Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 10, No. 2, 2024

Research on Regulations on Software Update of Intelligent Connected Vehicles

Yuzhe Wang [a], Zhapa Mu [b], Yongjian Zhu [c], Manna Wang [d], Xuebin Shao [e]

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

[a] wangyuzhe@catarc.ac.cn, [b] muzhapa@catarc.ac.cn, [c] zhuyongjian@catarc.ac.cn, [d] wangmanna@catarc.ac.cn, [e] shaoxuebin@catarc.ac.cn

Abstract: With the rapid development of intelligent connected vehicle technology, software updates have become the key to improving vehicle performance and safety. However, frequent software updates also create new challenges for information security and compliance. The purpose of this article is to discuss the management strategy of software update for intelligent connected vehicles and analyze the existing regulatory requirements to ensure the safety and effectiveness of the software update process.

Keywords: Over-The-Air (OTA); Intelligent and Connected Vehicle; Software Online Updating; Standard Regulation.

1. Introduction

Over the past few decades, the automotive industry has undergone tremendous changes, especially with the rapid development of intelligent networking technology [1], where the car is not just a simple means of transportation, but also a complex intelligent system. Connected and Autonomous Vehicles (CAVs) are connected to the Internet and enable the acquisition and exchange of information in real time, thereby improving driving safety, vehicle performance, and user experience. However, this transformation also comes with a number of challenges, especially in terms of software management and information security.

Before Over-the-Air (OTA) update technology was widely used in the automotive industry, when there was a problem with the car system, it was often necessary to rely on the automaker to repair it through recalls. This method is not only time-consuming, labor-intensive, but also costly. The introduction of OTA update technology has made online repair possible, significantly improving work efficiency and reducing maintenance costs [2]. As a result, many car manufacturers are adopting this technology. However, with the popularity of OTA upscaling technology, concerns about abuse have also arisen. Some automakers have taken a relatively arbitrary approach to software updates for connected cars, performing automatic updates without fully explaining the situation to users. Considering that cars are closely related to the safety of users' lives, some manufacturers rush to release intelligent connected car systems that are incomplete or not fully validated, trying to solve potential problems with subsequent software updates. There is a clear lack of rigor in this approach. At present, the management of automotive products mainly relies on type certification, which requires the standards of vehicles to comply with relevant national regulations. However, with the spread of software update technology, car manufacturers can easily bypass the existing automotive product management system and arbitrarily change key parameters such as vehicle safety, emissions, and energy consumption, thereby obtaining undue benefits. This situation can lead to problems with the consistency of automobile production and pose a challenge to the existing management system. Therefore, it is particularly necessary to carry out research on policies and regulations on software update of intelligent networked vehicles at home and abroad.

2. The Development of Automotive OTAs

The development of automotive over-the-air (OTA) technology is a revolutionary advancement in the field of intelligent and connected vehicles, which enables automakers to remotely update and manage vehicle software and firmware over wireless networks. The evolution of this technology began with the traditional way of updating physical media, such as CD, USB, etc., and the user needs to manually install the update into the vehicle, which is not only cumbersome, but also prone to version inconsistencies and security risks. With the advancement of wireless communication technology, especially the popularization of 3G, 4G and 5G networks, automakers are beginning to explore the possibility of remote updates over mobile networks, thus improving the convenience and efficiency of updates [3]

OTA technology is constantly expanding, adding new features and improving existing ones, in addition to fixing software vulnerabilities, allowing vehicles to continuously improve performance and user experience. This flexibility allows consumers to enjoy a wider range of automotive services, satisfying their needs for intelligence and personalization. At the same time, OTA technology also provides an important security guarantee for automakers, able to push security patches in a timely manner to protect vehicles from cyber-attacks and information leaks.

Changes in market demand are another important factor driving the rapid development of OTA technology. Modern consumers are not only concerned about the hardware performance of their cars, but also look forward to the ever-changing software features and services. In addition, the rise of emerging automakers such as Tesla has put tremendous competitive pressure on traditional automakers, prompting them to accelerate the speed and frequency of software updates to remain competitive in the market.

