the risk of malware infection by limiting the ability to modify firmware. For example, by adopting a digital signature, there is a possibility that the boot prevention of the unauthorized firmware and the installation prevention of the unauthorized program in the in-vehicle ECU can be realized (6.7.5 Limit ability to modify firmware).

For the connection between the server and the car, the cryptography used in many fields should be applied. As a result, it is possible to eliminate communication in which a valid certificate is not confirmed (6.7.10 Control communication to back-end servers).

7.5.2.2.3 Future outlook

No specific future developments are mentioned. Best practices provide a strong foundation (solid foundation) for developing critical processes for risk-based approaches that are maintained and updated as appropriate (1. Purpose of this document).

7.5.2.3 Federal motor vehicle safety standards; V2V communications NPRM

7.5.2.3.1 Summary

Issue	December 2016
Positioning	**Specifications** NPRM Advance notice for legislation (Draft) Comments are solicited at launch (Quit Now), and more than 400 comments have been received from OEMs, Tier 1/Tier 2, industry associations, and individuals.
Target	**Communications technology (outside of the vehicle)** Communication and message format used for V2V communication (It is not intended for OTA but is presented because it is mentioned internally.)

This is a bill for transmitting and receiving basic safety message (BSM) by V2V communication using DSRC, and a survey and analysis report as a premise. Ensuring interoperability in V2V communications is essential for the success of V2V communications systems, and this requires government action.

It covers a wide range of topics from the explanation of the investment effect of accident prevention to communication technology, BSM format, and cybersecurity.

BSM includes the vehicle speed, direction, brake condition, other vehicle information, etc., and it is assumed that a warning is issued to the driver when it is determined that there is a possibility of a collision by appropriately transmitting and receiving this information. It is considered that the accident which cannot be avoided by the conventional in-vehicle system can be avoided by grasping the information of the car in the blind spot, operation and behaviour information, and information at a long distance (> 300 m) which cannot be grasped by the conventional in-vehicle sensor and camera.

In the cyber security clause, the contents corresponding to cyber security best practices for modern vehicles are mentioned, such as protection of access points not only for V2V communication but also for the entire automotive architecture, security design based on NIST cyber security framework throughout the life cycle, and information sharing through Auto-ISAC.

As a security foundation, security credential management system (SCMS) using public key infrastructure (PKI) is adopted.

7.5.2.3.2 Items related to remote software updates

III.E.6 refers to software and security certificate updates, which is also mentioned in III.E.7 dealing with Cybersecurity.

Necessity

Periodic updates are expected to be required to address feature, security, and privacy issues.

Method

OTA reprogramming. It is assumed that OTA reprogramming will become common practice by the time the final draft is enacted. It is also possible to introduce new applications to in-vehicle devices using smartphones.

Condition

All updates require user approval. It has been stressed several times and requires a notification and approval mechanism.

Target

- Security certificates (certificates) and protocols
- Abnormal behaviour (misbehaviour) detection algorithms, policies
- CRL content, policies
- Device firmware

SCMS can update certificates and security protocols, but the software that implements security management is supplier-dependent and each supplier must be able to respond to security updates.

However, there is a strong need to comment on whether there are any issues regarding software updates. The company is also open for comment on how long it will take between the discovery of the vulnerability and the application of the patch (The comment period is currently over.).

In a related note, V2V communication devices are proposed to be hardwired to withstand intrusions targeting security credentials (equivalent to FIPS-140 Level 3), and it believes that certificates and security policies should be stored on FIPS-140 Level 3 storage. It should be noted that a proposal has been made that FIPS-140 Level 3 is required not only for storage but also for HSM (IV.D.5 (a).5).

7.5.2.3.3 Future outlook

V2V communication was expected to be legislated in 2019 and scheduled to begin application in 2021. It is estimated that the technology will be applied to 100% of new cars in 2023. It is assumed that OTA has become a common tool at the time of legislation.

8 Affiliate survey: System level (communications)

In this clause, we surveyed standards for communication protocols developed by ITU-T, ISO, and other organizations at the system level, and extracted requirements for OTA.

8.1 Bluetooth SIG

8.1.1 Introduction to the organization

Bluetooth SIG (Special Interest Group) is a standardization organization which carries out standardization and certification of Bluetooth. Membership includes Promoter, Associate, and Adopter, with seven Promoters, approximately 600 Associates, and approximately 30,000 Adopters.

8.1.2 Introduction of standards and publications

The survey did not identify any OTA specifications or issues.

8.2 IEEE 802 (car relations)

8.2.1 Introduction to the organization

The Institute of Electrical and Electronics Engineers (IEEE) is an academic society of electrical and electronic technology with its headquarters in the United States. It has more than 400,000 members and formulates standards, holds international conferences, and publishes papers. The IEEE 802 committee is studying standardization of LANs, and services and protocols at the data link layer and the physical layer are standardized.

8.2.2 Introduction of standards and publications

The survey did not identify any OTA specifications or issues.

8.3 ISO TC 22 ([b-30] to [b-32])

8.3.1 Introduction to the organization

The International Organization for Standardization (ISO), is a non-governmental organization that develops international standards. Headquartered in Geneva, Switzerland, it is a non-profit corporation under Swiss Civil Code. The official languages are English, French and Russian. Only one organization from each country can participate. The international standard (IS) published by the International Organization for Standardization is also called ISO.

The ISO is an independent non-governmental organization consisting of 162 members from national standards bodies. ISO is the world's largest voluntary development organization for international standards and promotes global trade by providing common standards among countries. Nearly 20,000 standards cover everything from industrial products and technologies to food safety, agriculture, and medicine.

ISO standardizes major industrial sectors under the Technical Committee (TC). There are many TCs in ISO, and standards related to automobiles are developed in TC 22.

8.3.2 Introduction of standards and publications

The following are some of the types of deliverables produced by ISO: International Standards (IS), Technical Specifications (TS) and Technical Reports (TR).

Although there is currently no ISO standard for remote software update for automobiles, SC31 (Data Communication) under TC 22 has established the following ISO standards for diagnostic communication and reprogramming.

- ISO 13400-1:2011, Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 1: General information and use case definition[28]
- ISO 14229 -1: 2013, Road vehicles – Unified diagnostic services (UDS) – Part 1: Specification and requirements[29]
- ISO 22901 -1: 2008, Road vehicles – Open diagnostic data exchange (ODX) – Part 1: Data model specification[30]

Hereinafter, the outline of each of them and the parts related to remote update are described.

8.3.2.1 ISO 13400 (DoIP)

8.3.2.1.1 Summary

ISO 13400 specifies a communication standard (DoIP) for Internet Protocol-based diagnostic services. ISO 13400 specifies examples of common use cases covered by DoIP, Internet communication protocols for service interfaces standardized by ISO 14229, and physical layer standards for DoIP.

Issue	2011
Positioning	**Standard** (Not legally binding) IS standard
Target	**Communication technology** Automotive diagnostic communications field

8.3.2.1.2 Items related to remote software updates

Since it is necessary to consider the relation between remote software update and software update by wired communication, it is also necessary to pay attention to the contents of this standard.

8.3.2.1.3 Future outlook

Nothing in particular.

8.3.2.2 ISO 14229 (UDS)

8.3.2.2.1 Summary

ISO 14229 (UDS) specifies diagnostic communication specifications for service levels between the diagnostic tool and the in-vehicle ECU.

Issue	2013
Positioning	**Standard** (Not legally binding) IS standard
Target	**Communication technology** Automotive diagnostic communications field

[28] https://www.iso.org/standard/53765.html

[29] https://www.iso.org/standard/55283.html

[30] https://www.iso.org/standard/41207.html

8.3.2.2.2 Items related to remote software updates

Since it is necessary to consider the relation between remote software update and software update by wired communication (diagnostic tool), it is also necessary to pay attention to the contents of this standard.

8.3.2.2.3 Future outlook

ISO 14229 is expected to be revised and a DIS issued.

8.3.2.3 ISO 22901 (ODX)

8.3.2.3.1 Summary

ISO 22901 specifies ODX as the format for exchanging diagnostic data. ODX is an XML-based standard used to describe diagnostic ECU data. Manufacturers of vehicles, ECUs and testers can describe and exchange ECU diagnostic data in the same ODX format independent of the vehicle manufacturer. Because ODX is designed as an open exchange format, it is suitable for use in joint projects between automakers.

Issue	2008
Positioning	**Standard** (Not legally binding) IS standard
Target	**Communication technology** Automotive diagnostic communications field

8.3.2.3.2 Items related to remote software update

This standard is for diagnosis reprogramming by wired line (diagnostic tool) and is not for remote software update itself, but it is necessary to pay attention to this standard when considering remote software update.

8.3.2.3.3 Future outlook

Nothing in particular.

8.4 ISO TC 204

8.4.1 Introduction to the organization

ISO/TC 204 is a committee dedicated to the standardization of ITS. The description of the scope is as follows[31]. The in-vehicle traffic information and control system is out of scope (Jurisdiction of ISO/TC 22).

Standardization of information, communication and control systems for urban and rural road transport, including intermodal and multimodal elements. These include travel information, traffic management, public and commercial transport, and emergency response services in the field of intelligent transport systems (ITS).

As of 2017, 12 working groups were working on ISO/TC 204 standardization on the following subjects:

(1) Conceptual design (system architecture)

(2) Interface (message sets, etc.)

(3) Frameworks (data dictionary, message template)

(4) System performance requirements

[31] http://www.jsae.or.jp/01info/its/2016_bro_j.pdf

(5) Test methods

The working groups are:

WG1:	Architecture (USA) *Combiner in parentheses
WG3:	ITS database technology (Japan)
WG4:	Automatic vehicle and equipment identification (Norway)
WG5:	Fee and toll collection (Sweden)
WG7:	General fleet management and commercial/freight (Norway)
WG8:	Public transport/emergency (USA)
WG9:	Integrated transport information, management and control (Australia)
WG10:	Traveller information systems (UK)
WG14:	Vehicle/roadway warning and control systems (Japan)
WG16:	Communications (USA)
WG17:	Nomadic Devices in ITS Systems (Korea)
WG18:	Cooperative systems (Germany)

8.4.2 Introduction of standards and publications

The survey did not identify any OTA specifications or issues.

