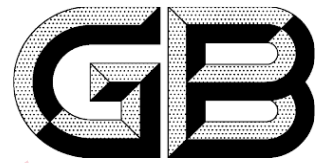


ICS 43.020
CCS T 40



NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA

GB 44495-2024

Technical requirements for vehicle cybersecurity

汽车整车信息安全技术要求

Issued on: August 23, 2024

Implemented on: January 01, 2026

**Issued by: State Administration for Market Regulation; Standardization
Administration of the People's Republic of China.**

Table of Contents

Foreword	3
1 Scope	4
2 Normative references	4
3 Terms and definitions	4
4 Abbreviated terms.....	6
5 Requirements for vehicle cybersecurity management system	7
6 Basic requirements for cybersecurity	8
7 Technical requirements for cybersecurity.....	9
8 Inspection and test methods	14
9 Same type determination	26
10 Implementation of standards	27
Bibliography	28

Foreword

This document was drafted in accordance with the rules given in GB/T 1.1-2020, *Directives for standardization - Part 1: Rules for the structure and drafting of standardizing documents*.

The technical content of this document refers to the United Nations Technical Regulation UN R155 *Uniform rules for the approval of vehicle cybersecurity and cybersecurity management system*.

Please note that some of the contents of this document may involve patents. The issuing organization of this document is not responsible for identifying patents.

This document is proposed and managed by 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 vehicle cybersecurity management system, basic requirements for cybersecurity, technical requirements for cybersecurity and same type identification, and describes the corresponding inspection and test methods.

This document applies to category M and category N vehicles, as well as category O vehicles that are equipped with at least one electronic control unit.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the version corresponding to that date is applicable to this document; for undated references, the latest version (including all amendments) is applicable 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

Terms and definitions given in GB/T 40861, GB/T 44373 and GB 44496, as well as the following, are applicable to this document.

3.1

vehicle cybersecurity

The state where the vehicle's electrical and electronic systems, components and functions are protected from asset threats.

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

3.2

cybersecurity management system; CSMS

System approach based on risk.

Note: Including organizational processes, responsibilities and governance to address risks associated with vehicle cyber threats and to protect vehicles from cyber-attacks.

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

3.3

risk

Impact of vehicle cybersecurity uncertainty.

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

3.4

risk assessment

The process of discovering, identifying and describing risks, understanding the nature of risks and determining the level of risks, and comparing the results of risk analysis with risk criteria to determine whether the risks are acceptable.

3.5

threat

Potential causes of unexpected events that may result in harm to systems, organizations, or individuals.

3.6

vulnerability

Weakness that can be utilized by one or more threats in an asset or mitigation.

3.7

on-board software update system

Software and hardware installed on the vehicle side that are capable of directly receiving, distributing and verifying upgrade packages from outside the vehicle, etc., to achieve software upgrade functions.

[Source: GB 44496-2024, 3.12]

3.8

over-the-air update