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

Research on Methods for Developing Software Identification Codes in Automotive Software Update Management Regulations

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

CATARC Automotive Test Center (Tianjin) Co., Ltd Tianjin, China
[a] yangnirunze@catarc.ac.cn, [b] wangmanna@catarc.ac.cn, [c] zhuyongjian@catarc.ac.cn

Abstract: As vehicles become increasingly digitized and intelligent, with growing demands for functional iterations, software updates (OTA) are becoming more frequent. National regulatory agencies have taken corresponding measures to address the risks associated with automotive software updates. To enhance the automotive industry's standards and maintaina healthy industry ecosystem, it is urgent to establish requirements for managing software identification codes and tracking software changes. Current software update management documents, primarily the UN R156 regulation and the forthcoming GB "General Technical Requirements for Automotive Software Updates," specify requirements for software identification codes. Based on the UN R156 regulation and research on existing automotive code systems in China, we propose ideas and methods for developing software identification codes.

Keywords: Software Identification Codes; Over-The-Air (OTA); UN R156; Standard Regulation GB.

1. Introduction

With the in-depth development of automotive electronics, there are more and more on-board ECUs (Electronic Control units) that support software updates. Originally designed to address software vulnerabilities in ECUs, software updates are now also used to improve user experience and reduce after-sales and maintenance costs. However, while any innovative technology has a profound impact on the quality of life of the public, it also comes with certain potential threats. Defective software updates, whether management errors or technical vulnerabilities, have the potential to affect the safety of vehicle users and even road participants.

The R156 Regulation, the Regulation on the Approval of Software updates for Vehicles and Uniform Regulations for Software update Management Systems, was published by the Working Group on Autonomous Vehicles of the United Nations World Vehicle Regulation Coordination Forum on February 5, 2021. The EU officially implemented this regulation in July 2022, and requires all new models to comply with it from that point on (that is, all applicable models exported to the EU must pass the relevant certification). The regulation focuses on the automotive software update function and puts forward a series of specific requirements to ensure the safety, controllability and compliance of the software update process, so as to comply with the intelligent and connected development trend of the automotive industry and further protect the rights and interests of consumers.

The software update regulations mainly put forward specific requirements for software update from the process system and technical requirements. SUMS are required to establish a Software Update Management System (SUMS), which consists of software update evaluation process, software update document management and secure software update process. SUMS requirements for the management of Software Identification numbers (RX Software Identification Numbers, hereinafter referred to as "RXSWIN") will be one of the key elements of the software update regulatory requirements. RXSWIN records the software version information of the system corresponding to a regulation, including the software version, software update point, and software update impact. Rxswin must be associated with the software version of the component of the system related to the regulation. Technical requirements cover general software update requirements and Over-the-Air (over-the-air) additional requirements. In the general requirements of software update, the authenticity and integrity of software update are required, and the update and access control of RXSWIN are required. The OTA additional requirements are mainly based on security and application scenarios, and put forward corresponding requirements, such as the need for a safe software rollback or abnormal processing state, the need to update without affecting driving safety, and the need to notify users of the content and results of the update.[1]

2. R156 Main Provisions and Requirements

2.1. Software Update Management System (SUMS)

The UN R156 regulation requires automobile manufacturers and suppliers to establish a sound software update management system to ensure the safe and reliable update of vehicle software. This system not only involves the process and strategy of software update, but also includes the verification before the update, the monitoring during the update and the verification after the update.

The vehicle manufacturer shall record and store all information related to the software update, including system configuration, software version, vehicle or system parameters before and after the update. This information needs to be auditable in order to track and verify compliance with software updates. Before making a software update, the automaker needs to conduct a thorough evaluation of the update, including the purpose of the update, the scope of

impact, and compatibility with the vehicle configuration. This helps ensure that the update does not introduce new safety risks or affect the proper operation of the vehicle. During the software update process, automakers need to have a set process to ensure that the vehicle's information is secure against unauthorized access and tampering. This includes encrypting and validating data during the update process to ensure data integrity and authenticity. Before implementing the first software update on a vehicle, an automaker should ensure that its software update process and model-specific software update management system are approved.