8.5 ITS Information and Communications System Promotion Council (ITS Information Forum) ([b-33] to [b-34])

8.5.1 Organization introduction

The ITS Information and Communication System Promotion Council[32] (Intelligent Transport Systems) is an organization that conducts R & D on ITS information and communication systems, promotes standardization of ITS, and conducts awareness-raising activities for the promotion of ITS. Approximately 100 organizations are part of it, including private companies and government-affiliated organizations from various industries. Since its establishment in 1999, it has produced concrete results such as the drafting of standards for DSRC (short-range communication), 700 MHz band intelligent transport system and 79 GHz band high-resolution radar.

8.5.2 Introduction of standards and publications

The ITS Information and Communication System Promotion Council has issued the following problem investigation reports.

Investigation Report on Issues for Advancement of ITS and Automatic Operation Using Cellular Communication Technology[33].

8.5.2.1 Investigation report on issues for advancement of ITS and automatic operation using cellular communication technology

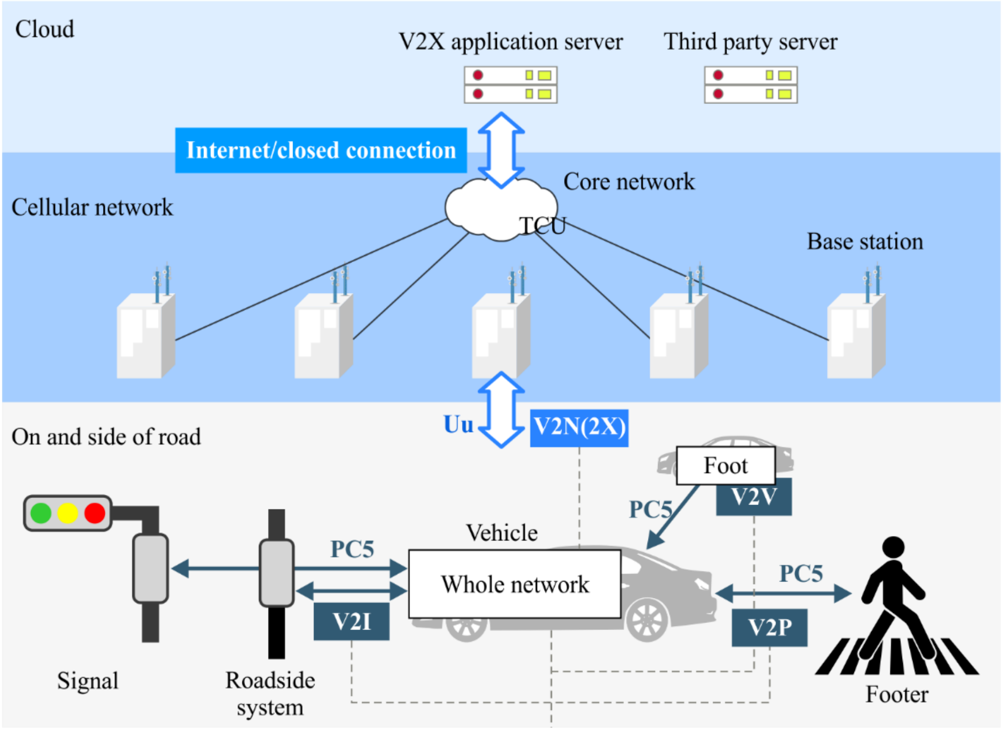
8.5.2.1.1 Summary

This report summarizes the issues in ITS and automatic operation using cellular V2X that are being examined by 3GPP, etc., and investigates countermeasures for practical application.

[32] https://itsforum.gr.jp/

[33] https://itsforum.gr.jp/Public/J7Database/p62/Cellular_system_201906.pdf

Issue	June 2019
Positioning	**Issue report** The issue itself is not legally binding.
Target	ITS and automatic operation using cellular V2X



FSTP.SS-OTA(21)_F8-1

Figure 8-1 – Overall configuration of cellular V2X[33]

8.5.2.1.2 Items related to remote software updates

Downloading software and mapping information for autonomous driving is outside the scope of this report.

8.5.2.1.3 Future outlook

It is expected that there will be additional use cases for collecting map information and surrounding information in autonomous driving.

8.6 ITU-T FG-VM

8.6.1 Introduction to the organization

The ITU-T Focus Group on Vehicular Multimedia (FG-VM) was established by the ITU-T SG16 in July 2018 to identify, organize, and propose activities to resolve issues related to the standardization of multimedia related to automobiles. The output, which is called a deliverable, from FG-VM is not a Recommendation or standard.

8.6.2 Introduction of standards and publications

FG-VM produced two deliverables as of April 2021 as follows:

– FGVM-01R2 [Flipbook] further endorsed as Recommendation ITU-T F.749.3 "Use cases and requirements for the vehicular multimedia networks".

– FG-VM-02 "Architecture of vehicle multimedia systems".

8.6.3 Future outlook

A deliverable on implementation aspects of vehicular multimedia systems will be produced.

8.7 ITU-T SG16 ([b-35] to [b-38])

8.7.1 Introduction to the organization

The International Telecommunication Union (ITU) is a specialized agency of the United Nations that consists of the ITU Telecommunication Standardization Sector (ITU-T), which deals with standardization, the ITU Radiocommunication Sector (ITU-R), which deals with wireless communications, and the ITU Telecommunication Development Sector (ITU-D), which deals with development. ITU comprises 193 member countries[34], 700 or more[35] Sector members/associates (as of September 2019).

ITU-T SG16 is a research committee that promotes standardization in the multimedia field. SG16 meetings are held once every nine months, and in questions under SG16, individual expert meetings are held separately from the SG16 meetings.

There are 14 questions under ITU-T SG16, of which Question 27/16 (*Vehicular multimedia communications, systems, networks, and applications*) is discussing the standardization of in-vehicle gateways. Standards standardized by ITU-T are published as Recommendations.

8.7.2 Introduction of standards and publications

This clause lists the major publications (date of issue)/source URLs that are considered to be related to remote (over the air, OTA) software updates for automobiles among the standards/publications published by ITU-T SG16.

ITU-T F.749.2: Service requirements for vehicle gateway platforms (March 2017)[36]

– It describes vehicle gateway platform (VGP) service requirements and use cases, as well as OTA requirements.

ITU-T H.550: Architecture and functional entities of vehicle gateway platforms (December 2017)[37]

– It is a Recommendation that describes the architecture and functional entities at the functional level of VGP, with OTA as an example of a use case.

ITU-T H.560: Communications interface between external applications and a vehicle gateway platform (December 2017)[38]

– This is a Recommendation that defines service requirements for communication interfaces between automobiles and external applications, and describes a service for managing software updates as one of the services.

Clauses 8.7.2.1 to 8.7.2.3.3 outline each of the Recommendations including a description of the parts that are related to remote update.

8.7.2.1 ITU-T F.749.2: Service requirements for vehicle gateway platforms

[34] https://www.itu.int/online/mm/scripts/gensel8

[35] https://www.itu.int/online/mm/scripts/gensel11

[36] https://www.itu.int/rec/T-REC-F.749.2/en

[37] https://www.itu.int/rec/T-REC-H.550/en

[38] https://www.itu.int/rec/T-REC-H.560/en

8.7.2.1.1 Summary

Issue	March 2017
Positioning	**Recommendation** (Not legally binding) ITU-T Recommendations
Target	**Use cases, communications technologies, and security** In-vehicle gateway

8.7.2.1.2 Items related to remote software updates

ITU-T F.749.2 describes a use case for remote software update of services and applications on VGP in clause 5.2 "Vehicle-to-cloud telematics scenario". The VGP defined here is an in-vehicle gateway for providing a communication function between devices in a vehicle and devices inside and outside the vehicle, and a function for communicating with a driver is also described in the upper layer. In addition, functions related to driving are outside the scope. Remote software updates are aimed at bug fixes and feature updates and require the entire software update process to be protected from cyberattacks.

Software management requirements are described in clause 8.6 "*Software management requirements*" and include the following requirements.

- Secure, secure, and flexible management
- Secure support for software management within VGP
- To support software management of a device connected to a VGP via an on-vehicle bus in a safe method.
- Determining the software version
- Signing and encrypting updates for log authenticity and verifiability

8.7.2.1.3 Future outlook

Related Recommendation ITU-T F.749.1 *Functional requirements for vehicle gateways* (November 2015) has been published.

8.7.2.2 ITU-T H.550 Architecture and functional entities of vehicle gateway platforms

8.7.2.2.1 Summary

Issue	December 2017
Positioning	**Recommendation** (Not legally binding) ITU-T Recommendations
Target	**Use cases, communications technologies, and security** In-vehicle gateway

8.7.2.2.2 Items related to remote software updates

ITU-T H.550 describes the architecture and functional entities at the functional level of VGP. This Recommendation describes an OTA software update as an example of a use case for reference points between entities controlling access to in-vehicle resources and entities controlling in-vehicle communication. At this reference point, ECU control messages for software update by the OTA are transmitted and received. The appendix describes the signalling flow in remote software update scenarios. In the signalling flow, VGP receives a software update request from the cloud server, and VGP responds to the cloud server after confirming the software version implemented. Update software is then received and installed from the cloud server. The update target is VGP and the internal ECU.

8.7.2.2.3 Future outlook

Nothing in particular.

8.7.2.3 ITU-T H.560: Communications interface between external applications and a vehicle gateway platform

8.7.2.3.1 Summary

Issue	December 2017
Positioning	**Recommendation** (Not legally binding) ITU-T Recommendations
Target	**Use cases, communications technologies, and security** In-vehicle gateway

8.7.2.3.2 Items related to remote software updates

ITU-T H.560 defines service requirements for communication interfaces between automobiles and external applications. One of the services is a software update management service, and the following requirements are listed.

- Providing a common, fast, secure, and flexible interface
- To provide several interfaces for safely applying a new software package. These interfaces should support the software update standards implemented in ECUs, such as TPM, which is standardized by TCG.
- Providing a database to securely store software
- Provides submodules for verifying, installing, configuring, removing, and tracing installation of software packages before they are applied

Also, an example of a data flow regarding software update from a cloud server via VGP is shown.

8.7.2.3.3 Future outlook

Nothing in particular.

8.8 ITU-T SG17 ([b-39])

8.8.1 Introduction to the organization

ITU-T SG17 is a research committee of ITU-T that promotes standardization in the security field. There are 14 questions under SG17, of which Question 13/17 (*Intelligent transport system security*) is standardizing security in ITS. Question 13/17 was a question that was approved at the TSAG meeting in May 2017. Prior to the launch of the Question, consideration had been underway in Question 6/17 (*Security for telecommunication services and Internet of things*).

