RESEARCH-ARTICLE FREE ACCESS

Research on Compliant Development of Vehicle Software Update Based on GB 44496-2024

Authors: Yudi Wang, Xianfeng Jia, Zhi Wu, Pengcheng Wang, Yongpei Jian, Junhua He Authors Info & Claims

ICAICE '24: Proceedings of the 5th International Conference on Artificial Intelligence and Computer Engineering
Pages 171 - 176 https://doi.org/10.1145/3716895.3716927

Published: 21 March 2025 Publication History Check for updates

To effectively regulate software update practices in the vehicle industry and ensure the security and reliability of update activities, China officially issued the mandatory national standard GB 44496-2024 “General Technical Requirements for Software Update of Vehicles” on August 23, 2024. This standard outlines the requirements for building a vehicle software update management system, specific technical implementation standards, and corresponding testing methods, providing guidance for vehicle software update activities. For all vehicle manufacturers wishing to sell vehicles in China, compliance with this standard is mandatory to regulate their software update activities. Against this backdrop, this paper conducts an in-depth study of GB 44496-2024, proposes a compliant development solution for vehicle software update and design a protection scheme for software update packages. Through this research, the paper aims to explore a scientific approach to vehicle software update within the framework of GB 44496-2024.

Aby Čína účinně regulovala postupy aktualizace softwaru v automobilovém průmyslu a zajistila bezpečnost a spolehlivost aktualizačních aktivit, vydala 23. srpna 2024 oficiálně závaznou národní normu GB 44496-2024 „Obecné technické požadavky na aktualizaci softwaru vozidel“. Tato norma stanoví požadavky na vytvoření systému správy aktualizací softwaru vozidel, specifické technické implementační normy a odpovídající testovací metody a poskytuje pokyny pro aktualizace softwaru vozidel. Pro všechny výrobce vozidel, kteří chtějí prodávat vozidla v Číně, je dodržování této normy povinné pro regulaci jejich aktualizací softwaru. V tomto kontextu tento článek provádí hloubkovou studii normy GB 44496-2024, navrhuje vývojové řešení pro aktualizaci softwaru vozidel, které je v souladu s normami, a navrhuje systém ochrany pro balíčky aktualizací softwaru. Prostřednictvím tohoto výzkumu si článek klade za cíl prozkoumat vědecký přístup k aktualizaci softwaru vozidel v rámci normy GB 44496-2024.

In recent years, a new wave of technological revolution is emerging, and the intelligence and network connectivity of automobiles have become the inevitable direction for the automotive industry's progress, which is important for the development of the vehicle industry in various countries. As the level of vehicle intelligence increases, vehicle software update has gradually become the norm. Software updates are categorized as offline update and Over-the-Air (OTA) update. Offline updates use physical media like diagnostic tools and USB drives, while OTA updates enable remote updates via wireless networks[1]. OTA technology allows manufacturers to quickly fix security vulnerabilities, introduce new features, and optimize performance, enhancing user experience and reducing costs[2]. However, widespread use of software updates brings challenges, including silent upgrades without user consent, unauthorized function changes, and cybersecurity and data risks[3].

V posledních letech se objevuje nová vlna technologické revoluce a inteligence a síťová konektivita automobilů se staly nevyhnutelným směrem pokroku automobilového průmyslu, což je důležité pro rozvoj automobilového průmyslu v různých zemích. S rostoucí úrovní inteligence vozidel se aktualizace softwaru vozidel postupně stala normou. Aktualizace softwaru se kategorizují jako offline aktualizace a bezdrátové aktualizace (OTA). Offline aktualizace používají fyzická média, jako jsou diagnostické nástroje a USB disky, zatímco aktualizace OTA umožňují vzdálené aktualizace prostřednictvím bezdrátových sítí [1]. Technologie OTA umožňuje výrobcům rychle opravit bezpečnostní zranitelnosti, zavést nové funkce a optimalizovat výkon, čímž se zlepšuje uživatelský komfort a snižují náklady [2]. Rozšířené používání aktualizací softwaru však s sebou nese výzvy, včetně tichých aktualizací bez souhlasu uživatele, neoprávněných změn funkcí a rizik pro kybernetickou bezpečnost a data [3].

To ensure the security of vehicles and the standardization of operations during software update, China officially released the GB 44496-2024 “General Technical Requirements for Software Update of Vehicles” on August 23, 2024. The introduction of this standard aims to provide normative guidance for vehicle software update activities. This paper conducts a

and security of software update activities.

