Research on Construction and Optimization of Vehicle Software Updates Management System

Hanyu Li, Wenxia Ji, Haijun Wang *, Yuwei Su

CATARC Intelligent and Connected Technology Co., LTd. 300000 No.68, East Xianfeng Road, Dongli, District, Tianjin, China

*wanghaijun2019@catarc.ac.cn

Abstract. With the development of intelligent vehicles in network connection, intelligence and architecture technology, vehicles have irreversibly required software iterative update both in firmware and software. The successive introduction of domestic and foreign regulations and policies has made the construction of vehicle software update management system a general trend, in order to better respond to the implementation of the relevant national policy requirements, to build a standardized, process-oriented vehicles software update process, empowering automotive industry enterprises to better grasp the regulations and build a process system that meets the requirements of the necessity to optimize the construction of the system is self-evident.

This article will provide a detailed description of vehicle software update management system construction and optimization measures, with the intention of facilitating the enhancement and implementation of vehicle software update management system capabilities.

Keywords: Intelligent and connected vehicles, Software update, Management System, OTA security.

1 BACKGROUND

Under the development trend of electrification, intellectualisation and internet connectivity of vehicles, software update technology is widely used and has become an indispensable part of enterprises to fix vehicle problems and improve user experience. The increase of electronic control systems in intelligent and connected vehicles makes the demand for update the control unit software and firmware increasingly strong when vehicles electronic components or software encounter problems.[1]

Since smart vehicles have the ability to communicate wirelessly, vehicle manufacturers have begun to implement remote over-the-air download (Over The Air, OTA) update of vehicle software wirelessly, which eliminates the need for a physical recall process and provides users with the most convenient and fastest software update services[2].OTA technology can reduce the recall cost of vehicles after mass production, realize the unified management of vehicle software and vehicle data, and improve the efficiency and quality of after-sales service.[3]Therefore, the emergence of OTA

V. Vasilev et al. (eds.), *Proceedings of the 2024 5th International Conference on Management Science and Engineering Management (ICMSEM 2024)*, Advances in Economics, Business and Management Research 306,
https://doi.org/10.2991/978-94-6463-570-6_137

technology poses a serious challenge to the current management standardization of automobiles. The construction of software update management system is essential for the whole vehicle enterprises.

2 DOMESTIC AND INTERNATIONAL REGULATORY REQUIREMENTS

The UN/WP.29, based on the current status and future development trend of OTA, the 181st Plenary Session of WP.29 adopted the technical regulation R156 Software Update and Software Updates Management System, which was formally published on 25th June 2020, and came into effect in January 2021.R156 covers all software updates, including updates provided by OTA and traditional means, and applies to all ECUs and software components of vehicles. R156 sets out the requirements for the certification of Software Updates Management System (SUMS), which standardize the process of implementing software updates and ensure that the process of software updates is safe, controlled and compliant. the SUMS specifies six aspects: the update process, online updates, the security policy, the update record, general requirements for the vehicle model, and the requirements for online updates[4].The regulations clearly state that having a Software Updates Management System (SUMS) Certificate of Conformity is a prerequisite for product type approval, i.e., vehicle manufacturers are not allowed to conduct VTA tests before obtaining a SUMS Certificate of Conformity. The regulation puts forward a clear framework of safety assurance and system requirements for vehicle manufacturers. The regulation applies to member states under the UNECE 1958 agreement[5]，totaling 54 contracting parties, including all EU countries, non-EU countries such as Eastern and Southern Europe, and non-European countries such as Australia, Japan and Korea. It applies to Class M, N, O, R, S and T vehicles,and all vehicles to be sold in these 54 countries must comply with the requirements of R156.

In order to further standardize, specify and refine the requirements related to the management of vehicle software updates, the Automotive Information Security Standard Working Group of the Intelligent Networked Vehicle Substandard Committee of the National Technical Committee of Auto Standardization has formulated the mandatory standard of General Technical Requirements for Software Update of Vehicles , which was formed into a draft standard in November 2021, and is expected to come into force in January 2026 on a mandatory basis.The standard formulates OTA development management methods, test management methods and remote upgrade management methods, while sorting out the records and filing forms of each link of R&D and after-sales, etc., and increasing the records of preparation and implementation of updates[6]. For the specific cases in China, two requirements of user confirmation and door anti-locking have been added to the test requirements. The standard is implemented through the SUMS and vehicle requirements, which are currently divided into general requirements, process requirements, information record requirements, safety-related requirements, and additional requirements specifically for OTA online updates. The formulation of the national standard will further enhance and improve the management capability and technical requirements of vehicle manufacturers and vehicle products, and provide guarantee for improving the safety of software online update.