8.8.2 Introduction of standards and publications

This clause lists the major publications (date of issue)/source URLs that are considered to be related to remote software updates for automobiles among the standards/publications published by ITU-T SG17.

ITU-T X.1373: Secure software update capability for intelligent transport system communication devices (March 2017)[39]

- This is a Recommendation describing a secure software update and describes each message content from a software update sequence.

[39] https://www.itu.int/rec/T-REC-X.1373/en

Clauses 8.8.2.1 to 8.8.2.1.3, outline each of Recommendation including a description of the parts that are related to remote update.

8.8.2.1 ITU-T X.1373: Secure software update capability for intelligent transport system communication devices

8.8.2.1.1 Summary

Issue	March 2017
Positioning	**Recommendation** (Not legally binding) ITU-T Recommendations
Target	**Communications technology (outside of the vehicle), update procedures, hardware** In-vehicle gateway

8.8.2.1.2 Items related to remote software updates

ITU-T X.1373 describes the software update procedure for the purpose of application to the onboard communication device in vehicle to infrastructure (V2I) communication. Communication inside the vehicle is outside the scope of the Recommendation. It also includes sample data formats and XML messages.

The following is the sequence of OTA remote software updates described in the Recommendation. In this Recommendation, the in-vehicle communication is outside the scope, so steps 2), 3), 10), 11), 12), and 13) are examples.

1) An update module is provided by the supplier. This step is processed asynchronously with the subsequent steps.

2) A vehicle mobile gateway (VMG) requests a software list from an ECU.

3) The ECU confirms the state of the software, creates a software module list and reports it to the VMG.

4) The VMG sends the collected list to the update server to check for updates.

5) The update server transmits receipt confirmation of the received list to the VMG.

6) The update server investigates the software state installed in the vehicle according to the list and determines the necessary software update.

7) Since the processing of step 6) may take time, the VMG periodically inquires the update server about the necessity of the update.

8) If the update exists, the update server sends the URL for the update to the VMG, and if not, sends only an acknowledgment.

9) If an update exists, the VMG connects to the update server to download the update module.

10) Before applying the update to the ECU, the VMG confirms the update application to the driver.

11) The driver confirms and permits the application of the update.

12) The VMG distributes the update file to the corresponding ECU and requests the application of the update.

13) Each ECU applies the update and reports the result to the VMG.

14) The VMG reports the results of the application to the update server.

15) The update server sends confirmation of receipt of the update information to the VMG. If the update application fails or an unapplied update is found, the update server repeats steps 6) through 14) until the application succeeds.

Clause 7.1 "General message format with security functions" describes how to authenticate message senders and verify message integrity. Here, one of a digital signature based on ITU-T X.509 using asymmetric cryptography by HSM and a message authentication code (MAC) using a common key should be used.

8.8.2.1.3 Future outlook

In the published version of ITU-T X.1373, communication inside the vehicle was excluded from scope, but the work to update ITU-T X.1373 is currently underway in Q13/17[40]. The revised version also covers in-vehicle communications and is scheduled to be issued in September 2022.

8.9 oneM2M ([b-40])

8.9.1 Introduction to the organization

1) oneM2M is a standardization organization that was established in July 2012 and is operated jointly by seven regional standardization organizations in Europe, North America and Asia (TSDSI (India) joined in 2015).

2) Main mission: Deliverables: TS (Technical Specification (normative)) and TR (Publication of Technical Report (informative), including test specifications for product certification)

3) Configuration Members:

   – Type 1 Partners (governing body): ARIB (Japan), ATIS (North America), CCSA (China), ETSI (Europe), TIA (North America), TSDSI (India), TTA (South Korea), TTC (Japan)

   – Members: Individual members that belong to Partner Type 1 (ApproX.200).

   – Type 2 Partners (outside participating organizations): OMA, Broadband Forum, Global Platform, CEN, CENELEC

   – Associate Members: CESG (United Kingdom), Ministry of Science, ICT and Future Planning (MSIP/Korea), National Institute of Standards and Technology (NIST/US), Pacific Northwest National Laboratory (United States), State Secretariat of Telecommunications and for the Information Society (Spain), United States Department of Transportation (United States).

8.9.2 Introduction of standards and publications

TR-0026 – Vehicular Domain Enablement[41]

Clauses 8.9.2.1 to 8.9.2.1.3 outline each of the Recommendation including a description of the parts that are related to remote update.

8.9.2.1 Vehicle information access API

8.9.2.1.1 Summary

Issue	September 2017
Positioning	**Technical report** (Not legally binding at this time) At present, the technical report (TR: Technical Report) has been established as an informative document, but from this point on, there are contents included in the technical specification (TS-0001 (Functional Architecture), TS-0003 (Security Solutions), etc.), and they become normative standards and technical specifications with binding force.

[40] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14820

[41] http://www.onem2m.org/technical/latest-drafts

Target	**Communication technologies, update procedures, use cases** Use case for oneM2M Technology in Vehicular Domain (remote maintenance, vehicle data collection/data wipe services, OTA update of ECU firmware)

8.9.2.1.2 Items related to remote software updates

(1) Use cases

The following four related topics are listed in clause 6.

– 6.2 Remote maintenance service

– 6.7 Vehicle data service

– 6.9 Vehicle data wipe service

– 6.11 Secure over – The-air firmware update for automotive ECUs

(2) Potential requirements

Potential requirements are described in clause 7.

(3) High level architecture

The high-level architecture of the vehicle for realizing (2) and (3) is described in clause 8.

(4) Security

Key issues related to security derived from the above are described in clause 9.4, and solutions are described in clauses 10.5 and 10.6.

8.9.2.1.3 Future outlook

TR-0026 *Vehicular Domain Enablement* was approved at the oneM2M TP # 31 meeting (September 18-22) and published as Release 3 with other TSs and TRs in December 2018.

Currently, ITU-T and oneM2M are working together to develop ITU Recommendations, and TS-0001 and other TRs are currently approved as ITU-T Recommendations as Release 2A. It is expected that the TS and TR of oneM2M will be referred to as ITU-T Technical Specifications and Technical Reports in developing countries, as the ITU-T is considering establishing Release 3 as an ITU-T Recommendation.

8.10 W3C ([b-41] to [b-46])

8.10.1 Introduction to the organization

World Wide Web Consortium (W3C)[42] The World Wide Web is a non-profit organization founded in 1994 to promote the standardization of various technologies used on the World Wide Web. As part of its activities, the GENIVI Alliance [43] The two companies have signed a memorandum of understanding (MoU) to collaborate on automotive (IVI) standardization. This report is treated as an integral part of GENIVI based on MoU.

8.10.2 Introduction of standards and publications

Here, the main publications (date of issue)/source URLs that are considered to be related to the remote software update of automobiles among the sites/publications published by the W3C are listed.

Automotive and Web at W3C[44]

[42] http://www.w3.org/

[43] http://www.genivi.org/

[44] http://www.w3.org/auto/

– Connected car cover page

Automotive Working Group[45],[46]

– A group working on specifications for HTML5, JavaScript and other application developers to enable Web connectivity through the next generation of in-vehicle information and communication systems (IVI) and protocols for accessing vehicle data. Chair: Jaguar Land Rover, Volkswagen (and an individual).

Automotive and Web Platform Business Group[47]

– Community in which non-W3C members can participate

Key specifications being developed by this WG:

Vehicle information service specification (VISS)[48]

– WebSocket-based API for client applications to GET/SET/SUBSCRIBE/UNSUBSCRIBE vehicle signals and data attributes with editor Jaguar Land Rover

Cyber-Security in the Connected Car Age GENIVI Conference – Seoul, October 21, 2015[49]

– In his talk the author introduced OTA reprogramming as "Remote software update emerging for quicker fix of security flaws".

Clauses 8.10.2.1 to 8.10.2.2.3 outline each of the document including a description of the parts that are related to remote update.

8.10.2.1 Vehicle information service specification (VISS)

8.10.2.1.1 Summary

Issue	(Draft) October 2016
Positioning	**Specifications** A WebSocket-based API for client applications to GET/SET/SUBSCRIBE/ UNSUBSCRIBE vehicle signals and data attributes. A feature that may be used when performing OTA reprogramming.
Target	**Update procedure** OTA Reprogramming

8.10.2.1.2 Items related to remote software updates

This is the first feature that will require update over the air.

8.10.2.1.3 Future outlook

To be determined.

[45] http://www.w3.org/auto/wg/

[46] https://www.w3.org/auto/charter-2018

[47] http://www.w3.org/community/autowebplatform/

[48] https://www.w3.org/TR/2016/WD-vehicle-information-service-20161020/

[49] https://lists.w3.org/Archives/Public/public-auto-privacy-security/2015Oct/att-0005/Cyber-security_Connected_Car_Age-GENIVI.pdf

8.10.2.2 Cyber-security in the connected car age

8.10.2.2.1 Summary

Issue	October 2015
Positioning	**Presentation proposal**[50] (Not legally binding).
Target	**Use case** OTA reprogramming

8.10.2.2.2 Items related to remote software updates

Clarified the benefits and concerns of the over the air update.

8.10.2.2.3 Future outlook

The specific prospect is unknown. However, the W3C is partnering with the GENIVI Alliance to push Web technologies into the automotive software platform.

8.11 Wi-Fi Alliance

8.11.1 Introduction to the organization

The Wi-Fi Alliance is a standards group that aims to promote wireless LAN products and has about 500 companies. The Alliance promotes collaboration among member companies, promotes Wi-Fi technology, and recommends rules for spectrum allocation. One current area of work is automotive, which considers the needs and use cases of Wi-Fi technology in the automotive segment.

8.11.2 Introduction of standards and publications

The survey did not identify any OTA specifications or issues.

8.12 5th generation mobile promotion forum (5GMF)

8.12.1 Introduction to the organization

The purpose of 5G Mobile Promotion Forum (5GMF)[51] is to contribute to the sound development of the use of telecommunications through research and development, standardization, liaison and coordination with related organizations, information collection, and public awareness activities, etc., in order to achieve the early realization of the 5th generation mobile communications system.

Activities are conducted by the Planning Committee, the Technical Committee, the Applications Committee, and the Network Committee, focusing on 5G trend surveys.

Security related to connected vehicles is being investigated by the Connected Vehicle SWG of the Security Investigation and Review Committee.

8.12.2 Introduction of standards and publications

There are no OTA issues from the 5th Generation Mobile Promotion Forum, but the following Workshop summaries have been issued.