Aby byla zajištěna bezpečnost vozidel a standardizace operací během aktualizace softwaru, Čína 23. srpna 2024 oficiálně vydala normu GB 44496-2024 „Obecné technické požadavky na aktualizaci softwaru vozidel“. Zavedení této normy si klade za cíl poskytnout normativní vodítko pro činnosti aktualizace softwaru vozidel. Tato práce se zabývá studií normy GB 44496-2024, navrhuje schéma vývoje pro aktualizaci softwaru vozidel v souladu s předpisy a navrhuje schéma ochrany pro balíčky aktualizací softwaru, čímž zajišťuje legalitu a bezpečnost činností aktualizace softwaru.

2 History of Software Update Policies and Regulations

2 Historie zásad a předpisů pro aktualizace softwaru

In recent years, the Chinese government has issued a series of regulatory policy documents concerning automotive software update activities, aiming to tightly monitor this field and ensure the effective protection of public safety and property.

V posledních letech vydala čínská vláda řadu regulačních dokumentů týkajících se aktualizací softwaru pro automobily s cílem důkladně sledovat tuto oblast a zajistit účinnou ochranu veřejné bezpečnosti a majetku.

On August 12, 2021, Ministry of Industry and Information Technology of the People's Republic of China issued the “Opinions on Strengthening the Administration of the Access of Intelligent Connected Vehicle Producers and Products”[4], aiming to strengthen the access management of intelligent connected vehicle manufacturers and products. In the third section of the document, it emphasizes the need to regulate over-the-air update activities. The document requires manufacturers to strengthen their management bilities and ensure product consistency in production.

inteligentních propojených vozidel“ [4] s cílem posílit správu přístupu výrobců a produktů inteligentních propojených vozidel. Ve třetí části dokumentu se zdůrazňuje potřeba regulovat činnosti bezdrátové aktualizace. Dokument vyžaduje, aby výrobci posílili své řídicí schopnosti a zajistili konzistenci produktů ve výrobě.

On April 15, 2022, Ministry of Industry and Information Technology Equipment Industry Development Center of the People's Republic of China issued the “Notice on the Filing of Automotive Software Online Upgrades”[5]. The notice specifies that automotive manufacturers, vehicles equipped with software update capabilities, and OTA update activities must all be filed with the relevant authorities. It also outlines the content and process for filing, providing clear guidance for the practical operations of relevant companies.

Dne 15. dubna 2022 vydalo Ministerstvo průmyslu a Centrum pro rozvoj průmyslu informačních technologií Čínské lidové republiky „Oznámení o podávání online aktualizací automobilového softwaru“ [5]. Oznámení specifikuje, že výrobci automobilů, vozidla vybavená funkcemi aktualizace softwaru a aktivity OTA aktualizací musí být všechny podány příslušným orgánům. Také popisuje obsah a postup podávání a poskytuje jasné pokyny pro praktické operace příslušných společností.

To regulate the behavior of automotive software update, Ministry of Industry and Information Technology of the People's Republic of China officially issued the mandatory national standard GB 44496-2024 “General Technical Requirements for Software Update of Vehicles”[6] on August 23, 2024. This standard comprises nine core chapters, including scope, terms and definitions, requirements for software update management system, vehicle requirements, and test methods. Chapter 4 of the regulation focuses on the requirements for the software update management system. Chapter 5 emphasizes the technical baseline for automotive software update.

Ministerstvo průmyslu a informačních technologií Čínské lidové republiky dne 23. srpna 2024 oficiálně vydalo závaznou národní normu GB 44496-2024 „Obecné technické

softwaru v automobilovém průmyslu. Tato norma se skládá z devíti základních kapitol, včetně rozsahu působnosti, pojmů a definic, požadavků na systém správy aktualizací softwaru, požadavků na vozidla a zkušebních metod. Kapitola 4 nařízení se zaměřuje na požadavky na systém správy aktualizací softwaru. Kapitola 5 zdůrazňuje technický základ pro aktualizaci softwaru v automobilovém průmyslu.

UN Regulation No. 156 - Software update and software update management system (R156)[7], published in 2021, sets clear software update standards impacting the global automotive industry. The GB 44496-2024 is a localized adaptation of the R156 based on China's national conditions. It adds emergency management processes and requires user confirmation before upgrades. And during the upgrade, the vehicle should not prevent users from unlocking the doors from the inside. Moreover, GB 44496-2024 provides detailed regulations on testing methods in Chapter 6.