With the popularity of OTA technology, regulations and standards are constantly evolving. For example, standards such as R156 and ISO 24089 issued by the United Nations put

forward requirements for the management of automotive software updates, ensuring the security and compliance of the update process. The implementation of these regulations not only regulates the behavior of automakers, but also strengthens consumer trust in the security of automotive software.

Looking to the future, the development of automotive OTA technology will continue to move in the direction of intelligence and automation. The rollout of 5G technology will further improve the speed and reliability of OTA updates, enabling large-scale data transmission and real-time updates. In addition, future OTA updates will be smarter, with the ability to automatically push updates based on vehicle usage and user preferences, improving the user experience. However, with the popularity of OTA technology, cybersecurity issues will also become a significant challenge, and manufacturers need to continuously strengthen security measures to ensure the safety of vehicles during the update process.

In short, the development of automotive OTA technology has not only changed the way the automotive industry manages software, but also promoted the entire industry to move towards a higher level of intelligence and digitalization. With the continuous advancement of technology and the growth of market demand, OTA will become an important part of the future of intelligent connected vehicles, greatly improving the safety, reliability and user experience of vehicles.

3. International Regulatory Standards

3.1. UNECE R156

R156 regulation, that is, WP.29/R156 issued by the United Nations Economic Commission for Europe (UNECE), mainly regulates automotive software updates and software update management systems (SUMS). The regulation was introduced to ensure the safety and reliability of connected vehicles when performing software updates, especially in the context of the increasing popularity of over-the-air (OTA) technology [4].

3.1.1. Background and Purpose

With the rapid development of intelligent and connected vehicles, the software system of vehicles is becoming more and more complex, and the frequency and importance of software updates are also increasing. The R156 regulation was introduced to regulate the behavior of car manufacturers when performing software updates; Ensure the security of the update process and prevent potential cyber security risks; Increase consumer trust in the security of connected vehicle software.

3.1.2. Scope of Application

The R156 regulation applies to all newly produced automobiles and sets out a timeline for implementation:

New vehicles will be required to comply with the regulation from July 2022.

Existing vehicles will have until July 2024 to comply with the regulations.

3.1.3. Software Update Management System (SUMS)

The R156 regulation requires automakers to establish a Software update Management System (SUMS) that should cover the following areas:

Online update requirements: Automakers must have complete documentation to ensure the quality and safety of software updates. This includes a detailed description of the vehicle parameters before and after the update, as well as documentation of the RXSWIN (Software Identifier) associated with the vehicle type.

Safety policy requirements: Manufacturers need to develop an effective safety management strategy to address the risks that may arise during the software update process and ensure the safety of the vehicle during the update process.

update Record Requirements: Automobile manufacturers are required to keep detailed records of the online update process to ensure the accuracy and safety of the operation, and the records should be completed by qualified technicians.

General requirements for vehicle models: Clarify the authenticity and completeness of software updates, ensure that each RXSWIN is uniquely identifiable, and prevent tampering.

Model Online update Requirements: Specify the safety requirements of the vehicle during the software update process, including preparation before the update, operational restrictions during the update, and post-update notifications and status confirmations.

3.1.4. Update Process

Regulation R156 specifies a standardized software update process that includes the following steps:

update preparation: Make sure the vehicle meets the necessary conditions, check whether the battery is sufficient, and provide the user with an update notification.

update implementation: During the update process, ensure that the user cannot drive the vehicle and avoid any actions that may affect the update.

Post-update confirmation: Once the update is complete, the user is notified of the update result, ensuring that all relevant documentation and user manuals are updated, and confirming the vehicle's safety status in the event of an update failure or interruption.

3.1.5. Compliance & Oversight

The R156 regulation requires automakers to remain compliant during the software update process and to be subject to oversight by the relevant regulatory bodies. This includes regular audits and inspections to ensure the effectiveness and security of their software update management system.

3.1.6. Conclusion

The implementation of the R156 regulation will help improve the software security of intelligent and connected vehicles, ensuring that consumers can enjoy the convenience of technological advancements while being fully secured. With the rollout and enforcement of regulations, it is expected to drive further developments in software management and cybersecurity in the automotive industry.

