



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 40861-2021

General Technical Requirements for Vehicle Cybersecurity

汽 信息安全通用技术要求

Issued on: October 11, 2021

Implemented on: May 1, 2022

**Issued by: State Administration for Market Regulation;
Standardization Administration of PRC..**

Table of Contents

Foreword

Introduction

1 Scope

2 Normative References

3 Terms and Definitions

4 Abbreviations

5 Protected Objects

6 Technical Requirements

Appendix A Information Security Threats

Bibliography

Foreword

This Document was drafted as per the rules specified in GB/T 1.1-2020 Directives for Standardization – Part 1: Rules for the Structure and Drafting of Standardizing Documents.

Please note some contents of this Document may involve patents. The issuing agency of this Document shall not assume the responsibility to identify these patents.

This Document was proposed by Ministry of Industry and Information Technology of the PRC.

This Document shall be under the jurisdiction of National Technical Committee for Standardization of Automobile (SAC/TC 114).

Drafting organizations of this Document: Zhejiang Geely Holding (Group) Co., Ltd.; Huawei Technologies Co., Ltd.; China Automobile Technology and Research Centre Co., Ltd.; Beijing Qihoo Technology Co., Ltd.; Daimler Greater China Ltd.; PSA Peugeot Citroen (China) Automotive Trading Co., Ltd. Shanghai Branch; Pan Asia Technical Automotive Centre Co., Ltd.; Guangzhou Automobile Group Co., Ltd.; Centre of Computer & Micro-Electronics Industry Development of MIIT; BMW China Services Ltd.; Volkswagen (China) Investment Co., Ltd.; Neusoft Corporation; Continental Holding China Co., Ltd.; Beijing Ypgreat Technology Limited.; China Academy of Information and Communications Technology; Dongfeng Motor Corporation Technical Centre; and China First Automobile Group Co., Ltd.

Chief drafting staffs of this Document: Yin Yang, Zhang Xuwu, Zhang Hang, Zhang Rongbo, Pan Kai, WU Hanbing, Zhang Yi, Lv Ming, Feng Zhimin, Feng Haitao, Zhang Jinchi, Guo Ying, Wang Zhe, Zhao Wen, Cheng Jingxiang, Yang Wenchang, Lu Zuohua, Sun Yaping, Li Yan, and Gao Changsheng.

Introduction

With the rapid development and application of intelligent and networking technologies, automobiles have gradually evolved from relatively isolated electromechanical systems to intelligent systems that can interact with the outside world. Information security issues derived from automobile networking have followed.

Different from the information security of communications and other industries that mainly cause property losses, as a high-speed vehicle for manning and carrying objects, when automobile information security problems occur, it shall not only cause property losses, but also seriously threaten personal and public safety.

Based on the hazards and incentives of automobile information security risks, this Document formulates general technical requirements for the protected objects (the

technical requirements of the entire automobile and its electronic and electrical systems and components can be determined based on the function design and risk assessment results); is used in conjunction with other management requirements standards; and guides the establishment of an automotive information security technology system. The standard framework is shown in Figure 1. While stipulating basic technical requirements such as principled requirements and systemic defence strategy requirements, specific technical requirements for sub-protected objects are formulated from the following eight dimensions:

1 Scope

This Document specifies the protected objects and technical requirements of vehicle cybersecurity.

This Document is applicable to M and N categories of vehicles, their electrical and electronic systems and components.

2 Normative References

The provisions in following documents become the provisions of this Document through reference in this Document. For the dated documents, only the versions with the dates indicated are applicable to this Document; for the undated documents, only the latest version (including all the amendments) is applicable to this Document.

3 Terms and Definitions

3.1 Vehicle cybersecurity

The electronic and electrical systems, components and functions of the vehicle are protected, so that its assets are not threatened.

3.2 Authenticity

An entity is a characteristic of the entity it claims.

3.3 Confidentiality

The characteristic that information is unavailable or non-disclosed to unauthorized individuals, entities, or processes.

3.4 Integrity

3.5 Availability

Accessible and usable characteristics according to the requirements of authorized entities.

3.6 Access controllability

The characteristic that is authorized and restricted based on the business and security requirements to ensuring the access to the asset.

3.7 Non-repudiation

The ability to prove the occurrence and origin of the alleged state of affairs or behaviour.

3.8 Accountability

The characteristic that ensures the behaviour of an entity can be uniquely traced back to that entity.

3.9 Preventability

3.10 Denial of service; DoS

3.11 Distributed denial of service; DDoS

The denial of service is realized by damaging or controlling multiple systems to take flood attack on the bandwidth and resources of the target system.

3.12 Backdoor

The channel that can bypass the management and control of security mechanisms such as system authentication and enter the information system.

3.13 Security important parameter

Security-related information includes authentication data such as secret keys and private keys, passwords, or other password-related parameters information.

3.14 Access control

The manner that ensures the access to assets is authorized and restricted based on business and security requirements.

4 Abbreviations

The following abbreviations are applicable to this Document.

5 Protected Objects

5.1 General

According to the category of protected objects, automobiles can be divided into three types of sub-protected objects: in-vehicle systems, out-of-vehicle communications, and