ISSN 0915-3160

通巻百二十三号

New Breeze

Quarterly of The ITU Association of Japan

No. 3
Vol. 31 july 2019
Summer

Special Feature

Connected Cars

Connected Cars: The Chance of a Lifetime for Industrial and Societal Reform
Trends in the Standardization of Connected Cars in ITU-T SG16
Standardization Trends in Security Technologies for Connected Cars at ITU-T
Software Updates for Connected Cars
Summary of Discussions on Vehicle Cybersecurity and Software Updates at the World Forum for Harmonization of Vehicle Regulations (WP.29)
Communicating via Connected Cars in the Event of a Natural Disaster
Connected Car Initiatives
Introduction to Vehicle Domain Services Provided by Connected Cars

New Breeze ISSN 0915-3160
Quarterly of The ITU Association of Japan
BN Gyoen Bldg., 1-17-11 Shinjuku, Shinjuku-ku,
Tokyo 160-0022 Japan
Tel: +81-3-5357-7610 Fax: +81-3-3356-8170
https://www.ituaj.jp/?page_id=310

Publisher: Toru Fukuoka

Editors: Junichi Kishimoto
Kaori Ohno
Naoko Ishida

Letters to *New Breeze*

New Breeze welcomes readers' opinions. Please send comments with your name, address, and nationality by e-mail, fax, or post to the editor.

e-mail address: kikanshi@ituaj.jp

Subscription forms are available on the ITU-AJ website:
http://www.ituaj.jp/english/subscription_form.pdf

Subscription Fee:

Single issue:	¥1,500
Annual subscription (4 issues):	¥6,000

C O N T E N T S

About ITU-AJ

The ITU Association of Japan (ITU-AJ) was founded on September 1, 1971, to coordinate Japanese activities in the telecommunication and broadcasting sectors with international activities. Today, the principle activities of the ITU-AJ are to cooperate in various activities of international organizations such as the ITU and to disseminate information about them. The Association also aims to help developing countries by supporting technical assistance, as well as by taking part in general international cooperation, mainly through the Asia-Pacific Telecommunity (APT), so as to contribute to the advance of the telecommunications and broadcasting throughout the world.

Connected Cars: The Chance of a Lifetime for Industrial and Societal Reform

Yuji Inoue
President, KNOWetNOVA Co. Ltd.
Toyota Info Technology Center (Retired)

1. Introduction

5G is a hot topic in the field of communications, and anticipation is increasing with the approach of the 2020 Olympics. Most people in the industry believe that powerful new 5G capabilities such as 4K/8K video and IoT connectivity will lead to creation of new businesses and will enrich all of our lives. However, there seems to be no real understanding of changes connected cars will bring to society in the near future. Awareness varies, with comments such as, "Why would cars need communication?", "Well, it will probably help reduce accidents," "Of course they will need to communicate if they are going to drive by themselves,", and "I guess cars need to connect for car sharing, but can't I just use the smartphone application?" Most people do not seem to think beyond that connecting will be a good thing.

"Connected, Autonomous, Shared/Service, Electric" (CASE) has been a popular key phrase in the media lately, and competition and collaboration with the ICT industry (largely the GAFAM companies) is shaking up the automobile industry and promises to inject it with new energy and vitality.

The author is convinced that the so-called digital transformation being discussed around the world ("Society 5.0" in Japan) will be triggered by connected cars even more than by 5G, and they will bring industrial and social reform and innovation over the coming ten years. The next few years will determine whether Japan can play a leading role in this new wave.

2. What is a Connected Car?

As you would expect, a "connected car" is a car that is connected. But this is not a passive thing, as the name may suggest. Most of the automobile industry has felt that "connecting" is more appropriate than being "connected to". Most images of connected cars so far have the vehicle in the center, making connections with other entities. This is a natural perception, given the 100-year history of the automobile industry, with OEMs holding the top position in the supply chain, as shown in Figure 1 (here, OEM refers to manufacturers that manufacture entire vehicles, such as Toyota. This is in contrast to the electronics sector, where OEMs are often subcontracted manufacturers).

However, connected cars are actually "cars that can accept connections." Already, many smartphones, PCs, IoT devices and other user devices are connected to the Internet, and there are computers and data centers performing tasks and providing services all over the world. These comprise a huge industry and social system. The truth is that connected cars are just a new entity that this existing network will connect to, and there will be no new network just for connected cars. Suppose, for the sake of argument, that an independent network was built for communication between self-driving vehicles. Even that were the case, many ICT businesses would encroach upon it, as shown in Figure 2.

Figure 1: Current manufacturing in the automobile sector

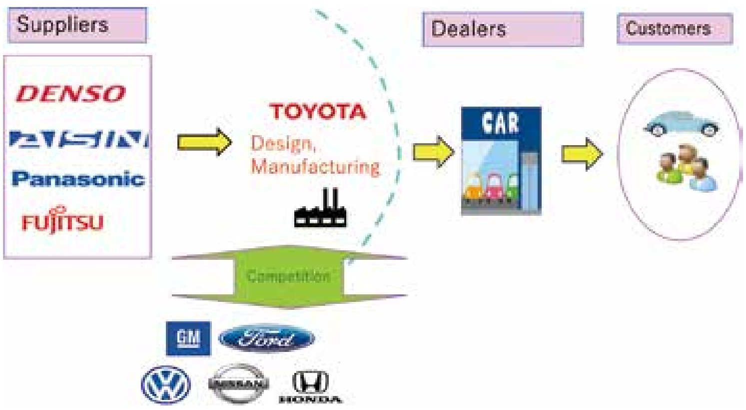
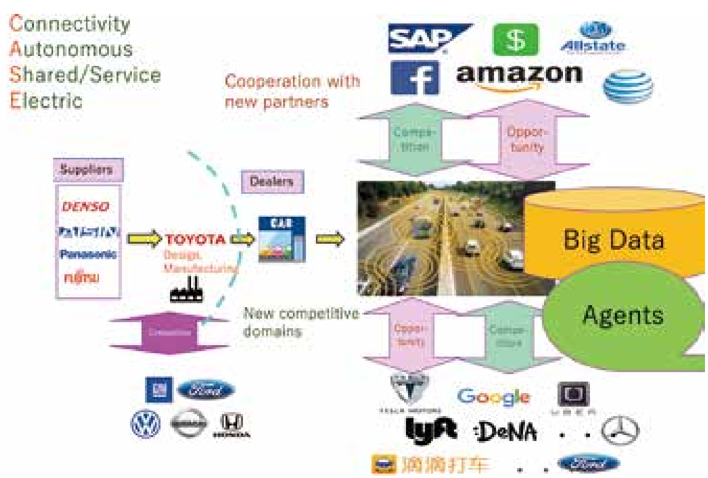


Figure 2: The CASE era: Cooperation and competition among different sectors



So, are connected cars to be just another new network user? The author thinks not, because in many aspects, such as price, functionality, industry structure, and role in society, they are very different from conventional network terminals.

3. Connected Cars: A powerful new force in the market

Consider price. Even light vehicles can cost a million yen, luxury vehicles can exceed tens of millions, and there are vehicles on the road worth over 100 million yen. Of course, they have a range of performance characteristics, but there are also elements such as navigation, entertainment and design, which are for comfort or to express human sentiments like individuality or social status. There are also many other important factors that differentiate automobiles, such as safety and environmental considerations. Smartphones and other existing terminals have no ability to move autonomously, but the basic functionality of automobiles is to move people and luggage, and when they are fully autonomous (Level 5), they will be able to move freely over a wide range and at high speed without a driver. The scale of the auto industry GDP is also several times that of the ICT industry.

So what sorts of capabilities will such connected cars have in the future? No one can predict accurately where these advances will lead, but we will focus on five new capabilities that connected cars are predicted to bring in the future, as follows. They are illustrated in Figure 3.

[New capability 1] Information processing power over 2000 times that of a PC

According to a Nikkei XTECH report[1], the processing power required to realize autonomous driving will be equivalent to 2,300 current PCs.

[New capability 2] 1 TB of non-volatile memory and large amounts of DRAM

According to a MONOist promotional report[2], 1 TB of flash memory will be needed to implement autonomous driving, including 256 GB for a dynamic map, and other aspects such as AI. Also including memory for other ordinary functionality, connected cars will require several times the memory of a current PC. Recent developments in memory technology and decreasing prices mean that the cost will no longer be a concern, so we can assume that connected cars will not be restricted by memory capacity.

[New capability 3] Highly reliable communication

The wireless communication requirements of connected cars are not yet settled. The main reasons for this are that the division of functionality between autonomy and cooperation for self-driving cars has not been finalized, and that a uniform division of such functions cannot be set due to great differences in the levels of communication and intelligent transport system (ITS) infrastructure in countries and regions around the world. A major challenge faced in development of autonomous driving technology is ensuring autonomy (the ability of a vehicle to move in standalone situations). From that perspective, strictly speaking, connected cars should not need communication. Mobility as a Service (MaaS) is a typical example of the need for communication. Rather than selling vehicles, a MaaS business such as car sharing sells transport, as described in Section 4. In such cases, all vehicles would be equipped with 5G or the current version of LTE.

Another example of a communication function outside of this trend is to provide communication between vehicles in times of large-scale disaster. This is described in another article in this special feature. Details can be found in the article, but the main point is that systems will be equipped with communication that uses unoccupied wideband signals such as Wi-Fi and digital terrestrial broadcasting and have a message box, in addition to having Dedicated Short Range Communications (DSRC) for ITS. There is also active research on new communication methods to meet the future demand for vehicle-to-vehicle communication, such as overlaying communication on radar functionality, which currently only functions as a sensor.

[New capability 4] Input and output of diverse types of information

The two photos at the top of Figure 3 show bumper models for a self-driving car from Continental Corp., which were exhibited at the Tokyo Motor Show in 2016. Front and rear bumpers are each equipped with about 10 sensors. These sensors play the role of a human driver's eyes, and can include cameras, radio-wave RADAR, and laser RADAR (called LiDAR). The bumpers are also equipped with environmental sensors for factors such as temperature and gases. Outputs include speakers and alarms, and a whole-body display is also being developed, so a diversity of input and output capabilities not seen in other terminals is also a strength.

Combining data from these sensors with vehicle running data, a single vehicle is expected to produce on the order of 100 GB/day [2]. If all 80 million vehicles in Japan were to transmit all of this data, it would amount an astronomical figure of eight exabytes/day (1 exabyte = 1,000 petabytes).

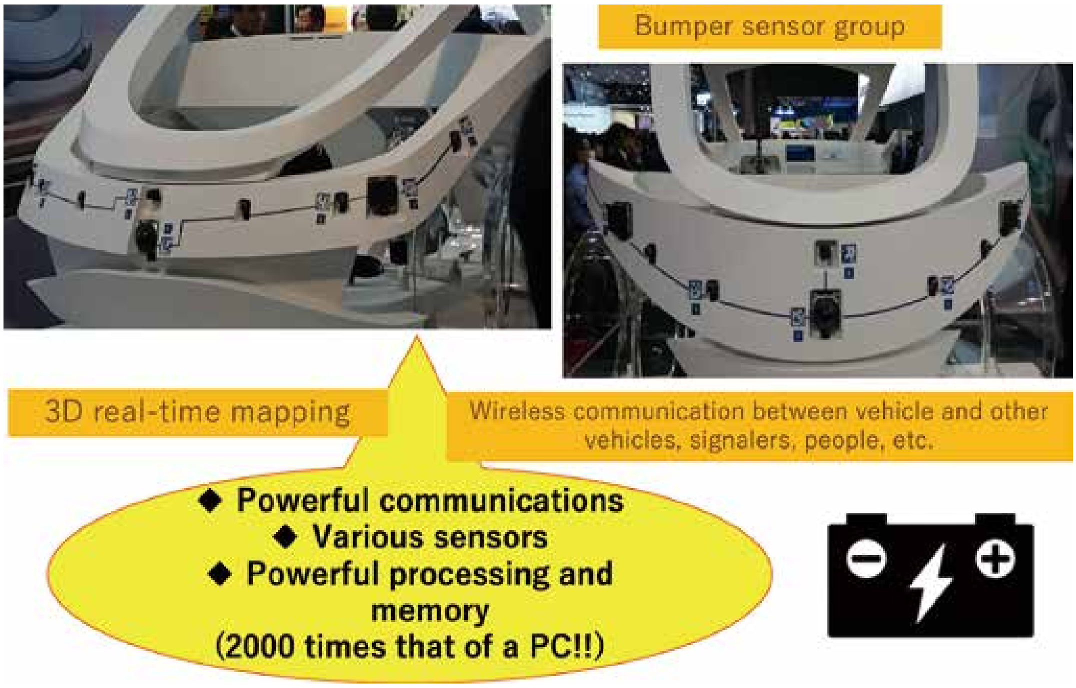
[New capability 5] High capacity battery

Current hybrid cars have battery capacities of around 4 kWh, and electric vehicles, in the range of 40 to 100 kWh, but energy self-sufficiency is expected to continue to increase. In the near future, connected cars will use sustainable energy, and regardless of the state of the ignition key, the vehicle will function full-time and be available as an active data communication hub, 24 hours a day.