SUMS specifies the update process (Figure 1) and the following three areas.[3]

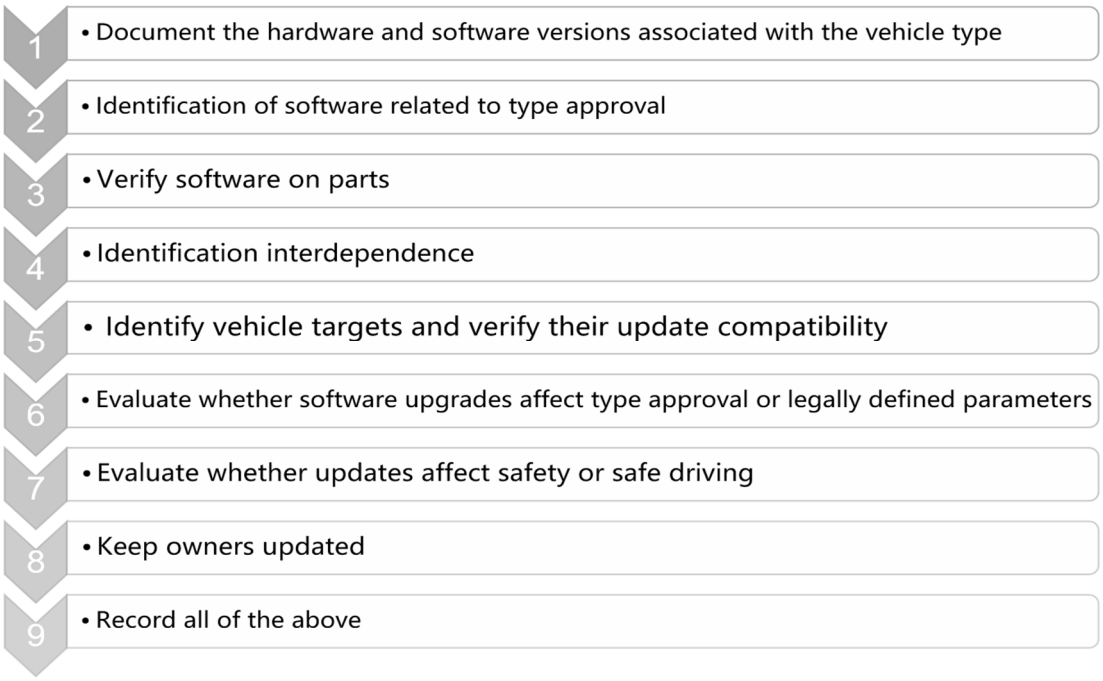

Figure 1. Software update process of WP.29/R156

(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 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.

2.2. Vehicle type approval (VTA)

The technical requirements for vehicle types in the R156 regulation can be divided into two main parts: software update requirements and online update (OTA) additional requirements.

(1) Software update requirements

Authenticity Integrity protection: The authenticity and integrity of software updates should be protected to reasonably prevent their damage and to reasonably prevent ineffective updates. This means that during the update process, it is necessary to ensure that the transmitted data has not been tampered with or corrupted.

Update and read of System Software Identification Information (RXSWIN): Each RXSWIN should be uniquely identifiable. When a vehicle manufacturer modifies the type approval related software, RXSWIN should be updated if it results in an extension or a new type approval. Each RXSWIN shall be easy to read in a standardized manner by using an electronic communication interface, at least through a standard interface (OBD port). The vehicle manufacturer shall protect the RXSWIN and/or software versions on the vehicle from unauthorized modifications. At the time of type approval, the vehicle manufacturer shall provide confidential information on the methods used to prevent unauthorized modification of the vehicle's RXSWIN and/or software

version.

