ISSN: 2664-9640

Analysis of domestic and international policies and regulations regarding software updates for intelligent connected vehicles

Nirunze Yang [a], Manna Wang [b], Yongjian Zhu [c], Qiujun Zhao [d]

CATARC Automotive Test Center (Tianjin) Co., Ltd Tianjin, China;

ayangnirunze@catarc.ac.cn, bwangmanna@catarc.ac.cn, czhuyongjian@catarc.ac.cn, dzhaoqiujun@catarc.ac.cn

Abstract

With the vigorous development of new-generation information technologies such as artificial intelligence and 5G communication, the global automotive industry has witnessed a new wave of technological revolution and industrial transformation. "Software-defined cars" have gradually become a trend in the industry, and the level of software has become a key indicator determining overall vehicle functionality and performance. OTA (Over-The-Air), as the most advanced technology for optimizing and iteratively upgrading intelligent connected car features, holds undeniable significance. Meanwhile, both domestically and internationally, a series of regulations and standards have been introduced, gradually standardizing the requirements for online car software updates. The newly released General Technical Requirements for GB Automotive Software update in China further signifies an increasing demand from regulatory authorities to standardize automotive software updates.

Keywords

Over-The-Air (OTA), Intelligent and Connected Vehicle, Software online updating, Standard Regulation GBIntroduction.

1. Introduction

In today's society, intelligent connected vehicles are rapidly developing, and the scale of in-vehicle software is expanding rapidly [1]. Correspondingly, the software update capability of vehicles needs to be enhanced to support iterative updates and efficient problem-solving for in-vehicle software. In addition to improving the efficiency of software iteration, changes and improvements are needed for the existing automotive safety regulatory framework. To ensure the safety of users' lives and properties, as well as compliance with legal requirements for information security and software updates post-update, changes in the development and management systems for vehicle software are required, along with changes in compliance regulations for update functionalities.

Before the application of Over-The-Air (OTA) update technology in the automotive industry, when car systems encountered problems, repairs could only be done through recalls by vehicle manufacturers. In contrast, OTA update technology enables online repairs, significantly reducing costs and improving work efficiency [2]. As a result, many automotive companies have adopted this technology [3-4]. However, concerns about potential misuse of OTA update technology have also emerged. Some car manufacturers perform software updates for intelligent connected vehicles in an arbitrary manner, automatically updating without fully explaining to the users. Considering the close relationship between cars and user safety, some car manufacturers hastily release intelligent connected vehicle systems with incomplete functionality and insufficient validation, hoping to address subsequent issues through software updates. This approach is clearly not rigorous enough, as the current automobile product

ISSN: 2664-9640

management relies on type approval and requires compliance with relevant national standards. However, with the widespread adoption of software update technology, car manufacturers can easily circumvent the existing automobile product management system and modify access parameters related to vehicle safety, emissions, energy consumption, and more. This may lead to inconsistencies in car production and pose challenges to the existing management systems. Therefore, it is necessary to conduct policy and regulatory research on software updates for intelligent connected vehicles, both domestically and internationally.

2. International legal standards

2.1. UNECE R156

The United Nations Economic Commission for Europe World Forum for Harmonization of Vehicle Regulations (UN/WP.29) released international regulations on automotive information security and Over-The-Air (OTA) updates in February 2021, namely WP.29/R155 (Network and Information Security Management System) and WP.29/R156 (Software Update and Software Update Management System), which specifically address OTA security for intelligent connected vehicles. New vehicles are required to implement the WP.29/R156 regulation starting from July 2022, while existing vehicles are required to comply with this regulation starting from July 2024 [5-6]. The "Software update Management System" (SUMS) is a systematic approach that defines organizational processes and procedures to meet the requirements of software updates [6].

SUMS defines the update process (as shown in Figure 1) and covers the following five aspects [6].