4. Using the emerging connected cars

In Japan, specialized services for cars began to appear during the late 1990s and early 2000s, such as collection of traffic congestion data for car navigation systems, and creation of navigable route maps during a disaster. In the USA, most

■ **Figure 3: New connected car features**



such systems were linked to smartphones. New transportation services such as Uber began to appear in 2009, and with the announcement of Apple's CarPlay and Google's Android Auto in 2013, communication-driven architectures emerged, having the vehicle as a mirror terminal for the smartphone. Currently, there are many implementations of OEM car navigation systems. All of these have been intended mainly to enhance and expand on navigation functions and entertainment services for drivers and passengers, and were not attempting to change how vehicles are used, with the exception of Uber's model.

In contrast, the new type of business model called Mobility as a Service (MaaS) has recently been in the limelight and is becoming more practical. Examples have included features such as discounted insurance based on driving ability or carefulness, and centralized booking and payment of transport to the desired destination, whether by train, car-share or other means[3]. Extensions to the concept of MaaS have also started to appear, with proposals for new connected cars and other vehicles based on CASE. One example is Toyota's e-Palette, which attracted attention at CES in 2018[4]. e-Palette is envisioned as the first model car implementing CASE, and this one vehicle is able to take various forms as needed, whether for ride-sharing, or as a showroom, accommodation, a mobile workshop, a restaurant, or a mobile bazaar. See the promotion video with Reference[4] for an overview of any of these applications.

5. Industrial and societal innovation due to connected cars (author's proposals)

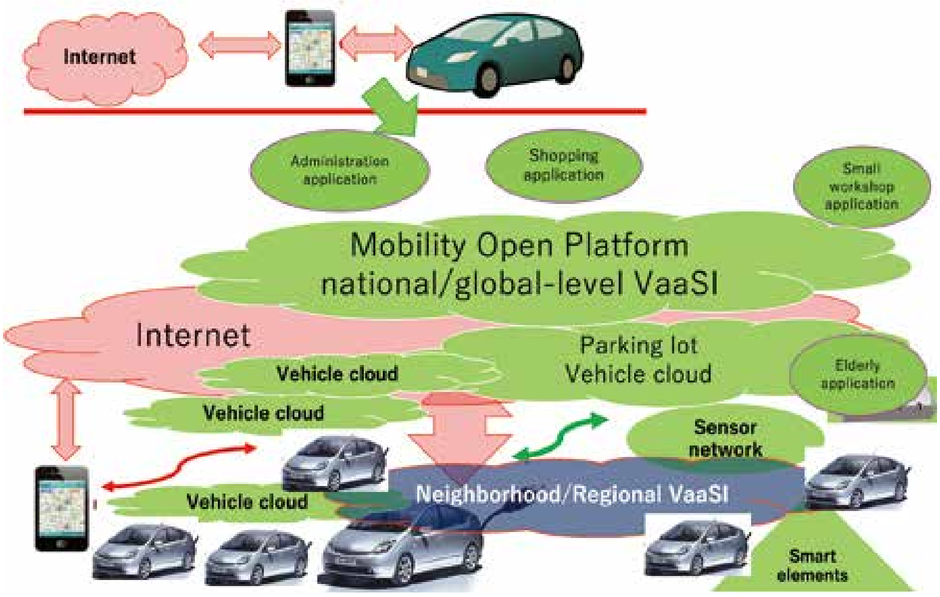
Here, we introduce a new MaaS industry that has begun to operate using the abundant capabilities and potential in the information and communication systems of connected cars. There are many other articles about self-driving and electric vehicles so we refer to them for details, but in this final section of this article, we propose that beyond simply making mobility more efficient and diverse, the capabilities of connected cars in the future will constitute Vehicles as a Social Infrastructure (VaaSI), creating new information and communication infrastructure in society and providing solutions to various social issues.

5.1 Level of connected car adoption

e-Palette and other connected cars (with CASE capabilities) are expected to be introduced and start spreading in society in 2020, as part of an Tokyo Olympic Showcase. Cars are generally replaced every nine years in Japan[5], so ten years from now, in 2030, we can expect that half of the 80 million cars being used in Japan will be equipped with CASE functionality. In other words, within ten years, 40 million vehicles operating in Japan will be equipped with the five new ICT capabilities described in Section 3. Of these, 10 million will be commercial vehicles operating throughout Japan, day and night, whether making deliveries, distributing mail, or collecting trash. On the other hand, 30 million will be for private use, and 95% of the time will be parked, either at home or at work. Thus, 28 million vehicles, each with the processing power of 2000 PCs will be unused (parked) and standing by.

Note that there are reports that the total number of vehicles will drop by 40% due to car sharing[6], but even if the 80 million figure drops to 48 million, it will be an ample amount for a distributed system, and will be effective for VaaSI as proposed in this section.

Figure 4: VaaSI overview



5.2 VaaSI: Establishing a platform

We propose that a new platform (apart from smartphones) be created that will realize various social functions using the powerful information and communication functions of connected cars (the five new capabilities discussed in section 3). An overview of this platform is shown in Figure 4. Space does not allow discussion of the details, but two main architectural points are as follows.

[Key Point 1] The sensors, display, and speakers of mobile connected cars are used for input and output of information for social services. Of course, they will be linked with smartphones.

With the cameras and other sensors on connected cars, it will be possible to collect real-time image, temperature, gas and other information on environment and other conditions in all corners of the country, day or night. This social data can be used to create detailed administrative services and new commercial services. With a ratio of one connected car per three residents, their information output capabilities would be readily available to residents from any connected car parked nearby, as a means of promoting administrative services, and they could also be linked with smartphones, TV and other mass media.

[Key point 2] Parked connected cars could be used as a local “mobility cloud”, with for example, ten cars in a parking lot providing the power of 20,000 PCs.

Tens of millions of connected cars could be connected organically, forming a hyper-distributed virtually layered platform that could be used in a layered fashion, from strictly-local to wide-area. This multi-layer cloud would manage and operate societal data, and also provide APIs to local society, businesses and individuals, to create new types of social service industries. To ensure that such community-contributed social services can be used safely and securely, the administrative system will ensure transparency and assignment of responsibility.

6. Conclusion

Connected cars have finally become devices that “allow connection.” There is a wide range of devices such as smartphones and PCs that already connect to the Internet, but connected cars differ from these on the following points.

- They are able to move autonomously,
- They can transport people and goods,
- They have thousands of times the processing power of PCs,
- They can connect with IoT devices (hub functionality),
- They can input and output information in a variety of formats (multimedia)
- Safety is a critical product feature,
- They can store sustainable energy,
- Etc.

Self-driving cars and car sharing are currently attracting attention, but with these strengths, a wide range of uses that we have not even imagined will undoubtedly emerge in the coming ten years. We look forward to Japan taking the lead in realizing these and incorporating them in society, creating social innovation, and triggering revitalization in industry.

References
[1] M. Kimura, “News Trend Commentary: ‘Semiconductor processing performance’ an issue with Toyota’s autonomous driving,” Oct. 24, 2017 Update. (in Japanese) http://tech.nikkeibp.co.jp/dm/atcl/feature/15/122200045/102300197/
[2] PR/MONOist, “Why fully autonomous driving vehicles need 1 TB of flash memory,” June 20, 2017 Edition (in Japanese) http://monoist.atmarkit.co.jp/mn/articles/1706/20/news001.html
[3] Jidounten LAB, “Introduction to MaaS,” Sept. 10, 2018 Update. (in Japanese) https://jidounten-lab.com/y_5750
[4] Toyota, “e-Palette Concept,” Jan. 9, 2018 Update. (in Japanese) https://newsroom.toyota.co.jp/jp/album/videos/20508200/
[5] Garbage News, “Graphing annual passenger car replacement (with a new car) rates,” Apr. 22, 2018 Update. (in Japanese) http://www.garbagenews.net/archives/2056638.html
[6] T. Miyata, “Shocking prediction of 40% drop in auto sales,” May 23, 2016 Update. (in Japanese) http://wedge.ismedia.jp/articles/-/6805

Trends in the Standardization of Connected Cars in ITU-T SG16

Hideki Yamamoto
Vice-chairman, ITU-T SG16
Network Systems Division, Telecom System Business Division,
Oki Electric Industry Co., Ltd.

1. Introduction

ITU-T is engaged in the standardization of security and applications in ITS communication, and is collaborating with various standardization organizations to this end. Specifically, studies related to security in ITS communication are being pursued by SG17 (Security), and discussions of services and applications are taking place in SG16 (Multimedia). Furthermore, for collaborative work with other organizations, ITU-T has provided a mechanism called CITS (Collaboration on ITS Communication Standards)[1] whereby we have reached out to establish collaboration and cooperation with ITU-R, ISO, IEEE, and regional standards organizations and forums in standardization efforts relating to ITS communication, where interoperability will be essential. The Focus Group on Vehicular Multimedia associated with ITS (FG-VM) was established at the SG16 meeting in July 2018, reflecting the growing interest in standardization related to ITS[2]. This article describes the positioning of FG-VM in SG16, introduces the existing ITS standards, and describes the activities of FG-VM.

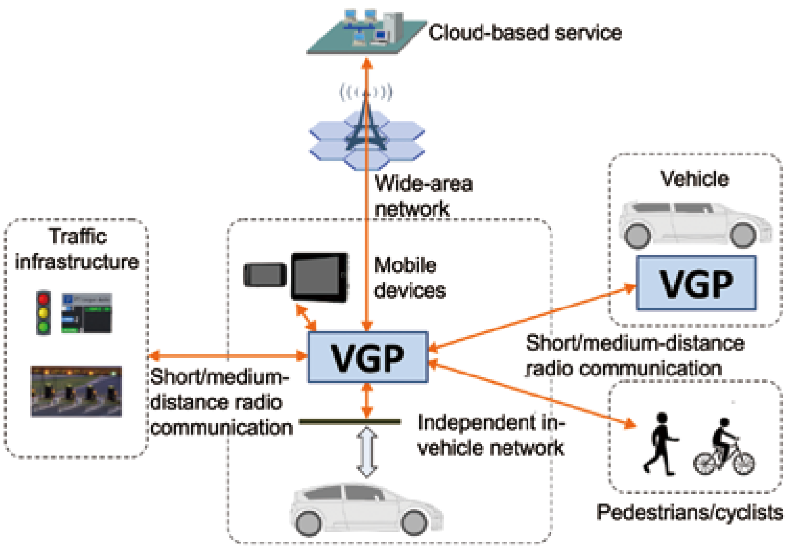
2. The status of ITS related standardization in SG16

SG16 has been promoting standardization not only of video compression techniques such as MPEG-2, H.264 and H.265 that are used in broadcasting and Internet video services, but also of technologies related to diverse services that use these techniques. With regard to Question 27 of SG16 (denoted as Q27/16), we are formulating ITS-related recommendations centered on vehicle gateways. Meanwhile, focus groups such as FG-VM are not aiming for specific standardization targets, but are laying the groundwork for standardization, including the study of specific use cases and the shortfalls of existing standards in promoting the popularization of these use cases. For this reason, members from outside ITU-T are also able to participate. Items requiring standardization that have been brought to light through the work of FG-VM will be recommended in Q27 or another SG16 Question. For example, it is conceivable that standardization of questions related to vehicle IPTV service terminals can be pursued in Q13, which deals with IPTV terminals. Other SGs may also be consulted if it is considered to be necessary.

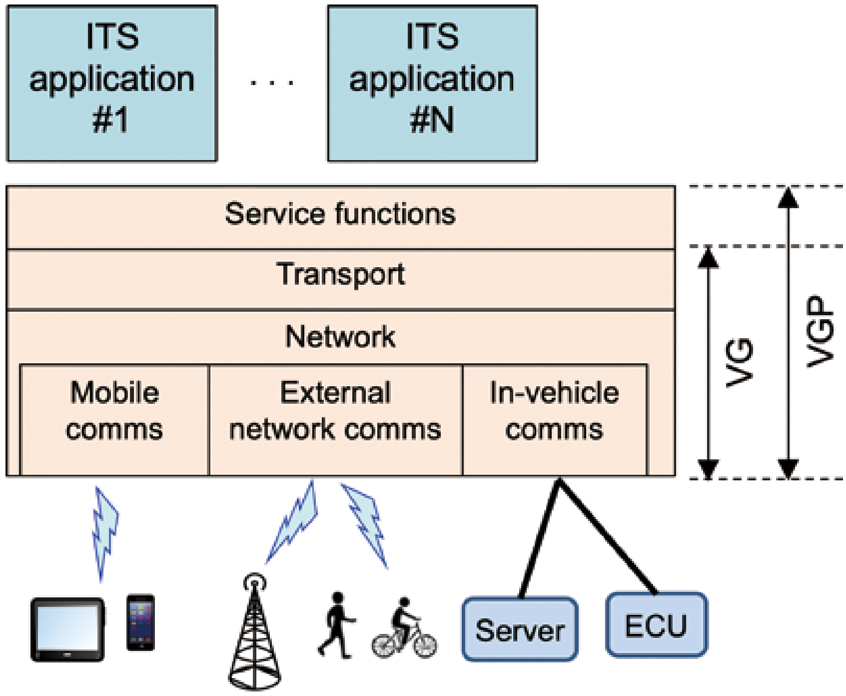
3. Q27/16 ITS-related Recommendations

In Q27/16, we are standardizing the requirements, functional components and communication interface of the Vehicle gateway platform (VGP). VGP is a set of ICT-related hardware and software that provides an execution environment for higher-level applications where communication is integrated using a Vehicle Gateway (VG). It is assumed that these higher-level applications include ITS, infotainment and the like. Figure 1 shows how VGP relates to external systems. VGP provides a communication

Figure 1: Relationship between VGP and external systems



■ **Figure 2: Scope of VGP**



■ **Table: ITS-related standard documents produced by ITU-T SG16**

Document number	Title	Publication year
ITU-T F.749.1	Functional requirements for vehicle gateways	2015
ITU-T F.749.2	Service requirements for vehicle gateway platforms	2017
ITU-T H.550	Architecture and functional entities of vehicle gateway platforms	2017
ITU-T H.560	Communications interface between external applications and a vehicle gateway platform	2017
HSTP-CITS-Reqs	Global ITS communication requirements	2014

platform for in-vehicle hand-held devices, ECUs and the like, as well as for communication outside the car. Figure 2 shows the scope of VGP. The table shows a list of ITS-related standard documents in ITU-T SG16. We have already completed the standardization of VG functional requirements, VGP service requirements, VGP architecture and functional components, and the communication interfaces between external applications and VGP. A VG consists of hardware mounted in a vehicle, and provides functions for real-time bidirectional communication with equipment both inside and outside the vehicle. It is required to support not only IP but also other communication protocols that are required for ITS services.