(2) OTA additional requirements

update failure Handling: Vehicle manufacturers should ensure that in the event of an update failure or interruption, the vehicle is able to restore the system to a previous version; Or after an update fails or is interrupted, the vehicle can be placed in a safe state.

Power Assurance: Vehicle manufacturers should ensure that software updates are performed only when the vehicle has sufficient power to complete the update process (including updates that may be required to revert to a previous version or where the vehicle is in a safe condition).

update affects vehicle safety: When the execution of an update could affect the safety of a vehicle, the vehicle manufacturer should demonstrate how the update can be performed safely. This should be achieved through technical means that ensure the vehicle is in a state where it can safely perform the update.

The vehicle manufacturer shall demonstrate that the vehicle user can be informed prior to the execution of the update, including:

(a) Purpose of the update. Including how critical the update is and whether the update is used for recall, safety and other purposes;

(b) any changes achieved by upgrading vehicle features;

(c) The expected time to complete the implementation of the update;

(d) any vehicle functions that may not be available during the execution of the update; (e) any instructions that may assist the vehicle user in carrying out the update safely;

In cases where it may be unsafe to perform an update while driving, the vehicle manufacturer shall demonstrate that:

(a) Ensure that the vehicle cannot be driven while the update is being carried out;

(b) Ensure that the driver cannot use any function that affects the safety of the vehicle or the successful execution of the update

After performing the update, the vehicle manufacturer shall:

(a) The user of the vehicle can be informed of the success or failure of the update;

(b) The user of the vehicle can be informed of the updates implemented and, if applicable, of any relevant updates to the user manual.

Prerequisites: The vehicle shall ensure that the prerequisites must be met before performing the software update, such as the vehicle is not parked, the battery voltage is low, the OBD port is connected to the device, and the door is not closed if any of the conditions are not met. [4]

The software update regulations pay special attention to the management and security requirements of RXSWIN. Since RXSWIN contains software version information and software integrity check data, the regulations stipulate that when the RXSWIN software update affects the type approval related to vehicle access, the RXSWIN of relevant parts shall be updated in a timely manner, and the RXSWIN can be accessed and modified only after authorization is required. To sum up, requirements for RXSWIN are put forward in the software update management system and vehicle type certification, that is, the preparation of RXSWIN should not only facilitate management but also ensure safety.[5]

3. Research on Code Rules of Automobile Code at Home and Abroad

3.1. RXSWIN

SUMS put forward requirements for RXSWIN in 7.1.1 Evaluating the Software update Process and 7.1.2 Keeping the update information for records:

Evaluate the software update process:

(1) Establish a process for accessing and updating RXSWIN information before and after software update, which should include the process and ability to update the corresponding software version information at the same time and verify the integrity and correctness of the information;

(2) The ability to verify that the software version of the type approved part on the vehicle is consistent with the information recorded by RXSWIN.

Update information: Record the version information and integrity verification data of RXSWIN and all related software before and after the update.

For RXSWIN, VTA proposed in 7.2.1 Software update requirements:

(1) Unique identification, type approval changes need to be updated simultaneously;

(2) The RXSWIN stored at the end of the car should be at least readable through a standard interface (such as OBD);

(3) If the RXSWIN is not stored at the end of the vehicle, the relationship between the software version of the vehicle or individual ECU and the type certification should be declared, and the software version information should be read at least through a standard interface (such as OBD) when the software is updated;

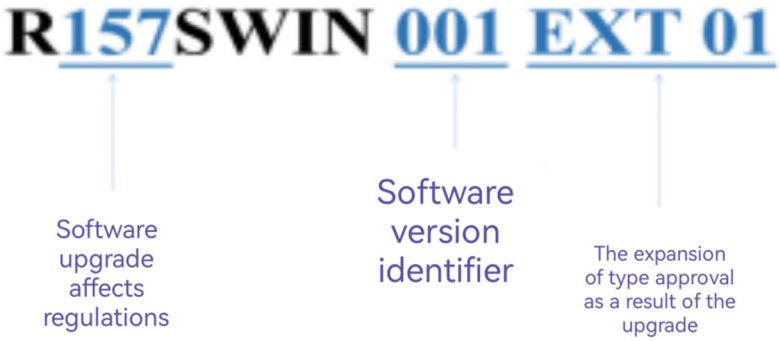

Figure 2. Type approval extension

(4) Protect RXSWIN from unauthorized modifications, and provide preventive methods in confidence during type approval.

