ICS 43.020

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 40857-2021

Technical requirements and test methods for cyber security of vehicle gateway

汽　网关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

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviations

5 Vehicle gateway network topology

6 Technical requirements

7 Test methods

Annex A Example of vehicle gateway topology

Annex B Examples of typical attacks

Bibliography

Foreword

This Standard 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”.

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

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

This Standard shall be under the jurisdiction of National Technical Committee on Automobiles of Standardization Administration of China (SAC/TC 114).

The drafting organizations of this Standard: Guangzhou Automobile Group Co., Ltd., China Automotive Technology and Research Center Co., Ltd., Pan Asia Automotive Technology Center Co., Ltd., SAIC Motor Technology Center, Beijing Automotive Research Institute Co., Ltd., Daimler Greater China Investment Co., Ltd., Geely Automobile Research Institute (Ningbo) Co., Ltd., Neusoft Group Co., Ltd., Chongqing Changan Automobile Co., Ltd., Dongfeng Motor Group Co., Ltd. Technology Center, Ministry of Transport Highway Research Institute.

Main drafters of this Standard: Shang Jin, Sun Hang, Gu Jijie, Li Baotian, Feng Haitao, Fei Xiao, Chen Xin, Lu Ming, Yang Chenghao, Chen Jingxiang, He Kexun, He Wen, Cheng Zhou, Liu Zhichao.

1 Scope

This Standard specifies cyber security technical requirements and test methods for vehicle gateway product hardware, communication, firmware, data.

This Standard is applicable to the design and implementation of cyber security of vehicle gateway products. It is also applicable to product testing, evaluation and management.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

3 Terms and definitions

3.1 vehicle gateway

an electronic control unit of which the main function is to safely and reliably forward and transmit data between multiple networks in the vehicle conversion between different communication protocols. Information can be exchanged among the functional domains that share communication data.

3.2 backdoor

3.3 entity of root of trust

A functional module that is used to support the establishment and transmission of the trust chain of the trusted computing platform that can provide external services such as integrity measurement, secure storage, and cryptographic computing.

4 Abbreviations

5 Vehicle gateway network topology

5.1 CAN gateway

The vehicle gateways in this type of structure mainly have CAN and/or CAN- FD bus interfaces, which can be called CAN gateways.

The typical CAN gateway topology is shown in Figure A.1 in Annex A.

5.2 Ethernet gateway

The vehicle gateway in this type of structure mainly has an Ethernet interface, which can be called an Ethernet gateway.

The typical Ethernet gateway topology is shown in Figure A.2.

5.3 Hybrid gateway

6 Technical requirements

6.1 Hardware cyber security requirements

6.1.1 Test according to 7.1a). The gateway shall not have backdoors or hidden interfaces.

6.1.2 Test according to 7.1b). The debugging interface of the gateway shall be disabled or set up security access control.

6.2 Communication cyber security requirements

6.2.1 CAN gateway communication cyber security requirements

6.2.1.1 Access control

The gateway shall establish a communication matrix between each CAN network. Establish an access control strategy based on CAN data frame identifier (CANID). After testing according to 7.2.1a), the data frame sent by the source port shall be detected at the destination port specified in the list. After testing according to 7.2.1b), data frames that do not meet the definition shall be discarded or logged.

6.2.1.2 Denial of service attack detection

The gateway shall perform CAN bus DoS attack detection on the CAN channel of the vehicle's external communication interface (for example: the channel connected to the OBD-II port and the channel connected to the vehicle information interaction system).

The gateway shall have a DoS attack detection function based on the CAN bus interface load. It shall have a DoS attack detection function based on one or more CANID data frame periods.

Test according to 7.2.1c) and d). When the gateway detects a DoS attack on one or more CAN channels, it shall meet the following requirements:

channel of the gateway shall not be affected;

6.2.1.3 Data frame health detection

The gateway shall check the data frame according to the signal definition in the communication matrix. The checking content includes DLC field, signal value validity. Test according to 7.2.1e), f). Discard or log data frames that do not meet the definition of the communication matrix.

6.2.1.4 Data frame anomaly detection

The gateway shall have a data frame abnormality detection function, that is, the mechanism for checking and recording the sending and receiving relationship between data frames is tested in accordance with 7.2.1g). Discard or log the abnormal data frames.

When the gateway detects that the transmission frequency of a data frame within a certain period of time is far from the predefined frequency, or the signal value content of the same data frame at adjacent times conflicts or jumps abnormally, discard or log data frames.

6.2.1.5 UDS session detection

6.2.2 Ethernet gateway communication cyber security requirements

6.2.2.1 Network domain

6.2.2.2 Access control

6.2.2.3 Denial of service attack detection