– 3GPP5G Security Workshop

[50] https://lists.w3.org/Archives/Public/public-auto-privacy-security/2015Oct/att-0005/Cyber-security_Connected_Car_Age-GENIVI.pdf

[51] https://5gmf.jp/ (in Japanese).

8.12.2.1 3GPP 5G security workshop

8.12.2.1.1 Summary

The necessary security conditions for ITS service provision by multiple service providers under the 5G environment provided by carriers are reported.

Issue	1 July 2019
Positioning	The issue itself is not legally binding.
Target	**Summary report** Multiple service providers providing ITS services in a 5G environment

8.12.2.1.2 Items related to remote software updates

It mainly describes the ITS service as a whole but does not describe only downloads of software and map information.

8.12.2.1.3 Future outlook

The application problem of network slicing to ITS field is expected to be examined.

9 Affiliate survey: System level (components)

In this clause, the standards for components such as chips developed by EVITA, TCG, etc. among the system level, and extracted the requirements for OTA are investigated.

9.1 EVITA ([b-47] to [b-51])

9.1.1 Introduction to the organization

EVITA (e-safety vehicle intrusion protected applications) is a project within the European Union's Seventh European Research and Development Framework Plan. The purpose of this project is to design, verify and prototype the architecture of the automotive network in order to prevent tampering and modification of security-related components and compromise of sensitive data in the automotive network. It was active between 2008 and 2011.

9.1.2 Introduction of standards and publications

Here, among the standards/publications published by EVITA, the main publications (date of issue)/source URLs that are considered to be related to remote software updates for automobiles are listed.

Deliverable D 2.1: Specification and evaluation of e-security relevant use cases (Dec. 2009)[52]

– This report describes the use cases of in-vehicle networks that may require security measures. 18 use cases are described, including active braking for safety measures, traffic information from off-vehicle entities, engine ECU replacements, remote diagnostics, and remote flushing (remote software update). For each use case, it describes the required functionality, the communication entities involved and how to communicate, the information to be communicated, the required data, and performance requirements. In the report following D 2.1, security requirements were extracted using these use cases.

Deliverable D 2.3 Security requirements for automatic on-board networks based on dark-side scenarios (Dec. 2009)[53]

[52] https://www.evita-project.org/Deliverables/EVITAD2.1.pdf

[53] https://www.evita-project.org/Deliverables/EVITAD2.3.pdf

- In this report, security threats are extracted, risks are calculated, and security requirements are extracted for the use cases of D 2.1. Using the security requirements of this report, a security architecture has been designed in subsequent reports.

Deliverable D 3.2 Secure on-board architecture specification (Aug. 2011)[54]

- This report describes the security architecture of EVITA. The architecture consists of hardware modules and a software framework. Hardware modules, called EVITA hardware security modules (HSM), come in three different levels of functionality and performance. The software framework consists of modules for communication control, cryptographic services, mutual authentication, policy determination, platform integration, secure storage, and security monitoring.

Deliverable D 3.3 Secure on-board protocols specification (July 2011)[55]

- This report describes a protocol specification for secure implementation of use cases in automotive networks. It extracts and classifies the secure in-vehicle protocols needed to implement D 2.1 use cases and designs the protocols as plug-ins to the D 3.2 security architecture. Protocols include key distribution protocols, session key establishment protocols, remote authentication protocols, access control protocols, time synchronization protocols, remote firmware update protocols, and the like.

Clauses 9.1.2.1 to 9.1.2.4.3 give the outline of each of the deliverable including a description of the parts that are related to remote update.

9.1.2.1 Deliverable D2.1: Specification and evaluation of e-security relevant use cases

9.1.2.1.1 Summary

Issue	December 2009
Positioning	**Report** (No legal force at this time)
Target	**Communications technology (in car)** automotive network

9.1.2.1.2 Items related to remote software updates

Use Case 17 describes remote software updates as remote flashing. The entities concerned are a service station and a diagnostic tool (DT) outside the vehicle, a communication unit (CU) inside the vehicle, an ECU in a power train area, and a power train controller (PTC). An example of updating the software of the power train controller (PTC) according to the sequence of Table 9-1 is described.

Table 9-1 – PTC's software update sequence

No.	Actor	Recipient	Data/Activity
1	Service station	CU	Connection request
2	CU	ECU	Connection request
3	ECU	-	Request processing/integrity checking, authentication
4	ECU	CU	Connection response
5	CU	Service station	Connection response
6	Service station	CU	ECU information request

[54] https://www.evita-project.org/Deliverables/EVITAD3.2.pdf

[55] https://www.evita-project.org/Deliverables/EVITAD3.3.pdf

Table 9-1 – PTC's software update sequence

No.	Actor	Recipient	Data/Activity
7	CU	ECU	ECU information request
8	ECU	-	Authentication/integrity checks, freshness checks
9	ECU	CU	ECU information response
10	CU	Service station	ECU information response
11	Service station	CU	Encrypted firmware update data
12	CU	ECU	Encrypted firmware update data
13	ECU	-	Authentication/integrity checks, freshness checks
14	PTC	-	Update data decoding and update execution

Relevant security elements include (equipment) authentication, data authentication, data freshness, non-repudiation, confidentiality, and anonymity.

9.1.2.1.3 Future outlook

The EVITA project was terminated in 2011 and as of September 2017, it is not expected that this publication will be revised.

9.1.2.2 Deliverable D 2.3 Security requirements for automatic on-board networks based on dark-side scenarios

9.1.2.2.1 Summary

Issue	December 2009
Positioning	**Report** (No legal force at this time)
Target	**Communications technology (in car)** Automotive network

9.1.2.2.2 Items related to remote software updates

This document extracts security requirements from the remote flashing remote software update use case (remote flashing). Table 9-2 lists the security requirements for remote software updates cited in this document.

Table 9-2 – Extracted security requirements

No.	Security requirements	Description
1	Authenticity_29	Firmware must be certified and programmed by the manufacturer when it is installed in the vehicle.
2	Authenticity_101	When a command is transmitted from an internal ECU to another internal ECU, data authentication shall be performed along the path of the function.
3	Authenticity_102	When a command is sent to the ECU for reprogramming, the origin of the code shall be authenticated.
4	Authenticity_103	To authenticate a data generation source when a message arrives at a vehicle from outside the vehicle.
5		To authenticate a data generation source along a path of a function when data are transmitted to a load side unit.
6	Integrity_101	To ensure completeness of a message when the message arrives at a vehicle from outside the vehicle.

Table 9-2 – Extracted security requirements

No.	Security requirements	Description
7		When data is transmitted to the load side unit, ensure message integrity along the path of the function.
8	Integrity_102	When a command is sent to the ECU for reprogramming, ensure the integrity of the command.
9	Integrity_103	When reprogramming commands are sent to the ECU, ensure the integrity of the firmware.
10	Integrity_104	When a command is sent from one internal ECU to another, ensure the integrity of the information along the functional path.
11	Access_101	To surely perform access control to a reprogramming function when a command is transmitted to an ECU for reprogramming.
12	Access_102	To surely perform access control of reading to a flash memory when a command is transmitted to an ECU for reprogramming.
13	Freshness_101	To surely keep freshness of a message when the message arrives at a vehicle from the outside of the vehicle.
14		To surely keep freshness of a message along a path of a function when data are transmitted to a load side unit.
15	Freshness_102	To surely keep freshness of information along a path of a function when a message as a command is transmitted from an internal ECU to another internal ECU.
16	Freshness_103	To surely maintain freshness of a command when the command is transmitted to an ECU for reprogramming.
17	Confidence_1	The vehicle ID shall be kept confidential, including during wireless communications.
18	Privacy_101	To perform access control to e-service message data when transmitting a message from a vehicle to an entity providing a service by target of evaluation (TOE) or an entity outside a car manufacturer.
19	Confidentiality_101	To surely protect secrecy of firmware data when a command is transmitted to an ECU for reprogramming.
20	Confidentiality_102	To surely protect secrecy of a firmware update event when a command is transmitted to an ECU for reprogramming.
21	Availability_101	To surely maintain the availability of a bus when information is exchanged between an ECU, a CU, a head unit, a sensor and other in-vehicle units.
22	Availability_102	To surely maintain availability of a CPU when information is exchanged between an ECU, a CU, a head unit, a sensor and other in-vehicle units.
23	Availability_103	To surely maintain the availability of a RAM when information is exchanged between an ECU, a CU, a head unit, a sensor and other in-vehicle units.
24	Availability_104	CU availability must be ensured when information is transmitted from the vehicle to nearby vehicles, roadside units, or other entities.
25		Ensure the availability of CUs when vehicles receive information from nearby vehicles, roadside units, or other authorized entities.

Table 9-2 – Extracted security requirements

No.	Security requirements	Description
26	Availability_105	To ensure the availability of a radio medium when information is transmitted from a vehicle to a nearby vehicle, a roadside unit, or other entity.
27		Ensuring that the availability of the radio medium is maintained when the vehicle receives information from nearby vehicles, roadside units, or other authorized entities.
28	Availability_106	To ensure the highest level of availability of a device required for a function having the highest level of priority when information is transmitted from a vehicle to a neighbouring vehicle, a roadside unit and other entities.
29	N/A	To ensure the highest level of availability of a device required for a function having the highest level of priority when a vehicle receives information from a neighbouring vehicle, a roadside unit, or other authorized entity.

9.1.2.2.3 Future outlook

The EVITA project was terminated in 2011 and as of September 2017, it is not expected that this publication will be revised.

9.1.2.3 Deliverable D3.2 Secure on-board architecture specification

9.1.2.3.1 Summary

Issue	August 2011
Positioning	**Report** (No legal force at this time) Examples of mounting in the automotive and semiconductor industries
Target	**Communications technology (car)** Automotive network

9.1.2.3.2 Items related to remote software updates

The envisioned use case in designing the architecture includes remote software updates.

The report designs three hardware security modules: EVITA full, medium, and light. The outline of each module is as follows.

EVITA full

– EVITA full is a security module designed for V2X and is the most powerful and high-performance of the three. The building blocks are summarized in Table 9-3.

Table 9-3 – EVITA full building blocks

No.	building block	Description
1	ECC-256 - GF (p)	256-bit Elliptic Curve Cryptographic Engine on NIST Recommended Curve P -256
2	WIRLPOOL	AES-based hash function engine. The hash value is 512 bits in length.
3	AES-128	AES engine with 128-bit key length for NIST standard block ciphers. Support for ECB, CBC, GCM and CCM usage modes.