RXSWIN contains the relevant regulatory identifier RX applicable to the electronic component to be updated and the software version SWIN YYYY installed on the electronic

component. The version number will only be updated if the update will affect the type approval. To illustrate this feature, here are two examples:

In accordance with the amendment to UNECE R157 [6], the software update changed the speed limit of the automatic lane-keeping assistance system ALKS from 60 km/h to 130 km/h. This update requires an extension of the type approval of the vehicle, so the RXSWIN will appear in this form: R157SWIN 001 EXT 01. RXSWIN remains unchanged, but has been extended, numbering as shown in Fig 2.

Another case is the update of the steering regulation UN R79[7] to add steering assistance, Tesla's autopilot mode, and Volkswagen's driving mode. As this is a new feature, this feature will change the type approval results of the vehicle. Therefore, the complete verification process of the software update should be re-executed, resulting in a new RXSWIN, as shown below:

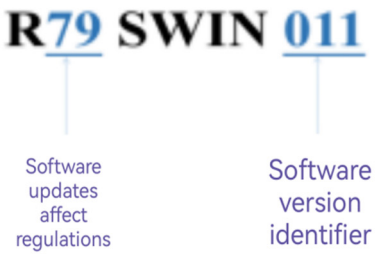

Figure 3. Type approval update

3.2. Domestic Automobile Related Code Situation

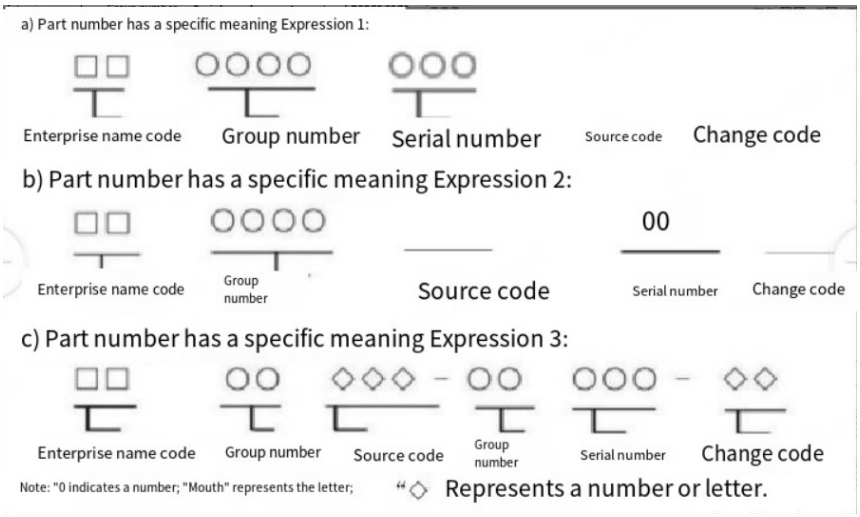

Figure 4. Expressions with a specific meaning

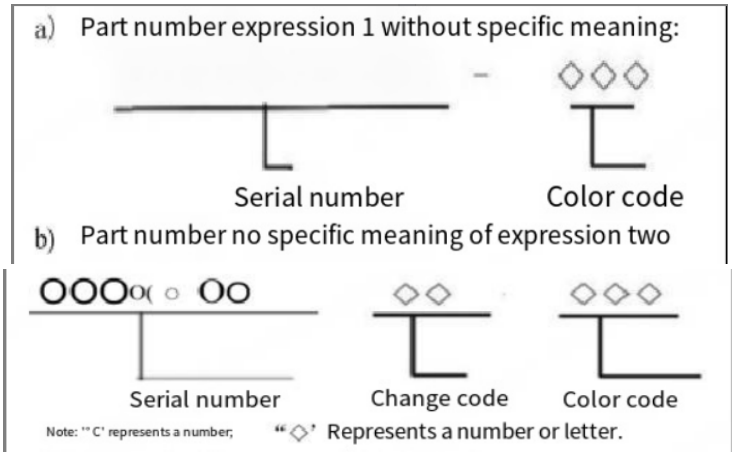

Figure 5. Expression with no specific meaning

On July 18, 2023, the National Standardization Management Committee of the Ministry of Industry and Information Technology issued the "National Vehicle Networking Industry Standard System Construction Guide (Intelligent Connected Vehicle) (2023 version)" has included the "automotive software identification code" into one of the key research directions of intelligent connected vehicle standards. At present, there are mainly EU UN R156 regulations and the forthcoming GB "General Technical Requirements for Automotive Software update" two