3 CORPORATE COMPLIANCE MANAGEMENT CONSTRUCTION

3.1 SU Management System Building Programme

The UN regulation UN ECE R156 Software Update and Software Updates Management System and the domestic GB General Technical Requirements for Software Update of Vehicles clearly state that automobile manufacturers should meet the“SUMS”and the“Vehicle Requirements”. Therefore, it is imperative for enterprises to lay out vehicles of SUMS.

3.2 Overview of the Content of the Institutional Framework

Based on the requirements of domestic and international regulations and standards such as ISO/SAE 24089 Road Vehicles - Software Update Engineering, UN ECE R156 Software Update and Software Updates Management System, GB General Technical Requirements for Software Update of Vehicles, Opinions on Strengthening the Management of Intelligent Connected Vehicle Manufacturing Enterprises and Product Entry and so on, the framework is set up to cover overall management, Software Update Management System framework covering overall management, software update activity management and safety management.

3.3 Route to System Building

The construction of SUMS follows the process model of PDCA, and is carried out in four stages: gap analysis, construction and implementation, system trial operation, and system optimization, so as to build a more comprehensive safety framework through scientific and systematic management means, further standardize the management of software update in the enterprise, enhance the management capability of software update, and achieve the goals of safety risk prevention and control and software update guarantee that meets the requirements of the laws and regulations.

Gap Analysis. In order to enhance the effectiveness of the implementation of the management system, at the early stage of the system construction, combined with ISO/SAE 24089, UN ECE R156, GB General Technical Requirements for Software Update of Vehicles and other domestic and international regulations, we carried out a gap analysis by means of research, diagnosed the coverage of the enterprise software update management process, compared the requirements of the regulations and standards, and sorted out the gap items.

Construction Implementation. In the process of system construction, based on the requirements of standards and regulations as well as the output of gap analyses, the responsible units, inputs and outputs, and upstream and downstream relations of software update activities are determined from the pre-update, update and post-update of software to form a software update management system applicable to the enterprise.(see Fig. 1)

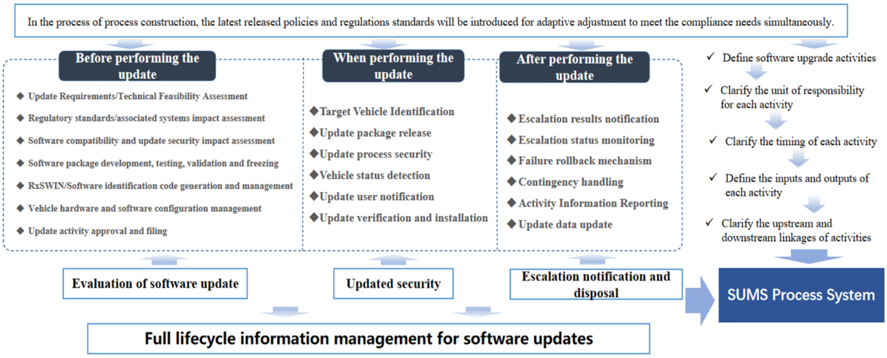

In the process of process construction, the latest released policies and regulations standards will be introduced for adaptive adjustment to meet the compliance needs simultaneously.
Before performing the update
◆ Update Requirements/Technical Feasibility Assessment
◆ Regulatory standards/associated systems impact assessment
◆ Software compatibility and update security impact assessment
◆ Software package development, testing, validation and freezing
◆ RxSWIN/Software identification code generation and management
◆ Vehicle hardware and software configuration management
◆ Update activity approval and filing
When performing the update
◆Target Vehicle Identification
◆Update package release
◆Update process security
◆Vehicle status detection
◆Update user notification
◆Update verification and installation
After performing the update
◆Escalation results notification
◆Escalation status monitoring
◆Failure rollback mechanism
◆Contingency handling
◆Activity Information Reporting
◆Update data update
✓ Define software upgrade activities
✓ Clarify the unit of responsibility for each activity
✓ Clarify the timing of each activity
✓ Define the inputs and outputs of each activity
✓ Clarify the upstream and downstream linkages of activities
Evaluation of software update
Updated security
Escalation notification and disposal
SUMS Process System
Full lifecycle information management for software updates