3.2. ISO 24089

ISO 24089 is a standard published by the International Organization for Standardization (ISO) to provide guidance on the safety of connected vehicles, particularly in software management and cybersecurity. The full name of the standard is ISO 24089:2021 - Road vehicles — Cybersecurity engineering — Guidelines for the management of cybersecurity risks in the lifecycle of road vehicles [5]

3.2.1. Background and Purpose

With the rapid development of intelligent and connected vehicles, the complexity of vehicle electronic systems and software is increasing, and cybersecurity issues are becoming

increasingly prominent. ISO 24089 provides a comprehensive cyber risk management framework; Guiding automakers and relevant stakeholders to effectively manage cybersecurity risks throughout the vehicle lifecycle; Promote standardization and consistency in cybersecurity in the automotive industry.

3.2.2. Scope of Application

ISO 24089 applies to all types of road vehicles, including passenger cars, commercial vehicles, and heavy vehicles. The standard applies to the entire life cycle of a vehicle, including the design, development, production, operation, maintenance, and end-of-life phases.

3.2.3. Core Content

The core content of ISO 24089 includes the following aspects:

3.2.3.1 Cybersecurity Risk Management

Risk identification: Identify cybersecurity risks associated with vehicles, including potential attack paths and threat sources.

Risk assessment: Assess the severity and likelihood of identified risks to determine their impact on vehicle safety.

Risk controls: Develop and implement controls to mitigate cybersecurity risks, including technical and administrative measures.

3.2.3.2 Lifecycle Management

Design phase: In the vehicle design phase, cyber security considerations are taken into account to ensure the design of the safety architecture.

Development phase: During the software development process, secure coding standards and tests are implemented to identify and remediate security vulnerabilities.

Production phase: Ensuring safety in the production process, including the management of the supply chain.

Operational phase: Implement continuous cybersecurity monitoring and maintenance measures during vehicle operation.

Maintenance and Scrapping Phase: Ensure the safe handling and destruction of data during vehicle maintenance and scrapping.

3.2.3.3 Compliance & Audit

Compliance requirements: Ensure that vehicles comply with relevant cybersecurity regulations and standards throughout their lifecycle.

Audits and Assessments: Conduct regular cyber security audits and assessments to verify the effectiveness of risk management measures.

3.2.4. Implementation Guidelines

ISO 24089 provides a set of implementation guidelines to help automakers and relevant stakeholders apply cybersecurity risk management frameworks in practice. These guidelines include:

Develop cybersecurity policies and procedures.

Establish cross-functional teams to ensure that all departments work together.

Conduct training and awareness raising to enhance employees' cybersecurity awareness.

3.2.5. Conclusion

The implementation of ISO 24089 will help improve the cybersecurity of connected vehicles, ensuring that consumers can enjoy the convenience of technological advancements while being fully secured. As cybersecurity threats continue to evolve, ISO 24089 provides a dynamic and adaptable risk management framework for the automotive industry, contributing to the industry's sustainable development.

3.3. R156 Regulation Different with ISO 24089

There are significant differences between the R156 regulation and the ISO 24089 standard when it comes to the safety management of connected vehicles. The R156 regulation is mainly aimed at automotive software updates and software update management systems (SUMS), and its core purpose is to ensure that the safety and reliability of the vehicle are guaranteed during the software update process. The regulation sets out specific implementation requirements and timelines that apply to all newly produced vehicles, emphasizing the compliance process that manufacturers must follow when making software updates to protect the safety of consumers.

In contrast, the ISO 24089 standard provides a comprehensive cybersecurity risk management framework that focuses on cybersecurity management throughout the vehicle lifecycle. The standard covers not only the identification and assessment of cybersecurity risks in the vehicle design and development phase, but also the safety management in the operation, maintenance, and end-of-life phases. ISO 24089 emphasizes continuous risk management and aims to improve the overall management of cybersecurity by automakers and relevant stakeholders.