Table 9-3 – EVITA full building blocks

No.	building block	Description
4	AES-PRNG	BSI-AIS 20 E.4 compliant AES-based pseudo-random number generator engine. A seed is provided from an internal true random number generator (TRNG).
5	COUNTER	At least 16 64-bit monotonically increasing counters.
6	Time counter	Counters that write UTC time synchronized with the outside
7	Internal CPU	The CPU inside the HSM. Proposed ARM Cortex M3 or similar CPU.
8	Internal RAM	RAM inside the HSM. At least 64 kilobytes.
9	Internal non-volatile memory	Flash memory inside the HSM. At least 32 kilobytes. (In addition, the ROM of 10 k bytes or more.)
10	Hardware API	A defined API for accessing HSM functionality from the main CPU and applications.

EVITA medium

– The EVITA medium is a security module designed for ECUs and has intermediate functions and performance among the three. EVITA full without the ECC -256 GF (p) and WHILLPOOL engines. In addition, the performance of the internal CPU is lower than that of the EVITA full. (For example, EVITA full is equivalent to Coretex[56] - M3 100 MHz versus EVITA medium such as Coretex-M3 50 MHz.)

EVITA light

– The EVITA light is a security module designed for sensors and actuators and is the least capable of any of the three. Among the building blocks of the host module, only the AES-128 engine, AES-PRNG, time counter, and hardware API are provided. Unlike the higher-level module, AES-PRNG is seeded by an external TRNG. As an option, specifications including internal RAM, internal non-volatile memory, and internal TRNG are set.

9.1.2.3.3 Future outlook

The EVITA project was terminated in 2011. As of September 2017, it is not expected that this publication will be revised. It should be noted that a chip conforming to the EVITA HSM is available from multiple chip vendors, e.g., Infineon, Renesas and NXP.

9.1.2.4 Deliverable D3.3 Secure on-board protocols specification

9.1.2.4.1 Summary

Issue	July 2011
Positioning	**Report** (No legal force at this time) Examples of mounting in the automotive and semiconductor industries
Target	**Communication technologies (car), update procedures, firmware** Automotive network

[56] ARM CPU architecture. See https://developer.arm.com/products/processors/cortex-m/cortex-m3.

9.1.2.4.2 Items related to remote software updates

This report describes the protocol specification for remote software update. The main entities involved in the remote software update are the service station and diagnostic tool (DT) as entities outside the vehicle, and the central communication unit (CCU) and ECU as entities inside the vehicle. Since the CCU functions as a key master (KMs) in the vehicle, it is also referred to as CCU-KM below. HSM_DT, HSM_CCU, HSM_ecu and HSM_oem refer to HSM provided in DT, CCU, ECU and OEM server, respectively.

The Remote Software Update Protocol consists of five steps: Remote Diagnosis, ECU Reprogramming Mode, Firmware Encryption Key Exchange, Firmware Download, and Firmware Installation and Verification. The steps are as follows.

Remote diagnosis

In this step, necessary information such as ECU type, firmware version, and last update date is collected from the ECU. The algorithm of the protocol is as follows:

1) DT generates symmetric key Mk in HSM_DT.

2) DT exports Mk from HSM_DT. When exporting, Mk is encrypted in HSM_DT with CCU public key Pk_ccu. Write exported data as Exported-DT_Mk.

3) DT signs the data combining Exported-DT_Mk and the time stamp with the private key Sk_dt of DT and sends Exported-DT_Mk, the time stamp, and the signature to CCU-KM.

4) CCU-KM checks the freshness of the received timestamp, verifies the signature, and authenticates the DT.

5) CCU-KM imports Exported-DT_Mk into HSM_CCU if the checks and validations in 4 are correct. At the time of import, Exported-DT_Mk is decrypted in the HSM_CCU by the secret key Sk_ccu of the CCU.

6) CCU-KM exports Mk from HSM_CCU. When exporting, Mk is encrypted in the HSM_CCU by the public key Pk_ecu of the ECU or the common key Psk according to the type of the ECU. Write the exported data as Exported-CCU_Mk.

7) The CCU-KM signs the data obtained by combining Exported-CCU_Mk and the time stamp with the private key Sk_ccu of the CCU-KM and sends the Exported-CCU_Mk, the time stamp and the signature to the ECU.

8) The ECU receiving the data confirms the approval of the CCU/DT based on the policy, checks the freshness of the time stamp, and verifies the signature.

9) If 8 passes correctly, the ECU imports Exported-CCU_Mk into HSM_ecu. At the time of import, Exported-CCU_Mk in HSM_ecu is decrypted by the secret key Sk_ecu or the common key Psk of the ECU.

10) The ECU adds a signature or MAC to the data obtained by combining the Ack and the time stamp and transmits it to the CCU-KM.

11) CCU-KM checks the signature/MAC and timestamp of the received data.

12) If the result in step 11 is correct, the CCU-KM adds a signature to the data obtained by combining the Ack and the time stamp and transmits it to the DT.

13) DT checks the signature and timestamp of the received data.

14) When step 13 is verified, the DT transmits a request for reading diagnostic information such as the state and log information from the ECU according to the option selected by the employee of the service station and reads the information.

ECU reprogramming mode

In this step, when the type of ECU is expected, DT shifts the ECU from the application mode to the reprogramming mode.

1) The MAC generated by Mk is added to the data obtained by combining the seed request instruction and the time stamp by DT and transmitted to the ECU.
2) The ECU checks the integrity and freshness of the data.
3) If the check of 2 is correct, the ECU generates a seed Na in HSM_ecu and extracts data ε (Na) Mk obtained by encrypting Na with Mk.
4) An ECU adds a MAC generated by Mk to data obtained by combining ε (Na) Mk and a type stamp and transmits the data to DT. The ECU generates a key Smk for shifting to the reprogramming mode from Na by HSM_ecu.
5) DT checks the integrity and freshness of the received data.
6) DT decodes Na with HSM_DT and generates Smk from Na if the check of 5 is correct.
7) DT exports Smk from HSM_DT. At this time, Smk is exported in a state encrypted with Mk. Export data should be listed as Exported_Smk.
8) DT adds the MAC generated by Mk to the data obtained by combining Exported_Smk and the time stamp and transmits it to the ECU.
9) The ECU checks the integrity and freshness of the received data.
10) If 10 is correct, the ECU takes the Smk from Exported_Smk in HSM_ecu and compares it with the Smk calculated by HSM_ecu itself in 4.
11) When the comparison of 10 matches, the ECU shifts to a reprogramming mode.
12) The ECU adds the MAC generated by Mk to the data obtained by combining the Ack and the time stamp to inform that the mode is shifted to the reprogramming mode and transmits the data to DT.
13) DT checks the integrity and freshness of the received data and confirms the mode transition of the ECU.

Firmware encryption key exchange

In this step, the firmware encryption key is exchanged.

1) DT adds the signature generated by Sk_dt to the firmware encryption key request and the time stamp and transmits it to the OEM server. The request includes information about the ECU such as ECU type, ECU identification number, and firmware version.
2) The OEM server authenticates and checks the integrity of the received data.
3) The OEM server exports the firmware encryption key SSK from HSM_oem if 2 is checked correctly. At this time, the SSK is exported in an encrypted state by using the public key Pk_ecu or the common key Psk of the ECU according to the type of the ECU. Export data as Exported-OEM_SSK.
4) The OEM server adds the signature generated by the OEM server public key Sk_oem to the data obtained by combining Exported-OEM_SSK and the time stamp, and transmits it to DT.
5) DT authenticates the received data.
6) When 5 is correct, DT adds the MAC generated by Mk to the data obtained by combining Exported_SSK and the time stamp and transmits the data to ECU.
7) The ECU authenticates the received data.
8) If 7 is correct, the ECU imports Exported_SSK into HSM_ecu.

9) The ECU adds the MAC generated by Mk to the data obtained by combining the Ack and the time stamp to inform that the SSK has been imported, and sends it to DT.

Firmware download

In this step the DT downloads the encrypted and signed firmware received from the OEM server to the ECU.

1) The DT is encrypted by SSK and transmits the signed firmware data, the ECU configuration register (ECR) reference and the time stamp to the ECU.

2) The ECU decodes and verifies the data received by the HSM_ecu and deploys the firmware to the RAM. Note that the download of 1 and the check of 2 are repeated for each block.

3) When all the firmware data are downloaded by the ECU, DT adds the MAC generated by Mk to the data obtained by combining the transfer_exit message and the time stamp and transmits it to the ECU.

4) The ECU performs the authentication of 3.

5) If 3 is correct, the ECU adds the MAC generated by Mk to the data obtained by combining the Ack indicating that the download is completed and the time stamp, and transmits the data to DT.

Firmware installation verification

In this step, the downloaded firmware is installed in the ECU.

1) The ECU verifies the signature of the firmware data with a preinstalled OEM manufacturer verification key before reprogramming.

2) If 1 is correct, the ECU installs the firmware. Installation is performed while computing the ECR trust chain.

3) After the firmware is installed, the ECU performs a software consistency check using a callback routine provided by the ECU supplier.

4) The ECU compares the current ECR of the firmware with the reference ECR value.

5) The ECU presets the ECR value of HSM_ecu for secure boot when the comparison of 4 matches.

6) The ECU increments the counter value of HSM_ecu.

7) The ECU performs hardware reset and erases the routine for reprogramming from the flash memory.

8) The ECU starts the application.

9.1.2.4.3 Future outlook

The EVITA project was terminated in 2011 and as of September 2017, it is not expected that this publication will be revised.

9.2 HIS ([b-52] to [b-54])

9.2.1 Introduction

The Hersteller initiative Software (HIS) is a committee consisting of Audi, BMW, Daimler, Porsche, Volkswagen, etc., and is intended to help car manufacturers learn the principles and methods of ECU software and quality assurance. HIS standardized the specification of SHE, a secure hardware module, in 2009.

9.2.2 Introduction of standards and publications

This clause lists the major standards/publications issued by HIS that are considered to be related to remote software updates for automobiles (date of issue).

SHE-Secure Hardware Extension - Functional Specification Version 1.1. (Apr. 2009) [b-52]

– This document describes the specifications of the SHE standard for hardware security modules for in-vehicle microcomputers. Since this document is not available to the public, details of its contents are not included in this report.

The following clause provides an overview of the SHE specifications extracted from published documents.