Fig. 1. Full lifecycle information management for software updates

The construction of SUMS is carried out in several aspects, including software update assessment process, safe software update process, update notification and disposal. The software update evaluation process mainly includes: evaluation of update demand and feasibility of update technology, evaluation of update system dependency, evaluation of the impact of type certification, evaluation of software compatibility, evaluation of vehicle safety and continuous operation. Update security mainly includes: authenticity and integrity verification of the update package, security measures in the update process, vehicle status and appropriateness of software code. Update notification and disposal mainly include: notification of update contents and update results, and emergency disposal of update emergencies.

After the completion of the system specification, the relevant personnel responsible for system construction to convene a review meeting on the formation of the management system specification document for the demonstration of the review.

System Trial Run. After the completion of the SUMS, in accordance with the control requirements of the management system specification document, the enterprise shall publish and implement the SUMS document and enter the trial run stage. Software update management personnel shall be in accordance with the requirements of the sums, software update management activities related to the landing exercise, the formation of the relevant business SUMS trial run records, verify the appropriateness of the system specification, the adequacy and effectiveness of the system, according to the results of the trial run of the system to correct, change.

System Optimization. After the system trial run, carry out the system review and optimization and rectification, for process operation, personnel awareness, supporting tools and templates to carry out evaluation and summary of the work, and for the trial run of the system found in the process of the system document itself there are problems, in accordance with the continuous improvement control mechanism to improve, to ensure that to achieve the goal of perfecting the construction of software update management system, to ensure that the system's consistency, validity, appropriateness and adequacy. The system is consistent, effective, appropriate and sufficient.

4 RECOMMENDATIONS FOR THE OPTIMIZATION OF SYSTEM BUILDING

4.1 Building an Efficient Management Organization

When building a system, establishing a reasonable and efficient organizational structure will make the building process faster. Enterprises should establish a reasonable organizational structure, so that the division of labour in each process of software update is clear. Set up Vehicle Software Update Management Committee as the decision-making organization of SUMS, responsible for the implementation of domestic and international policies, regulations and standards of software update requirements, the company's deployment of vehicle software update decision-making, etc.; the committee set up Vehicle Software Update Office under the committee, the director of the Vehicle Software Update Management Committee and the director of the Vehicle Software Update Office, responsible for the day-to-day operation of the SUMS. The director of the Vehicle Software Updates Management Committee shall also be the director of the Vehicle Software Update Office, responsible for the daily operation of the SUMS. Set up a Working Group on Software Updates, responsible for the implementation and execution of the SUMS in each department, and process management and correspondence based on the update plan.Enterprises should define the business flow of the whole process of software update, clarify the relationship between upstream and downstream, ensure that each business can be carried out effectively in accordance with the procedures, realize the rapid delivery of software development, and improve the efficiency of software development.(see Fig. 2.)

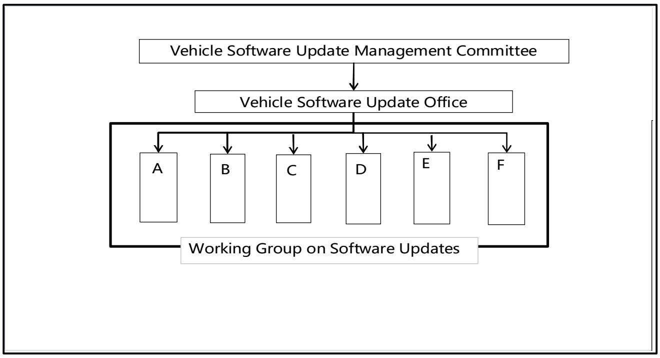

Vehicle Software Update Management Committee
Vehicle Software Update Office
A
B
C
D
E
F
Working Group on Software Updates