Předpis OSN č. 156 – Aktualizace softwaru a systém správy aktualizací softwaru (R156) [7], vydaný v roce 2021, stanoví jasné standardy pro aktualizace softwaru s dopadem na globální automobilový průmysl. Norma GB 44496-2024 je lokalizovanou adaptací normy R156 založenou na národních podmínkách Číny. Přidává procesy pro řešení nouzových situací a vyžaduje potvrzení uživatele před aktualizacemi. Během aktualizace by vozidlo nemělo bránit uživatelům v odemykání dveří zevnitř. Norma GB 44496-2024 navíc v kapitole 6 stanoví podrobné předpisy o zkušebních metodách.

The release of the GB 44496-2024 standard marks a significant step for China in the field of automotive software upgrade management. It provides strong support for technological innovation while ensuring the effective implementation of user safety and regulatory policies. In the face of the stringent standards, vehicle manufacturers must actively respond to ensure the compliance of their software update activities. Therefore, this paper conducts a study on software update and proposes a universal methodology for compliant development.

dání normy GB 44496-2024 představuje pro Čínu významný krok v oblasti správy

bezpečnosti uživatelů a regulačních politik. Vzhledem k přísným standardům musí výrobci vozidel aktivně reagovat, aby zajistili soulad svých aktivit v oblasti aktualizací softwaru s předpisy. Tato práce proto provádí studii aktualizací softwaru a navrhuje univerzální metodologii pro vývoj v souladu s předpisy.

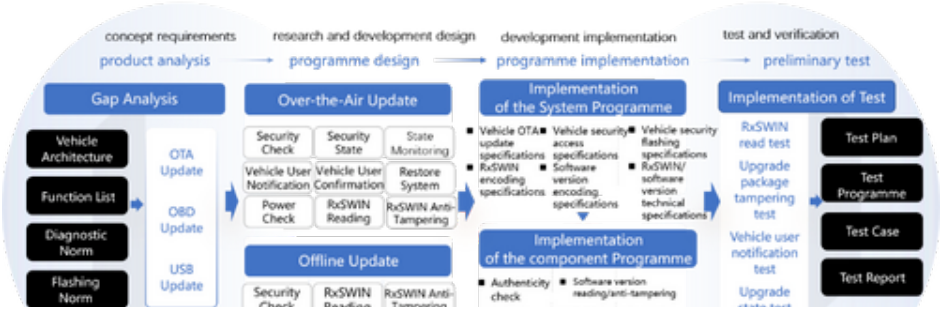
3 Compliant Development and Design of Software Update

3. Vývoj a návrh aktualizací softwaru v souladu s předpisy

The GB 44496-2024 sets clear normative requirements for the entire lifecycle of software update, encompassing the stages before, during, and after the upgrade. As shown in Figure 1, the software upgrade technical compliance development process designed in this paper covers the following key stages: gap analysis, development scheme design, implementation of the scheme, and baseline testing.

Norma GB 44496-2024 stanoví jasné normativní požadavky pro celý životní cyklus aktualizace softwaru, zahrnující fáze před, během a po upgradu. Jak je znázorněno na obrázku 1 , proces vývoje technické shody upgradu softwaru navržený v tomto dokumentu zahrnuje následující klíčové fáze: analýzu mezer, návrh vývojového schématu, implementaci schématu a základní testování.

Figure 1. Obrázek 1.



The software update technical compliance development process.

Proces vývoje technické shody aktualizací softwaru.

3.1 Gap Analysis 3.1 Analýza mezer

Vehicle manufacturers must conduct a comprehensive status investigation and gap analysis for existing vehicle types to comply with GB 44496-2024. Questionnaires and on-site interviews are used to thoroughly analyze the current state and identify non-compliant elements. Based on the survey findings, targeted requirements for corrective actions are developed.

Výrobci vozidel musí provést komplexní šetření stavu a analýzu nedostatků u stávajících typů vozidel, aby splňovaly požadavky normy GB 44496-2024. Dotazníky a pohovory na místě se používají k důkladné analýze současného stavu a identifikaci neshodných prvků. Na základě zjištění z průzkumu se vypracovávají cílené požadavky na nápravná opatření.