4. Focus Group on Vehicular Multimedia (FG-VM)

With the integration of diverse means of communication and broadcast networks and advances in automatic driving technology and the like, it is thought that the car of the future will be more like a living room on wheels. Under these circumstances, FG-VM was established under SG16 in July 2018 for the purpose of clarifying the issues to be standardized in order to realize new vehicle multimedia services. The group is chaired by Jun Li of China's Telematics Industry Application Alliance (TIAA), and the vice-chairs are Gaëlle Martin-Cocher of BlackBerry (Canada) and Kaname Tokita of Honda R&D (Japan). Three WGs have been established to conduct studies relating to use cases, requirements, architecture and implementations, and are currently engaged in discussions of these issues. As the source of the proposal, TIAA is considering the development of satellite entertainment services for vehicles in China. The output of FG-VM is expected to include use cases and standardization issues of services such as these. The sixth FG-VM meeting will be held in Budapest, Hungary on September 11-12, 2019, just before the next SG16 meeting in October 2019.

References
[1] Naito: Recent standardization trends in ITS communication from the perspective of ITU-T SG16, ITU Journal Vol. 47 No. 10 (2017, 10)
[2] Yamamoto: ITU-T SG 16 3rd Meeting Report, ITU Journal Vol. 48 No. 10 (2018, 10) (in Japanese)

Standardization Trends in Security Technologies for Connected Cars at ITU-T

Koji Nakao
Former Vice-chairman, ITU-T SG17
National Institute of Information Communications Technology

1. The significance and necessity of security standardization for connected vehicles

As vehicles become more autonomous and connect to networks such as the Internet, ensuring the security of their on-board systems has become a top priority for the car industry. In recent years, the deployment of new connection services and autonomous driving functions in vehicles has also made them potential targets for malicious hackers. Furthermore, it is envisaged that large numbers of ECUs (electronic control units) incorporated into modern vehicles will be connected via diverse external networks such as Wi-Fi, mobile phone networks, and the Internet. Ensuring the security of complex systems provided by vehicles is therefore an urgent issue.

Various standards organizations have already begun to take steps towards achieving international standardization with regard to the above issues from the viewpoint of ensuring security in the connected car era. By drawing up standardized international technical specifications such as security frameworks for connected cars, threat analysis and security countermeasures, these efforts have resulted in a useful common reference for many stakeholders with an interest in international standards, and can be expected to provide materials such as international certification rules. This article outlines the trends in connected car security standardization in ITU-T SG17 (Security).

2. Standardization activities at SG17

(1) ITS Security: Question 13

ITU-T SG17 is a study group aimed at security standardization in general. One of its assigned tasks is to work on Question 13, which relates to Intelligent Transport System (ITS) security. This is a new Question that was established in the fall of 2017. It builds on the assumption of a connected car environment, and covers a wide range of topics including the formulation of security frameworks and guidelines, and the technical issues associated with connected cars.

(2) Current status of work on ITS security recommendations

ITU-T SG17 Question 13 is currently working on the Recommendations shown in the table.

Details of Recommendations that are of particular interest in this table are outlined below.

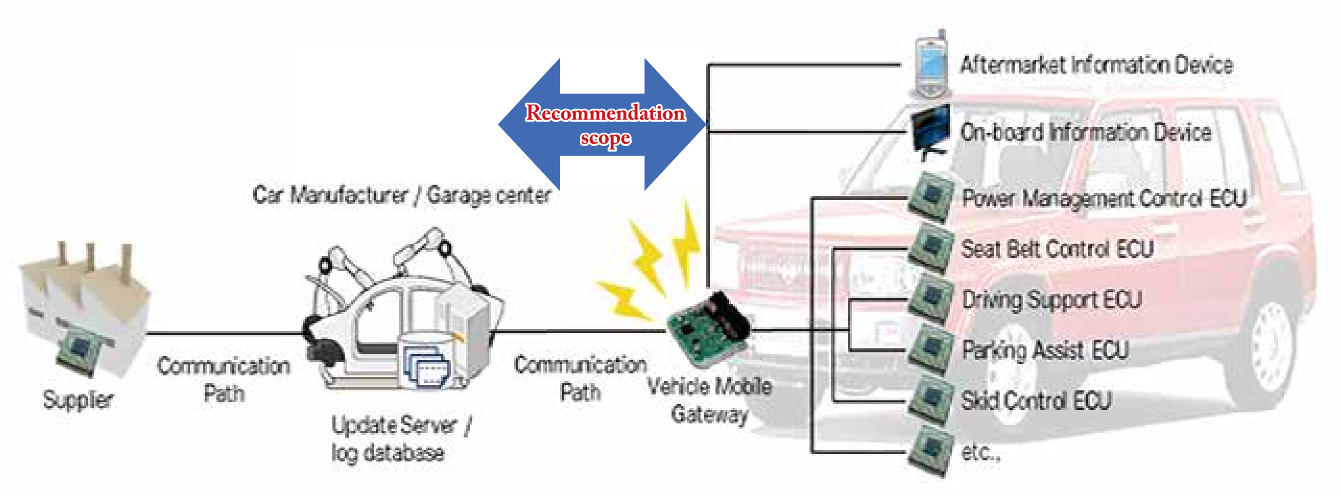
A) Revision of Recommendation X.1373 (Secure software update capability for intelligent transportation system communication devices)

Overview: Recommendation X.1373 was issued in March 2017. This Recommendation describes a secure procedure for updating software and firmware that runs on ECUs (electronic control units) installed in cars. It includes provisions regarding the use of electronic signatures to confirm the completion of updates (scope: see Figure 1). We are currently

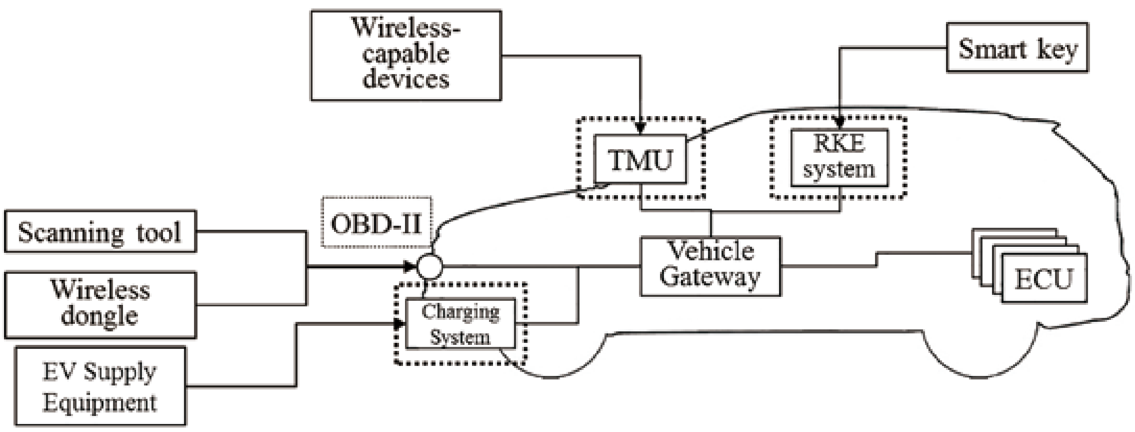
Table: Recommendations being worked on by ITU-T SG17 Question 13

Recommendation	Title	Date of finalization
X.1373rev	Secure software update capability for intelligent transportation system communication devices	Sep-21
X.itssec-2	Security guidelines for V2X communication systems	Sep-19
X.itssec-3	Security requirements for vehicle accessible external devices	Mar-20
X.itssec-4	Methodologies for intrusion detection system on in-vehicle systems	Mar-20
X.itssec-5	Security guidelines for vehicular edge computing	Sep-21
X.edrsec	Security guidelines for cloud-based event data recorders in automotive environment	Sep-21
X.eivnsec	Security guidelines for the Ethernet-based in-vehicle networks	Sep-21
X.fstiscv	Framework of security threat information sharing for connected vehicles	Sep-21
X.mdcv	Security-related mis-behavior detection mechanism based on big data analysis for connected vehicles	Dec-20
X.srcd	Security requirements for categorized data in V2X communication	Dec-20
X.stcv	Security threats in connected vehicles	Sep-19

■ **Figure 1: Scope of the former Recommendation X.1373 (this scope is expanded in the current revision)**



■ **Figure 2: Expected interfaces and external equipment**



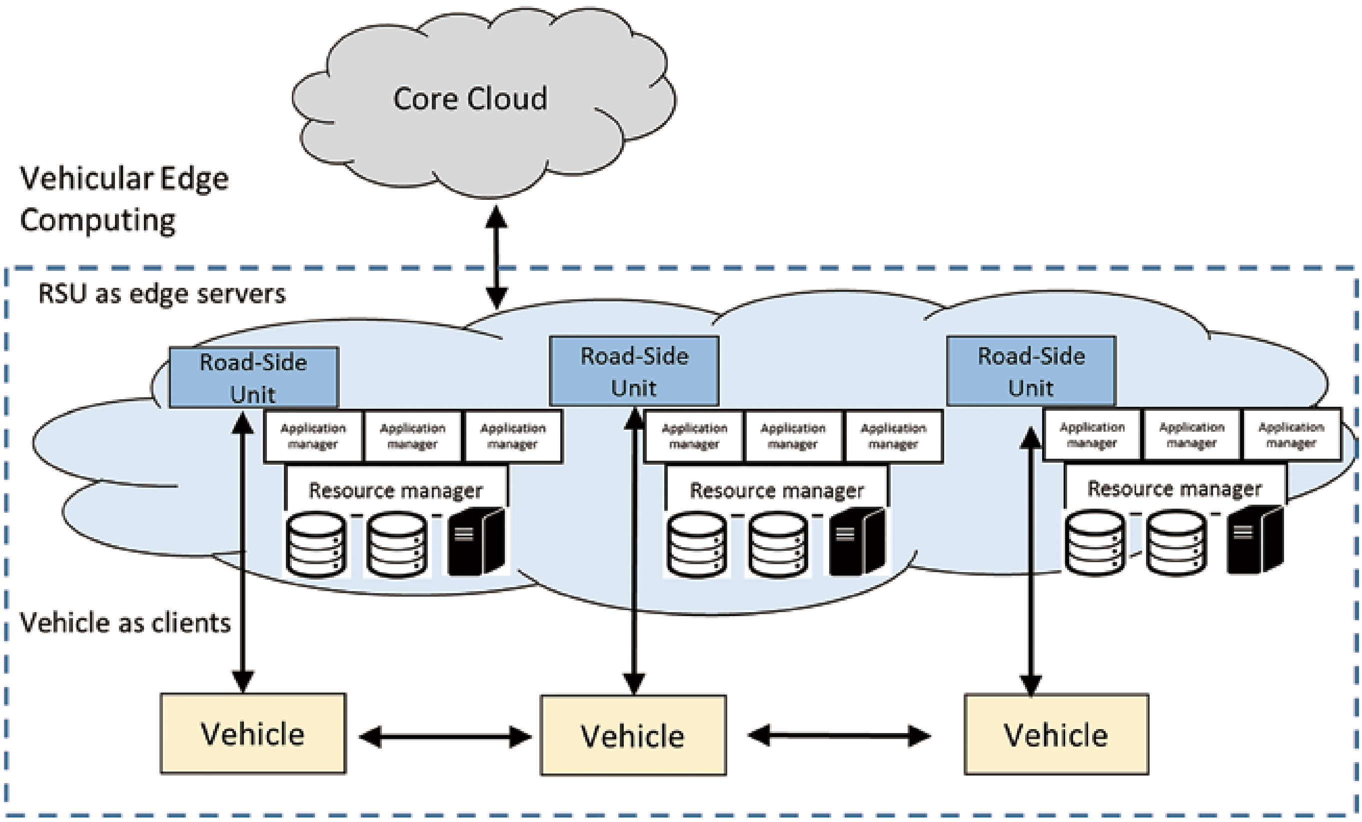
making revisions to this Recommendation, and are expanding its scope to reflect the requirements of OEM vendors around the world.

B) Draft Recommendation X.itssec-2 (Security guidelines for V2X communication systems)
Overview: Assuming communication takes place over connections between vehicles, between vehicles and the roadside (infrastructure), between vehicles and nomadic devices (e.g., smartphones), and between vehicles and people, we are extracting use cases and threat models that can be assumed for each type of connection, and are deriving security guidelines for each type of connection.

