ICS 43.020
CCS T 40

National Standard of the People's Republic of China

GB 44495-2024

Technical Requirements for Vehicle Cybersecurity

Published date: 2024-08-23 **Implemented date: 2026-01-01**

Published by **State Administration for Market Regulation**
Standardization Administration of the People's Republic of China

Table of Contents

Foreword

This document was drafted in accordance with the provisions given in GB/T 1.1-2020 Directives for Standardization - Part 1: Rules for the Structure and Drafting of Standardizing Documents.

For the technical content of this document, reference was made to the United Nations Regulation No. 155 (UN R155) Uniform Provisions Concerning the Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuing body of this document shall not be held responsible for identifying any or all such patent rights.

This document was proposed by and is under the centralized management of the Ministry of Industry and Information Technology of the People's Republic of China.

Technical Requirements for Vehicle Cybersecurity

1 Scope

This document specifies the requirements for cybersecurity management system, basic requirements for cybersecurity, technical requirements for cybersecurity and determination of the same type, and describes the corresponding inspection and test methods.

This document is applicable to vehicles of categories M and N, as well as category O if fitted with at least 1 electronic control unit.

2 Normative References

The following normative documents contain provisions which, through reference in this text, constitute indispensable provisions of this document. For dated references, only the dated edition applies to this document. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 40861 General Technical Requirements for Vehicle Cybersecurity

GB/T 44373 Intelligent and Connected Vehicle - Terms and Definitions

GB/T 44464-2024 General Requirements of Vehicle Data

GB 44496 General Technical Requirements for Software Update of Vehicles

3 Terms and Definitions

For the purposes of this document, the following terms and definitions and those given in GB/T 40861, GB/T 44373 and GB 44496 apply.

3.1

vehicle cybersecurity

a state in which the electronic and electrical systems, components and functions of a vehicle are protected to ensure that the assets of the vehicle are not threatened

[Source: GB/T 40861-2021, 3.1]

3.2

cybersecurity management system; CSMS

a systematic, risk-based approach

Note: It includes organizational processes, responsibilities and governance and is used to address risks associated with cyber-threats to vehicles and protect vehicles from cyber-attacks.

[Source: GB/T 44373-2024, 3.11, modified]

3.3

risk

the impact of uncertainty in vehicle cybersecurity

Note: Risk is expressed in terms of attack feasibility and impact.

3.4

risk assessment

the process of finding, identifying and describing a risk to comprehend the nature of risk and to determine the level of risk, and of comparing the results of risk analysis with risk criteria to determine whether the risk is acceptable

3.5

threat

a potential cause of an unwanted incident, which may result in harm to a system, organization or individual

3.6

vulnerability

a weakness in an asset or mitigation measure that may be exploited by one or more threats

3.7

on-board software update system

software and hardware installed on the vehicle side and capable of directly receiving, distributing and checking update packages from outside the vehicle to realize software update

[Source: GB 44496-2024, 3.12]

3.8

over-the-air update

software update by using a wireless means rather than cables or other local connections for transmitting the update package to the vehicle

Note 1: "OTA update" is also referred to as "remote update".

Note 2: "Local connections" generally refer to the physical connections through OBD interface, universal serial bus (USB) interface, etc.

[Source: GB 44496-2024, 3.3]

3.9

offline update

software update other than over-the-air update

[Source: GB 44496-2024, 3.13]

3.10

sensitive personal information

personal information that may lead to discrimination against vehicle owners, drivers, passengers or people outside the vehicle, or seriously endanger people or property once leaked or illegally used

Note: It includes the vehicle's track of whereabouts, audios, videos, images and biometric recognition features.

4 Abbreviations

For the purposes of this document, the following abbreviations apply.

CAN: Controller Area Network

ECU: Electronic Control Unit

HSM: Hardware Security Module

NFC: Near Field Communication

OBD: On-Board Diagnostics

RFID: Radio Frequency Identification

USB: Universal Serial Bus

VLAN: Virtual Local Area Network

VIN: Vehicle Identification Number

V2X: Vehicle to Everything

WLAN: Wireless Local Area Networks

5 Requirements for Cybersecurity Management System

5.1 Vehicle manufacturers shall have a cybersecurity management system for the life cycle of vehicles.

Note: The life cycle of vehicles includes the development stage, production stage and post-production stage of vehicles.

5.2 The cybersecurity management system shall include the following contents.

- Establish an internal process for managing vehicle cybersecurity within the organization.
- Establish processes for identifying, assessing, classifying and handling vehicle cybersecurity risks and for verifying the handling of identified risks, and ensure that the vehicle risk assessment is kept up-to-date.
- Establish a process for testing vehicle cybersecurity.
- Establish a monitoring, response and vulnerability reporting process for cyber-attacks, cyber-threats and vulnerabilities against vehicles, which shall meet the following requirements:
  - A vulnerability management mechanism shall be included, and activities such as the collection, analysis, reporting, handling, release and reporting of vulnerabilities shall be clearly defined;
  - A process for providing relevant data and analyzing cyber-attacks shall be established, such as analyzing and detecting cyber-attacks, threats and vulnerabilities based on vehicle data and vehicle logs;
  - A process for ensuring the continuous monitoring of cyber-attacks, cyber-threats and vulnerabilities shall be established, and vehicles shall be included in the monitoring scope no later than the date of vehicle registration;
  - A process for ensuring that identified cyber-attacks, cyber-threats and vulnerabilities are responded to and handled within a time limit shall be established;
  - A process for assessing the effectiveness of cybersecurity measures implemented in the event of new cyber-attacks, cyber-threats and vulnerabilities shall be established.
- Establish A process for managing the vehicle cybersecurity interdependency between the organization and its contracted suppliers, service providers and other vehicle manufacturer sub-organizations.