Detailed information on software updates, including update steps, security measures, and vehicle architecture, is systematically collected through questionnaires. An on-site analysis and interview meeting is organized to gain deeper insights. The situation is then analyzed and compared with GB 44496-2024 requirements for gap analysis. An analysis report is then compiled, outlining the scope and content of the necessary corrective actions for software update. Based on this, a practical and feasible rectification plan is formulated.

Podrobné informace o aktualizacích softwaru, včetně kroků aktualizace, bezpečnostních opatření a architektury vozidla, jsou systematicky shromažďovány prostřednictvím dotazníků. Pro získání hlubších poznatků je uspořádána schůzka s analýzou a pohovorem na místě. Situace je poté analyzována a porovnána s požadavky normy GB 44496-2024 na analýzu nedostatků. Poté je sestavena analytická zpráva, která

3.2 Development Scheme Design

3.2 Návrh rozvojového schématu

Vehicle software upgrade technology can be divided into two main categories: OTA update and offline update. According to the GB 44496-2024, both update methods must implement protection mechanisms for upgrade packages and standardized management of RXSWIN/ software version numbers.

Technologii aktualizace softwaru vozidel lze rozdělit do dvou hlavních kategorií: aktualizace OTA a offline aktualizace. Podle normy GB 44496-2024 musí obě metody aktualizace implementovat ochranné mechanismy pro aktualizační balíčky a standardizovanou správu čísel verzí RXSWIN/softwaru.

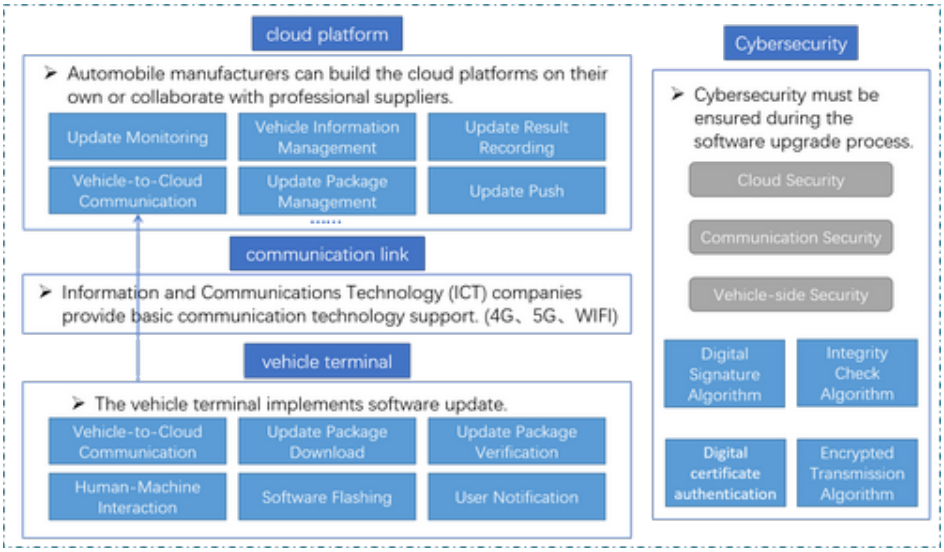
3.2.1 OTA Update. 3.2.1 Aktualizace online (OTA).

The OTA update system follows a “Cloud-Network-Terminal” architecture, which encompasses three core components: the cloud platform, communication link, and vehicle terminal,[8] as shown in Figure 2. Automobile manufacturers can choose to build the cloud platforms on their own or collaborate with professional suppliers to establish them. Additionally, automobile manufacturers need to design the update logic for vehicle terminals to ensure a smooth and efficient update. It is important to note that strict security measures must be implemented throughout the entire update process to ensure comprehensive cybersecurity.

Systém aktualizací OTA se řídí architekturou „Cloud-Network-Terminal“, která zahrnuje základní komponenty: cloudovou platformu, komunikační spojení a terminál vozidla, [8] jak je znázorněno na obrázku 2. Výrobci automobilů se mohou rozhodnout, zda si

profesionálními dodavateli. Výrobci automobilů musí navíc navrhnout logiku aktualizace terminálů vozidel, aby byla zajištěna hladká a efektivní aktualizace. Je důležité si uvědomit, že v celém procesu aktualizace musí být zavedena přísná bezpečnostní opatření, aby byla zajištěna komplexní kybernetická bezpečnost.

Figure 2. Obrázek 2.



The architecture of “Cloud-Network-Terminal”.