Fig. 2. Full lifecycle information management for software updates

4.2 Optimization of Security Mechanisms

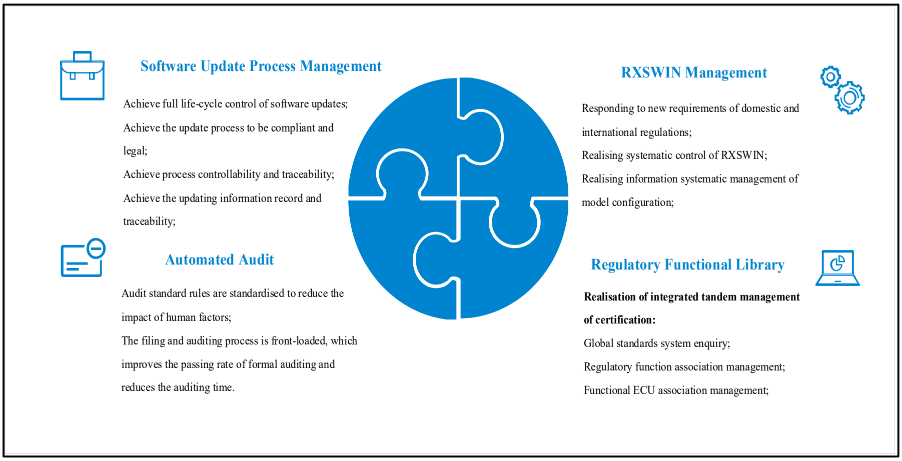
In order to address possible problems with OTA updates, various measures can be taken to prevent vehicles from being remotely attacked as well as data tampering, such as through integrity verification, authentication and key management. Data integrity requires that data is not authorized to be accessed and tampered with without permission. Studies have shown that tampered data packets may allow vehicles to be attacked remotely, threatening the safety of the vehicle and its users[7].Service integrity requires that software updates are not interfered with by malware or other malicious modifications throughout the process (DOS attacks, selective forwarding, node capture, etc.)[8].Service integrity may be compromised from the time the package is downloaded to the time it is installed. In order to avoid the data integrity and service integrity of OTA service being compromised, the data integrity of the update package should be verified both in the cloud and at the end of the vehicle to prevent unauthorized access and tampering of the update package.[9] Data integrity assurance in the update is mainly achieved through the hash function, common hash functions are MD5, SHA-1, SHA-256, etc. The verification of the hash value ensures the integrity of the firmware data. For car companies, the use of hash values for verification will lead to excessive data memory occupation, you can use the hash function to verify the integrity of automotive ECU data system. The system verifies the transmitted data through the hash function to ensure the integrity of the data in the transmission and storage process, thus reducing the risk of ECU data being attacked and tampered with, and making verification more convenient and faster.

To ensure the efficiency and reliability of the OTA update process, OEMs and network operators may choose to use robust and reliable communication protocols to establish efficient communication between the cloud and the vehicle. In addition, robust software programs need to be designed to meet the need to be able to automatically renew, auto-detect, and perform failure restarts in the event of an update interruption[10].

4.3 Integration Management

Facing the requirements of the regulations, enterprises should establish and improve the software update management system, covering the whole life cycle of the software update management system and standardized processes, and pay attention to the strategy of the software update related activities and the recording and storage of information on the implementation details. Enterprises should also set up corresponding safety strategies to ensure the reliable implementation of the update, and carry out a comprehensive assessment of the software update, focusing on its impact on the parameters/systems related to type approval or vehicle safety-related functions, as well as the relevance of the updated systems/functions to the systems/functions of other vehicles and the compatibility with the existing configuration of the vehicle. In order to ensure effective handling of software update contingencies, the enterprise should establish a risk control system and emergency response process for software update events. In addition, the key to effective compliance of the software update management system is its application, so enterprises need to apply the management system in the development of specific vehicle models to realize the implementation of the system on the ground. Enterprises should actively participate in the review of regulatory agencies to ensure that the application of OTA update complies with laws, regulations and regulatory requirements.

In the face of the shortcomings of traditional system-building,Enterprises can adopt the “tool + system”integration management method to carry out the construction of SUMS.The design of the software management platform is shown in the following below.(see Fig. 3.)



Software Update Process Management

Achieve full life-cycle control of software updates;
Achieve the update process to be compliant and legal;
Achieve process controllability and traceability;
Achieve the updating information record and traceability;

Automated Audit

Audit standard rules are standardised to reduce the impact of human factors;
The filing and auditing process is front-loaded, which improves the passing rate of formal auditing and reduces the auditing time.