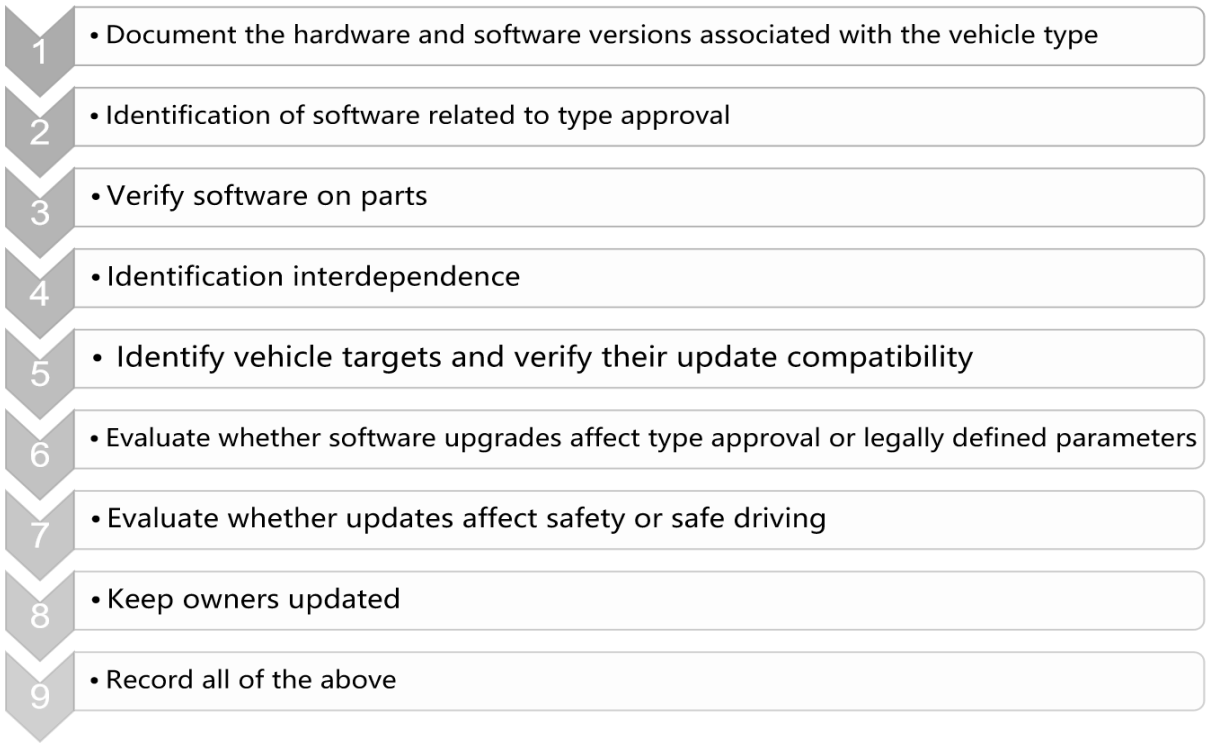

Figure 1 Software upgrade process of WP.29/R156

(1) Online update Requirements

During the process of online updates, automotive manufacturers must have corresponding documentation to ensure the quality and safety of their products. Effective security management is required for the updated files to ensure their safety. These documents cover the entire software update process and provide evidence of compliance with all relevant standards, describing all types of files related to certification system configuration. They provide detailed

ISSN: 2664-9640

descriptions before and after the update, as well as documentation indicating whether the vehicle parameters meet the required specifications. Software documentation related to the RXSWIN (Software Identifier) specific to the vehicle type is provided to describe the situation before and after the update, along with results obtained after retesting the vehicle with the new version in use. A document is needed that includes compatibility and latest configuration information for the target vehicle to facilitate the update and verification registration.

(2) Security Policy Requirements

During the process of online updates, automotive manufacturers should implement appropriate protection measures to ensure their own security and reliability. Effective security management policies need to be developed by automotive manufacturers to address the impacts of updates. To ensure vehicles are adequately protected during the update process and to prevent unexpected incidents caused by driver misoperation before initiating the update. Special attention should be paid to the development system update to avoid damaging the software. The functionality and code of the software used in the vehicle should be validated to ensure normal operation.

(3) update Record Requirements:

Automotive manufacturers are required to have clear requirements for online update records. Specifically, the online update process needs to be performed by designated technical personnel to ensure accuracy and safety of operations.

(4) General Requirements for Vehicle Models:

For online updates, automotive manufacturers have other clarifications and requirements. These include protecting the authenticity and integrity of software updates, preventing issues such as leaks or failures. Ensuring each RXSWIN (Software Identifier) is uniquely identifiable and preventing unauthorized tampering with a vehicle's RXSWIN.

(5) Requirements for Vehicle Online updates:

Explicitly state the safety requirements for vehicles during the software update process. This includes the following:

Before the update:

1)The vehicle must meet necessary prerequisites.

2)Sufficient battery power in the vehicle is required before performing the update.

3)When the update may affect vehicle safety, it should be ensured that the update is conducted safely.