6 Basic Requirements for Cybersecurity

6.1 The development process of vehicle products shall follow the requirements for the cybersecurity management system.

6.2 Vehicle manufacturers shall identify and manage the risks related to vehicles and suppliers.

6.3 Vehicle manufacturers shall identify critical elements of vehicles, conduct risk assessment on vehicles and manage the identified risks.

Note 1: The risk assessment shall cover all elements of the vehicle concerned and their interactions, and further consider the interactions between these elements and external systems.

Note 2: Critical elements include but are not limited to those that contribute to vehicle safety, environmental protection or theft prevention, as well as system components that provide connectivity or parts of the vehicle architecture that are critical to cybersecurity.

6.4 Vehicle manufacturers shall take handling measures based on the requirements of Chapter 7 to protect vehicles from being affected by the risks identified in the risk assessment. If the handling measures are not related to the identified risks, the vehicle manufacturer shall explain their irrelevance. If the handling measures are insufficient to address the identified risks, the vehicle manufacturer shall take other measures and explain the rationality of using them.

6.5 In case of any private network environment, the vehicle manufacturer shall take measures to protect the private network environment for storing and executing after-sales software, services, applications or data for the vehicle concerned.

Note: For example, sandbox-specific environment.

6.6 Vehicle manufacturers shall conduct tests to verify the effectiveness of the cybersecurity measures taken.

6.7 Vehicle manufacturers shall take appropriate measures for the vehicle to:

- Identify cyber-attacks against the vehicle;
- Monitor cyber-attacks, cyber-threats and vulnerabilities relevant to the vehicle and obtain data.

6.8 Vehicle manufacturers shall use publicly available, published and valid cryptographic algorithms and select appropriate parameters and options depending on the specific cryptographic algorithm and service scenario.

6.9 Vehicle manufacturers shall meet one of the following cryptographic module requirements:

- Use cryptographic modules that comply with the requirements of international, national or industry standards;
- Justify the use of cryptographic modules in case of failure to use cryptographic modules required by international, national or industry standards.

6.10 Default security settings shall be used for vehicles. For example, the default connection password of WLAN shall meet the complexity requirements.

6.11 The requirements for in-vehicle data processing, default non-collection, accuracy range application, desensitization processing, personal consent and significant notification in vehicle data processing activities shall comply with the requirements of 4.2.2 in GB/T 44464-2024.

7 Technical Requirements for Cybersecurity

7.1 Security requirements for external connections

7.1.1 General security requirements

7.1.1.1 External connection systems, such as systems with remote control function on the vehicle side and authorized third-party applications, shall be free of security vulnerabilities of high level or above that were announced by any authoritative vulnerability platform of the automotive industry 6 months ago and have not been handled yet.

Note 1: Authoritative vulnerability platforms of the automotive industry include the National Vulnerability Database - China Automobile Vulnerability Database (NVDB-CAVD) and other vulnerability platforms recognized by competent government authorities.

Note 2: Handling methods include vulnerability elimination, mitigation measure development and other appropriate actions.

7.1.1.2 The non-service-essential network ports of the vehicle shall be disabled.

7.1.2 Security requirements for remote control

7.1.2.1 The authenticity and integrity of remote control instruction information shall be verified.

7.1.2.2 Access control shall be set for remote control instructions, and unauthorized remote control instructions shall be disabled.

7.1.2.3 A security log function shall be provided to record remote control instructions. The contents recorded in the security logs shall at least include the time, sender, remote control object and operation results of the remote control instructions, and relevant security logs shall be kept for at least 6 months.

7.1.2.4 The integrity of the system with remote control function on the vehicle side shall be verified.

7.1.3 Security requirements for third-party applications

7.1.3.1 The authenticity and integrity of authorized third-party applications shall be verified.

Note: Third-party applications refer to the service applications provided to users by entities other than vehicle manufacturers and their suppliers, including third-party entertainment applications.

7.1.3.2 Prompts shall be provided for the installation of unauthorized third-party applications, and access control shall be implemented for installed unauthorized third-party applications to restrict such applications from directly accessing system resources, personal information, etc.

7.1.4 Security requirements for external interfaces

7.1.4.1 Access control protection shall be implemented for external interfaces of the vehicle to prevent unauthorized access.

Note: External interfaces include USB interface, diagnostic interface and other directly accessible physical interfaces.

7.1.4.2 Access control shall be implemented for files in devices connected via the USB interface and SD card interface of the vehicle, allowing only read/write access to files in specified formats or installation and execution of application software with specified signatures.

7.1.4.3 The vehicle shall address the virus in devices connected to USB ports.

7.1.4.4 For sending write operation instructions for key configuration and calibration parameters through the diagnostic interface to the vehicle, security strategies such as identity authentication or access control shall be adopted.

7.2 Communication security requirements

7.2.1 When the vehicle communicates with the vehicle manufacturer's cloud platform, the authenticity of the identity of the communication object shall be verified.