Architektura „Cloud-Network-Terminal“.

During the OTA update, the cloud platform is responsible for tasks such as OTA update package management and upgrade push. The in-vehicle controllers are divided into update master nodes and slave nodes. The OTA master is responsible for downloading the update package from the cloud platform and flashing it to the target ECUs. The slave nodes, which are the target ECUs for the update, receive the update packages from the OTA master and complete their own software update[9].

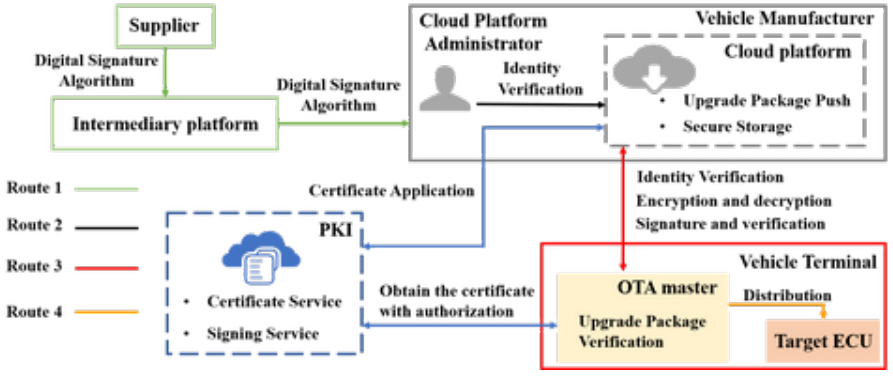
Během aktualizace OTA je cloudová platforma zodpovědná za úkoly, jako je správa balíčků aktualizací OTA a odesílání upgradu. Řídicí jednotky ve vozidle jsou rozděleny na hlavní uzly aktualizací a podřízené uzly. Hlavní uzl OTA je zodpovědný za stahování

aktualizaci, přijímají aktualizační balíčky z hlavního uzlu OTA a provedou vlastní aktualizaci softwaru [9].

During OTA updates, the OTA master verifies update package authenticity and integrity. The OTA cloud platform signs and encrypts the package. The vehicle decrypts and verifies the signature. The protection scheme for the update package during the update process is illustrated in Figure 3. The update flow involves: supplier to vehicle manufacturer (Route 1), manufacturer uploading to cloud platform (Route 2), cloud platform pushing to vehicle, and OTA master receiving the update package (Route 3), and master node distributing to target ECU for upgrade (Route 4).

Během aktualizací OTA ověřuje hlavní uzel OTA pravost a integritu aktualizačního balíčku. Cloudová platforma OTA balíček podepíše a zašifruje. Vozidlo dešifruje a ověří podpis. Schéma ochrany aktualizačního balíčku během procesu aktualizace je znázorněno na obrázku 3. Tok aktualizace zahrnuje: od dodavatele k výrobci vozidla (Trasa 1), odeslání balíčku výrobcem na cloudovou platformu (Trasa 2), odeslání balíčku cloudovou platformou do vozidla a příjem aktualizačního balíčku hlavním uzlem OTA (Trasa 3) a distribuci aktualizace hlavním uzlem do cílové řídicí jednotky ECU (Trasa 4).

Figure 3. Obrázek 3.



chnical solution for update package protection.

After the supplier completes development, it signs the upgrade package and transmits it to an intermediary platform. The vehicle manufacturer verifies the signature of the received upgrade package to ensure its authenticity and integrity. The manufacturer designates cloud platform administrators to upload the upgrade package to the cloud platform, with identity verification to prevent unauthorized access. Additionally, to ensure the storage security of the cloud platform, access control is implemented using the principle of least privilege. For important data, the platform employs encrypted storage, using symmetric encryption algorithms such as AES-256 to encrypt it, while securely storing the corresponding keys.

Poté, co dodavatel dokončí vývoj, podepíše balíček aktualizace a odešle jej na zprostředkující platformu. Výrobce vozidla ověří podpis přijatého balíčku aktualizace, aby zajistil jeho pravost a integritu. Výrobce určí administrátory cloudové platformy, kteří nahrají balíček aktualizace do cloudové platformy, a ověří identitu, aby se zabránilo neoprávněnému přístupu. Pro zajištění bezpečnosti úložiště cloudové platformy je navíc implementováno řízení přístupu na základě principu nejnižších oprávnění. Pro důležitá data platforma využívá šifrované úložiště s využitím symetrických šifrovacích algoritmů, jako je AES-256, a zároveň bezpečně ukládá odpovídající klíče.