9.2.2.1 SHE-Secure Hardware Extension – Functional Specification Version 1.1.

9.2.2.1.1 Summary

Issue	April 2009
Positioning	**Standard Specifications (private)** (No legal force at this time) Examples of mounting in the automotive and semiconductor industries
Target	**Hardware** Automotive ECU

9.2.2.1.2 Items related to remote software updates

SHE is an HSM having an AES engine for common key block ciphers, a secure flash memory for storing keys, IDs, etc. The outline of the specifications of the encryption engine and the secure flash memory will be described below.

First, the AES encryption engine supports ECB, CBC, and CMAC as usage modes. It also offers a PRNG with AES in feedback mode.

The secure flash memory consists of 15 key slots and one ID slot. The key slot consists of one ROM slot, 13 flash memory slots, and one RAM slot. A key for generating random numbers is set in the ROM slot. The flash memory slots include one master key, one secure boot MAC key, one secure boot MAC value, and 10 application key slots. The RAM slot is used to store keys for applications. The ID slot is a ROM slot and stores a user ID (UID) which is a unique ID of the HSM. These keys are 128 bits long, and the UID is 120 bits long.

The key slot of the flash memory has a counter value of 28 bits and a flag of 6 bits. The counter value is incremented upon key update and is used to prevent replay attacks. The flag defines the use of the key and the access control to the key.

The update of the secure flash memory on the SHE is performed by the memory update protocol specified in the specification. When the remote software is securely updated, the secure boot MAC value on the secure flash memory must be updated, and the memory must be updated according to the protocol.

9.2.2.1.3 Future outlook

HIS SHE compliant chips from multiple chip vendors is provided. Infineon and NXP, for example, offer SHE chips.

9.3 TCG ([b-55] to [b-67])

9.3.1 Introduction to the organization

Trusted Computing Group (TCG)[57] (NPO) is a non-profit organization established in 2003 with the aim of developing and disseminating industry standards for various types of hardware and software necessary for building reliable platforms and infrastructures as well as integrated public specifications. The organization is made up of approximately 90 member companies worldwide and a liaison of approximately 30 national institutions, universities, and industry associations. Within this

[57] https://trustedcomputinggroup.org/

framework, the Information-technology Promotion Agency, Japan (IPA) and the National Institute of Information and Communications Technology (NICT) have joined as liaison organizations and are actively participating.

The main activities are to establish specifications for the various hardware and software components of the platform/infrastructure by working groups (W Gs) specializing in each of them, to coordinate relationships with other standards from a technical perspective by the Technical Committee (consist of engineers from member companies of the Board of Directors), which is an umbrella organization of the WGs, and to evaluate, finalize, and publish the specifications by the Executive Board based on the activities/opinions of the government agencies in the above liaison. At the same time, these specifications have been proposed to ISO, IETF, etc., which have experience as standardization bodies, and have been certified by these bodies, and as a result, have been certified as international open standards (cognition).

In order to revitalize activities in various regions of the world, TCG is making efforts to establish branches based on local languages in each region (TCG official language is English). The Japan branch was established in 2008. The significance of TCG is explained on the website of the Japan branch of TCG as follows[58].

– *The TCG organization is made up of several working groups that allow experts in individual technical fields to work together on specifications. In these working groups, each member in a competitive and collaborative position is responsible for developing specifications that are interoperable and technologically neutral*.

In 2004, a number of notebook and desktop PCs around the world were loaded with the TCG's (TPM; Trusted Platform Module, ISO/IEC 11889 certified) chip. Since then, the scope of application has been expanded to include mobile phones/smartphones, automatic teller machines (ATMs), point of sales (POS) terminals, routers and other network equipment, industrial equipment, critical infrastructure such as hospitals/police/power plants, and Internet of things (IoT) including automobiles.

Currently, there are 13 permanent member companies (AMD, Cisco, Dell, Fujitsu, HP, HPE, Huawei, IBM, Infineon, Intel, Juniper, Lenovo, Microsoft), and Fujitsu is active as a Japanese company.

9.3.2 Introduction of standards and publications

Here, among the standards/publications published by the TCG, the main publications (date of issue)/source URLs that are considered to be related to the remote software update of automobiles are listed.

TCG TPM 2.0 Library Profile for Automotive Thin Specification, Version 1.1 (May 2018)[59]

– As part of the activities of the Automotive Services Study Sub-Group, which is under the auspices of the Embedded Working Group within the TCG, the TCG aims to minimize the need for a full TPM based on the assumption that a general-purpose TPM is attached to each in-vehicle microcomputer (ECU), which is said to have several dozen to several hundred TPM devices per vehicle. It aims to perform secure OTA software updates for individual ECUs. The first edition was published in March 2015. After that, various updates were made, and the revised edition was published in May 2018. Continue to use ISO 15408 compliant Protection Profile (PP)[60] was published. This made it possible to realize products based on this specification (TPM for automobiles).

[58] https://trustedcomputinggroup.org/work-groups/regional-forums/japan

[59] https://trustedcomputinggroup.org/wp-content/uploads/TCG_TPM_2.0_Automotive_Thin_Profile_v1.1-r15.pdf

[60] https://trustedcomputinggroup.org/wp-content/uploads/TCG_PP_AT_TPM_v1p0_pub.pdf

Guidance for Securing IoT Using TCG Technology (September 2015)[61]

– An official document from the National Institute of Standards and Technology (NIST) (SP 800-147: BIOS Protection Guidelines) published as part of the activities of the IoT Considerations Study Subgroup under the Embedded Working Group within the TCG.[62] Citing "secure software/firmware update mechanisms" for IoT in general, including automobiles.

Clauses 9.3.2.1 to 9.3.2.2.3 give an outline of each standard/publication including a description of the parts that are related to remote update.

9.3.2.1 Automotive Thin Spec

9.3.2.1.1 Summary

Issue	31 May 2018
Positioning	**Specifications** (Not legally binding) This Automotive Thin specification is a TPM 2.0 specification certified as an international standard specification under ISO/IEC 11889.[63] This specification is based on the assumption that the OTA software update of a large number of in-vehicle ECUs is used as a use case, and only the necessary commands are required under the assumption. It is assumed that in the near future, for example, when OTA support at the time of recall is legislated/established as a guideline, OTA software update of in-vehicle ECU based on this specification may be presented as one of the recommended technical solutions. (It is considered that the general understanding can be gained that the legislation/guideline formulation is possible only when there is a prospect of a solution based on specific and publicly available specifications. TCG seems to be aiming for that).
Target	**Security, Hardware, Use cases (ECU software update)** On-vehicle security chip, its specification and operation flow using OTA software update of on-vehicle ECU as one use case.

9.3.2.1.2 Items related to remote software updates

In this specification, the OTA software update of the in-vehicle ECU is described as follows:

1) A chip (Automotive Thin) based on this specification acquires a hash of software at that time of a part (ECU) in charge, generates an electronic signature with a secret key held by the chip itself, and transmits it to an on-vehicle head unit.

2) After the centre receives the information via the head unit and determines the authenticity of the information using the certificate (public key), it analyses the current status, selects the optimal patch, and delivers it to the in-vehicle ECU via the head unit.

3) After updating the software, the Automotive Thin acquires the hash of the updated software again, generates an electronic signature with the secret key held by itself, and transmits it to the in-vehicle head unit.

4) After the Centre receives the information via the head unit and determines the authenticity of the information using the certificate (public key), it confirms the completion of the update of the OTA software and stores the log in a manner that ensures verifiability in the future (error branches at each node are also described in that document ().

[61] https://www.trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_IoT_1_0r21.pdf

[62] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf

[63] https://trustedcomputinggroup.org/tpm-library-specification/

The document, "Confirm the completion of OTA software updates and maintain logs to ensure future verifiability" or (Accountability) is considered to have a very significant meaning. This part, which was not described much in the first edition, is described in detail in a section (4.9) in the revised specification as follows.

- *"4.9 Audit and accountability: TCG supports "audit and accountability" from vehicles to third parties based on a total ecosystem including a chip as Hardware Root of Trust (HRoT = TPM), a security network attestation protocol (TNC: Trusted Network Communications), and central key management (PKI: Public Key Infrastructure) with Remote Center."*

Other official documents, such as those from the National Institute of Standards and Technology (SP 800-19: Mobile Agent Security)[64] clause 3.3 describes Accountability (11, 19/52).

The TCG is confident of its ability to achieve this with technology based on the open standard TPM.

To accomplish this, Automotive-Thin has the following building blocks:

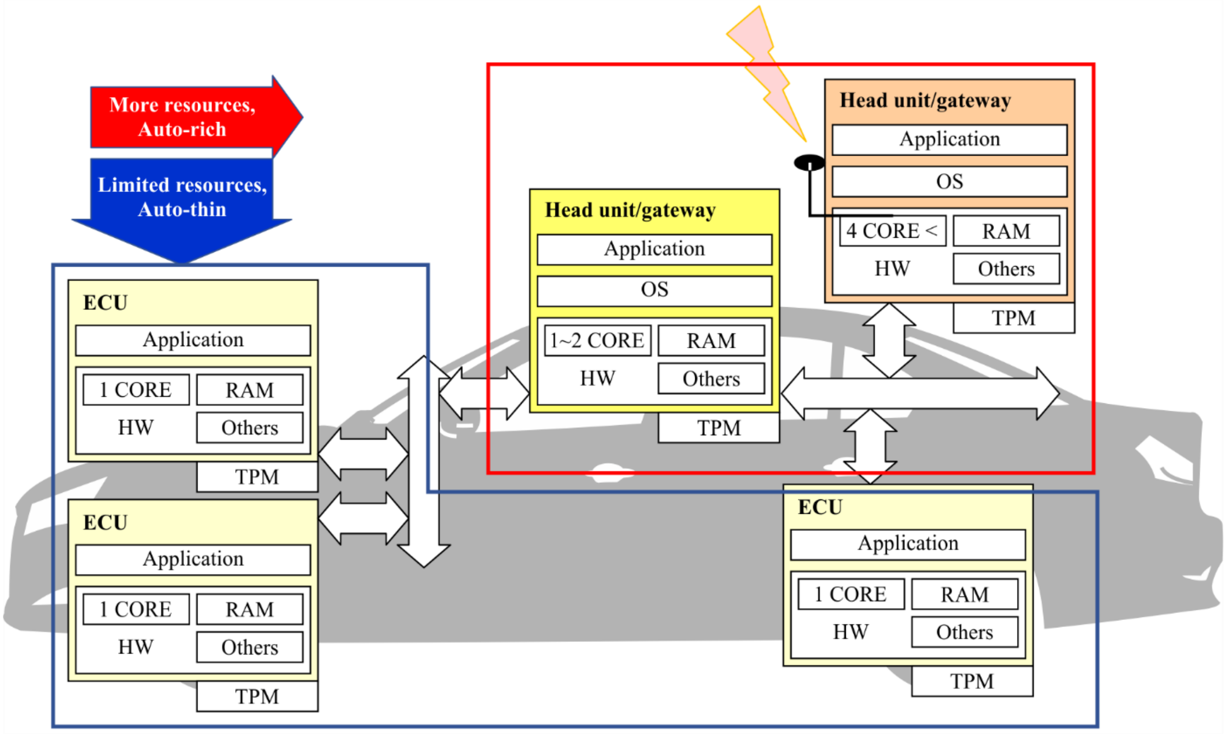
- At least one of RSA 2048 or ECC P 256.
- At least one symmetric algorithm. AES 128 is recommended, others are allowed.
- SHA -256. Other hash algorithms are allowed.