C) Draft Recommendation X.itssec-3 (Security requirements for vehicle accessible external devices)
Overview: By focusing on interfaces that are deployed in cars to facilitate external access, such as OBD-II, telematic management units (TMUs), remote keyless entry (RKE) systems, and charging systems, we are identifying threats and security requirements for access from external devices (scanning tools, wireless dongles, smart keys, etc.) and are summarizing them as standardized documents. Figure 2 shows the interfaces and external equipment assumed in this draft Recommendation.

D) Draft Recommendation X.itssec-4 (Methodologies for

■ **Figure 3: The concept of edge computing for vehicles**



intrusion detection system on in-vehicle systems)

Overview: This draft Recommendation focuses on methods of detecting intrusions into Controller Area Networks (CANs) that have a direct impact on ECUs, and presents a summary of lightweight intrusion detection methods that can be assumed to be installed in vehicles, including signature-based, entropy-based and self-similarity-based detection methods.

E) Draft Recommendation X.itssec-5 (Security guidelines for vehicular edge computing)

Overview: This draft Recommendation assumes the vehicular edge computing environment shown in Figure 3, analyzes the threats and vulnerabilities inherent in this environment, and summarizes its security requirements based on use cases provided as reference.

F) Draft Recommendation X.stcv (Security threats in connected vehicles)

Overview: In the Cyber Security Recommendation formulated by WP29 (World Forum for Harmonization of Vehicle Regulations) of UNECE (United Nations World Forum for Harmonization of Vehicle Regulations), based on the security threats summarized in the agreements between OEM vendors of each country, we are promoting a Recommendation for security threat information in Question 13 with the aim of using it as common threat information in ITU-T SG17. (Due to be finalized in September 2019)

3. Conclusion

This article has presented an overview of the ongoing Recommendation work under ITU-T SG17 Question 13. Most of these activities are based on proposals from Korea (principally, Hyundai Motor) and China (security vendors in cooperation with Chinese OEMs). Japan also recognizes the need for active participation in important draft Recommendations, including assessing the feasibility of questions and examining their details. As a new work item, a group comprising Chinese communications carriers and 20 Chinese OEM providers submitted a proposal at the ITU-T SG17 meeting held in January 2019, regarding security guidelines for network-based driving assistance in autonomous vehicles. This proposal was put on hold because it was too soon for a new work item, but we will continue to monitor and study future relevant developments.

Software Updates for Connected Cars

Seigo Kotani, Ph. D.
Project general manager of Task Force Auto-OTA-Updating
Connected Car Working Group
Telecommunication Technology Committee, Japan
Fujitsu Ltd.

Takashi Tsukamoto
Information-technology Promotion Agency, Japan

1. Introduction

Automobiles have existed for a long time as independent entities, establishing a solid presence on their own, but recently, they have begun a major transformation, connecting to general-purpose networks as "connected cars". It has been 20 years since ordinary PCs began connecting to the Internet the 1990s, so it is undeniable that the vehicles, to which we entrust our lives, are behind the times, but advances are starting to be made in Europe, the USA and Japan, with clear awareness of, resolve, and tangible motivation toward generating good returns.

A common function needed for many of the use cases anticipated in this process is secure remote software update of vehicle systems. Here, the word *software* is used in a broad sense to mean any information held in the vehicle.

There are various such functions targeting different systems and with different names, such as "reprogramming" or "flashing", proposals and discussion of regulations and standards are ongoing at various facilities and organizations.

To quickly collect, analyze, absorb and understand these efforts, and to help in the work of incorporating them in measures taken in Japan, the Telecommunications Technology Committee (TTC) has issued a report after collecting, studying and analyzing activities around the world related to Over-The-Air (OTA) technology, which is a type of remote software update technology. This article refers this report (TR-1068), introducing the current state and issues regarding software (in the broad sense) updates for connected cars.

2. Current state of software updates

Recent automobiles are each equipped with dozens of ECUs (microcomputers) that implement various functions such as controlling operation (engine, breaks, steering, etc.), advanced driver assistance systems (ADAS: ACC, LKA, etc.), multimedia (navigation, audio, HUD, etc.), and body control (power windows, lighting control, etc.).

Each ECU runs its own software, coordinating control through the vehicle network to implement each of the functions described above. The software for each ECU in a vehicle is stored in memory before the vehicle is shipped, but this software often needs to be updated after the vehicle is shipped, to improve functionality or repair newly discovered bugs. Updating the software after the vehicle has shipped in this way is called reprogramming. Note that this process is already common for devices like PCs and smartphones.

Currently, reprogramming of automobiles is usually done by a dealer or automobile service center. Each individual vehicle must be brought to the center where a mechanic uses a dedicated device with a wired connection to perform the procedure. However, it is also becoming more common recently, in vehicles such as Teslas, for the vehicle to have a wireless connection to the manufacturer's servers, and to have technology to perform remote software updates without needing a technician. This type of remote software update technology is called over-the-air (OTA) reprogramming. Given that we entrust our lives to our vehicles, there is in fact, some room for concern regarding this type of operation on them.

In a narrow sense, OTA reprogramming refers to updates of ECU software (OS, applications), but it can also refer more broadly to updates of other data such as software configuration data, or navigation mapping data. Here, we introduce the concept, without any particular restriction on the scope of reprogramming.

The figure is an example of reprogramming as shown in TR-1068.

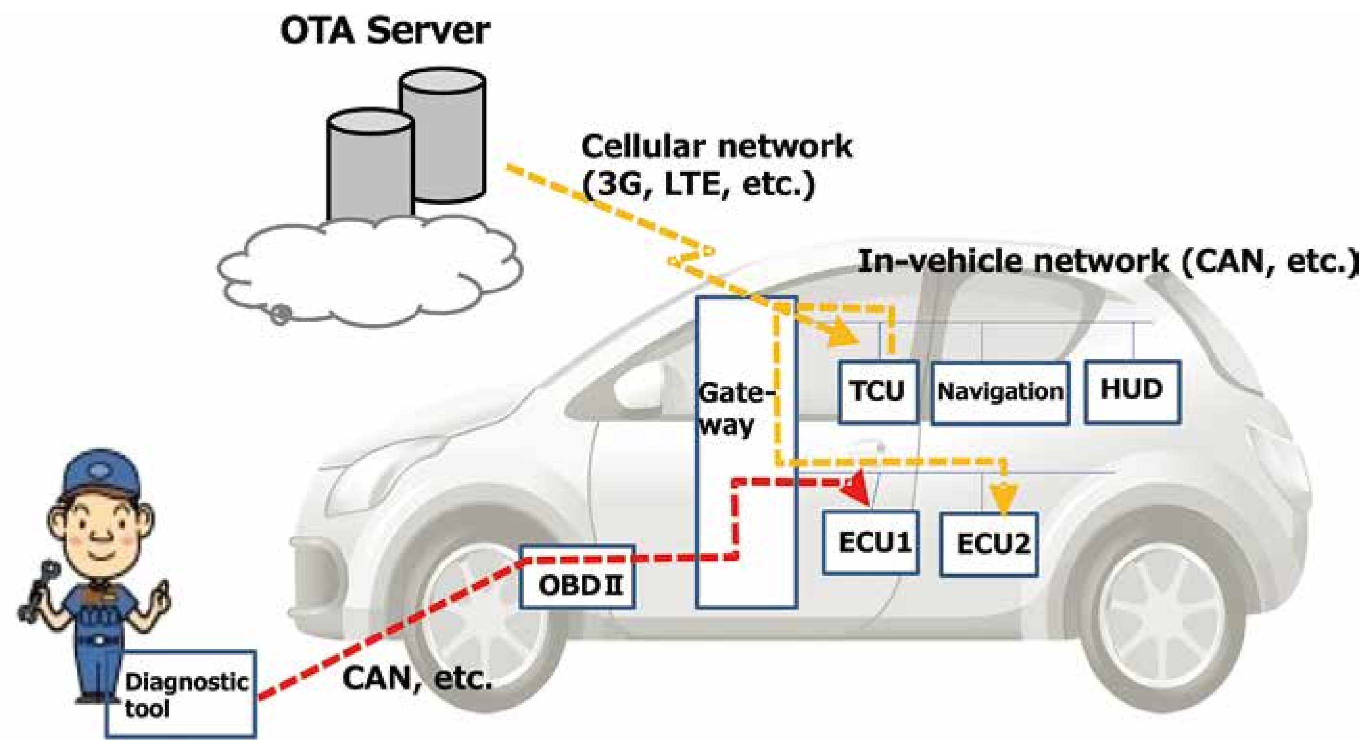
TR-1068 focuses on the use case of remote software updates for vehicle systems as described above, summarizing the results of studying the current activities of government agencies, industry and academic organizations and NPOs within and outside of Japan. Note that TR-1068 refers to public information as of the end of September, 2017, unless otherwise mentioned. Details of activities at related organizations and the content and status of documents created vary, so they have been categorized in three levels for easy understanding. These levels in TR-1068 are vehicle level, communications system level, and component system level. An overview of each of them is given below.

Chapters for each organization give an overview of the organization and published materials (and state of publication) in a fixed format. Each publication is introduced with an overview of its placement and what it deals with, a description of the content of remote software updates, and future prospects. For placement and weighting, publications are given a category, such as regulation, recommendation, guideline, specification, technical report, or proposal, and any legal restrictions are noted.

(1) Vehicle level

The scope of work in TR-1068 is a survey of trends in standardization, but for descriptions at the vehicle level, it examines the broader scope of basic vehicle-level standards and regulations being done by organizations such as the UNECE World Forum for Harmonization of Vehicle Regulations (WP.29), and selects requirements related to remote software updates

■ Figure: Example of reprogramming
(Red: Conventional wired reprogramming, Yellow: OTA reprogramming)



(OTA reprogramming). Specific organizations and associations examined in the study include SAE, US DOT/NHTSA, 5GAA, and ACEA, in addition to UNECE WP.29 and ITS/AD TFCS as mention above.

Fortunately, this special feature also includes a contribution on the state of WP29 activities, by Dr. Tetsuya Niikuni of the Ministry of land, Infrastructure, Transport and Tourism (MLIT), National Traffic Safety and Environment Laboratory. Please refer to those pages for details regarding WP29.

(2) Communication system level

At the systems level, TR-1068 surveyed specifications related to communication protocols being created by organizations such as ITU-T and ISO and selects requirements related to OTA.

Standards for communication protocols being created by ITU-T and ISO apply to this level. Specifically, the organizations and associations dealt with include ITU-T SG16, ITU-T SG17, ISO TC22, ISO TC204, IEEE 802, Wi-Fi Alliance, W3C, Bluetooth SIG, and oneM2M.

(3) Component system level

Within the system level, regulations for chips and other components, being created by groups such as the Trusted Computing Group (TCG) and E-safety vehicle intrusion protected applications (EVITA) were studied, and requirements related to OTA were selected. That is, although they are also at the system level, these specifications are created by organizations such as TCG and EVITA, and are related to components that are actually implemented in automobiles.

Specific organizations and associations dealt with include TCG, EVITA, and HIS.

3. Consolidation of issues

Increasing data transmission time is an example that is likely to become an issue when actually implementing and applying OTA in vehicles, but we expect that it will be resolved by extracting difference data, distributing it, installing it, and verifying afterwards, and that it is increasingly likely that 5G will be able to resolve it.

Other issues fall mainly into flash memory write times, checking and certifying completeness before and after reprogramming, and attacks on security during the OTA reprogramming process. It will be essential to increase the sophistication of measures against this sort of attack.

On a slightly different point, according to the analysis in TR-1068, related organizations are still in the process of consolidating issues regarding standardization of remote update technologies for automobiles.

For example, NHTSA states that, "Prior to on-road testing, entities are encouraged to consider the extent to which simulation and track testing may be necessary. Testing may be performed by the entities themselves, but could also be performed by an independent third party." We expect this presumes accountability based on public standard specifications.

There may also be areas where such accountability is not adequately regulated in concrete terms. Accountability (by a third party) is extremely important, but there is still some concern that a clear definition and how it will be endorsed has not yet been adequately presented.

The term accountability needs some further discussion. While it is extremely regrettable, recent trends have led to an increasing need to assume the worst of people, rather than the best, when taking measures. As an example, attempting to create a perfect countermeasure would clearly be very expensive, and for automobiles, to which we entrust our lives, guaranteeing safety is imperative.

In such conditions, accountability amounts to continually evaluating what this means. That is, the best possible effort must be devoted at the time (some point in the past, excluding security holes and vulnerabilities discovered after the time), and after that, the situation must be inspected by a third party if trouble should occur. This will help to eliminate vexatious or frivolous litigation and false accusations, as can arise from serial claimants.

This will help individual victims, and also reduce costs around the world.

Looking more broadly to include the field of autonomous driving, it is also an urgent matter to apply the same security measures to systems in this field, such as distribution of dynamic maps for autonomous driving, event data recorders (EDR), and tier pressure monitoring systems (TPMS). The importance and meaning of accountability is also obvious in these areas.

From these perspectives, the activities and status of UNECE WP29, as mentioned earlier, are extremely significant. As such, realizing accountability and ensuring third party verification and certification must be studied and discussed on a global scale, transcending the borders of any one country.

4. Summary

Remote software update technology for onboard systems on "connected cars", or vehicles which have and use communication functions, is being studied at various domestic and international organizations. We have discussed the state of such study, for the purpose of consolidating related issues, based on descriptions in TR-1068.