Before pushing the upgrade package, the cloud platform and the vehicle undergo mutual authentication, such as signature and verification technology. To ensure secure transmission along Route 3, OTA platform calculates the HASH value of the update file using the SHA-256 algorithm [10]. It digitally signs this HASH value using PKI (Public Key Infrastructure) services to generate a signed file. Upon receiving the package, the upgrade master node verifies the validity of this signed file to confirm the reliability of the upgrade package's source and the integrity of its content. In terms of encryption, the OTA platform generates a 256-bit random key, which is used in conjunction with the AES-256 encryption algorithm to encrypt the upgrade package. After receiving the encrypted upgrade package, the master node decrypts it using the previously obtained random key to restore the original, unencrypted upgrade file.

vzájemným ověřováním, například technologií podpisu a ověřování. Pro zajištění bezpečného přenosu po trase 3 vypočítá platforma OTA hodnotu HASH aktualizačního souboru pomocí algoritmu SHA-256 [10]. Tuto hodnotu HASH digitálně podepíše pomocí služeb PKI (Public Key Infrastructure) a vygeneruje podepsaný soubor. Po přijetí balíčku hlavní uzel aktualizace ověří platnost tohoto podepsaného souboru, aby potvrdil spolehlivost zdroje aktualizačního balíčku a integritu jeho obsahu. Z hlediska šifrování platforma OTA generuje 256bitový náhodný klíč, který se používá ve spojení s šifrovacím algoritmem AES-256 k zašifrování aktualizačního balíčku. Po přijetí zašifrovaného aktualizačního balíčku jej hlavní uzel dešifruje pomocí dříve získaného náhodného klíče a obnoví původní nešifrovaný aktualizační soubor.

Once the OTA master node completes the verification of the upgrade package, it distributes the package to the target ECU for upgrade. The ECU, based on its hardware and software architecture, performs a secondary verification using digital signatures or Hash-based Message Authentication Codes (HMAC). If the verification is successful, the ECU proceeds with the upgrade installation. In industry practice, this step may be executed or omitted depending on the vehicle's actual architecture.

Jakmile hlavní uzel OTA dokončí ověření upgradovacího balíčku, distribuuje jej do cílové řídicí jednotky ECU k upgradu. Řídicí jednotka ECU na základě své hardwarové a softwarové architektury provede sekundární ověření pomocí digitálních podpisů nebo kódů ověřování zpráv založených na hashování (HMAC). Pokud je ověření úspěšné, řídicí jednotka ECU pokračuje v instalaci upgradu. V průmyslové praxi může být tento krok proveden nebo vynechán v závislosti na skutečné architektuře vozidla.

For the upgrade slave nodes, measures are taken to ensure that the RXSWIN/software versions are updatable, readable, and tamper-proof. Specifically, the RXSWIN/software versions stored on the vehicle side should be readable through standard interfaces (such as the OBD interface) and should be updated after the update. Additionally, measures such as encrypted storage and secure access are implemented to ensure that the RXSWIN/

U upgradovaných podřízených uzlů jsou přijata opatření k zajištění aktualizovatelnosti, čitelnosti a ochrany proti neoprávněné manipulaci s verzemi RXSWIN/softwaru. Konkrétně by verze RXSWIN/softwaru uložené ve vozidle měly být čitelné prostřednictvím standardních rozhraní (například rozhraní OBD) a měly by být po aktualizaci aktualizovány. Dále jsou implementována opatření, jako je šifrované úložiště a zabezpečený přístup, aby se zajistilo, že verze RXSWIN/softwaru uložené ve vozidle nebudou neoprávněně pozměněny.

In practical operations, abnormal situations may arise during update. To ensure vehicle safety, GB 44496-2024 requires restoring the software version to a previous one or placing it in a safe state if an upgrade fails. This is achieved using the A/B partitioning method. Separate storage areas are allocated for the current running version of the software and the target version to be upgraded. While the system in Partition A is operating normally and providing services, the software refresh operation is carried out on Partition B. Once the software in Partition B is successfully flashed and passes a rigorous verification process, the system will automatically load the new version of the software from Partition B during the next restart. If an error occurs during the software flashing process in Partition B, the system will automatically roll back to Partition A and continue to boot and operate with the original system in Partition A. This design enhances upgrade reliability, shortens rollback time, and minimizes the impact of upgrade failure on vehicle operation[9].

