GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 43.020

CCS T 40

GB/T 40856-2021

Technical Requirements and Test Methods for Cybersecurity of On-board Information Interactive System

车载信息交互系统信息安全技术要求及试验方法

Issued on: October 11, 2021 **Implemented on: May 1, 2022**

Issued by: State Administration for Market Regulation;

Standardization Administration of the People's Republic of China.

Table of Contents

Technical Requirements and Test Methods for Cybersecurity of On-board Information Interactive System

1 Scope

This Standard specifies the technical requirements and test methods for the cybersecurity of hardware, communication protocols and interfaces, operating systems, application software and data of on-board information interactive system.

This Standard is applicable to the guidance of original equipment manufacturers, component suppliers and software suppliers in the implementation of the design, development, verification and production for the information security technology of on-board information interactive system.

2 Normative References

The contents of the following documents constitute indispensable clauses of this document through 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/T 25069 Information Security Technology - Glossary

GB/T 40861 General Technical Requirements for Vehicle Cybersecurity

GM/T 0005-2012 Randomness Test Specification

3 Terms and Definitions

What is defined in GB/T 25069 and GB/T 40861, and the following terms and definitions are applicable to this document.

3.1 On-board Information Interactive System

On-board information interactive system refers to a communication system installed on the vehicle and with at least one of the following functions:

a) Externally, it can establish connections and perform data exchange functions through communication technologies, such as cellular networks and short-distance communications. Internally, it can perform functions, such as:

storage and transmission of sensitive personal information used by the on-board information interactive system shall reduce the number of exposed pins.

5.1.3 In accordance with 6.1 d), perform the test. The number of exposed communication lines shall be reduced among the key chips used by the on-board information interactive system. For example, the on-board information interactive system using multi-layer circuit boards may adopt the mode of internal wiring to conceal the communication lines.

5.1.4 In accordance with 6.1 e), perform the test. The circuit boards and chips should not expose readable screen printings that are used to mark the port and pin functions.

5.2 Security Requirements for Communication Protocols and Interfaces

5.2.1 Security of external communication

5.2.1.1 Security of communication connection

In accordance with 6.2.1.1 a), perform the test. The on-board information interactive system shall implement identity authentication of the platform server or the external terminal. When the identity authentication is successful, in accordance with 6.2.1.1 b), perform the test, and the on-board information interactive system and the platform server or the external terminal can realize communication and interaction of business data.

5.2.1.2 Security of communication transmission

In accordance with 6.2.1.2, perform the test. The data content transmitted between the on-board information interactive system and the platform server or the external terminal shall be encrypted, and the national encryption algorithm should be used.

5.2.1.3 Security of communication termination response

When communicating with the on-board information interactive system, the following requirement shall be satisfied:

a) In accordance with 6.2.1.3 a), perform the test. When the data content verification fails, the response operation shall be terminated;

b) In accordance with 6.2.1.3 b), perform the test. When the identity authentication fails, the response operation shall be terminated.

5.2.1.4 Security of telecommunication protocol

5.2.1.4.1 Security of on-board public telecommunication protocol

The on-board public telecommunication protocol shall be tested in accordance with 6.2.1.4.1. A secure communication protocol with TLS 1.2 version and above, or at least

the same level of security shall be adopted.

5.2.1.4.2 Security of on-board private telecommunication protocol

The on-board private telecommunication protocol shall satisfy the following requirements:

a) In accordance with 6.2.1.4.2 a), perform the test. It shall support the update of data encryption keys in a secure mode;

b) In accordance with 6.2.1.4.2 b), perform the test. The used keys shall be securely transmitted.

5.2.1.5 Security of short-distance communication protocol

5.2.1.5.1 Security of short-distance communication password application

The security of short-distance communication password application shall satisfy the following requirements:

a) In accordance with 6.2.1.5.1 a), perform the test. The default password shall be a strong-complexity password that includes at least Arabic numerals, uppercase and lowercase Latin letters, and a length of not less than 8 digits;

NOTE: Bluetooth is not limited to the requirements of the above clause.

b) In accordance with 6.2.1.5.1 b), perform the test. Different on-board information interactive systems shall use different default passwords;

c) In accordance with 6.2.1.5.1 c), perform the test. When changing the password, restrict the user in the setting of the password required by a) or prompt the user of risks;

NOTE: Bluetooth is not limited to the requirements of the above clause.

d) In accordance with 6.2.1.5.1 d), perform the test. For the login authentication of the human-machine interface or the interface between different on-board information interactive systems across the trust network, the password anti-brute force cracking mechanism shall be supported. In addition, in accordance with 6.2.1.5.1 e), perform the test; the password file shall be set with security access control.