7.2.2 When the vehicle establishes V2X direct communication with other vehicles, road side units, mobile terminals, etc., the validity and legitimacy of certificates shall be verified.

7.2.3 The vehicle shall use an integrity protection mechanism to protect external wireless communication channels other than RFID and NFC.

7.2.4 The vehicle shall have an access control mechanism for data operation instructions from external communication channels.

Note: Data operation instructions from external communication channels include instructions such as code injection, data manipulation, data overwriting, data wiping, and data writing.

7.2.5 The vehicle shall verify the validity or uniqueness of received external critical instruction data.

Example: For vehicle control instructions sent by the remote control server, the vehicle may use a gateway to verify the validity or uniqueness of such instructions.

Note: Critical instruction data refers to instruction data that may affect driving and property safety, including but not limited to vehicle control instruction data.

7.2.6 The vehicle shall take confidentiality protection measures for sensitive personal information sent outside the vehicle.

7.2.7 The vehicle shall have a security mechanism to defend against physical manipulation attacks, and at least have an identification mechanism for components used for direct wireless communication with the outside.

Note: Components for direct wireless communication with the outside include but are not limited to on-board information interactive systems, excluding short-range wireless sensors.

7.2.8 Components used for direct wireless communication between the vehicle and the outside shall have security mechanisms to prevent unauthorized privileged access.

Note: Unauthorized users may gain the root user or privileged user permission of the system through the debugging interface.

7.2.9 The vehicle shall zone the internal network and protect the zone boundary. Cross-domain requests within the vehicle's internal network shall be subject to access control and follow the principle of deny by default and the principle of least privilege.

Note: Zone boundary protection measures include physical isolation and logical isolation (such as whitelist, firewall and VLAN).

7.2.10 The vehicle shall be able to identify any denial-of-service attack on its communication channels and handle the attack accordingly.

Note 1: Attack handling includes interception or discarding of attack packets, automatic recovery of affected systems and logging.

Note 2: Vehicle communication channels include mobile cellular communication, V2X,

CAN bus and on-board Ethernet.

7.2.11 The vehicle shall be able to identify malicious V2X data and diagnostic data, and take protection measures.

Note: V2X data includes the data sent by RSU to the vehicle and the data between vehicles.

7.2.12 A function of recording critical communication cybersecurity incident logs shall be available, and such logs shall be stored for at least 6 months.

Note: Critical communication cybersecurity incidents shall be determined by the vehicle manufacturer according to the results of risk assessment. Cybersecurity incident logs shall include information such as time and cause of incident.

7.3 Security requirements for software update

7.3.1 General security requirements

7.3.1.1 The on-board software update system shall use a security protection mechanism to protect its trusted root, boot loader and system firmware from being tampered with, or to make them unable to start normally after they are tampered with.

7.3.1.2 The on-board software update system shall be free of security vulnerabilities of high level or above that were announced by any authoritative vulnerability platform of the automotive industry 6 months ago and have not been handled yet.

Note 1: Authoritative vulnerability platforms of the automotive industry include the National Vulnerability Database - China Automobile Vulnerability Database (NVDB-CAVD) and other vulnerability platforms recognized by competent government authorities.

Note 2: Handling methods include vulnerability elimination, mitigation measure development and other appropriate actions.

7.3.2 Security requirements for OTA update

7.3.2.1 The vehicle and OTA update server shall be authenticated to verify the authenticity of their identity and re-verified when the download is resumed from interruption.

Note: Common authentication methods include the use of certificates for identity authentication.

7.3.2.2 The vehicle shall verify the authenticity and integrity of the downloaded update package.

7.3.2.3 Cybersecurity incidents that occur during OTA updates shall be logged, and such logs shall be stored for at least 6 months.

7.3.3 Security requirements for offline update

7.3.3.1 If the on-board software update system is used for offline update, the vehicle shall verify the authenticity and integrity of the offline update package.

7.3.3.2 If the vehicle does not use the on-board software update system for offline update, protection measures shall be taken to ensure the security of the flashing access terminal or to verify the authenticity and integrity of the update package.

7.4 Data security requirements

7.4.1 The vehicle shall use secure access technology or secure storage technology to protect the stored private keys in symmetric and asymmetric keys from unauthorized access and acquisition.

7.4.2 The vehicle shall use secure access technology, encryption technology or other security technologies to protect the sensitive personal information stored within it from unauthorized access and acquisition.

7.4.3 The vehicle shall adopt a security defense mechanism to protect the VIN stored in the vehicle and other data used for identification from unauthorized deletion and modification.

Note: Security defense mechanisms that prevent data from unauthorized deletion and modification include security access technology and read-only technology.

7.4.4 The vehicle shall use a security defense mechanism to protect the critical data stored within it from unauthorized deletion and modification.

Note: The critical data include key configuration parameters such as braking parameters, airbag deployment thresholds and traction battery parameters, as well as other data generated during vehicle operation that may affect driving safety.

7.4.5 The vehicle shall use a security defense mechanism to protect the security logs stored within it from modification and unauthorized deletion.

7.4.6 The vehicle shall have the function of deleting personal information, and such information shall not include the personal information that must be retained as specified in laws, administrative regulations and mandatory national standards.