standards on the software identification code requirements, GB on the basis of R156 requirements for a more detailed interpretation, the overall requirements of the two are basically the same, but the software identification code preparation rules have not made specific provisions.

According to QC/T 265-2023 "Auto parts numbering Rules", auto parts numbering rules are divided into expressions with specific meaning bits and expressions without specific meaning, from the current market situation, the coding rules of the automotive industry related code can basically be classified according to these two ways.[8]

Examples of this are given below:

HJ 1350-2024 "Technical Specification for Disclosure of Motor Vehicle Environmental Protection Information" Information disclosure number coding rules: Information disclosure number consists of 29 digits, Spaces and letters, coding rules are shown in Figure 6. The first and second digits are "CN"; The 3rd, 6th, 9th, 12th and 23rd digits are space symbols; The fourth and fifth digits are motor vehicles and engines, and the corresponding codes for motor vehicles and engines are shown in Table 1; The 7th and 8th positions are the pollution emission stage of vehicles, the position code of parallel import pilot enterprise vehicles is "PX", and the position code of pure electric vehicles and fuel cell electric vehicles is "00"; The 10th and 11th bits are the noise emission stage, and the engine's position code is "00"; Digits 13-16 are the code automatically generated by the vehicle environmental information disclosure platform when the enterprise registers an account; The number 17-22 is the serial number of the vehicle/model of the enterprise information disclosure; Numbers 24-29 are the car/model configuration serial number.[9]

