ICS 43.020

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 40855-2021

Technical requirements and test methods for cybersecurity of remote service and management system for electric vehicles

电动汽　远程服务与管理系统信息安全 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

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.

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 was proposed by the Ministry of Industry and Information Technology of the People's Republic of China.

This document shall be under the jurisdiction of National Technical Committee of Auto Standardization (SAC/TC 114).

The drafting organizations of this document: Neusoft Corporation, China Automotive Technology and Research Center Co., Ltd., Beijing Institute of Technology Xinyuan Information Technology Co., Ltd., Daimler Greater China Ltd., Beijing Qihoo Technology Co., Ltd., Beijing Automotive Technology Center, National Computer Network Emergency Response Technical Team/Coordination Center of China, Volkswagen (China) Investment Co. Ltd., Ford Motor (China) Ltd., FAW Car Co., Ltd., Huawei Technologies Co., Ltd., Dongfeng Motor Corporation Technical Center, China Academy of Information and Communications Technology, SAIC-GM-Wuling Automobile.

The drafters of this document: Chen Jingxiang, Xie Hanguang, Liu Xiaochun, Fang Xiyu, Chen Yikun, Du Zhibin, Li Gang, Yan Minrui, Li Feng, Wang Hui, Zhang Lijia, Xiang Xiaoli, Li Muxi, Pan Kai, Chen Huarong, Gui Li, Feng Heng.

1 Scope

This document specifies the requirements and test methods for cybersecurity of remote service and management system for electric vehicles.

This document applies to data communication between the on-board terminals of battery electric vehicles, plug-in hybrid electric vehicles and fuel-cell electric vehicles, vehicle enterprise service and management platforms and public service and management platforms.

2 Normative references

The contents of the following documents constitute the indispensable clauses of this document through normative references in the text. 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.

3 Terms and definitions

Terms and definitions determined by GB/T 19596, GB/T 32960.1-2016, GB/T 32960.3-2016, and the following ones are applicable to this document.

A system for collecting, processing and managing electric vehicle information, and providing information services for networked users. It is composed of a public service and management platform, an enterprise service and management platform and an on-board terminal.

A platform, which is established by the state, local government or its designated agency, for data collection and unified management of electric vehicles within the jurisdiction.

A platform, which is established by the vehicle companies themselves, or by a thirdparty technical unit on a commission basis, to manage electric vehicles and users within the service range, and to provide safe operation services and management.

A device or system, which is installed on the motor vehicle to collect and save the key state parameters of the vehicle and system components, and to send it to the platform.

When data is exchanged between platforms, it serves as a remote service and management platform for the sender of vehicle data.

When data is exchanged between platforms, it serves as a remote service and management platform for the receiver of vehicle data.

Perform integrity verification on the target program of the device based on the root of trust.

4 Abbreviations

5 Information security requirements

5.1 Overall structure diagram

See Figure 1 for the overall structure of information security of the remote service and management system for electric vehicles.

5.2 Security requirements for on-board terminal

5.2.1 General requirements

The on-board terminal shall ensure the hardware, firmware, software systems, data storage, network port transmission, remote upgrades, logs, and system information security, and meet the basic requirements of confidentiality, integrity, and availability.

5.2.2 Functional requirements

5.2.2.1 On-board terminal hardware

The hardware security requirements of the on-board terminal are as follows:

a) There shall be no backdoors or hidden interfaces;

5.2.2.2 On-board terminal firmware

The on-board terminal shall be equipped with the function of security startup, and shall be able to protect the root of trust which is used for secure start, through the root of trust entity.

5.2.2.3 On-board terminal software system

The software system requirements of the on-board terminal are as follows:

a) It shall be equipped with the ability to determine and authorize application access and operation permissions to system resources;

b) Trusted verification should be carried out.

5.2.2.4 On-board terminal data storage

The data storage requirements of the on-board terminal are as follows: stored in accordance with the requirements of GB/T 32960.3-2016 shall be guaranteed;

5.2.2.5 On-board terminal network port transmission security

5.2.2.6 On-board terminal remote upgrades

If the on-board terminal is provided with the remote upgrade function, the onboard terminal shall have an upgrade package verification mechanism to verify the integrity of the upgrade package and the authenticity of the source.

5.2.2.7 On-board terminal log

The log function requirements of the on-board terminal are as follows:

the on-board terminal, such as the detection of cyber-attacks, shall be recorded;

include but not limited to: date and time (accurate to the second), vehicle unique identification code, and event type;

allowed to read by authorized applications in an authorized manner;

f) There shall be an upload mechanism for information security event logs, to use a secure communication protocol to send information security event log information to the enterprise platform.

5.2.2.8 On-board terminal system security

The on-board terminal shall not have high-risk and higher security vulnerabilities that were announced by authoritative vulnerability platforms 6 months ago and have not been dealt with.