4)Prior notification should be provided to vehicle users before executing the update.

During the update:

Ensure that users do not drive the vehicle and refrain from using any functions that may impact vehicle safety or the update process.

After the update:

1)Notify the vehicle user of the success or failure of the update and any implemented changes.

2)Ensure that all updates related to the user manual are clearly explained.

3)Ensure that the vehicle can enter a safe state in case of update failure or interruption.

WP.29/R156 sets forth requirements for automotive manufacturers regarding security measures and update systems, establishing a standardized process for software updates and enhancing the overall safety of the update process.

2.2. Germany VDA Recall Management Using Over- the-Air Updates

Policy Area: The German Association of the Automotive Industry (VDA) has developed a series of management policies for Over-The-Air (OTA) technology to ensure the security, reliability, and legality of OTA software updates. The following are VDA's management policies for

ISSN: 2664-9640

OTA:VDA emphasizes that OTA technology must comply with relevant safety requirements, such as protecting vehicle networks from attacks and malicious software intrusion, and ensuring that software updates do not affect vehicle operation and driving safety. VDA requires that OTA technology protect the personal data privacy of vehicle owners, such as vehicle location, travel routes, and other information, to prevent misuse or leakage. VDA emphasizes that OTA technology must comply with relevant legal regulations and standards, such as the EU's ECU Software Update Regulation. To ensure the reliability and stability of OTA technology, VDA requires automotive manufacturers to conduct thorough testing and verification before implementing OTA software updates, including functional testing, performance testing, compatibility testing, and security testing.To address issues that may arise during OTA software updates, VDA recommends that automotive manufacturers establish reliable rollback mechanisms before implementing OTA updates to ensure a quick recovery to the previous stable state.

Regulatory measures primarily include the following aspects: VDA is responsible for developing standards and specifications related to OTA technology to ensure that OTA software updates comply with relevant legal regulations and standards. These standards and specifications provide guidance for automotive manufacturers, helping them follow the correct procedures and processes when implementing OTA technology. VDA recognizes certain independent third-party organizations responsible for auditing and certifying OTA technology for automotive manufacturers or other relevant companies. These organizations assess and test OTA technology, processes, security aspects, and more to ensure compliance with relevant legal regulations and standards. VDA also conducts regular supervision and inspections, sampling checks, and reviews on automotive manufacturers that have implemented OTA technology to ensure their OTA technology meets the relevant standards and legal requirements.To promote the better development of OTA technology, VDA has established a data-sharing platform where automotive manufacturers can share OTA technology data and information. This helps accelerate the research and promotion of innovative OTA technology to better adapt to the increasingly complex demands of vehicle software updates [7].

2.3. UL 5500

UL5500 is a standard specific to electric vehicles and hybrid vehicles, which includes management methods for software updates. The main aspects of software update management under the UL5500 standard are as follows:

Under the UL5500 standard, software development for electric vehicles and hybrid vehicles needs to comply with a series of safety and quality standards, such as ISO 26262 and SPICE. Before performing software updates, thorough testing and verification are required to ensure that the software updates comply with relevant standards and specifications. The UL5500 standard supports software updates through OTA technology but imposes a set of requirements for security and privacy protection. For example, OTA updates must utilize encrypted communication technology to prevent malicious attacks and data breaches. Clear options need to be provided to vehicle owners, allowing them to choose whether to accept specific software updates. To ensure the success and reliability of software updates, the UL5500 standard requires manufacturers to have standardized on-board diagnostic tools in place to detect and verify the process and results of software updates, as well as record relevant information. When performing software updates, the UL5500 standard also mandates the establishment of reliable rollback mechanisms by manufacturers to ensure a return to the previous stable state if needed. Additionally, software updates require version and change management to maintain a historical record and traceability of issues.

ISSN: 2664-9640

2.4. Japanese laws and regulations

To accelerate the development of the autonomous driving industry, Japan has successively issued or revised documents such as the Road Vehicle Transport Act, Vehicle Specific Modification Permit System, Road Transport Vehicle Security Standards, and Examination Affairs Regulations to regulate key aspects of applying, reviewing, verifying, and licensing automobile OTA remote update management.

Japan applies automobile OTA remote update technology to retrofit currently sold vehicle models. They stipulate that automotive manufacturers with OTA remote update retrofit capabilities need to establish corresponding network security and software update system management systems. National regulatory authorities periodically review the implementation of these established system management systems. Additionally, automotive manufacturers are required to submit application materials for automobile software updates to the Japanese Ministry of Land, Infrastructure, Transport, and Tourism (MLIT) and can only execute automobile OTA remote updates after obtaining approval from MLIT [8-10].