TR-1068 discusses various types of active study on remote update of onboard systems (of software and data used by the software), by various organizations and agencies. Such study suggests that when implementing remote updates, security is extremely important and realizing accountability is highly significant. Accountability is also important when strengthening security in chips and other components according to public standard specifications.

As remote updates to onboard systems become more common, it will be necessary to reliably recognize the value (does it generate any benefit?), effectiveness and convenience of specific use cases. As is widely known, cost consciousness is very high in the automotive industry.

It is hoped that autonomous driving will be realized in the near future in Japan, the USA, and Europe, and as there is ongoing study of recall measures that can be accomplished without transporting vehicles back to the factory, guaranteeing accountability in remote update of onboard systems should be extremely significant in protecting against serial claimants.

5. Conclusion

Vehicle recalls have recently become a huge issue, with millions of vehicles handled per incident. Of the various reasons, approximately 30% are currently said to be due to software, and this proportion is expected to increase in the future.

As with PCs and smartphones, the ability to make repairs remotely, without recovering the vehicle itself, will benefit both the manufacturers and the users. For details on TR-1068, on which this article is based, please see the following URL.

(in Japanese) https://www.ttc.or.jp/document_db/information/view_express_entity/1071

Summary of Discussions on Vehicle Cybersecurity and Software Updates at the World Forum for Harmonization of Vehicle Regulations (WP.29)

Tetsuya Niikuni
UNECE WP.29 GRVA/CSTF Co-Chair
National Traffic Safety and Environment Laboratory

Hideo Himeno
Japan Automobile Standards Internationalization Center (JASIC)

1. Introduction

In December 2016, the United Nations World Forum for Harmonization of Vehicle Regulations (UNECE/WP.29) established the UN Task Force on Cyber security and OTA (Over-The-Air, i.e., wireless update) issues (abbreviated to TFCS) in order to identify security issues pertaining to vehicles. Currently (as of November 2018), discussions are being held to draft internationally harmonized regulations relating to vehicle cybersecurity and software updates. The results of these discussions have been compiled into a proposal document for the Working Party on Automated/Autonomous and Connected Vehicles (GRVA), which is the parent body of TFCS. This document presents an outline of the discussions in TFCS, focusing on the contents of this proposal document.

2. Proposal document on vehicle cyber security

The proposal document on vehicle cyber security covers two main topics.

- Guidance on vehicle cyber security
- A draft regulation for the application of cyber security to vehicles

These topics are discussed below.

2.1 Guidance on vehicle cyber security

The document offers guidance for vehicle manufacturers, and summarizes the measures and principles that they should adopt during vehicle development to ensure that data and information related to the control of vehicles cannot be misappropriated. Its contents are mainly concerned with security measures that are considered to be necessary for ensuring vehicle safety.

● Principles of cyber security

The principles of cyber security indicate the cyber security measures that vehicle manufacturers should systematically implement at each stage of the vehicle life cycle (development, design, manufacture, use, etc.).

Principles relating to organizational requirements:

- Ensure that security is ingrained into an organization by establishing a system where security is managed and promoted at the highest echelons (where decisions can be made that permeate through the entire organization)
- Create a system that can continuously monitor cyber security throughout the organization
- Create a mechanism that maintains security throughout the organization, including related suppliers and service providers

Principles relating to vehicles:

- In structures built to store and communicate data (e.g., in-vehicle network equipment), vehicle manufacturers must adopt designs such that improper operation of one component cannot affect the whole system or any other part thereof
- Consider software security over the life of the vehicle
- Consider the security aspects of data storage and transfer
- Vehicle manufacturers should evaluate security functionality by carrying out testing, etc.
- Vehicle manufacturers should design their vehicles to cope with unauthorized use of data, etc.
- Vehicle manufacturers should design vehicles that can detect and respond to unauthorized use of data

The above requirements constitute guidance that vehicle manufacturers should reflect as much as possible in the development of vehicles.

2.2 Draft regulation for the application of cyber security to vehicles

A characteristic of the proposal document is the proposal that an authorizing body should certify the extent to which vehicle manufacturers adhere to the requirements shown in the guidance presented in section 2.1. An overview of the draft provision relating to this proposed regulation is presented below.

Envisaged applications and scope of the proposed regulation:

The concept of a Cyber Security Management System (CSMS) is defined for activities related to vehicles and their development. Instead of regulating the manufactured products (vehicles, components and systems) themselves, a CSMS consists of rules to guide the actions of vehicle manufacturers and other organizations, and mechanisms whereby these rules are implemented. The organizations targeted by a CSMS include not only vehicle manufacturers but also other organizations in their supply chain.

Structure of the proposed regulation:

The authorizing body issues approvals after confirming that the cyber security requirements indicated in the proposed draft regulation have been properly implemented by the vehicle manufacturing organization in question. For this reason, vehicle types are only approved after the vehicle manufacturer has obtained a certificate demonstrating that CSMS certification has been achieved.

Vehicle type certification:

To obtain approval for a vehicle type, the vehicle manufacturer must first demonstrate to the authorizing body that the requirements certified by a valid CSMS certificate have been applied to the vehicle type requiring certification.

An outline of the proposal document including the draft cyber security regulation proposed by TFCS has been described above. A characteristic of this proposal document is that instead of the requirements shown in the guidance in their own right, it proposes a draft regulation that includes rules for checks by the authorizing body as to whether vehicle manufacturers are complying with the requirements. This makes it unnecessary to make frequent alternations to the regulation in order to keep up with rapid advances in information technology. Also, since it does not specify any specific technology (e.g., a specific encryption algorithm) as a regulation, it does not expose any attack targets.

3. Proposal document on vehicle software updates

Like the proposal document on vehicle cyber security, the proposal document on software updates covers two main topics.

- Guidance on vehicle software updates
- A draft regulation for implementing vehicle software updates

These topics are discussed below.

3.1 Guidance on vehicle software updates

The following requirements have mainly been proposed for vehicle safety.

- ○ If a software download is interrupted (e.g., due to a break in communication), it should still be possible to start the system in the state it was in before the transfer started.
- ○ Before installing the downloaded software, the driver should be notified about what has been updated.
- ○ If the process of installing an update places restrictions on the operation of functions controlled by the software, especially functions related to vehicle safety, then the vehicle must be made inoperable during this installation process.
- ○ The vehicle manufacturer must inform the user about the success or failure of the update, and must also ensure that the details of any functional changes caused by the update are notified to the user and reflected in the instruction manual (the manner in which instruction manuals are to be updated is not specified in this proposal).

About OTA updates (over-the-air wireless updates):

OTA updates must comply with the following requirements.

- ○ For updates that require additional actions by the user (e.g., tasks that requires an operation other than driving), the running of OTA updates while driving must be prohibited.
- ○ If the completion of an OTA update requires any work to be carried out by an engineer with specialist knowledge (that an ordinary vehicle user does not have), then the vehicle manufacturer must ensure that the OTA update is completed by a suitably skilled engineer.

3.2 Draft regulation for implementing vehicle software updates

Like the proposed regulation on vehicle cyber security, this document proposes a mechanism whereby the vehicle manufacturer's systematic software update process is implemented by a mechanism that can be checked by a certifying authority. An overview of the draft provision relating to this proposed regulation is as follows.

Envisaged applications and scope of the proposed regulation:

The concept of a software update management system

(SUMS) is defined with respect to the software update mechanism for vehicles. SUMS itself does not specify manufactured products (vehicles, parts or systems), but represents a set of rules that apply to actions performed by a vehicle manufacturer or other organization for software updates and a mechanism for implementing these rules. The organizations targeted by a SUMS include not only vehicle manufacturers but also other organizations in their supply chains and the like. A vehicle manufacturer must demonstrate how it has configured SUMS in order to implement the guidelines shown in section 3.1. In the draft regulation proposed by TFCS, SUMS certification is essential for approval of a vehicle type.

Vehicle type certification:

To gain approval for a vehicle type, the vehicle manufacturer must first demonstrate to the authorizing body that the requirements certified by a valid SUMS certificate have been applied to the vehicle type in question. In particular, the manufacturer must demonstrate to the authorizing body that the vehicle will be developed, designed and produced based on the manufacturer's SUMS, and that compatibility with this SUMS can be maintained during the use phase.

4. Definition of software reference number

To make the software update process transparent, TFCS studied a method that matches the software installed in vehicles with approvals issued by the authorizing body. This study proposes the idea of defining a RxSWIN (Regulation x Software Identification Number) as number that aggregates the version information of software installed on the in-vehicle systems of approved vehicle types (including multiple software packages when a system comprises multiple units, each with its own software). Operational rules such as version control of software to be updated using RxSWIN can be set by individual vehicle manufacturers for each system.

5. Conclusion

An outline of the proposed regulation for vehicle security and software updates (including OTA) was presented at the United Nations World Forum for Harmonization of Vehicle Regulations (UNECE/WP. 29). As of October 2018, GRVA member countries are reviewing this proposal, and its contents will be discussed at the second GRVA meeting scheduled to be held in January 2019.

Cover Art

Bijinga (Picture of beautiful women).

Utagawa Toyokuni (1769-1825)

Collection of the Art Research Center (ARC)
Ritsumeikan University
Object number: arcUP0029

Communicating via Connected Cars in the Event of a Natural Disaster

Yasubumi Chimura
Chair, Connected Car Working Group
The Telecommunication Technology Committee
Director, Manager of OKI Innovation HR Developments
Corporate Infrastructure Group
Oki Electric Industry Co., Ltd

Yoshiharu Doi
Toyota InfoTechnology Center Co., Ltd. (Retired)

Chang-Yi Luo
President
Toyota InfoTechnology Center Co., Ltd. (Retired)

1. Introduction

In October 2018, the Recommendation "Specification Information and Communication System using Vehicle during Disaster" was approved at a management session of the APT (Asia-Pacific Telecommunity) in Ulaanbaatar, Mongolia. This standard, which is referred to as V-HUB (Vehicle HUB), is mainly the work of the TTC Connected Car Expert Committee, and the studies leading towards its standardization were led by ASTAP (Asia-Pacific Telecommunity Standardization Program).

This article introduces the aims of V-HUB standardization, and describes the background, outline and use cases of this technology. Future standardization plans, including the collection of traffic accident information, are also discussed.

2. Background of the V-HUB study

In the Great East Japan Earthquake, which occurred in the Tohoku region on March 11, 2011, large areas of Japan's communication network were put out of action, hampering efforts to rescue victims and implement recovery activities. It is reckoned that this caused a reduction of 20–30% in the rate at which people were rescued during the 72-hour period following the disaster. To learn from this experience, countries, carriers and vendors have studied ways of rapidly setting up network functions in the aftermath of a disaster, and have conducted several verification trials.

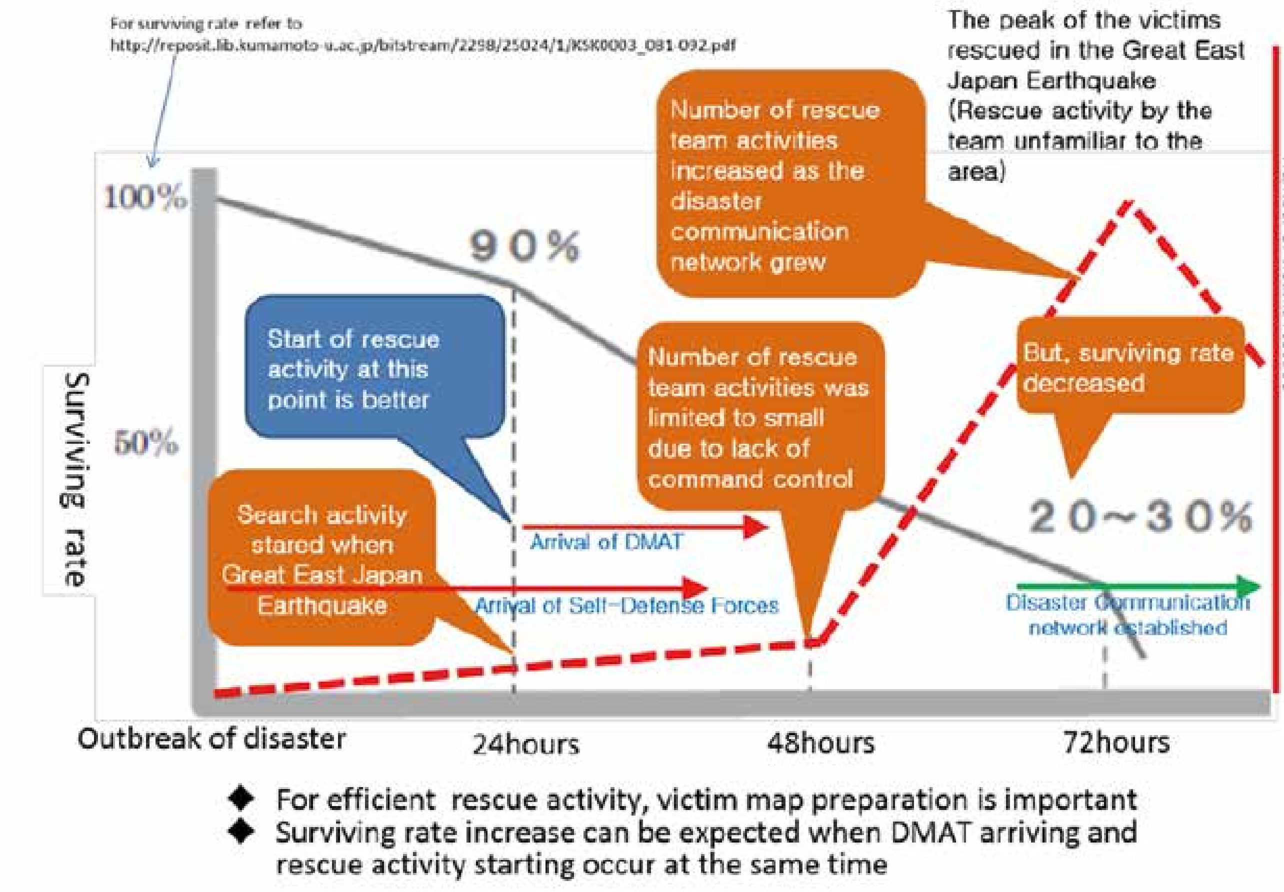
In the TTC Connected Car Expert Committee, organizations including Toyota InfoTechnology Center, the National Institute of Information and Communications Technology (NICT), Keio University and Oki Electric Industry conducted a survey of verification trials both in Japan and abroad on the use of vehicles to establish communication systems in the event of a disaster. In 2014, they presented their use case report (APT/ASTAP/REPT-21) to ASTAP and proposed the standardization of V-HUB specifications to the Expert Group on Disaster Risk Management and Relief System (EG-DRMRS).