RXSWIN Management

Responding to new requirements of domestic and international regulations;
Realising systematic control of RXSWIN;
Realising information systematic management of model configuration;

Regulatory Functional Library

Realisation of integrated tandem management of certification:
Global standards system enquiry;
Regulatory function association management;
Functional ECU association management;

Fig. 3. Software management platform design

Introducing the vehicle software management platform, the platform integrates six panels of software updates, which comprehensively covers the whole process of software updates, RXSWIN management, system audits, and meets the compliance requirements of R156 and GB and OTA filing requirements.The automation and compliance of the whole life cycle process of software update system construction can not only meet the requirements of regulations, but also improve the efficiency of enterprise configuration management.By integrating the process system into the configuration management tool and focusing on the regulatory requirements,the working efficiency can be increased by nearly 35%, and the enterprise can free itself from the dependence on the consultant, reduce the personnel investment, and realize the systematic management of the software update system construction and update filing activities.

4.4 High-Quality Development of Software

In the process of software development, the quality of software delivery often determines the success of the software development project.

To ensure high quality software development, we need to formulate software update process management procedures, define the business flow of the whole process of software update, clarify the upstream and downstream interface relationship, ensure that each business can be carried out effectively in accordance with the procedures, to achieve rapid delivery of software development, and improve the efficiency of software development. Secondly, it defines the software quality assurance process, establishes a comprehensive testing strategy, including software unit testing, system integration testing, vehicle functional testing, etc., covering all software testing scenarios required by the standards, monitors the quality status of the software and establishes quality metrics during the software development process to ensure that the quality of the software meets the standards and requirements. Third, establish the software version management process, record and control the hardware and software configuration information in the update process, formulate the software version release plan, carry out software version management according to the plan, and track the latest status of the software version, organize the final version review meeting for the final software configuration information, and after the review is passed by the departments, release the latest software configuration of the update activity and carry out the maintenance to ensure that each update There are clear version records and change history. Fourthly, a reasonable release strategy is formulated to clarify the update method, release cycle and release channels to ensure the smooth progress of software update.

5 CONCLUSION

The current programme for the construction of SUMS is not perfect. This paper starts from domestic and foreign regulations, systematically introduces the construction of SUMS, as well as construction optimization analysis, puts forward the construction of efficient organizational structure, optimization of safety mechanism, integration management of three aspects of the optimization programme, to help enterprises to improve the ability of software update construction.

REFERENCES

1. ZHU Y , WU S. (2022)Analysis on Software Online Updating Regulations for Intelligent and Connected Vehicles. Au- tomotive Digest (Chinese), 10:6-10.
2. RIGGS C, RIGAUD C, BEARD R, et al. A Survey on Con- nected Vehicles Vulnerabilities and Countermeasures. Journal of Traffic and Logistics Engineering, 6(1): 11 16,(2019).
3. Wang D,Tang L,Chen B.(2018)The Research of OTA Function Design for Intelligent and Connected Vehicle.Automobile Technology,10: 29-33.
4. Kun, D. and Jiayi, L., Special Purpose Vehicle, UN Regulation Introduction, 78-81,4(2018).
5. UNITED NATIONS. Software update and software update management system, UN Regulation No. 156. https://unece.org/sites/default/files/2021-03/R156e.pdf.(2020 04-04) [2022- 07- 29]
6. Jie Gao,Qing Wang.A Design Scheme of OTA Upgrade Service Platform for Electric vehicles,Computer Knowledge and Technology,13(8):209-211.(2017)
7. KNOCKEL J, CRANDALL J R. Protecting Free and Open Communications on the Internet Against Man-inthe-mid- dle Attacks on Third-party Software: we're FOCI'd// USENIX Workshop on Free and Open Communications on the Internet, Bellevue, WA, (2012).
8. KUPPUSAMY T K, DELONG L A, CAPPOS J. Uptane: Security and Customizability of Software Updates for Vehi- cles. IEEE Vehicular Technology, 13 (1): 66-73,(2018).
9. WANG J, WEN H, CHEN Y.(2024) Analysis on Key Technology and Regulatory Requirement for Automotive Over the Air Update. Automotive Digest (Chinese), 4: 19-27.
10. Xiaohui Dong.Research on Secure FOTA Upgrade Method for In-vehicle Domain Controller Architecture[D]. Changchun:Jilin University,(2022).