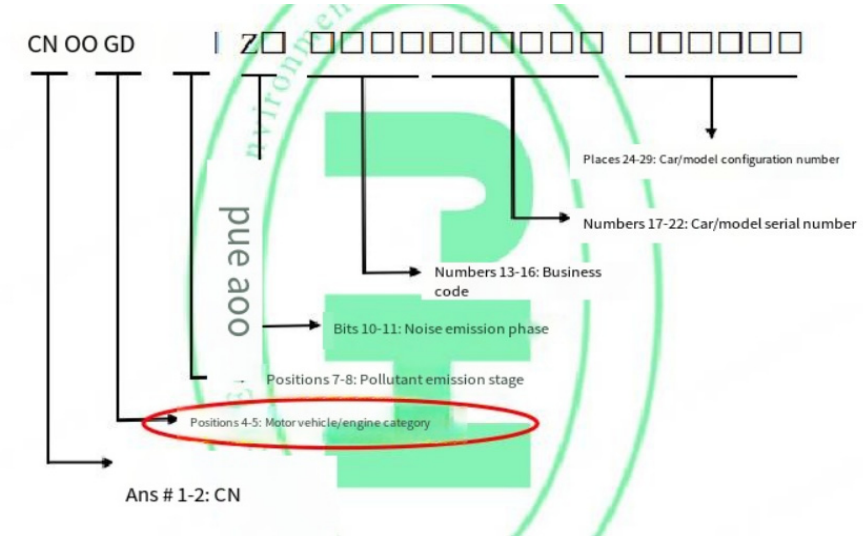

Figure 6. Information disclosure number coding rules

Table 1. Code table of motor vehicle and engine categories

serial number	Car (machine) class	code
1	Light petrol vehicle	QQ
2	Light gasoline hybrid	QH
3	Light diesel vehicle	QC
4	Light diesel hybrid	QZ
5	Light gas vehicle	QR
6	Light gas hybrid	QG
7	Light dual-fuel vehicle	QL
8	Light methanol single fuel vehicle	QB
9	Light methanol hybrid electric vehicle	QX
10	Light diesel/methanol dual fuel vehicle	QS
11	Heavy-duty diesel vehicles	ZC
12	Heavy-duty diesel hybrid	ZH
13	Heavy-duty gas vehicle	ZR
14	Heavy-duty gas hybrid	ZG
15	Heavy duty dual fuel vehicle	ZS
16	Heavy duty methanol single fuel vehicle	ZJ
17	Heavy duty methanol single fuel vehicle	ZM
18	Heavy-duty diesel/methanol dual fuel vehicles	ZB
19	Heavy duty gasoline vehicle	ZQ
20	Three-wheeled car	TC
21	Pure electric vehicle	QD
22	Fuel cell electric vehicles	RD
23	motorcycle	MT
24	moped	QM
25	Heavy-duty diesel engine	CJ
26	Heavy duty gasoline engine	QJ
27	Heavy-duty gas engine	RJ
28	Heavy duty dual fuel engine	SJ
29	Engines for three-wheeled cars	TJ
30	Heavy-duty methanol mono-fuel engine	JJ
31	Heavy duty diesel/methanol dual fuel engine	BJ

GB 9417-1988 "Automobile Product Model preparation Rules":

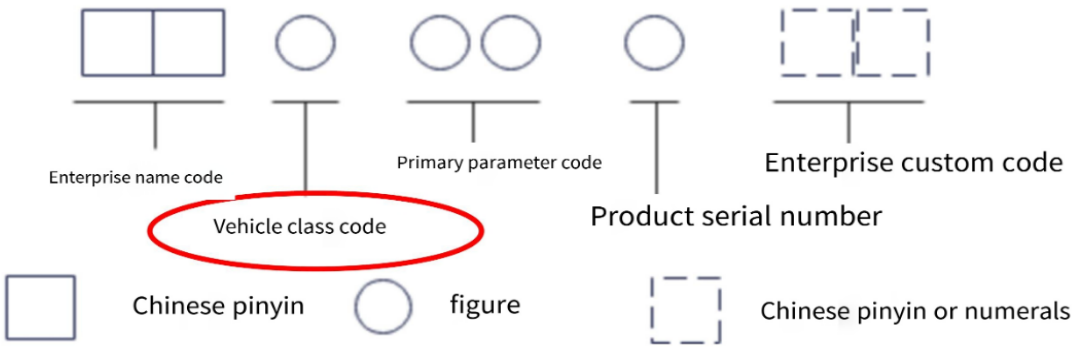

Figure 7. Rules for model preparation of automotive products

Vehicle Class Code:
1 truck; 2 Off-road vehicles; 3 Dump truck;
4 traction car; 5 Special purpose cars; 6 passenger cars;
7 Car; 8 blank; 9 Semi-trailers and special semi-trailers
Main parameter code:
1/2/3/4/5/9 is the total mass of the vehicle;
6 is the length of the vehicle;
7 is the engine displacement. [10]

In order to increase reliability and security, check bits are also added to important codes such as automotive VIN and ICCID that have identity functions.