3. Domestic standard regulations

The Ministry of Industry and Information Technology (MIIT) formulated a series of OTA-related technical standards in 2019, such as the "Specification for Data Exchange of Vehicle Electronic Control Unit Software update" and the "Technical Specification for In-vehicle Terminal OTA update." The Chinese government has issued multiple policy documents to encourage and guide the automotive industry in strengthening research and application of OTA technology. For example, in 2017, MIIT released the "Development Plan for New Energy Vehicles (2016-2020)," which explicitly supports the development of technologies such as remote diagnostics and remote updates. In 2019, MIIT published the "Guidelines for Pilot Demonstration and Promotion of Intelligent Connected Vehicles," encouraging enterprises to engage in the practical application of vehicle OTA technology.

The Chinese government emphasizes that OTA technology must comply with relevant safety requirements, such as protecting vehicle networks from attacks and malicious software intrusion, and ensuring that software updates do not affect vehicle operation and driving safety. Additionally, the Chinese government mandates the use of encrypted communication technology in OTA technology to prevent malicious attacks and data breaches. To strengthen the regulation of OTA technology, the Chinese government has established an OTA technology management system and a remote update information announcement platform. The OTA technology management system is primarily used to record vehicle software update information and audit results for regulatory purposes. The remote update information announcement platform is used to publish relevant technical specifications, security alerts, laws, and regulations, providing references for automotive manufacturers and consumers.

On November 25, 2020, the State Administration for Market Regulation issued the "Notice on Further Strengthening the Supervision of Automotive Remote update (OTA) Technical Recalls." The notice states that automotive manufacturers should use OTA methods to rectify defective automotive products according to the requirements of the "Regulations on the Management of Defective Automotive Product Recalls" and its implementing measures. They are also required to promptly file with the Quality Development Department of the State Administration for Market Regulation [11].

On July 30, 2021, MIIT issued the "Opinions on Strengthening the Management of Intelligent Connected Vehicle Manufacturers and Product Access." The opinions regulate online software updates to ensure consistency in product production and strengthen supervision and enforcement to consolidate foundational capabilities [12].

ISSN: 2664-9640

On April 15, 2022, the Equipment Industry Development Center of the Ministry of Industry and Information Technology released the "Notice on Filing Work for Automotive Software Online updates." The notice requires companies to register their own management capabilities, vehicle models, functionalities, and specific update activities. Following the relevant provisions of the "Administrative Measures for Road Motor Vehicle Manufacturers and Products Access" and the "Opinions on Strengthening the Management of Intelligent Connected Vehicle Manufacturers and Products Access," the Equipment Industry Development Center organized the filing work for automotive software online updates, also known as OTA updates [13].

The GB (National Standard of China) "General Technical Requirements for Automotive Software updates" is expected to be published in 2024. It emphasizes that automotive software updates must comply with relevant laws, regulations, and standards, and strictly follow software development processes and quality management systems for design, coding, testing, and verification. Regarding OTA updates, automotive software updates can be performed using OTA technology but must meet a set of security and privacy protection requirements. For example, OTA updates must use encrypted communication technology to prevent malicious attacks and data breaches. Clear options need to be provided to vehicle owners, allowing them to choose whether to accept specific software updates. Additionally, automotive software updates must meet relevant safety requirements, such as protecting vehicle networks from attacks and malicious software intrusion, and ensuring that software updates do not affect vehicle operation and driving safety. Furthermore, automotive software updates need to have security mechanisms such as software integrity verification and hardware authentication. Personal data privacy of vehicle owners, such as vehicle location and travel routes, must be protected to prevent misuse or leakage. The process and results of software updates also need to be recorded and protected. Moreover, reliable rollback mechanisms must be established during automotive software updates to ensure a return to the previous stable state if necessary. Additionally, version and change management are required for software updates to maintain historical records and traceability of issues.

4. Summarize the comparison and development suggestions

Currently, there are certain differences in the regulatory provisions regarding OTA updates among countries. However, there is a general consensus that OTA updates can be considered as a form of "retrofitting" vehicles or as a means of quality recalls. Specific regulations on OTA updates have been introduced by organizations such as the United Nations and Japan, while Germany and China have yet to introduce corresponding detailed guidelines. In China, OTA updates are managed through filing. Regarding the necessity of type approval, it is generally recognized by major countries and regions that OTA updates involving type approval need to be approved, and independent institutions are required to conduct audits for OTA updates that comply with standards. However, there is no specific definition in China regarding the clarity of OTA update steps.