The above is mentioned in the documents published in the following projects related to the Government of Japan and will be introduced for reference.

- *"2015 Strategic Innovation Creation Program (Automatic traveling system): A research and development project on security technologies related to the use of V2X and other external information"*[65]
- *An architecture for adding a security module to each in-vehicle ECU has been proposed. In this system, each ECU uses a Trusted Platform Module (TPM) which is already widely used in ordinary computers. However, as shown in Figure 9-1, instead of uniformly using the same module for all ECUs, it is proposed to use a higher-functional module (Auto-Rich TPM) for the head unit and the in-vehicle gateway (GW) portion, which serve as an entrance for communication with the outside, and a simpler module (Auto-Thin TPM) for the other ECUs (However, all ECUs are expected to utilize Auto-Thin TPM).*

[64] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-19.pdf

[65] http://www.meti.go.jp/meti_lib/report/2016fy/000459.pdf



FSTP.SS-OTA(21)_F9-1

Figure 9-1 – Examples of using TPM Auto-Rich and Auto-Thin

By using both Auto-Rich and Auto-Thin, the head unit/in-vehicle GW verifies the signature of the ECU in the vehicle, and only the signature of the head unit/in-vehicle GW is verified at the other end of the communication. If there is an unauthorized ECU in the vehicle, it is detected by the Auto-Rich TPM of the head unit/in-vehicle GW and reported to the Remote Centre. By using this method, the load of the communication partner is reduced, but resources are required for the Auto-Rich TPM of the head unit/vehicle GW.

9.3.2.1.3 Future outlook

It is not known when the OTA response to recalls will be legislated/made into guidelines, but there has been an increase in the percentage of recalls caused solely by software (reported to be approximately 30% as of 2013)[66] is easy to understand, so it is not too far off. The standard recommendations of UNECE WP.29, referred to in clause 3.4 of this revised report, are considered to be one of the major acceleration factors.

The TCG claims that the specification is valid in terms of OTA and reprogramming concepts, not only in response to recalls, but also in the secure delivery of dynamic maps required for autonomous driving. That is, the in-vehicle map at that time is accurately grasped, and the optimum update information is distributed to support the automatic driving. For that reason, TCG believes the future of the specification is promising in terms of accountability.

9.3.2.2 Guidance for securing IoT using TCG technology

9.3.2.2.1 Summary

Issue	14 September 2015
Positioning	**Guidance** (Not legally binding) Citing guidelines published by NIST, this guidance explains how to update remote software in IoT in general using TCG technology. Based on the fact that the TCG

[66] http://techon.nikkeibp.co.jp/article/STORE/20131216/322880/?rt=nocnt

	specification is an open standard specification, it claims that it meets NIST regulations, including accountability.
Target	**Security, Hardware, Use cases (software update)** Remote software update operation flow using a security chip based on TCG specifications, communication specifications, etc.

9.3.2.2.2 Items related to remote software updates

The guidelines emphasize that the TCG specification is an open standard and emphasize the significance of updating remote software based on the open standard.

In point 3 of clause 9.3.2.1.2, *use cases,* it emphasizes the need for a mechanism to securely check the software status (edition number) of a device and a mechanism to securely update the software in order to maintain the device's health.

In addition, the section entitled "maintaining accountability" clearly states that secure log management and retention is the essence of accountability and enabling forensic analysis. This indicates that the TCG is strongly aware of the NIST document (SP 800-19) cited in 5.1. 2.1. 2. In other words, it can be read that TCG claims that the accountability emphasized in SP 800-19 can be realized by TCG technology, which is an open standard specification.

Clause 4.4.1 *Availability* refers to the NIST document (SP 800-147) as follows:

– *The NIST document [800-147] describes requirements for PC-platform firmware-updates that are also applicable to IoT-devices.*

9.3.2.2.3 Future outlook

This document presents the specific development of the NIST document as a guideline using the open standard TCG technology in a world where many devices, including automobiles, are connected, and may be used in various fields. Also, since this area moves quickly, revision work may be performed frequently.

10 Issues identified concerning standardization and practical application

Based on this survey, issues concerning standardization and practical application were identified.

This clause summarizes the previous clauses and summarizes the issues based on them.

10.1 Summary/descriptions of clauses 7-10

The study/analysis activities were based on the knowledge/connections of the original and revised Working Groups. Here is a summary.

In clause 7, the technical report of SAE and the guideline of NHTSA were described. The SAE technical report describes security and availability when implementing OTA. The cybersecurity best practice of NHTSA also mentions points to keep in mind when implementing reprogramming (wired/OTA) in vehicles (debug and development mode access restrictions, key management, diagnostic access restrictions, etc.). In both cases, it is not mandatory to implement OTA reprogramming, but rather a high-level requirement for implementing reprogramming functions. The survey result on the document "Principles of Automobile Cybersecurity" issued by ACEA was also reported. It also includes a description of OTA reprogramming, drawing attention as the intent of a group of the world's leading auto vendors.

One of the points of appeal in this revision is 7.4 This paper introduces recent trends related to UNECE WP.29 described in the clause. In WP.29, the output of the TFCS was submitted at GRBA-04 in September 2019, approved at the WP.29 meeting in March 2020 at the earliest, and is expected to take effect in 6 months thereafter. In line with this, each country will promote the enactment of laws and regulations. Japan is promoting domestic standardization/legislation based on the draft of the UN WP.29 standard. These movements are considered to have an extremely large influence on a global scale. It is hoped that this revision will provide accurate and quick communication of these developments to the readers.

Clause 8 describes ITU-T Recommendations and ISO standards. For OTA reprogramming, ITU-T SG17 issued Recommendations on software update procedures, data formats, etc., the W3C issued drafts on APIs for accessing vehicle signals and data attributes considered necessary for software update, and oneM2M issued technical reports on use cases, potential requirements, high level architecture, etc. The ITU-T SG17 Recommendation states that in-vehicle communications are outside the scope of the Recommendation. In addition, although the ISO does not directly cover OTA reprogramming, it should be noted that the International Standards for Diagnose Communications were established in TC 22. None of this is intended to force implementation of OTA reprogramming.

Clause 9 summarizes the state of examination and formulation of the system level and the functions/specifications of components required for OTA reprogramming. Specifically, an analysis of the information released by each of the three organizations, EVITA, HIS, and TCG. As a result, it was found that a number of actual automobile vendors were proceeding to the concrete examination stage, guided by these activities. In the description of EVITA, "The EVITA Project was completed in 2011 and as of September 2017, it appears that there are no plans to revise this publication" as described under the topic of prospects. The main purpose of this report is to grasp recent remarkable trends and report them as issues to be discussed in the future. For that purpose, it is necessary to examine this description. In its future outlook section, HIS states that "Several chip vendors offer HIS SHE compliant chips". Therefore, it is important to recognize that it has reached the practical stage. In the description of TCG, as each movement to be noticed from the viewpoint of "Identify issues for standardization and commercialization", 9.3.2.1.2 "Confirm the completion of OTA software updates and maintain logs to ensure future verifiability", 9.3.2.2.3 "Secure log management and retention is the essence of accountability "maintaining accountability" and analysability "enabling forensic analysis" as described and introduced in this Technical Paper . These are assumed to be firmly established, and as a result, it is assumed that the sophistication of measures against security attacks and the recognition of the importance of ensuring accountability are increasing.

As a result, it was confirmed that the technical development including the processing flow of OTA reprogramming, which is the main focus of this report, and the activities for the standardization are under discussion in the organizations mentioned in this report, based on the judgment based on the public information as of the end of September 2017. It was also confirmed that there were differences among organizations in the progress of discussions, whether conclusions were reached/pending in the middle stage, whether issues were solved/remained, etc. The results of these surveys are expected to play an important role in considering and realizing remote vehicle replacement technologies in the future.

In addition to the above, there is no doubt that prompt and accurate report on extremely important global trends, including the publication of the [b-68] WP.29 Recommendation, based on the publication of the revised edition as of the end of September 2019 were carried out.

10.2 Problem arrangement based on the descriptions up to the previous clause

Among those that are likely to be problems in actual application/implementation, for example, the increase in data transfer time is caused by the difference in data extraction, distribution/installation/post-test and 5G applications. Therefore, it is considered that there is a high possibility that the problem will be solved.

The main remaining challenge is the amount of time it takes to write to flash memory, integrity check before and after reprogramming, security attacks during OTA reprogramming. These are suggested by the descriptions in clauses 3 to 5. It is considered that upgrading of countermeasures against these attacks is indispensable.

From a slightly different point of view, to summarize the discussions so far, it is considered that the issues for standardization in remote update technology for automobiles have not been completely mapped out. For example, in clause 7.5.2.1.1 (5) of this report "The test may be conducted by an entity such as a car manufacturer or a parts manufacturer, or by an independent third party." mentioned above is considered to be premised on the assurance of accountability based on the open standard specifications, but there are aspects that cannot be said to be sorted out. In this regard, the progress from the first edition to the revised edition which is described in clause 9.3.2.1.2 of this Technical Paper. that the expansion of the weight of accountability and the presentation of concrete measures should have an extremely significant direction.

These issues should be discussed in the future.