7.4.7 The vehicle shall not directly transmit data overseas.

Note: This provision does not apply to users who access overseas websites through browsers, send messages overseas using communication software, install third-party applications that may involve cross-border data transfer, or engage in other autonomous user actions.

8 Inspection and Test Methods

8.1 General

The inspection and test methods include the CSMS inspection, basic requirements inspection and technical requirement test:

- Documentation related to the vehicle manufacturer's cybersecurity assurance capability are checked to confirm that the vehicle manufacturer meets the requirements specified in Chapter 5;
- Documentation related to cybersecurity in the process of vehicle development and production are checked to confirm that the vehicle under test (VUT) complies with the requirements specified in Chapter 6;
- The test scope of technical requirements for vehicle cybersecurity are confirmed according to 8.3 based on the identified risks of the vehicle and the relevance of handling measures in Chapter 7, and tests shall be carried out according to the test scope to confirm that the vehicle meets the requirements specified in Chapter 7.

Note: The test scope includes the clauses of Chapter 7 applicable to the VUT and the test objects corresponding to each applicable clause.

8.2 Inspection of basic requirements for cybersecurity

8.2.1 Inspection requirements

8.2.1.1 The vehicle manufacturer shall keep documentation describing the cybersecurity of vehicles during development and production, including documentation submitted and that retained for future reference.

8.2.1.2 The documentation submitted shall be in Chinese and include at least:

- a summary document demonstrating that the vehicle meets the requirements specified in Chapter 6;
- a list of documentation retained for future reference, with the version information.

8.2.1.3 The vehicle manufacturer shall retain the process documentation related to vehicle cybersecurity locally in a secure manner for future reference, and take tamper-proofing measures for documentation retained for future reference after inspection.

8.2.1.4 The vehicle manufacturer shall make a self-declaration on the consistency and traceability of the documentation submitted and retained for future reference with the vehicle.

8.2.2 Inspection methods

8.2.2.1 Check the documentation submitted by the vehicle manufacturer and confirm the inspection scheme, including the inspection scope, method and schedule and a list of necessary supporting documentation for on-site inspection.

8.2.2.2 Check the cybersecurity-related process documentation retained for future reference at the vehicle manufacturer's site according to the inspection scheme confirmed in 8.2.2.1, to confirm the vehicle's compliance with the requirements of Chapter 6.

8.3 Test on technical requirements for cybersecurity

8.3.1 Test conditions

8.3.1.1 Requirements for test environment

The test involving wireless short-range communication shall be performed in a test environment where the vehicle is free of signal interference.

8.3.1.2 Requirements for test status

The test samples include the vehicle and the components involved in the test scope determined in 8.1, and shall meet the following requirements:

- The test samples can operate normally;
- Functions related to vehicle cybersecurity are enabled;
- During the test, if the speed of the VUT is greater than 0 km/h or the VUT may start unexpectedly, place the VUT on a vehicle chassis dynamometer test bench or in a road environment that ensures the safe operation of the vehicle.

8.3.1.3 Requirements for test input

The vehicle manufacturer shall provide necessary test inputs to support the completion of the test according to the test scope determined in 8.1.

8.3.2 Security test for external connection

8.3.2.1 General security test

8.3.2.1.1 Security test for system vulnerability

The tester shall use a vulnerability scanning tool to scan the external connection system of the vehicle for vulnerabilities, and compare the test results with the list of high-level and above security vulnerabilities announced by the authoritative vulnerability platform of the automotive industry 6 months ago and with the vulnerability handling plan for the external connection system of the vehicle provided by the vehicle manufacturer, to determine whether the vehicle meets the requirements of 7.1.1.1.

8.3.2.1.2 Security test for non-service-essential network ports

The tester shall network the VUT with the scanning and testing equipment through communication channels such as WLAN, on-board Ethernet and cellular network according to the list of vehicle service ports provided by the vehicle manufacturer, use the scanning and testing equipment to test the open ports of the VUT, and compare the list of open ports of the vehicle obtained from the test with the list of vehicle service ports, to determine whether the vehicle meets the requirements of 7.1.1.2.

8.3.2.2 Security test for remote control

8.3.2.2.1 Security test for authenticity and integrity verification

The tester shall carry out the test according to the following method and sequence to determine whether the vehicle meets the requirements of 7.1.2.1:

a) Log in to the remote vehicle control program account and test whether normal remote vehicle control instructions may be triggered;

b) Forge, tamper with and send the remote vehicle control instruction to check whether the instruction may be forged or tampered with and whether the vehicle executes the instruction.

8.3.2.2.2 Security test for permission control of remote control instruction

The tester shall construct and send remote control instructions beyond the permissions according to the application scenario of remote vehicle control instructions and the permission files provided by the vehicle manufacturer, to determine whether the vehicle meets the requirements of 7.1.2.2.

8.3.2.2.3 Security test for security logging

The tester shall carry out the test according to the following method and sequence to determine whether the vehicle meets the requirements of 7.1.2.3:

a) Trigger the remote vehicle control function, and check whether there is a security log and whether the contents recorded in the security log include information such as the time, sender, remote control object and operation results of the remote control instructions;

b) Check whether the time span of security logging is not less than 6 months or whether security incident logs can be kept for at least 6 months.

8.3.2.2.4 Security test for integrity

The tester shall determine whether the vehicle meets the requirements of 7.1.2.4 according to the supporting documentation provided by the vehicle manufacturer for system integrity verification of the remote vehicle control function.