GB 16735-2019 "Road Vehicle Identification Number (VIN)":

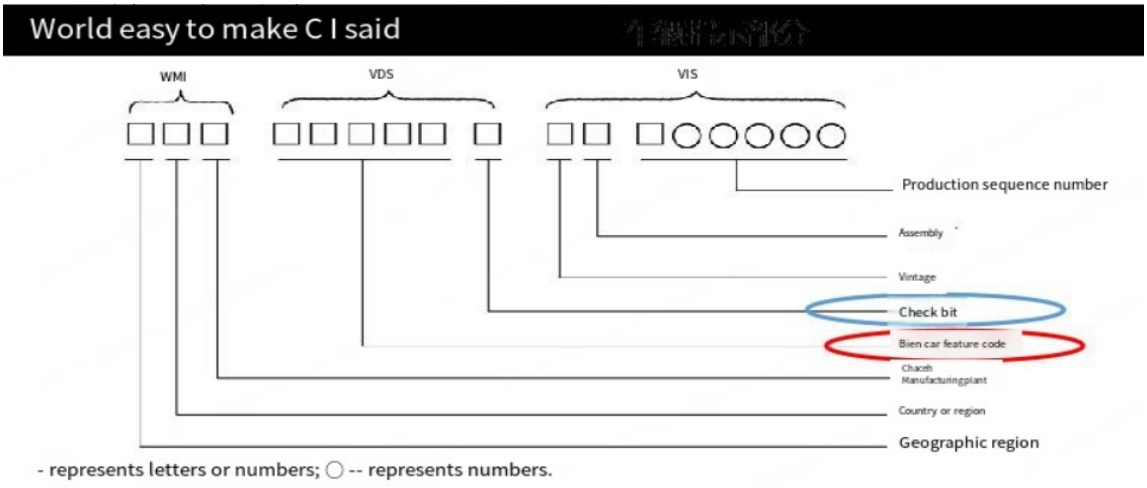

Figure 8. Schematic diagram of vehicle identification code structure of complete and/or incomplete vehicle manufacturers with an annual output of 1000 or more vehicles

Table 2. Description of vehicle characteristics [11]

Type recognition of moving vehicles	vehicle specific power
passenger vehicles	Body type, power system characteristics
coach	Vehicle length, powertrain characteristics
Truck (including tractor, special operation vehicle)	Body type, maximum design total mass of vehicle, powertrain characteristics
trailer	Body type, maximum total design mass of the vehicle
Motorcycles and mopeds	Vehicle type, powertrain characteristics
Incomplete vehicle	Body type, maximum design total mass of vehicle, powertrain characteristics
● For engine-only vehicles including, at a minimum, a description of the fuel type, engine displacement and/or maximum net engine power; For vehicles with other drive types, at least the peak drive motor power should be included (if the vehicle has multiple drive motors, it should be the sum of the peak power of the multiple drive motors; For other drive types of motorcycles a description of drive motor rating, engine displacement and/or maximum net engine power (if any). ● The body types are divided into load-bearing body, cab-chassis, cab-chassis and so on.	

4. Revelation of Compiling Method of Automobile Software Identification Code

At present, car companies that have established software identification codes mainly use two storage and maintenance methods: car storage and non-car storage.