Bibliography

[1] TTC Technical Report TR-1068 version 2
Current standardization movement and issues before practical use for over the air updating in vehicle (November 2016)
https://www.ttc.or.jp/document_db/information/view_express_entity/1071

[2] The Case for Cellular V2X for Safety and Cooperative Driving (November 2016)
http://5gaa.org/news/white-paper-placeholder-news-for-testing/

[3] 5GAA Report shows superior performance of Cellular V2X vs DSRC (October 2018)
http://5gaa.org/news/5gaa-report-shows-superior-performance-of-cellular-v2x-vs-dsrc/

[4] Toward fully connected vehicles: Edge computing for advanced automatic communications (December 2017)
http://5gaa.org/news/toward-fully-connected-vehicles-edge-computing-for-advanced-automotive-communications/

[5] ACEA Principles of Automobile Cybersecurity
http://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf

[6] ISO/SAE AWI 21434 Road Vehicles – Cybersecurity engineering (Under Development)
https://www.iso.org/standard/70918.html

[7] Firmware Update Over The Air (FOTA) for Automotive Industry (August 2007)
https://www.sae.org/publications/technical-papers/content/2007-01-3523/

[8] Over the Air Software Update Realization within Generic Modules with Microcontrollers Using External Serial FLASH (March 2017)
https://www.sae.org/publications/technical-papers/content/2017-01-1613/

[9] Analysis of Software Update in Connected Vehicles (April 2014)
https://www.sae.org/publications/technical-papers/content/2014-01-0256/

[10] OTA flashing: the challenges and solutions (January 2016)
https://www.sae.org/news/2016/01/ota-reflashing-the-challenges-and-solutions

[11] Feasibility Study for a Secure and Seamless Integration of Over the Air Software Update Capability in an Advanced Board Net Architecture (April 2016)
https://www.sae.org/publications/technical-papers/content/2016-01-0056/

[12] Safe and Secure Software Updates Over The Air for Electronic Brake Control Systems (September 2016)
https://www.sae.org/publications/technical-papers/content/2016-01-1948/

[13] OTA updating bringing benefits, challenges (August 2016)
https://www.sae.org/news/2016/08/ota-updating-brings-benefits-challenges

[14] Improvement of the Resilience of a Cyber-Physical Remote Diagnostic Communication System against Cyber Attacks (April 2019)
https://www.sae.org/publications/technical-papers/content/2019-01-0112/

[15] System Engineering for Automated Software Update of Automotive Electronics (April 2018)
https://www.sae.org/publications/technical-papers/content/2018-01-0750/

[16] Measures to Prevent Unauthorized Access to the In-Vehicle E/E System, Due to the Security Vulnerability of a Remote Diagnostic Tester (March 2017)
https://www.sae.org/publications/technical-papers/content/2017-01-1689/

[17] Over-the-air (OTA) programming allows remote software updates: Over-the-air affair (February 2019)
https://www.sae.org/news/2019/02/over-the-air-remote-programming

[18] OTA will drive cybersecurity programs (April 2018)
https://www.sae.org/news/2018/04/ota-will-drive-cybersecurity-programs

[19] UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles (June 2020)
https://www.unece.org/info/media/presscurrent-press-h/transport/2020/un-regulations-on-cybersecurity-and-software-updates-to-pave-the-way-for-mass-roll-out-of-connected-vehicles/doc.html

[20] UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles (June 2020)
http://www.unece.org/fileadmin/DAM/trans/doc/2020/WP.29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

[21] Proposal for a Recommendation on Cyber Security (September 2019)
https://wiki.unece.org/pages/viewpage.action?pageId=87623695
TFCS 16 -08 (Chair) ECE-TRANS-WP.29-GRVA -2019 -02 e Cyber Security Proposal latest version.docx

[22] Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues (September 2019)
https://wiki.unece.org/pages/viewpage.action?pageId=87623695
TFCS 16 -09 (Chair) ECE-TRANS-WP.29-GRVA -2019 -03e Software update proposal latest.docx

[23] Automated Driving Systems 2.0 (September 2017)
https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[24] Cybersecurity Best Practices for Modern Vehicles (October 2016)
https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf

[25] Federal Motor Vehicle Safety Standards; V2V Communications NPRM (December 2016)
http://www.safercar.gov/v2v/pdf/V2V%20NPRM_Web_Version.pdf
https://www.gpo.gov/fdsys/pkg/FR-2017-01-12/pdf/2016-31059.pdf

[26] NIST Cyber Security Framework
https://www.nist.gov/cyberframework

[27] SAE J 3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (January 2016)

[28] ISO/IEC 27000: 2016 Information technology – Security techniques – Information security management systems – Overview and vocabulary

[29] NIST FIPS PUB 140-2: Security Requirements for Cryptographic Modules (July 2007)

[30] ISO 13400-1:2011 Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 1: General information and use case definition
https://www.iso.org/standard/53765.html

[31] ISO 14229-1:2013
Road vehicles – Unified diagnostic services (UDS) – Part 1: Specification and requirements
https://www.iso.org/standard/55283.html

[32] ISO 22901-1:2008 Road vehicles – Open diagnostic data exchange (ODX) – Part 1: Data model specification
https://www.iso.org/standard/41207.html

[33] Investigation Report on Issues for Advancement of ITS and Automatic Operation Using Cellular Communication Technology
https://itsforum.gr.jp/Public/J7Database/p62/Cellular_system_201906.pdf

[34] 5 GMF Security Ad Hoc Activities (17 June 2019)
TTC Seminars

[35] ITU-T F.749.2: Service requirements for vehicle gateway platforms (March 2017)
https://www.itu.int/rec/T-REC-F.749.2/en

[36] ITU-T F.749.1: Functional requirements for vehicle gateways (November 2015)
https://www.itu.int/rec/T-REC-F.749.1/en

[37] ITU-T H.560: Communications interface between external applications and a vehicle gateway platform (December 2017)
https://www.itu.int/rec/T-REC-H.560/en

[38] ITU-T H.550 Architecture and functional entities of vehicle gateway platforms (December 2017)
https://www.itu.int/rec/T-REC-H.550/en

[39] ITU-T X.1373: Secure software update capability for intelligent transport system communication devices (March 2017)
http://www.itu.int/rec/T-REC-X.1373/en

[40] TR-0026-Vehicular Domain Enablement
http://www.onem2m.org/technical/latest-drafts

[41] Automotive and Web at W3C
http://www.w3.org/auto/

[42] Automotive Working Group
http://www.w3.org/auto/wg/

[43] Vehicle Information Access API
https://www.w3.org/TR/2017/WD-vehicle-information-api-20170605/

[44] Vehicle Signal Server Specification
https://www.w3.org/TR/2016/WD-vehicle-information-service-20161020/

[45] Automotive and Web Platform Business Group
http://www.w3.org/community/autowebplatform/

[46] Cyber-Security in the Connected Car Age GENIVI Conference - Seoul (21 October 2015)
https://lists.w3.org/Archives/Public/public-auto-privacy-security/2015Oct/att-0005/Cyber-security_Connected_Car_Age-GENIVI.pdf

[47] Deliverable D 2.1: Specification and evaluation of e-security relevant use cases (December 2009)
https://www.evita-project.org/Deliverables/EVITAD2.1.pdf

[48] Deliverable D 2.3 Security requirements for automatic on-board networks based on dark-side scenarios (December 2009)
https://www.evita-project.org/Deliverables/EVITAD2.3.pdf

[49] Deliverable D 3.2 Secure on-board architecture specification (August 2011)
https://www.evita-project.org/Deliverables/EVITAD3.2.pdf

[50] Deliverable D 3.3 Secure on-board protocols specification (July 2011)
https://www.evita-project.org/Deliverables/EVITAD3.3.pdf

[51] Arm Ltd., Cortex-M3
https://developer.arm.com/products/processors/cortex-m/cortex-m3

[52] SHE-Secure Hardware Extension - Functional Specification Version 1.1. (April 2009)
https://argus-sec.com/hersteller-initiative-software-his-security-hardware-extension-she/

[53] Infineon AUDO MAX SHE Enhances In-Vehicle Security and Tamper-Proofs Electronic Control Units
https://www.infineon.com/cms/en/about-infineon/press/market-news/2011/INFATV201111-012.html

[54] 32 bit microcomputer with on-chip security function for body gateway
http://www.nxp.com/docs/en/supporting-information/E_SecurityMCU_JA.pdf

[55] TCG (Trusted Computing Group)
https://trustedcomputinggroup.org/

[56] TCG TPM 2.0 Library Profile for Automotive Thin Specification, Version 1. 1 (May 2018)
https://trustedcomputinggroup.org/wp-content/uploads/TCG_TPM_2.0_Automotive_Thin_Profile_v1.1-r15.pdf

[57] Guidance for Securing IoT Using TCG Technology (September 2015)
https://www.trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_IoT_1_0r21.pdf

[58] NIST SP 800-147: BIOS Protection Guidelines
https://www.trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_IoT_1_0r21.pdf

[59] NIST SP 800-19 - Mobile Agent Security
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-19.pdf

[60] 2015 Strategic Innovation Creation Program (Automatic traveling system): A research and development project on security technologies related to the use of V2X and other external information
http://www.meti.go.jp/meti_lib/report/2016fy/000459.pdf

[61] Protection Profile Automatic-Thin Specific TPM Version 1.0 (December 2018)
https://trustedcomputinggroup.org/wp-content/uploads/TCG_PP_AT_TPM_v1p0_pub.pdf

[62] Guidance for Securing IoT Using TCG Technology (September 2015)
https://www.trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_IoT_1_0r21.pdf

[63] An official document from the National Institute of Standards and Technology (NIST) (SP 800-147: BIOS Protection Guidelines) published as part of the activities of the IoT Considerations Study Subgroup under the Embedded Working Group within the TCG
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf

[64] This Automotive Thin specification is a TPM 2.0 specification certified as an international standard specification under ISO/IEC 11889
https://trustedcomputinggroup.org/tpm-library-specification/

[65] National Institute of Standards and Technology (SP 800-19: Mobile Agent Security)
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-19.pdf

[66] 2015 Strategic Innovation Creation Program (Automatic traveling system): A research and development project on security technologies related to the use of V2X and other external information
http://www.meti.go.jp/meti_lib/report/2016fy/000459.pdf

[67] It is not known when the OTA response to recalls will be legislated/made into guidelines, but there has been an increase in the percentage of recalls caused solely by software (reported to be approximately 30% as of 2013)
http://techon.nikkeibp.co.jp/article/STORE/20131216/322880/?rt=nocnt

[68] UNECE WP.29 – World Forum for Harmonization of Vehicle Regulations (WP.29)
https://unece.org/transport/vehicle-regulations/wp29-world-forum-harmonization-vehicle-regulations-wp29