8.3.2.3 Security test for third-party applications

8.3.2.3.1 Security test for authenticity and integrity verification

The tester shall obtain an authorized third-party application, tamper with its code with tools, and then install and execute the tampered authorized third-party application to determine whether the vehicle meets the requirements of 7.1.3.1. If the tampered authorized third-party application is restricted from accessing resources beyond the access control permission, it is deemed that the application is not running normally and that the vehicle meets the requirements.

8.3.2.3.2 Security test for access control

The tester shall carry out the test according to the following method and sequence to

determine whether the vehicle meets the requirements of 7.1.3.2:

a) Install an unauthorized third-party application to test whether the vehicle sends a prompt;

b) Use the installed unauthorized third-party application to access resources beyond the access control permission, to test whether such resources may be accessed.

8.3.2.4 Security test for external interface

8.3.2.4.1 Security test for access control of external interface

The tester shall use an unauthorized user or tool to access the external interfaces of the vehicle according to the summary documentation or list of external interfaces provided by the vehicle manufacturer, to determine whether the vehicle meets the requirements of 7.1.4.1.

8.3.2.4.2 Security test for access control of USB interface and SD card interface

The tester shall inject files in specified formats, application software with specified signatures, other files in non-specified formats and other application software with non-specified signatures respectively into the mobile storage medium with USB interface and SD card interface according to the summary documentation of USB interface and SD card interface or the list of file types supported by USB interface and SD card interface provided by the vehicle manufacturer, connect the mobile storage medium to the vehicle's USB interface and SD card interface respectively, and try to execute files in non-specified formats and application software with non-specified signatures, to determine whether the vehicle meets the requirements of 7.1.4.2.

8.3.2.4.3 Security test for USB anti-virus function

The tester shall inject a virus file into the mobile storage medium through USB interface, connect the mobile storage medium to the vehicle's USB interface and try to execute the virus file, to determine whether the vehicle meets the requirements of 7.1.4.3.

8.3.2.4.4 Security test for identity authentication of diagnostic interface

The tester shall carry out the test to determine whether the vehicle meets the requirements of 7.1.4.4 with either of the following two test methods as applicable:

a) Use an unauthorized user or tool to send a write operation instruction for key vehicle configuration and calibration parameters from the diagnostic interface, to test whether the vehicle executes the operation instruction;

b) Use a tool to send a write operation instruction for key vehicle configuration and calibration parameters from the diagnostic interface, to test whether the vehicle has an access control mechanism.

8.3.3 Communication security test

8.3.3.1 Security test for identity authenticity verification for cloud platform communication

The tester shall carry out the test to determine whether the vehicle meets the requirements of 7.2.1 according to the cloud platform list provided by the vehicle manufacturer and the type of communication protocol adopted, using any of the following three test methods as applicable.

a) If the vehicle communicates with the vehicle manufacturer's cloud platform in a private network or virtual private network environment, the tester shall confirm whether the vehicle meets the requirements of 7.2.1 according to the supporting documents on communication identity authenticity of the vehicle cloud platform provided by the manufacturer.

b) If the vehicle communicates with the vehicle manufacturer's cloud platform in a public network environment using a public communication protocol, the tester shall use a network data packet capture tool to capture data packets and parse the communication message data, to check whether the vehicle verifies the identity authenticity of the vehicle manufacturer's cloud platform. If data packets cannot be captured with the network data packet capture tool, the tester shall confirm whether the vehicle meets the requirements of 7.2.1 according to the supporting documents on communication identity authenticity of the vehicle cloud platform provided by the manufacturer.

c) If the vehicle communicates with the vehicle manufacturer's cloud platform in a public network environment using a private communication protocol, the tester shall confirm whether the vehicle meets the requirements of 7.2.1 according to the supporting documents on communication identity authenticity of the vehicle cloud platform provided by the manufacturer.

8.3.3.2 Security test for V2X communication identity authentication

The tester shall carry out the test according to the following method and sequence to determine whether the vehicle meets the requirements of 7.2.2:

a) Precondition the vehicle as per 8.3.1.2, issue a legitimate certificate to the VUT and communicate with the VUT normally from the test equipment to test whether the vehicle can receive direct communication messages from the test equipment;

b) Construct an invalid certificate and a forged identity certificate respectively, and send communication messages to the vehicle to test whether the vehicle can identify the invalid certificate and forged identity certificate.

8.3.3.3 Security test for communication channel integrity

The tester shall trigger the transmission of external wireless communication data of the vehicle in turn according to the list of external communication channels such as vehicle mobile cellular communication, WLAN and Bluetooth provided by the vehicle manufacturer, and capture the packets of external wireless communication channel data of the vehicle with test equipment, to check whether an integrity protection mechanism is adopted for the channels and determine whether the vehicle meets the requirements of 7.2.3. If packets of vehicle mobile cellular communication data cannot be captured with the test equipment, the tester shall determine whether the vehicle meets the requirements of 7.2.3 according to the supporting documentation on integrity protection of vehicle mobile cellular communication channel provided by the manufacturer.

8.3.3.4 Security test against unauthorized operations

The tester shall use an unauthorized identity to operate, clear and write the vehicle data beyond the access control mechanism in turn through the external communication channel of the vehicle to check whether the data may be operated, cleared and written and determine whether the VUT meets the requirements of 7.2.4.