In addition, the R156 regulation is mandatory, requiring car manufacturers to follow specific legal regulations and be supervised by regulatory bodies, while the ISO 24089 standard is a voluntary standard, although not mandatory, but recommended for manufacturers to follow, to improve standardization and consistency in the industry. Overall, R156 focuses on compliance and security for software updates, while ISO 24089 focuses on comprehensive cybersecurity risk management, covering a broader range of content and implementation phases.

4. Domestic Regulatory Standards

The Notice on Further Strengthening the Supervision of Over-the-air (OTA) Technology Recalls is an important policy document issued by the State Administration for Market Regulation of the People's Republic of China (SAMR) to enhance the supervision of the remote software update process to ensure the safety and rights of consumers. The notice requires automakers to file with regulators, submit detailed update plans and risk assessments, and establish a comprehensive recall mechanism to deal with potential safety hazards before making OTA updates. At the same time, manufacturers are required to inform users of the update content and potential risks in advance, and regulators will conduct regular supervision and inspection to ensure the implementation of various regulations. The implementation of this notice will help standardize the OTA update behavior in the automotive industry and enhance consumer trust in intelligent connected vehicles.

The "Opinions on Strengthening the Access Management of Intelligent Connected Vehicle Manufacturers and Products" was issued by the Ministry of Industry and Information Technology (MIIT) on July 30, 2021. The Opinions clarify the requirements for access management of ICV manufacturers, including enterprise qualification review, product technical standards, quality management system and safety assessment. By establishing a strict access mechanism, it aims to ensure the safety, reliability and technological

advancement of intelligent networked vehicles, and prevent potential safety risks. At the same time, the opinion also encourages enterprises to strengthen technological innovation and research and development, promote the sustainable development of the intelligent networked vehicle industry, enhance the competitiveness of the overall industry, and protect the legitimate rights and interests of consumers.

GB 44496-2024 "General Technical Requirements for Automotive Software updates" has been released in August 2024 and is a national standard formulated in China for automotive software updates, aiming to ensure the security, reliability and transparency of the software update process. The standard covers aspects such as software update management system and vehicle model testing. Its release provides specifications and guidance for automakers and software developers, helping to improve the quality and safety of automotive software management.

5. Conclusion

R156, ISO 24089, the Opinions on Strengthening the Access Management of Intelligent Connected Vehicle Manufacturers and Products, and the Notice on Further Strengthening the Supervision of Vehicle Remote update (OTA) Technology Recalls, as well as GB, jointly emphasize the compliance and management requirements for intelligent networked vehicles in terms of software updates and cybersecurity. These regulations and standards are designed to ensure that automakers can effectively protect user data, vehicle functional safety and cybersecurity when performing software updates, and promote the healthy development of the automotive industry. Looking ahead, with the continuous advancement of intelligent networked vehicle technology, the improvement of relevant regulations and standards will further promote the standardization of the industry, enhance consumer trust, and ensure the development of intelligent vehicles in a safe and reliable environment.

References

[1] Feng Wanjun, Fu Jinyong, Zhang Heli, et al. Vehicle body Power Area ECU Upgrade and software Matching in vehicle OTA System [C]// China Society of Automotive Engineers. 2019 Annual Conference Proceedings of China Society of Automotive Engineers (4). China Machine Press, 2019: 5.

[2] Zhang Qian,. A car that the OTA industry application of the overall framework of [J]. Journal of practical technology, 2020 (11) : 100-102. The DOI: 10.16638 / j.carol carroll nki. 1671-7988.2020.11.032.

[3] WANG Dongliang, Tang Lishun, Chen Bo, et al. Research on OTA function Design of Intelligent Connected Vehicle [J]. Automotive Technology,2018(10):29-33.

[4] Shi Qingguo, Shang Haili, Ma Jie et al. OTA upgrade plan for intelligent Connected vehicles [C]// China Society of Automotive Engineers. 2018 China Automotive Engineering Society annual Conference proceedings.

[5] ISO. (2021). ISO 24089:2021 - Road vehicles -- Cybersecurity engineering -- Guidelines for the management of cybersecurity risks in the lifecycle of road vehicles. International Organization for Standardization.