V praktickém provozu mohou během aktualizace nastat abnormální situace. Pro zajištění bezpečnosti vozidla vyžaduje norma GB 44496-2024 obnovení verze softwaru na předchozí verzi nebo jeho uvedení do bezpečného stavu, pokud se upgrade nezdaří. Toho se dosahuje metodou dělení A/B. Pro aktuální verzi softwaru a cílovou verzi, která má být upgradována, jsou přiděleny samostatné úložné oblasti. Zatímco systém v oddílu A funguje normálně a poskytuje služby, operace aktualizace softwaru se provádí v oddílu B. Jakmile je software v oddílu B úspěšně nainstalován a projde přísným ověřovacím procesem, systém při dalším restartu automaticky načte novou verzi softwaru z oddílu B. Pokud během procesu blikání softwaru v oddílu B dojde k chybě, systém se automaticky vrátí do oddílu A a bude pokračovat v bootování a provozu s

Establish a safety state model for vehicle software upgrade to clearly defining the preconditions for the upgrade. Meanwhile, it must be ensured that the current battery level of the vehicle is sufficient to support the entire upgrade process or to enable a recovery to the safe state in case of an upgrade failure. Before the update, conduct a check of the status of the vehicle. The update should only proceed if all preconditions are met.

Vytvořte model bezpečnostního stavu pro aktualizaci softwaru vozidla, který jasně definuje předpoklady pro aktualizaci. Současně je nutné zajistit, aby aktuální úroveň nabití baterie vozidla byla dostatečná k podpoře celého procesu aktualizace nebo k umožnění obnovení do bezpečného stavu v případě selhání aktualizace. Před aktualizací zkontrolujte stav vozidla. Aktualizace by měla proběhnout pouze tehdy, jsou-li splněny všechny předpoklady.

To ensure user safety, it is allowed to unlock the vehicle doors from the inside during the update. Furthermore, when there are potential risks that may affect driving safety, the vehicle is configured so that it cannot be driven during the execution of the update. Additionally, to prevent unexpected situations during the upgrade, controllers related to vehicle safety, such as those for door locks associated with property security and parking controllers related to functional safety, should remain functional.

Pro zajištění bezpečnosti uživatelů je během aktualizace povoleno odemykat dveře vozidla zevnitř. Kromě toho, pokud existují potenciální rizika, která mohou ovlivnit bezpečnost jízdy, je vozidlo nakonfigurováno tak, aby s ním nebylo možné během provádění aktualizace pojízdně jezdit. Aby se předešlo neočekávaným situacím během aktualizace, měly by navíc zůstat funkční řídicí jednotky související s bezpečností vozidel, jako jsou například zámky dveří související se zabezpečením majetku a parkovací řídicí jednotky související s funkční bezpečností.

e a software update user notification and inform the user through the human-machine

the vehicle should be in before the upgrade (e.g., the vehicle should be in “Park” mode) and so on. If the current state of the vehicle does not meet the upgrade conditions, guide the user to make the necessary adjustments until all conditions are met. In addition, the user must select either “Agree” or “Reject” the upgrade before it can proceed. After the update, inform the user about the results of the update and explain the functional changes brought by this update. If the update fails, guide the user to attempt the update again, with a limit on the number of reattempts. If the update is still unsuccessful after the allowed number of attempts, advise the user to contact the vehicle manufacturer's after-sales department for technical support.

3.2.2 Offline Update.

Offline update is refined into OBD and USB approaches. In OBD update, the diagnostic tool verifies the authenticity and integrity of the package, while update ECU ensures reading, updating, and tamper-proofing of RXSWIN/software version. USB update covers two cases: updating the in-vehicle infotainment system (IVI), where the IVI verifies the package and handles the RXSWIN/software version, and updates extending to other ECUs, where the IVI acts as the master node for verification, while the ECUs handle the management of RXSWIN/software version.

3.3 Development Scheme Implementation and Testing

After finalizing the technical development scheme, create a detailed functional design specification document and hand it to the technical team or external suppliers for implementation. Once development is complete, conduct comprehensive preliminary testing of update functionalities to ensure stability and compliance with technical standards. According to GB 44496-2024, prepare a test item example checklist, as shown in Table 1, and issue a professional, detailed test report.

Table 1.