5.2.1.5.2 Security of on-board Bluetooth communication protocol

The on-board information interactive system with on-board Bluetooth communication function shall satisfy the following requirements:

a) In accordance with 6.2.1.5.2 a), perform the test. The on-board information

5.2.3.2.1 In accordance with 6.2.3.2 a), perform the test. The on-board information interactive system shall support routing isolation; isolate the communication of the core business platform that executes the vehicle control commands and collects personal sensitive information; isolate the internal communication of the non-core business platform in the internal communication and the external network communication of the non-core business platform in the external communication.

NOTE: non-core business platform refers to a business platform other than the core business platform.

5.2.3.2.2 In accordance with 6.2.3.2 b), perform the test. The communication between the on-board information interactive system and the core business platform capable of executing the vehicle control commands and collecting personal sensitive information should adopt private network or virtual private network communication, which is isolated from the public network.

5.2.3.3 Security of communication interface in the vehicle

The on-board information interactive system shall satisfy the following requirements:

a) In accordance with 6.2.3.3 a), perform the test; set a whitelist for legal commands;

b) In accordance with 6.2.3.3 b), perform the test; verify the source of the bus control command.

5.3 Security Requirements for Operating System

5.3.1 Security configuration of operating system

In terms of the security configuration of operating system, the on-board information interactive system shall satisfy the following requirements:

a) In accordance with 6.3.1 a), perform the test; prohibit the highest-privileged users from directly logging in, and restrict ordinary users' privilege escalation operations;

b) In accordance with 6.3.1 b), perform the test; delete or disable useless accounts; use a strong-complexity password that includes at least Arabic numerals, uppercase and lowercase Latin letters, and a length of not less than 8 digits;

c) In accordance with 6.3.1 c), perform the test; have an access control mechanism to control users, processes and other subjects to access files, databases and other objects;

d) In accordance with 6.3.1 d), perform the test; prohibit unnecessary services, for example, FTP services, etc.; in accordance with 6.3.1 e), perform the test;

prohibit unauthorized remote access services.

5.3.2 Secure invocation control capability

5.3.2.1 Communication function control mechanism

5.3.2.1.1 Making calls

The on-board information interactive system with the function of making calls shall satisfy the following requirements:

a) In accordance with 6.3.2.1.1 a), perform the test. The invocation of the operation of making callings can only be executed after the user expressly consents;

b) In accordance with 6.3.2.1.1 b), perform the test. The invocation of the operation of calling for call forwarding service can only be executed after the content of the service is clearly indicated to the user and the user expressly consents.

NOTE: in emergency situations, emergency functions, for example, E-Call, are not limited to the requirements of the above clause.

5.3.2.1.2 Three-way calling

The on-board information interactive system with three-way calling function shall be tested in accordance with 6.3.2.1.2. The invocation of the operation of three-way calling can only be executed after the user expressly consents.

5.3.2.1.3 Sending short messages

The on-board information interactive system with the function of sending short messages shall be tested in accordance with 6.3.2.1.3. The invocation of the operation of sending short messages can only be executed after the user expressly consents.

NOTE: in emergency situations, emergency functions, for example, E-Call, are not limited to the requirements of the above clause.

5.3.2.1.4 Sending multimedia messages

The on-board information interactive system with the function of sending multimedia messages shall be tested in accordance with 6.3.2.1.4. The invocation of the operation of sending multimedia messages can only be executed after the user expressly consents.

5.3.2.1.5 Sending emails

The on-board information interactive system with the function of sending emails shall

d) When data is being transmitted, in accordance with 6.3.2.1.7 d), perform the test. The user shall be prompted with the corresponding status on the interactive interface;

e) In the above-mentioned c) and d), in accordance with 6.3.2.1.7 e), perform the test. The mode of status prompt shall be different.

5.3.2.2 Local sensitive function control mechanism

5.3.2.2.1 Positioning function

The on-board information interactive system with an interactive interface shall satisfy the following requirements when invoking the positioning function:

a) In accordance with 6.3.2.2.1 a), perform the test. The positioning function can only be executed after the user expressly consents;

b) In accordance with 6.3.2.2.1 b), perform the test. Provide the user with the background positioning control function to configure whether the application software can invoke the positioning function;

c) In the above-mentioned a) and b), in accordance with 6.3.2.2.1 c), perform the test. Let the user separately operate.

d) When invoking the positioning function, in accordance with 6.3.2.2.1 d), perform the test. The user should be prompted with the corresponding status on the interactive interface.