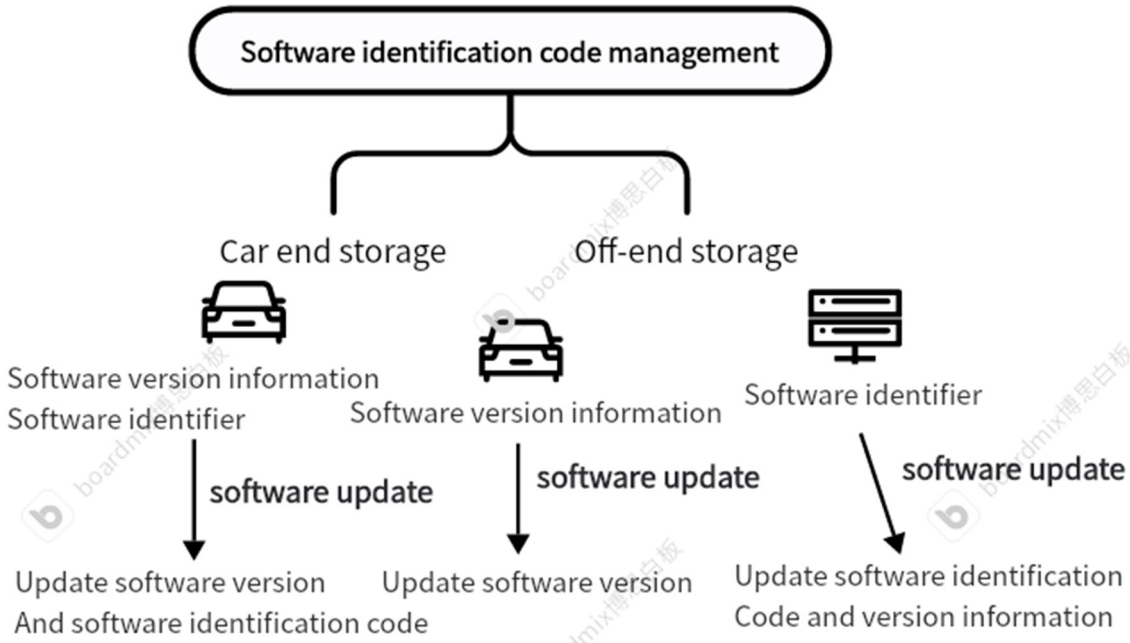

Figure 9. Software identification code management method

According to the background of the software identification code, it is suggested that the software identification code should at least reflect the core information such as regulatory information and vehicle type information, and ensure the uniqueness. Based on the above premise, this paper proposes two software identification code compilation schemes:

Scheme 1: Vehicle code (vehicle announcement number) + regulatory category (number) + age number (age number in VIN rules) + serial number + Custom.

Solution 2: WMI (see Figure 8)+ (internal vehicle model, enterprise custom)+ regulatory category (number)+ age number (age number in VIN rules)+ serial number + custom.

When it comes to the change of software identification code, for a certain regulation of a certain vehicle type, if the type certification needs to be re-performed, the category number field of the regulation should be re-filled; If it is only extended on the basis of the original certified model, and no regulatory changes are involved, only add one to the serial number field.

The above schemes are only part of the suggestions for software identification code compilation. As to whether the rules of software identification code compilation need to be unified in the next step, the application and storage methods of software identification codes still need to be further studied.

References

[1] SHI Qingguo, Shang Haili, Ma Jie et al. OTA update scheme for intelligent Connected vehicles [C]// China Society of Automotive Engineers.2018 Annual Conference Proceedings of China Society of Automotive Engineers. China Machine Press,2018:7.

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

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

[4] Wang Jiangdong, Li Xupeng. R156 software updates to the understanding of the management system and implement Suggestions [J]. Journal of quality and certification, 2022, (7) : 48-50 + 56. DOI: 10.16691 / j. carol carroll nki. 10-1214 / t. 2022. 07.001.

[5] Wang Teng, Liu Chuang, Li Changlong, et al. Construction and implementation of R156 based on RXSWIN remote updating [J/OL]. The abstract, 1-6 [2024-08-14]. https:// doi.org/ 10. 19822/ j.cnki.1671-6329.20220305.

[6] UNITED NATIONS. Software update and software update management system, UN Re-gulation No.157[S/OL]. (2020-06-25) [2022-07-06].

[7] Uniform provisions concerning the approval of vehicles with regard to steering equipment, UN Regulation No. 79.

[8] QC/T 265-2023,Auto parts numbering rules.

[9] HJ 1350-2024,Technical specification for motor vehicle environmental information disclosure.

[10] GB 9417—1988,Rules for model preparation of automobile products.

[11] GB 16735—2019,Road Vehicle Vehicle Identification Number (VIN).