8.3.3.5 Security test for validity or uniqueness verification of critical instruction data

The tester shall use the test equipment to record the critical instruction data according to the list of critical instruction data provided by the vehicle manufacturer and resend the recorded instruction data, to check whether the vehicle makes response and determine whether the vehicle meets the requirements of 7.2.5.

8.3.3.6 Security test for confidentiality of sensitive personal information

The tester shall trigger the function of transmitting sensitive personal information from the vehicle to the outside according to the list of functions provided by the vehicle manufacturer

and capture the transmitted data packets using the port and access permission provided by the vehicle manufacturer, to check whether the sensitive personal information transmitted by the vehicle is encrypted and determine whether the vehicle meets the requirements of 7.2.6.

8.3.3.7 Security test against physical manipulation attacks

The tester shall replace the components used for direct wireless communication between the VUT and the outside with those unauthorized of the same model and install them at the same locations of the VUT according to the list of components used for direct wireless communication between the VUT and the outside provided by the vehicle manufacturer, and then start the vehicle, to check whether such components function abnormally or whether the vehicle gives an alarm for abnormal component connection and determine whether the vehicle meets the requirements of 7.2.7.

8.3.3.8 Security test against unauthorized privileged access to components used for direct communication between the vehicle and the outside

The tester shall carry out the test to determine whether the vehicle meets the requirements of 7.2.8 based on the system permission design scheme for components used for direct wireless communication with the outside provided by the vehicle manufacturer, using either of the following two test methods as applicable:

a) If the system only has privileged access users, test whether it is possible to log in to the system without authorization;

b) If the system has or may be configured with users with different permissions, log in to the system in the way of an unprivileged user and use the system's privilege escalation method to escalate the privilege of the unprivileged user, to test whether the privilege-escalated user has privileged access.

8.3.3.9 Security test for isolation of in-vehicle secure zone

The tester shall carry out the test to determine whether the vehicle meets the requirements of 7.2.9 according to the sample communication matrix and access control list provided by the vehicle manufacturer, using either of the following two test methods as applicable:

a) If physical isolation measures are used, verify whether the physical isolation scheme provided by the vehicle manufacturer is effective;

b) If logical isolation measures are used, send data frames that do not conform to the logical isolation strategy provided by the vehicle manufacturer to test whether such data frames may be received at the designated destination port.

8.3.3.10 Security test for identification of and protection against denial-of-service (DoS) attacks

The tester shall precondition the vehicle as per 8.3.1.2 and use the denial-of-service attack test equipment to successively attack the communication channels of the vehicle such as mobile cellular communication, V2X, CAN bus and on-board Ethernet with the vehicle in stationary and moving states respectively, to determine whether the vehicle meets the requirements of 7.2.10.

8.3.3.11 Security test for malicious data identification

The tester shall precondition the vehicle as per 8.3.1.2, and send malicious data not expected under the current vehicle conditions to the vehicle to determine whether the vehicle meets the requirements of 7.2.11.

8.3.3.12 Security test for communication cybersecurity log

The tester shall carry out the test according to the following method and sequence to

determine whether the vehicle meets the requirements of 7.2.12 based on the logging mechanism and storage path of critical vehicle communication cybersecurity incidents provided by the vehicle manufacturer:

a) Construct and trigger a critical vehicle communication cybersecurity incident to check whether the incident is recorded according to the logging mechanism of critical communication cybersecurity incidents;

b) Check whether the time span of logging is not less than 6 months or whether incident logs can be kept for at least 6 months.

8.3.4 Security test for software update

8.3.4.1 Test for general security requirements

8.3.4.1.1 Test for security protection mechanism

The tester shall judge whether the vehicle meets the requirements of 7.3.1.1 according to the supporting documentation on the security of security protection mechanism for trusted root, boot loader and system firmware of the on-board software update system provided by the vehicle manufacturer.

8.3.4.1.2 Security test for vulnerability

The tester shall use a vulnerability scanning tool to scan the on-board software update system for vulnerabilities, and compare the test results with the list of high-level and above security vulnerabilities announced by the authoritative vulnerability platform of the automotive industry 6 months ago and with the vulnerability handling plan for the on-board software update system provided by the vehicle manufacturer, to determine whether the vehicle meets the requirements of 7.3.1.2.

8.3.4.2 Security test for OTA update

8.3.4.2.1 Security test for server identity authentication

The tester shall carry out the test to determine whether the VUT meets the requirements of 7.3.2.1 according to the list of OTA update servers provided by the vehicle manufacturer and the type of communication protocol adopted, using any of the following three test methods as applicable.

a) If the vehicle communicates with the OTA server in a private network or virtual private network environment, the tester shall confirm whether the vehicle meets the requirements of 7.3.2.1 according to the supporting documentation for the identity authentication security function of the OTA update server provided by the manufacturer.

b) If the vehicle communicates with the OTA server in a public network environment using a public communication protocol, the tester shall use the test equipment to capture data packets and parse the communication message data to check whether the vehicle verifies the identity authenticity of the OTA update server; interrupt and then resume the download, use the test equipment to capture data packets and parse the communication message data to check whether the identity authenticity is verified again. If data packets cannot be captured with the test equipment, the tester shall confirm whether the vehicle meets the requirements of 7.3.2.1 according to the supporting documents for the identity authentication security function of the OTA update server provided by the manufacturer.

c) If the vehicle communicates with the OTA update server in a public network environment using a private communication protocol, the tester shall confirm whether

the vehicle meets the requirements of 7.3.2.1 according to the supporting documentation for the identity authentication security function of the OTA update server provided by the manufacturer.