5.3.2.2.2 Function of call recording

When invoking the call recording function, the on-board information interactive system with an interactive interface shall be tested in accordance with 6.3.2.2.2. The function of call recording can only be executed after the user expressly consents.

5.3.2.2.3 Function of human-machine interaction

When invoking the function of human-machine interaction, the on-board information interactive system with an interactive interface shall be tested in accordance with 6.3.2.2.3. The function of human-machine interaction can only be executed after the user expressly consents.

NOTE: the human-machine interaction function here refers to the interaction function involving personal biometric information, such as: fingerprints, voices, images and videos, etc.

5.3.2.2.4 Operation of user data

When processing user data, in accordance with 6.3.2.2.4, perform the test. The

operating system shall be accordingly authorized, for example, when the application software needs to invoke the reading or writing operation of phone book data, call records, Internet-accessing records, short message data and multimedia message data, the operating system shall be executable under the authorization of the application software.

5.3.3 Secure startup of operating system

The on-board information interactive system shall satisfy the following requirements:

a) In accordance with 6.3.3 a), perform the test. The startup of the operating system shall start with a root of trust that cannot be modified;

b) In accordance with 6.3.3 b), perform the test. The on-board operating system can only be loaded after the operating system signature is verified in the trusted storage area, so as to prevent the loading of a tampered operating system;

c) Before executing other secure startup codes, in accordance with 6.3.3 c), perform the test; the integrity of the code shall be verified.

5.3.4 Update of operating system

The on-board information interactive system shall satisfy the following requirements:

a) In accordance with 6.3.4 a), perform the test. It shall have the anti-rollback verification function of the system mirror;

b) When the installation of the updated mirror image fails, in accordance with 6.3.4 b), perform the test. It shall restore to the version before the update or enter a secure status;

NOTE: the secure status refers to the status, in which, security threats are not introduced to the entire vehicle through the on-board information interactive system.

c) In accordance with 6.3.4 c) and d), perform the test. There shall be a security mechanism to verify the integrity of the updated mirror image and the reliability of the source.

5.3.5 Isolation of operating system

In accordance with 6.3.5, perform the test. Except for necessary interfaces and data, such as: functions like making calls and data like phone books and short messages, which can be shared, there shall be no communication between multi-operating systems with preset functions in parallel.

5.3.6 Security management of operating system

b) In accordance with 6.4.1 b), perform the test. There shall be no high-risk and above security vulnerabilities that were announced by the authoritative vulnerability platform 6 months ago and have not been dealt with;

NOTE: the dealing includes modes like eliminating vulnerabilities and formulating mitigation measures, etc.

c) In accordance with 6.4.1 c), perform the test. There shall be no malicious behaviors, such as: unauthorized collection or disclosure of personal sensitive information and unauthorized data transmission, etc.;

d) In accordance with 6.4.1 d), perform the test. Sensitive personal information shall not be stored in plain text;

e) In accordance with 6.4.1 e), perform the test. It shall have a session security protection mechanism, for example, a mechanism that randomly generates session ID;

f) In accordance with 6.4.1 f), perform the test. Use a strong-complexity password that includes at least Arabic numerals, uppercase and lowercase Latin letters, and a length of not less than 8 digits, or prompt the user of risks;

g) In accordance with 6.4.1 g), perform the test. It shall comply with the cryptographic requirements and shall not directly write the private key in the code; in accordance with 6.4.1 h), perform the test; use verified and secure encryption algorithms and parameters; in accordance with 6.4.1 i), perform the test; the same key shall not be repeatedly used for different purposes;

h) In accordance with 6.4.1 j), perform the test. The used random number shall comply with GM/T 0005-2012 and other related standards on random number and shall be ensured to be generated by a verified and secure random number generator.

5.4.2 Security of application software code

The security of application software code on the on-board information interactive system shall satisfy the following requirements:

a) In accordance with 6.4.2 a), perform the test. When using third-party components, the application software developer shall identify the already-known vulnerabilities in the public vulnerability database and install patches;

b) For unmanaged code, in accordance with 6.4.2 b), perform the test. The secure allocation, usage and release of memory space shall be ensured;

c) In accordance with 6.4.2 c), perform the test. The application software installation package shall adopt a code signing authentication mechanism;

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------