Authenticity and integrity test of update package	Tampering with the upgrade package to verify if it can still upgrade normally.	Damage the update package, the update cannot be performed
RXSWIN tamper test	RXSWIN should be protected from unauthorized modification.	Use an unauthorized diagnostic device to OBD but cannot rewritten the RXSWIN.
Failure Protection Test	Interrupt the upgrade process and observe whether the vehicle can roll back to the previous available version or be placed in a safe state.	When the update is failed, the vehicle can restore the system to the previous version
Electricity Guarantee Test	Upgrade without meeting the set battery status to verify if the upgrade can proceed.	Under the condition that other prerequisites are satisfied, the vehicle is in the state of not satisfying the power guarantee, and the online upgrade is failed.
User Notification and Confirmation Testing	Record the content of user notifications and verify whether necessary notifications and confirmations have been made.	The vehicle can inform the relevant information and obtain confirmation from the user.
Upgrade Condition Confirmation Test	Upgrade without meeting the set preconditions (including battery status) to verify if the upgrade can proceed.	The upgrade cannot proceed if any of the preconditions are not met.
Door Anti-Lock Test	During the upgrade, attempt to open the door from inside to verify if it can be opened.	During the upgrade, the door can be unlocked from the inside of the vehicle.
Vehicle Safety Test	Carry out corresponding tests according to the list of online upgrade items that may affect vehicle safety, check and record the results of online upgrade and vehicle status of the vehicle.	Park the vehicle on a ramp and perform an online upgrade of electronic parking brake. The vehicle can successfully update and does not slip away.
Driving safety test	During the online upgrade execution. (a) Try to put the vehicle in driving condition, check and record the results of the online upgrade of the vehicle and the	(1) Unable to drive the vehicle while upgrading. (2) Start the upgrade when the upgrade conditions are met, and try to shift the vehicle during the upgrade

	successful execution of the online upgrade or affect the safety of the vehicle, and check and record the online upgrade results and the corresponding vehicle function status.	

Test item example checklist

4 Conclusions

This paper provides an interpretation and analysis of GB 44496-2024 “General Technical Requirements for Software Update of Vehicles” and conducts an in-depth study of compliant automotive software update development.

This paper focuses on how to design and implement update that meet the security and stability requirements according to the standard, and proposes a software update technical development solution and a protection scheme for software update packages to ensure the smooth progress of the update.

In summary, this research provides strong support and valuable reference for the compliant development of automotive software update.

Acknowledgments

This work was financially supported by the National Key Research and Development Program of China (Grant Nos. 2023YFB3107400, 2023YFB3107405).

References

[1] Wang D X, Tang L S, Chen B. 2018. Research on the OTA Function Design of Intelligent Connected Vehicle. Automotive Technology, 517(10): 33-37.

Go to Citation | Google Scholar

[2] Khurram M., Kumar H., Chandak A., et al. 2016. Enhancing Connected Car Adoption: Security and

ICAICE

[3] Kim K., Kim, J. S., Jeong S., et al. 2021. Cybersecurity for Autonomous Vehicles: Review of Attacks

Show all references

Index Terms

Research on Compliant Development of Vehicle Software Update Based on GB 44496-2024

Security and privacy

Formal methods and theory of security

Security requirements

Recommendations

Component-Based Software Update Process in Collaborative Software Development

APSEC '08: Proceedings of the 2008 15th Asia-Pacific Software Engineering Conference

Component-based software engineering (CBSE) has emerged as a key technology for developing and maintaining large scaled software systems in an outsourcing environment. These software components tend to be developed…

Read More

SS standard compliant agile software development: an industrial case study

ICAICE

long tradition of developing standards that strictly sets quality goals and prescribes engineering processes and…

Read More

Research on Intelligent Vehicle Platoon Driving Experiment System Based on Wireless Communication

APCIP '09: Proceedings of the 2009 Asia-Pacific Conference on Information Processing - Volume 02

Intelligent vehicle platoon driving is a process of the flexible formation based on the coordination between vehicle and infrastructure in the intelligent vehicle-infrastructure system, which can increase the density of road traffic, simplify t…

Read More

Comments

DL Comment Policy

Comments should be relevant to the contents of this article, (sign in required).

Got it

0 Comments

Share

Best Newest Oldest

Nothing in this discussion yet.

Privacy Do Not Sell My Data

View full text | Download PDF

View Table of Contents

ICAICE