8.3.4.2.2 Security test for authenticity and integrity verification of OTA update package

The tester shall carry out the test according to the following method and sequence to determine whether the vehicle meets the requirements of 7.3.2.2.

a) Use the normal update package provided by the vehicle manufacturer to trigger the OTA update, to test whether the update function is normal.

b) After confirming that the OTA update function is normal, construct an update package with damaged authenticity and integrity, download or transmit this update package to the vehicle according to the method and permission provided by the vehicle manufacturer, and perform software update to test whether the update is successful. If the vehicle cybersecurity protection mechanism does not support downloading or transmitting this update package to the vehicle, check whether the vehicle meets the requirements of 7.3.2.2 according to the supporting documentation of OTA update cybersecurity protection mechanism provided by the vehicle manufacturer.

8.3.4.2.3 Security test for OTA update cybersecurity incident log

The tester shall carry out the test according to the following method and sequence to determine whether the vehicle meets the requirements of 7.3.2.3:

a) Construct an update security incident and check whether there is an OTA update cybersecurity incident log;

b) Check whether the time span of logging is not less than 6 months or whether incident logs can be kept for at least 6 months.

8.3.4.3 Security test for offline update

8.3.4.3.1 Security test for offline update using on-board software update system

The tester shall construct forged and tampered update packages respectively, download or transmit such an update package to the vehicle ~~on-board terminal~~ with an offline update tool, and perform offline update to determine whether the vehicle meets the requirements of 7.3.3.1.

8.3.4.3.2 Security test for offline update without using on-board software update system

The tester shall carry out the test using either of the following test methods as applicable to determine whether the vehicle meets the requirements of 7.3.3.2:

a) Connect a non-authenticated flashing access terminal to the flashing interface of the vehicle and perform offline update to test whether the vehicle can identify the non-authenticated flashing access terminal;

b) Construct forged and tampered update packages respectively, connect a flashing access terminal to the flashing interface of the vehicle, and perform offline update to test whether the update is executed or successful.

8.3.5 Data security test

8.3.5.1 Security test against unauthorized acquisition and access of key

The tester shall determine the test components according to the vehicle password use scheme, and determine whether the vehicle meets the requirements of 7.4.1 using any of the following three test methods as applicable:

a) If secure access technology is used to store the key, perform attacks such as cracking and extraction through the component access interface to test whether the key may be accessed and acquired without authorization;

b) If the key is stored in a hardware security module such as HSM, check whether the vehicle is equipped with a hardware security module to protect the key at the location indicated in the document describing the installation location of the hardware security module;

c) If the key is stored in a secure software storage form, check whether the key is stored in a secure manner according to the supporting documentation provided by the vehicle manufacturer to ensure the secure storage of the vehicle key.

8.3.5.2 Security test against disclosure of sensitive personal information

The tester shall confirm the test components according to the list of sensitive personal information functions and the list of storage addresses, trigger the sensitive personal information recording functions of the vehicle in turn, and carry out the test according to the following method and sequence to determine whether the vehicle meets the requirements of 7.4.2:

a) If secure access technology is used to protect the stored sensitive personal information, access the stored sensitive personal information with a user without access control permission through the component debugging interface according to the description of sensitive personal information storage area and address range, to test whether unauthorized access to sensitive personal information is allowed;

b) If encryption technology is adopted to protect the stored sensitive personal information, extract the stored sensitive personal information with a software analysis tool through the component debugging interface according to the description of sensitive personal information storage area and address range, to test whether the information is stored in ciphertext;

c) Trigger the vehicle's functions of recording sensitive personal information in turn, then log in to the system, and retrieve sensitive personal information from the test components, to test whether sensitive personal information that is not stored in the list of sensitive personal information functions and the list of storage addresses may be retrieved.

8.3.5.3 Security test against unauthorized deletion and modification of vehicle identification data

The tester shall confirm the test components according to the list of data stored in the vehicle for vehicle identification (such as VIN) and the storage address, and use the software analysis tool to delete and modify the data stored in the vehicle for vehicle identification (such as VIN) without authorization, to determine whether the vehicle meets the requirements of 7.4.3.

8.3.5.4 Security test against unauthorized deletion and modification of critical data

The tester shall confirm the test components according to the list of critical data stored in the vehicle and the storage address, and use the software analysis tool to change the critical data stored in the vehicle through the component debugging interface to determine whether the vehicle meets the requirements of 7.4.4.

8.3.5.5 Security test against modification and unauthorized deletion of log files

The tester shall confirm the test components according to the list of security logs stored in the vehicle and the storage address, and carry out the test according to the following method and sequence to determine whether the vehicle meets the requirements of 7.4.5:

a) Modify security log files through the component debugging interface according to the list of security logs stored in the vehicle and the storage address, to test whether such security log files may be modified;

b) Use the software analysis tool through the component debugging interface according to the list of security logs stored in the vehicle and the storage address to test whether such security log files may be deleted without authorization.

