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.

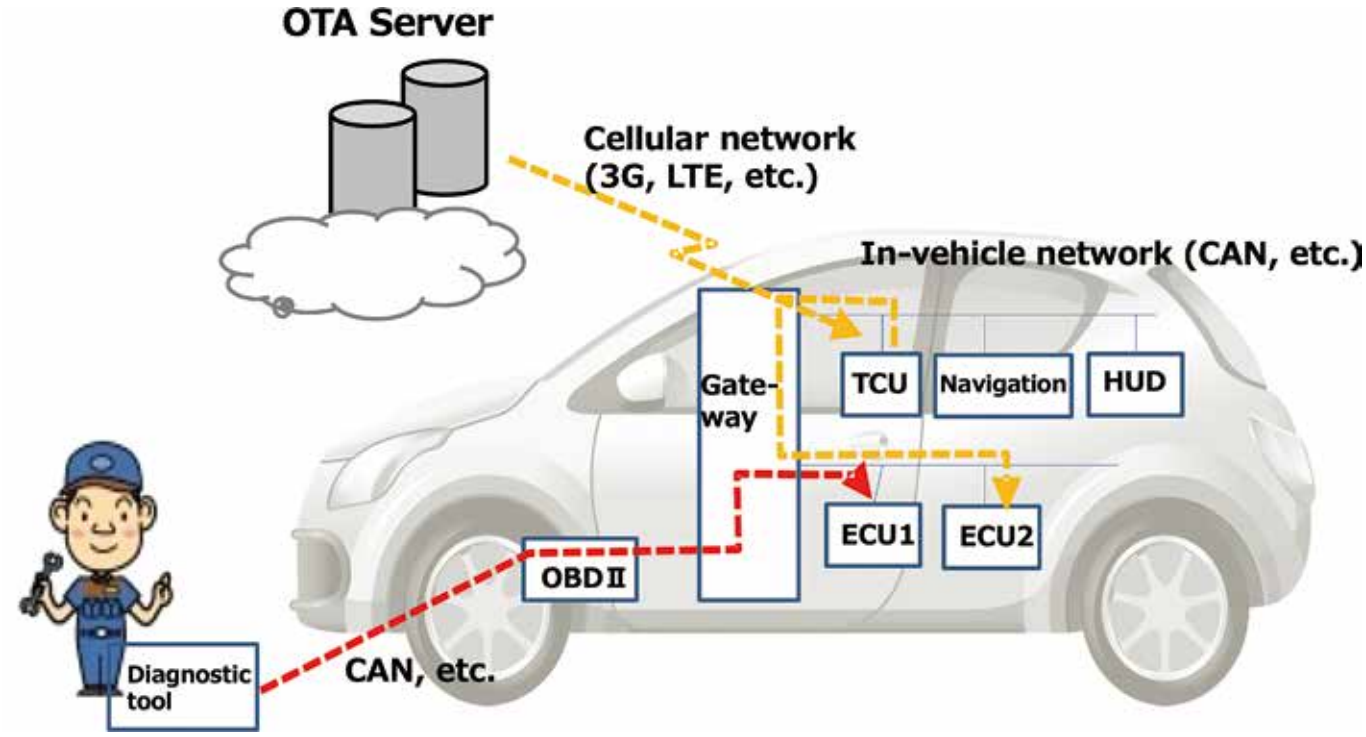
TR-1068 focuses on the use case of remote software updates for vehicle systems as described above, summarizing the results of studying the current activities of government agencies, industry and academic organizations and NPOs within and outside of Japan. Note that TR-1068 refers to public information 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