

ICS 43.020
CCS T 40



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB 44496-2024

General technical requirements for software update of vehicles

汽车软件升级通用技术要求

Issued on: August 23, 2024

Implemented on: January 1, 2026

**Issued by: State Administration for Market Regulation;
Standardization Administration of China**

Table of Contents

1	Scope
2	Normative References
3	Terms and Definitions
4	Requirements for Software Update Management System
4.1	General Requirements
4.2	Process Requirements
4.3	Requirements for Documents and Records
4.4	Requirements for Security Assurance
4.5	Additional Requirements for Over-the-air Update
5	Vehicle Requirements
5.1	General Requirements
5.2	Additional Requirements for Over-the-air Update
5.2.10	For
6	Test Methods
6.5	User Notification Test In terms of
6.10	Driving Safety Test In terms of
6.12	Result Notification Test In terms of
7	Same Type Determination
8	Motor Vehicle Product Instruction Manual
9	Implementation of the Standard

Foreword

This document was drafted in accordance with the rules provided in GB/T 1.1-2020 Directives for Standardization - Part

1.Rules for the Structure and Drafting of Standardizing Documents. Please be noted that certain content of this document may involve patents. The institution issuing this document does not undertake the responsibility of identifying these patents. This document was proposed by and shall be under the jurisdiction of Ministry of Industry and Information Technology. General Technical Requirements for Software Update of Vehicles

1 Scope

GB 44496-2024 is the Chinese national standard on general technical requirements for

software update of vehicles, in the field of road vehicles engineering. It carries no /T suffix, which in the Chinese system means compliance is mandatory: a product or a practice within its scope has to meet it to be lawfully made, sold or carried out in China. It was issued on 23 August 2024 by the State Administration for Market Regulation; Standardization Administration of China, and has been in force since 1 January 2026. Classification: ICS 43.020, CCS T 40. This page is published from the official record of the standard held by the Chinese standards administration: the identification, the dates, the classification and the issuing body are taken from there. The clause text, the tables and the numeric limits are in the document itself, which is delivered complete in English translation.

This document specifies the management system requirements and vehicle requirements for software update of vehicles, as well as same type determination and motor vehicle product instructions, and describes the corresponding test methods. This document is applicable to Category-M, Category-N and Category-O vehicles with software update functions.

2 Normative References

The contents of the following documents constitute indispensable clauses of this document through the normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB 44495-2024 Technical Requirements for Vehicle Cybersecurity

3 Terms and Definitions

The terms and definitions defined in GB 44495-2024, and the following are applicable to this document.

3.1 software The part of an electronic control system that consists of digital data and commands.

3.2 software update The process of updating a certain version of software to a new version through an upgrade package (including changing the configuration parameters of the software).

3.3 over-the-air update; OTA update Software update that wirelessly transmits the update package to the vehicle rather than using cables or other local connections.

3.4 software identification number; SWIN A unique identifier defined by the vehicle manufacturer and used to represent software information of a vehicle system related to type approval.

3.5 software update management system; SUMS A systematic method developed to

standardize the processes and procedures for completing software updates in relevant organizations.

3.6 update package A software package used for software updates.

4.1 General Requirements

4.1.1 When producing vehicles with software update functions, the vehicle manufacturer shall have a software update management system.

4.1.2 For each software update, the vehicle manufacturer shall record and securely store the relevant information required in

4.3 for at least 10 years after the production of the vehicle model is suspended.

4.1.3 When a software identification number is available, regardless of whether the software identification number is stored on the vehicle, the vehicle manufacturer shall at least ensure that.

4.1.4 When the software identification number is not available or the software identification number is present but not stored on the vehicle, the vehicle manufacturer shall at least ensure that.

4.2 Process Requirements

4.2.1 There shall be a process that can uniquely identify all initial and updated software version information and related hardware component information in vehicle systems related to type approval or recall. The software version information shall at least include the software version number and the integrity validation data of the corresponding update package.

4.2.2 When a software identification number is available, the following processes shall be in place.

4.2.3 A process shall be in place to identify target vehicles for software update.

4.2.4 A process shall be in place to confirm the compatibility of software update with target vehicle configurations. At a minimum, this process shall include confirming the compatibility with the latest known hardware and software configurations of the target vehicle before releasing a software update.

4.2.5 A process shall be in place to identify the pertinence between the vehicle system being updated and other vehicle systems.

4.2.6 A process shall be in place to evaluate, identify and record whether the software update will affect type approval-related vehicle systems before releasing the software update, and shall at least include whether the software update will affect relevant parameters.

4.2.7 A process shall be in place to evaluate, identify and record whether the software update will add, change or enable any functions that do not exist or are not enabled at the time of type approval, or whether it will change or disable any other parameters or functions defined in the standards and regulations related to type approval before releasing the software update. The evaluation shall at least include.

4.2.8 A process shall be in place to evaluate, identify and record whether the software update will affect any other systems other than

4.2.6 and 4.2.7 (this system may be related to vehicle safety and continuous operation) before releasing the software update, or whether it will add or change the functions at the time of vehicle registration.

4.2.9 A process shall be in place to notify vehicle users of the information of each software update.

4.3 Requirements for Documents and Records

4.3.1 There shall be relevant documents describing the process of software update performed by the vehicle manufacturer and demonstrating compliance with this document.

4.3.2 There shall be a document describing the vehicle system configuration related to type approval. This document shall at least record the software and hardware information of the vehicle system and relevant vehicle or vehicle system parameters.

4.3.3 When software identification numbers are available, each software identification number shall have an auditable record. This record shall include at least.

4.3.4 There shall be a document recording the target vehicle and confirming its configuration and software update compatibility.

4.3.5 There shall be a document describing the information of each software update. The document shall at least record.

4.4 Requirements for Security Assurance

4.4.1 A process shall be in place to protect the update package and reasonably prevent it from being tampered with before execution.

4.4.2 The entire software update process, including the process of releasing software update, shall be protected to reasonably protect it from damage.

4.4.3 A process shall be in place to validate and confirm the functions of the updated software and the rationality of the code.

4.4.4 An emergency management mechanism shall be in place to handle software update emergencies.