8.3.5.6 Test method for personal information clearing function

The tester shall use the personal information clearing function of the VUT, confirm the test components, trigger the personal information recording functions of the vehicle in turn and clear the personal information stored in the vehicle, to check whether such personal information is completely deleted through the component debugging interface according to the list of personal information stored in the vehicle and the storage address provided by the vehicle manufacturer, and determine whether the vehicle meets the requirements of 7.4.6.

8.3.5.7 Test method for prevention of direct cross-border data transfer

The tester shall enable all mobile cellular communication channels and WLAN communication channels of the vehicle, successively simulate that the VUT is not powered on, just powered on, and powered on with various pre-installed data transmission functions normally enabled, then use a network data packet capture tool to capture data packets from the external communication network channels simultaneously for not less than 3600 s in total and parse the communication message data, to check whether the destination IP address contains an overseas IP address and determine whether the vehicle meets the requirements of 7.4.7.

9 Determination of the Same Type

9.1 Criteria for direct determination of the same type of cybersecurity

Vehicles meeting the following requirements are considered to be of the same type:

- The cybersecurity management system is effective;
- The vehicles have the same electronic and electrical architecture and take the same cybersecurity handling measures;
- The hardware model and software version number (except for those that do not affect cybersecurity) of the central gateway of the vehicles are the same;
- The hardware model and software version number (except for those that do not affect cybersecurity) of the on-board software update system of the vehicles are the same;
- The hardware model and software version number (except for those that do not affect cybersecurity) of the components with cellular mobile communication system function of the vehicle are the same;
- The type and version of protocol and the type and quantity of interfaces used for vehicle wireless communication are the same or reduced;

Note: Wireless communication modes include WLAN, Bluetooth, NFC, cellular communication and V2X.

- The type and quantity of external interfaces of the vehicles are the same or reduced;
- The IP address or domain name of the vehicle manufacturer's cloud platform that is directly connected to the vehicle and generates data interaction, is the same.

9.2 Criteria for determination of the same type after verification of cybersecurity test

If the vehicle type is changed in relation to 9.1 and meets the following requirements, only

supplementary tests need to be carried out on the technical requirements related to the changed parameters and the type may be extended upon approval:

- The cybersecurity management system is effective;
- The vehicles have the same electronic and electrical architecture and take the same cybersecurity handling measures;
- The type of protocol and the type of interface used for vehicle wireless communication are the same or reduced;
- The type of external interfaces of the vehicles is the same or reduced.

9.3 Criteria for direct determination of the same type of data processing function

Vehicles meeting the following requirements are considered to be of the same type:

- The manufacturer and version of anonymization algorithm of the vehicles are the same;
- The hardware model and software version number (except for those that do not affect the anonymization policy) and the manufacturer of the controller used for anonymization algorithm of the vehicles are the same;
- The hardware model and main parameter configuration (sampling resolution, sampling field-of-view angle and sampling frame rate) and the manufacturer of vehicle camera and other acquisition equipment for the anonymization function are the same;
- The triggering scenario for the anonymization function of the vehicles is the same.

10 Implementation of Standard

For new vehicles under type approval, the standard shall be executed from the implemented date of this document.

For vehicles with type approval, the standard shall be executed from the 25th month since the implemented date of this document.

Bibliography

[1] UNR155 Uniform Provisions Concerning the Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System

Amendment No. 1 to the National Standard

GB 44495-2024 *Technical Requirements for Vehicle Cybersecurity*

This amendment was approved by the State Administration for Market Regulation (Standardization Administration of the People's Republic of China) on January 28, 2026, and shall enter into force on January 28, 2026.

I. "1 Scope" was revised as follows: "This document specifies the cybersecurity assurance requirement, basic cybersecurity requirements, cybersecurity technical requirements, and type equivalence determination for vehicles, and describes the corresponding inspection and test methods. This document applies to M and N vehicles and does not apply to special vehicles modified from type II chassis or vehicles that have already obtained type approval."

II. The title of Chapter 5 and the "information security management system requirements" in 6.1, as well as the "information security management system" in 5.1, 5.2 and 8.1, were replaced with "cybersecurity assurance requirements". The term "3.2 Cybersecurity management system" in the terms and definitions was deleted".

III. In Chapter 8, all occurrences of "examination" are replaced with "inspection", and all occurrences of "for inspection" in 8.2.1.1, 8.2.1.2, 8.2.1.3 and 8.2.1.4 are replaced with "available for inspection".

IV. In 9.1 and 9.2, the first listed item "the cybersecurity management system is effective" is replaced with: "the cybersecurity assurance–related contents in the inspection and test report for the technical requirements for cybersecurity of vehicles are valid, and the date of issuance is not more than three years prior".

V. The text in Chapter 10 was changed from "For new vehicles under type approval, the standard shall be executed from the implemented date of this document." to: For new vehicles under type approval, the standard shall be executed from the 7th month since the implemented date of this document.

National Standard of
the People's Republic of China

Technical Requirements for Vehicle Cybersecurity

GB 44495-2024

*

Published by Standards Press of China

No. A2, Hepingli West Street, Chaoyang District, Beijing (100029)

No. 16, Sanlihe North Street, Xicheng District, Beijing (100045)

Website: www.spc.net.cn

Service hotline: 400-168-0010

First edition in August 2024

*

Book No.: 155066·1-77470