Table 1: Comparison of OTA Regulations among Countries

Contrast items	UN	Germany	UL	Japan	China
Attitude towards OTA	A modification of a vehicle	As a means of quality recall	A modification of a vehicle	A modification of a vehicle	As a means of quality recall + vehicle reengineering

ISSN: 2664-9640

Are there OTA update regulations	Yes	No (Red Book)	No (Standard)	Yes	No (ICP Filing Management)
Whether the OTA requires type approval	Approval is required for updates involving type approval	No	No	Approval is required for updates involving type approval	Approval is required for updates involving type approval
Whether the OTA requires an independent authority to conduct an OTA update compliance review	Yes	No	No	Yes	Yes
Whether the OTA update steps are clear	Yes	Yes	Yes	Yes	No

In accordance with the government's policies, the establishment of a filing management system for automotive software online updates can serve as a means for quality recalls and vehicle rejuvenation. We suggest collecting relevant record information and requirements regarding online updates of automotive software, analyzing and summarizing actual issues, and promoting the revision of standards frameworks to enhance the management capabilities of automotive manufacturers. Additionally, we recommend gradually establishing a regulatory system for automotive software online updates specifically targeting the functionality of software online updates to adapt to the development of intelligent connected vehicles in China. This system aims to ensure the safety of software online updates for intelligent connected vehicles, enhance their operational security, and promote rapid development in the intelligent connected vehicle industry.

Acknowledgements

This work was supported by the National Key Research and Development Program of China (No. 2021YFB2501300, 2021YFB2501302).

References

[1] Feng Wanjun, Fu Jinyong, Zhang Heli, et al. Powertrain/Body Controller Update Method In Vehicle OTA and Software Version Matching [C]// China Society of Automotive Engineers.2019 Annual Conference Proceedings of China Society of Automotive Engineers (4). China Machine Press,2019:5.

[2] Shi Qingguo, Shang Haili, Ma Jie et al. OTA Upgrade Solution for Intelligent Networked Cars [C]// China Society of Automotive Engineers.2018 Annual Conference Proceedings of China Society of Automotive Engineers. China Machine Press,2018:7.

[3] ZHANG Qian. A Holistic Framework OTA Automotive Applications [J]. Journal of practical technology, 2020 (11) : 100-102. The DOI: 10.16638 / j.carol carroll nki. 1671-7988.2020.11.032.

ISSN: 2664-9640

[4] WANG Dongliang, Tang Lishun, Chen Bo, et al. The Research of OTA Function Design for Intelligent and Connected Vehicle [J]. Journal of automotive technology, 2018 (10) : 29-33. DOI: 10.19620 / j.carol carroll nki. 1000-3703.20181065.

[5] UNITED NATIONS. Cyber security and cyber security management system, UN Regulation No. 155[S/OL]. (2020-04-04)[2022-07-29].

[6] UNITED NATIONS. Software update and software update management system, UN Re-gulation No.156[S/OL]. (2020-04-04) [2022-07-29].

[7] Association of the German Automotive Industry. Upgrade Recall Management with over-the-Air Downloads [S/OL]. (2020) [2022-07-29].

[8] the cabinet. The road transport vehicles act amendment [S/OL]. [2022-07-29] (2019-05-17).

[9] Japanese Ministry of Land, Infrastructure and Transport. Special Permit Act for Motor Vehicles [S/OL]. (2020-04-01) [2022-07-29].

[10] Japanese Ministry of Land, Infrastructure and Transport. Safety Standards for Road Transport Vehicles, [S/OL].(2019-05-28) [2022-07-29].

[11] The State Administration for Market Regulation. Notice on Further Strengthening the Supervision of Automobile Remote Upgrade (OTA) Technology Recall; [2020] No. 123 [S/OL]. (2020-11-25) [2022-07-29].

[12] Quality Development Bureau of the General Administration of Market Regulation. Supplementary Notice on the Filing of Automotive Remote Upgrade (OTA) Technology Recall [S/OL]. (2021-06-04) [2022-07-29].

[13] Equipment Industry Development Center, Ministry of Industry and Information Technology. Notice on Filing Online Upgrade of Automotive Software: Equipment Center [2022] No. 229 [S/OL].(2022-04-15) [2022-07-29].