After holding workshops and other discussion events involving other Asian countries over a period of five years, an agreement was reached between 15 Asian countries in 2018, resulting in an APT Recommendation on Standard Specification Information and Communication System using Vehicle during Disaster (APT/ASTAP/REC-02).

3. Overview of V-HUB

V-HUB provides a communication interface that allows the on-board communication equipment in road vehicles to be used to establish a temporary telecommunication network for geographical regions or organizations that have become unable to use ordinary networks due to large-scale natural disasters or the like. It is envisaged that this V-HUB technology could be used for purposes such sharing information about the location and condition of people in need of assistance so that search and rescue teams in the local area can coordinate their efforts more effectively, gathering information such as the condition of evacuees and the needs of evacuation shelters in regions where communications have been cut off, and sharing information about local or national government organizations that may be able to operate communication infrastructure. Instead of standardizing a new means of communication, V-HUB works by using existing communication technology. For example, it defines how ITS 700-MHz radio beacons, 5.8-GHz DSRC systems, Wi-Fi, and

■ **Figure 1: Reduction of emergency rescue rate in the aftermath of a disaster**

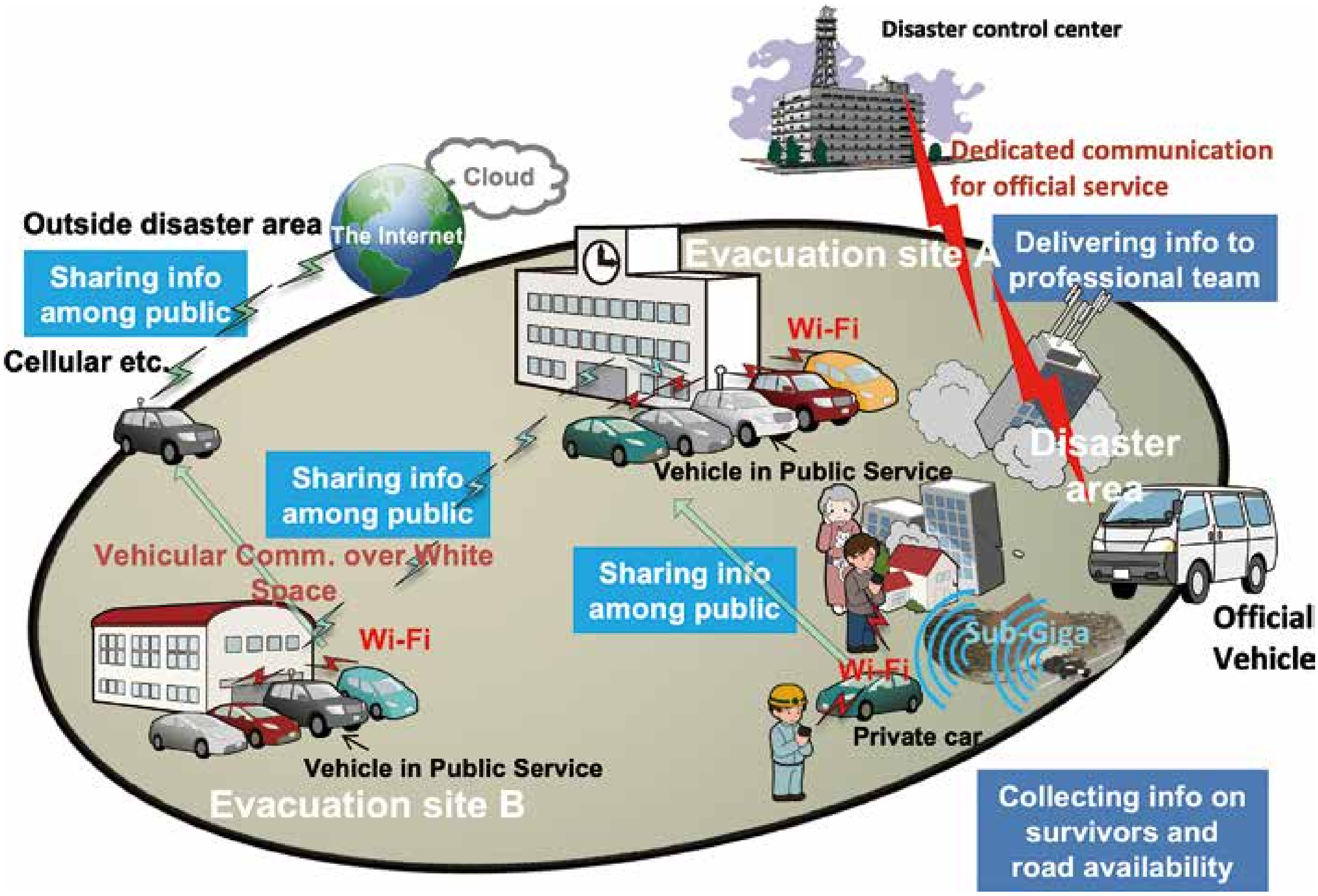


terrestrial digital communication (white space) technology can be used in the event of a disaster.

When V-HUB gathers information about disaster victims, it uses ITS V2P (vehicle-to-pedestrian) communication in the 700 MHz band, which will normally be used for reducing accidents involving pedestrians. V2P terminals carried by victims can if necessary transmit rescue request information (such as the victim's location and vital signs), which is picked up by the V-HUB of a nearby vehicle. The V-HUB uses a wireless interface such as Wi-Fi to share this information with other V-HUBs, and when this information has traveled far enough to reach the system of a rescue team in the local area, the victim's rescue request information is conveyed to the rescue team's system. Safety information and evacuation center information (required resources, required medical support information, etc.) from evacuees in areas where traditional means of communication are broken can also be shared between V-HUBs and transmitted to local and national government rescue centers. Information can be shared between V-HUBs in various ways, such as constructing a network by relaying radio signals (multi-hop connection), using DTN (delay/disruption tolerant networking) to transmit information between vehicles as they pass one another, and using white space in the terrestrial digital spectrum. These methods can be flexibly selected and even combined simultaneously to suit the current circumstances.

Since V-HUB only transfers information when it is possible to do so, it is inherently subject to delays to some extent. Thus, although it works well with non-real-time applications like text messaging, it cannot be used for real-time applications like phone calls. In addition, since there are currently limits on available radio bandwidth and transmission rate, it is more suited to the exchange of information via text messages than via video content. However, if high-bandwidth communication methods such as millimeter-wave communication become available in the future, then it may also be possible to transmit high-bandwidth data.

■ Figure 2: V-HUB use cases



4. Future work

To put V-HUB into practical use, it will be necessary to promote its use at disaster-affected sites, and to formulate guidelines for their use. We hope to achieve this by working together with government agencies and organizations.

Efforts should also be made to promote the use of V-HUB in ordinary situations. In 2015, the United Nations announced that it was setting Sustainable Development Goals (SDGs), including a 50% reduction in traffic fatalities, and in recent years the reduction of traffic accidents has become an important social issue across Asia. We intend to work towards establishing V-HUB as a social problem-solving method that is capable of solving these issues. To reduce traffic fatalities, it is essential to be able to identify where and how accidents have occurred. Most Asian countries do not yet implement adequate digital accident record creation and data analysis. For this reason, we proposed ASTAP for the standardization of traffic accident records and data analysis methods in Asia, and our proposal was approved. In the future, we plan to cooperate with traffic accident reduction initiatives across Asia, and to promote the use of V-HUB in ordinary situations.

5. Conclusion

The next ASTAP Meeting (ASTAP-31) will take place in Japan in June 2019. At the Industry Workshop that is due to be held at ASTAP-31, we will set up a panel display to explain the background and outline of the V-HUB APT Recommendation, and the development and verification status of communication equipment and applications that use it. We hope that many people will learn about the efforts being made to promote V-HUB, and we also hope to reduce the damaging effects of natural disasters in Asia as much as possible. Finally, we would like to express our gratitude to the many people involved in the V-HUB review and standardization process.

Reference

TTC Report, January 2019: Introduction to the Activities of the Connected Car Expert Committee — “APT Recommendation for V-HUB Systems: Standardization of communication systems using road vehicles in disaster situations across Asia” (in Japanese)

Connected Car Initiatives

Masaharu Hamaguchi
Radio System Technology TG,
Advanced ITS Info-communication Systems Committee,
ITS Info-communications Forum
Senior Manager, IoT Application Development & Business Promotion Division
ICT Business Division, Oki Electric Industry Co., Ltd.

1. Overview

Intelligent Transport Systems (ITS) are progressing to a new level as Big Data is being used more practically, and with advancements in communication networks and artificial intelligence (AI). This represents the arrival of a connected-car society, creating new value and business opportunities by connecting vehicles to communication networks. Moving vehicles are becoming sensors, and the information they obtain is collected through various wireless communications networks, and this promises to advance the IoT further and to realize Mobility as a Service (MaaS). Since FY2013, the ITS Info-communications Forum (ITS Forum) has been conducting a comprehensive study of communication technologies related to automated driving, and since FY2015, it has been collaborating with the Japan Automobile Manufacturers Association (JAMA) in a study of communication technologies. This article introduces the current state of ITS Forum activities to realize communication for automated driving in the connected car society, including an example of a study by Oki Electric Industry Co. Ltd. (OKI).

2. Realizing a Connected Car Society

Currently in Japan, various independent ITS services are being provided using telecommunications, such as congestion and other traffic information through VICS, automatic fee collection services through ETC, safe driving support services through ETC 2.0 and ITS Connect, and vehicle management and information services from automobile manufactures utilizing mobile telephones. In December 2016, the Ministry of Internal Affairs and Communications (MIC) established the “Study Group Focusing on the Realization of Connected Car Society,” which published a report in August 2017. With advancements in mobile networks, such as fifth generation mobile communication systems (5G) and DSRC, as well as developments in AI, connected cars are expected to become more common. This article reports on a study of policies and initiatives toward realizing a connected car society, such as (1) new services and businesses created utilizing data, (2) the nature of wireless communication networks to support a connected car society, and (3) construction of a safe and convenient platform for it. It includes a consolidation of communication requirements for realizing the connected car society, and an examination of the strict requirements on communication in the area of safety, in particular for communication supporting automated driving.

3. Connected Car Initiatives

An important technology for realizing connected cars is Vehicle to Everything (V2X) communication. In the area of safety, as for automated driving, requirements include strong real-time performance and high quality communication. We introduce activity studying V2X, mainly for automated driving.

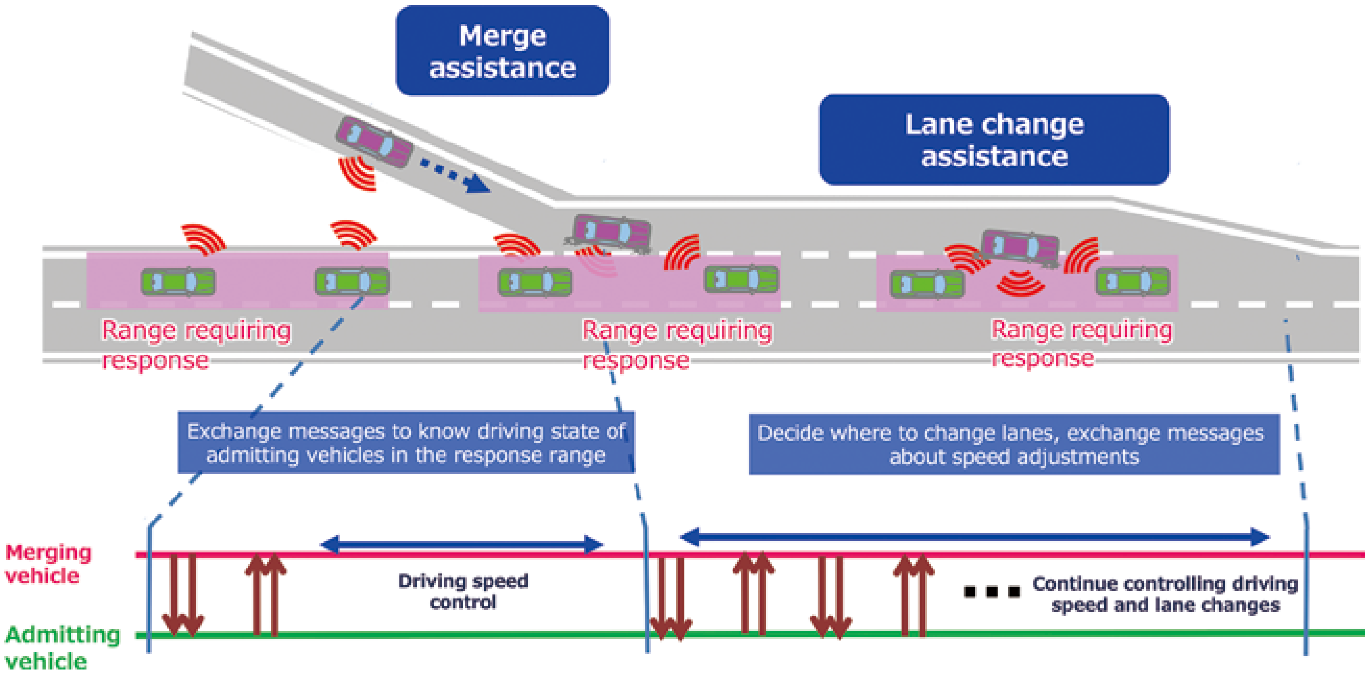
3.1 Study of Communication Supporting Automated Driving

Realizing automated driving is a Strategic Innovation Promotion Program (SIP) theme being promoted by the Cabinet Office in Japan, and starting in FY2017, MIC has been conducting a “Survey and Study on Message Set and Protocol for Automated Driving Assistance Communication.” With communication use cases from the JAMA study as communication requirements, the objective and result was an analysis of conditions that will satisfy performance requirements, through study of the message set and protocol, based on ITS communication in Japan, including application and upper communication layers. The ITS forum is promoting this study and the sharing of information, while also contributing results from practical technical studies.

The figure shows an example of studying communication to assist merging onto a freeway. Results of the study confirmed the need to link applications with aspects of communication control, such as the timing of transmissions and how many transmissions are needed. Communication control parameters for each use case are selected, including this result, and compiled into a draft communication specification. By applying these results to use cases from the communication draft specification in the future, improvements in stability of vehicle behavior, traffic flow, and other factors will be verified, both theoretically and in practical tests, toward creation of a draft specification for communication supporting automated driving, the highest priority study item for connected cars.

In FY2017, OKI also received and performed a contract from the MIC, to conduct the “Study of highly accurate positioning systems for automated driving,” which is a SIP theme for implementing automated driving systems. They have studied technologies that complement satellite positioning, which suffers degraded accuracy at intersections among high-rise buildings, and advanced R&D to implement highly accurate pedestrian positioning for automated driving on public roads.

■ Figure: Example study of communication to assist merging on a freeway



They conducted studies of conditions for infrastructure devices satisfying a target measurement accuracy of 10 cm in ideal traffic conditions, and to achieve the target performance under real environments with multipath effects, assuming that Wi-Fi and smartphone applications for positioning foreseeable in 2020 and beyond would be used for implementation. Accurate positioning in vehicles using V2X technology is expected to play an important role in advancing various types of services in connected cars.

3.2 Trends outside of Japan —5GAA—

The 5G Automotive Association (5GAA) was initiated in September 2016, mainly by major German automakers, to link together the automotive and ICT industries (chiefly telecom) and promote implementation of future ITS services based on the 5G specification, creating new business opportunities. As of October 2018, it had 102 corporate members. OKI has been a member since October 2017, and is currently studying the potential for cellular V2X, while analyzing the latest discussion related to 5G with automated driving and connected cars around the world.

4. Future prospects

In the MIC roadmap for realizing a connected car society, promoting cooperation among SIP automated driving systems and ITU standardization activities are stipulated as the core of the connected-car society realization project. This project was based on initiatives for automated driving technology in the “Public and private ITS concept/roadmap 2018.”

We anticipate enabling more-advanced automated driving and great changes in daily life through study of radio communication network technologies, toward realizing the safest, most secure, and comfortable connected car society in the world.

Introduction to Vehicle Domain Services Provided by Connected Cars

Kaname Tokita
ISO TC 22/SC 31/WG 8 VDS Convener
Honda R&D Co., Ltd. Automobile Center

1. Expectations for Connected Cars

With the spread of Information and Communication Technology (ICT), all objects related to daily life are expected to be connected to the Internet. Vehicles are no exception, and there is increasing anticipation for new services that will emerge when they do connect to the network. There is not strict definition of a connected car, but it is generally understood to mean a vehicle that is connected to a network and is able to provide various new services.

Many services to be provided by connected cars have been studied, and among these, ITU-T has proposed the Vehicle Domain Service, which we introduce here.

2. Vehicle Domain Service (VDS) Concept

Generally, vehicle domain information refers to the traffic conditions surrounding the vehicle. The primary basic information elements are related to actively moving bodies such as the types, sizes, positions, and speed of vehicles operating near the vehicle, but also include other traffic participants, such as pedestrians and cyclists.

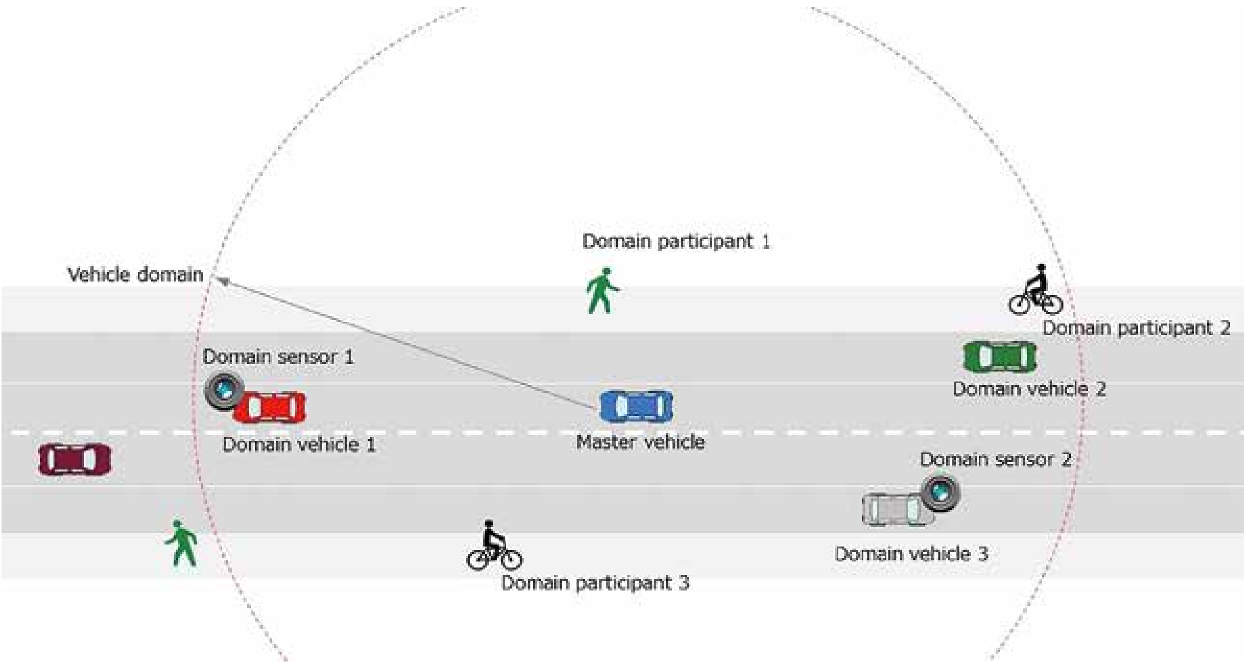
Vehicle domain information also includes road conditions such as vehicle width, number of lanes, the shape of the road ahead and intersections, and static information such as whether there are traffic signals or cross-walks, and generally comprises all traffic information surrounding the vehicle.

This vehicle domain information is very important as basic information for making driving decisions, but its value is increasing dramatically as input for advanced systems that support vehicle operators, and the new autonomous driving systems that are being developed feverishly around the world today.

Vehicle domain information is collected through communication with other traffic participants near the vehicle, and by detecting information using various types of sensors in the vehicle. VDS information is generally defined as being constructed using both of these types of sources.

A configuration for obtaining VDS information in this way is shown in Figure 1. A vehicle provides the VDS, generating it by integrating information obtained through communication and from its sensors.

■ Figure 1: Information retrieval with VDS



3. Standardization Activities for VDS for Driving Decisions

The primary application area for VDS is to provide information needed for vehicle operation. This corresponds to vehicle domain information as implemented in the vehicle, so the applicable standardization area would be ISO TC 22 (Road vehicle). As such, initial proposals were under TC 22, sub-committee 31 (SC 31); Data communication.

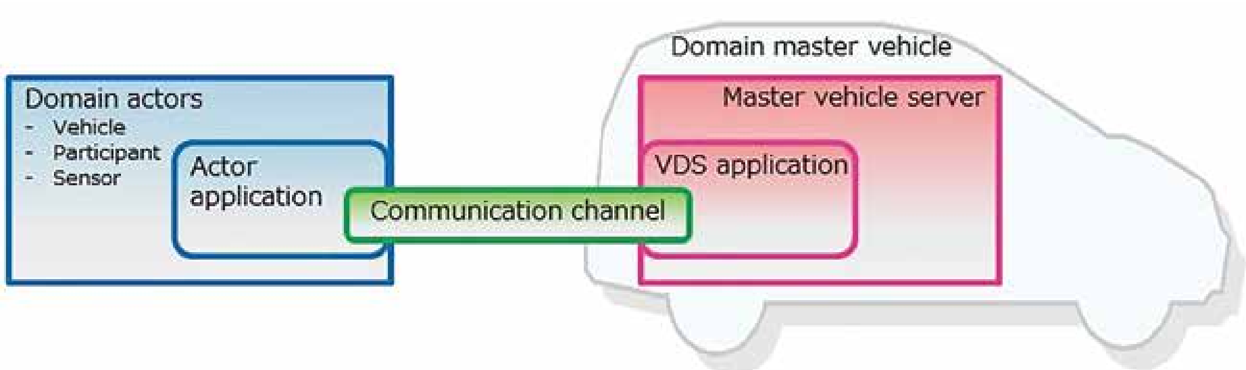
Detailed discussion is beyond the scope of this article, but work was proposed at the SC 31 general meeting held in September 2017 in Germany, and a new work item proposal (NWIP) was submitted in November of that year. Work began when it was approved as ISO 23239 in January 2018. In April of that year, it was registered as working group 8 (WG8) under SC 31.

The scope of ISO23239 is shown in Figure 2. VDS is implemented in a vehicle, and provides information for making driving decisions.

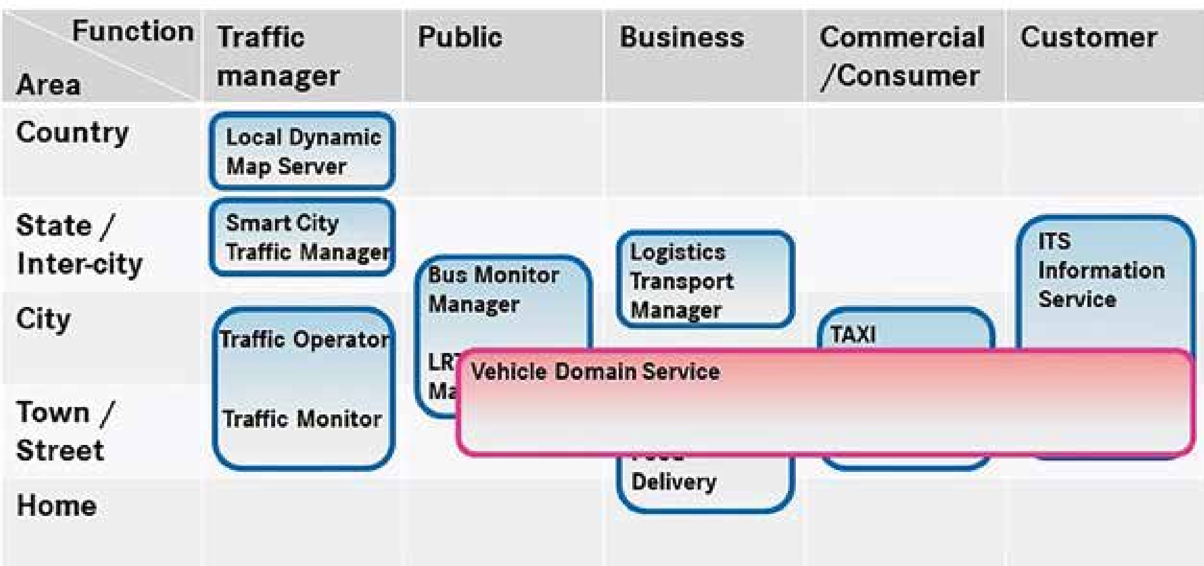
4. VDS in Smart City Traffic

VDS collects information for making driving decisions, but this is not the limit of its value. The latest traffic and road conditions are part of the information generated, so it can have significant influence on driving plans for other vehicles, either

■ **Figure 2: Scope of standardization work**



■ **Figure 3: Smart City data structure model**



approaching or planning to follow the same route. If many vehicles transmit such information and it is consolidated and provided to other nearby vehicles, vehicles sharing this information will be able to make better decisions. VDS bundled and shared in this way could function as information infrastructure for traffic conditions in the city.

When all traffic and road condition information in a city is available as data, and vehicles moving within the city are connected, it is referred to as a smart city, or smart traffic. VDS can be incorporated into smart city data transmission structures and can function as part of the information infrastructure.

City transportation functions are grouped according to the scope of geographical links and the objectives of mobility and transport. Traffic in a city has a hierarchical structure, geographically and functionally, so transmission of information related to traffic also has a similar structure.

Figure 3 shows an example model of the information structure in a smart city. The vertical axis shows geographical expanse, ranging from homes (the starting point for mobility in a city) to the entire country. The horizontal axis shows types of function or objective for mobility in the city. It comprises individual transport (Customer), commercial transport (Consumer), business transport (Business), goods transport (Logistics), public transport (Public), and traffic control (enterprise). VDS can share information among various functional groups in the range of Home to Street, and can provide various services.

5. VDS Standardization Activities in Smart City

The scope of ISO TC 22/SC 31 work is communication implemented within vehicles, so standardization of information sharing with surrounding vehicles, and functionality for exchanging information in a smart city as described above, are beyond its scope. So far, most of the work has been in the area of on-board control communication, such as controlling electric car charging, diagnostic device communication, the controller-area network (CAN), the Local Interconnect Network (LIN), and on-board Ethernet. For this reason, there has been a shortage of standardization professionals who specialize in new work areas such as that discussed in this proposal.

Accordingly, it has been necessary to collaborate with standardization organizations in the area of information exchange in smart cities.

Recently at ITU-T, Study Group 16; multimedia (SG16), has been standardizing data interfaces with vehicles, and Study Group 20; smart city (SG20), has been standardizing data transmission for smart cities. Several focus groups (FG) were also started in March 2018 to find new standardization themes in the field of communications, and one of these was Focus Group Vehicle Multimedia (FG-VM), to explore new standardization themes within and outside of vehicles. In light of such activity, it seemed necessary to be cooperating with ITU-T.

6. ITU-T and VDS Collaborative Study

To consult with the ITU-T on how to collaborate on standardization, we first consulted with the Japanese government Telecommunications Technology Committee (TTC), and were directed to the open coordinating committee within ITU-T standardization committees, called the CITS. CITS consults on how to proceed in cooperating with other related standardization organizations. Accordingly, we participated in the CITS meetings held in Nanjing, China, in September 2018 on September 6 and 7. ITS-2018 workshops were held for the first day and a half, on topics related to autonomous driving, next-generation communications, and Smart City, and CITS was held on the afternoon of the second day.

In the ITS-2018 workshops, we heard about activities in Europe regarding Smart City, and upon hearing discussion of the multi-layer implementation of urban transport their point seemed very relevant. When we introduced VDS, we received generally favorable responses.

At the CTS meetings, we gave an overview of VDS, and offered a proposal for collaboration. There were questions regarding the relationship with SAE and TC 204, some exchange of ideas, and we received positive responses. As a result, it was agreed to investigate collaboration with SG16 and SG20, and to send a letter explaining these circumstances to other related standardization organizations.

7. Other Developments and Future Prospects

Using consultation results from CITS, we coordinated with ITU-T SG16, and it was decided to initiate a Joint Project Team (JPT). This was reported to the ISO TC 22/SC 31 council, and preparation to issue a liaison letter is progressing.

On other fronts, an ITU-SAE Workshop was held in Detroit, USA, on October 8-9 2018, and during the same week, on October 11, the first meeting of FG-VM was held in Ottawa, Canada. We participated in both of these, introducing VDS, and discussing future developments.

We also received positive responses at these meetings, but discussion was broader, focusing on general, non-specialized issues, particularly at FG-VM, to give more open access to the JPT for SG 16, which was less familiar with VDS.

Thereafter, technical and specialist discussion began at ISO and ITU-T, checking against the specifications of the JPT. Many issues arise when standardizing a new field, but given participation from many experts and stakeholders, we hope to achieve a very meaningful standard.

= A Serial Introduction Part 4 = Winners of ITU-AJ Encouragement Awards 2018

In May every year, The ITU Association of Japan (ITU-AJ) proudly presents ITU-AJ Encouragement Awards to people who have made outstanding contributions in the field of international standardization and have helped in the ongoing development of ICT.
These Awards are also an embodiment of our sincere desire to encourage further contributions from these individuals in the future.
If you happen to run into these winners at another meeting in the future, please say hello to them.
But first, as part of the introductory series of Award Winners, allow us to introduce some of those remarkable winners.

Hiroki Harada
NTT DOCOMO, INC.
Hiroki.harada.sv@nttdocomo.com https://www.nttdocomo.co.jp/english/
Fields of activity: 3GPP LTE-Advanced and 5G standardization

3GPP Standardization Activity on LTE-Advanced and Aspects of the 5G Physical Layer

I am extremely honored to receive the ITU-AJ Encouragement Award, and would like to thank the ITU Association of Japan and all those who supported my nomination and selection.

I have been contributing to 3GPP RAN WG1 work developing the physical layer specification for radio access technologies since 2012. In particular, I have worked on LTE-Advanced enhancements for small cell deployment, Licensed-Assisted Access (LAA) to unlicensed spectrum using LTE-Advanced, initial access/mobility technologies in 5G New Radio and others. Actually, these technologies attracted worldwide attention and high expectations when 3GPP standardization work began on them, and I was able to contribute to early development of 3GPP specifications for those technologies by leading technical discussions in 3GPP.

Since, with the spread of smart phones and tablets, there was a worldwide desire for an enhanced mobile broadband service with high-speed and large capacity, there was a need to study on how to efficiently increase the density of mobile network deployment in high traffic areas. NTT DOCOMO has been proposing a concept of next generation mobile network for 5G, in which small cells using higher frequencies are integrated into the mobile network based on macro cells, so that both high speed and large capacity can be achieved, together with stable connectivity and wide coverage. My first important mission in 3GPP work was to propose an efficient cell discovery mechanism for such a next generation network. However, most companies were initially skeptical of the proposal. I think that for standardization, it is important to first clarify the common targets among stakeholders, and then it is necessary to have both consistency and flexibility to achieve a consensus among the large number of stakeholders with their different interests. Hence, I had many extensive discussions with other companies, and also provided computer simulation results showing quantitative effects of the proposals, thanks to internal discussion and cooperation. Finally, after about one and a half years of work, the proposed mechanism was ready to be introduced as a 3GPP specification. Through this experience, I was able to contribute to early development of 3GPP 5G specifications by leading initial access and mobility related discussions with excellent engineers from global vendors and operators involved in 3GPP standardization.

I am fully committed to further evolution of mobile communication technologies and services based on 5G, which will make our lives more convenient and fulfilling.

Mami Miyazaki
Nippon Telegraph and Telephone East Corporation
mami.miyazaki@east.ntt.co.jp http://www.ntt-east.co.jp/en/
Fields of activity: Global business development

Technical Assistance in Deployment of Indonesia's Optical Access Network (FTTH)

It is a great honor to receive the ITU-AJ Encouragement Award, and I extend my thanks to the Selection Committee and to all those who supported and encouraged me along the way.

About the time NTT East broke the 10 million FTTH subscriber mark in 2013, Indonesia committed to full-scale deployment of FTTH services. They recruited several thousand telecom engineers and contractors, and moved quickly to extend fiber to the home. A number of efficiency, quality, and safety issues emerged as the rollout continued, and NTT East stepped forward with an offer of technical assistance to share the company's experience and expertise.

NTT East was willing to share its knowhow, but there seemed to be some reluctance at the local level in Indonesia to accept our suggestions, and the technology transfer project languished.

Eventually we were able to build trust and get the project back on track by not pushing NTT East's own specifications and methods but by proposing specific improvements based on understanding and respect for local conditions and ways of doing things as well as by sharing detailed information on why certain methods were chosen. We also kept in mind how things went when FTTH was first deployed in Japan and how things developed. By responding with sincerity and earning the trust of local engineers, I was astounded by the speed and momentum as the rollout continued.

Responsibility for this project in a very different environment promoting FTTH services in Indonesia has certainly contributed to my own personal growth. Incorporating favorable attributes of both Indonesia and Japan will clearly be advantageous for both countries.

Melody International Ltd.

Melody International Ltd.
support@melody.international https://melody.international
Fields of activity: ITU SME / ITU-D e-Health

Melody International

Safe and Secure Delivery for Mothers All Over the World

Under the slogan "safe and secure delivery for mothers all over the world", we have developed the world's first cloud platform connecting doctors and expectant mothers based on IOT-loaded fetal monitors. We are currently introducing the technology to hospitals in Japan and abroad.

Working in partnership with Chiang Mai and Kagawa Universities we have already deployed this service in Chiang Mai, Thailand (JICA project). The service has helped detect high-risk pregnancies at an early stage and enabled many expectant mothers in rural and mountainous areas that lack obstetric care to be transferred to medical facilities. In recognition of this contribution, Chiang Mai University was awarded a Best Public Service Award 2017 by the Office of the Prime Minister of Thailand. A decision has now been made to roll out these services to all public hospitals in Chiang Mai Province, with plans in place to build a referral network linking 25 hospitals.

In cooperation with a local NGO, services have also commenced in rural areas in Myanmar.

We are looking to further expand our services in regions of Asia and Africa that suffer from high mortality rates among mothers and babies due to a lack of specialist medical care. We want to contribute to WHO Sustainable Development Goals (SDG) 3.1 and 3.2 and help bring down the global maternity mortality rate.

Please contact us if you have a project that could benefit from our services. We are eager to engage with projects that address SDG 3: good health and well-being for all people.

Toru Yamada

NEC Corporation
t-yamada@ap.jp.nec.com http://www.nec.com
Fields of activity: ITU-T SG20, ASTAP

IoT and Smart City Standardization in ITU-T SG20

I am honored to receive the ITU-AJ Encouragement Award, and would express my appreciation to the ITU-AJ and all who helped me along the way.

ITU-T Study Group 20 (SG20) was established in 2015 to study standardization in IoT and smart cities areas. I have been closely involved in SG20 since its establishment, participating in meetings as an editor for several Work Items, and offering regular suggestions and proposals.

Smart city projects are typically promoted by central or local governments, so we have a good number of members from ministries in charge of smart city projects in different countries in ITU-T SG20. The ability to discuss smart cities with the very people charged with implementing them in their respective countries is a special feature of ITU-T SG20. By participating in SG20, I hope to elevate Japan's presence through contributing to IoT and smart city standards, while also contributing to market expansion in a smart city field. Recently in April 2019, I was appointed to a Vice-Chairman of ITU-T SG20. In this capacity, I will do my best with your kind advice.

51st Celebration of World Telecommunication and Information Society Day

17 May 2019 at KEIO PLAZA HOTEL

The ITU Association of Japan

Ceremony at Keio Plaza Hotel, Tokyo

Award winner and Honorable guests

MIC Minister's Award winner
Dr. ITO

Honorable Guest : Mr. KUNISHIGE
Parliamentary Vice-Minister , MIC

Anniversary Keynote Presentation:
Dr. NOGUCHI

Honorable Guest: Mr. SUZUKI
Director-General for Global Issues, MOFA

ITU-AJ Special Achievement
Award winner Ms. WAKAMIYA

List of the Award Winners on 17 May 2019

MIC Minister's Award

Dr. Yasuhiko ITO (KDDI (Retired))

ITU-AJ Special Achievement Award

Ms. Masako WAKAMIYA
(Mellow Club / Broadband School Association)

ITU-AJ Accomplishment Awards

Mr. Hirofumi AIZAWA (BHN)
Mr. Muneo ABE (Mitsubishi Electric)
Mr. Chenghock NG (NEC)
Mr. Junichi OSAWA (KDDI Foundation)
Dr. Dai KASHIWA (NTT Communications)
Mr. Yasuhiro KATO (ARIB)
Mr. Toshiro KAWAHARA (NTT DOCOMO)
Dr. Masahito KAWAMORI (Keio University)
Mr. Kaoru KUSHIDA (NTT-East)
Mr. Susumu TANAKA (YACHIYO ENGINEERING)
Mr. Yasubumi CHIMURA (OKI)
Mr. Koji NAKAO (NICT)
Mr. Masayuki HAYASHI (NHK-Itec)
Dr. Yutaka MIYAKE (KDDI Research)

ITU-AJ Encouragement Awards

Ms. Minami ISHII (ARIB)
Mr. Eiichiro ICHIKAWA (NTT-East)
Mr. Hiroyuki IDE (JICA)
Dr. Takeshi USUI (KDDI Research)
Ms. Tomoko UCHIYAMA (SHAPLA NEER)
Mr. Tsukuru KAI (NTV)
Dr. Atsushi KANNO (NICT)
Mr. Yuya KUNO (NTT DOCOMO)
Mr. Hirokuni KONDO (KDDI Foundation)
Dr. Motoharu SASAKI (NTT)
Mr. Shinya TAKEUCHI (NHK)
Mr. Atsushi TAKEDA (FUJI TV)
Dr. Kazuki TAKEDA (NTT DOCOMO)
Mr. Susumu NAKAZAWA (B-SAT)
Mr. Masaru MITANI (NHK)
Mr. Takuya MIYASAKA (KDDI Research)
Mr. Masahide MURAKAMI (NTT DOCOMO)
Mr. Naoto YOSHIDA (NTT-East)
Welltool Co., Ltd.
NTT SOLMARE CORPORATION
Zeus Inc.
TANABIKI Inc.

通巻百二十三号
定価　一冊　一、六二〇円（本体価格 一、五〇〇円、消費税 一二〇円）　年間購読料　六、四八〇円（本体価格 六、〇〇〇円、消費税 四八〇円）