

ICS 430.020

CCS T 40



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

GB/T 40861-2021

**General Technical Requirements for Vehicle
Cybersecurity**

汽车信息安全通用技术要求

Issued on: October 11, 2021

Implemented on: May 01, 2022

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

Table of Contents

GENERAL TECHNICAL REQUIREMENTS FOR VEHICLE CYBERSECURITY.....	0
TABLE OF CONTENTS	1
FOREWORD	2
INTRODUCTION	3
GENERAL TECHNICAL REQUIREMENTS FOR VEHICLE CYBERSECURITY.....	5
1 SCOPE.....	5
2 NORMATIVE REFERENCES	5
3 TERMS AND DEFINITIONS.....	5
4 ABBREVIATIONS	7
5 PROTECTED OBJECTS	8
6 TECHNICAL REQUIREMENTS	9
APPENDIX A.....	17
BIBLIOGRAPHY	22

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:

- a) Authenticity;
- b) Confidentiality;
- c) Integrity;
- d) Availability;
- e) Access controllability;
- f) Non-repudiation;
- g) Accountability;
- h) Preventability.

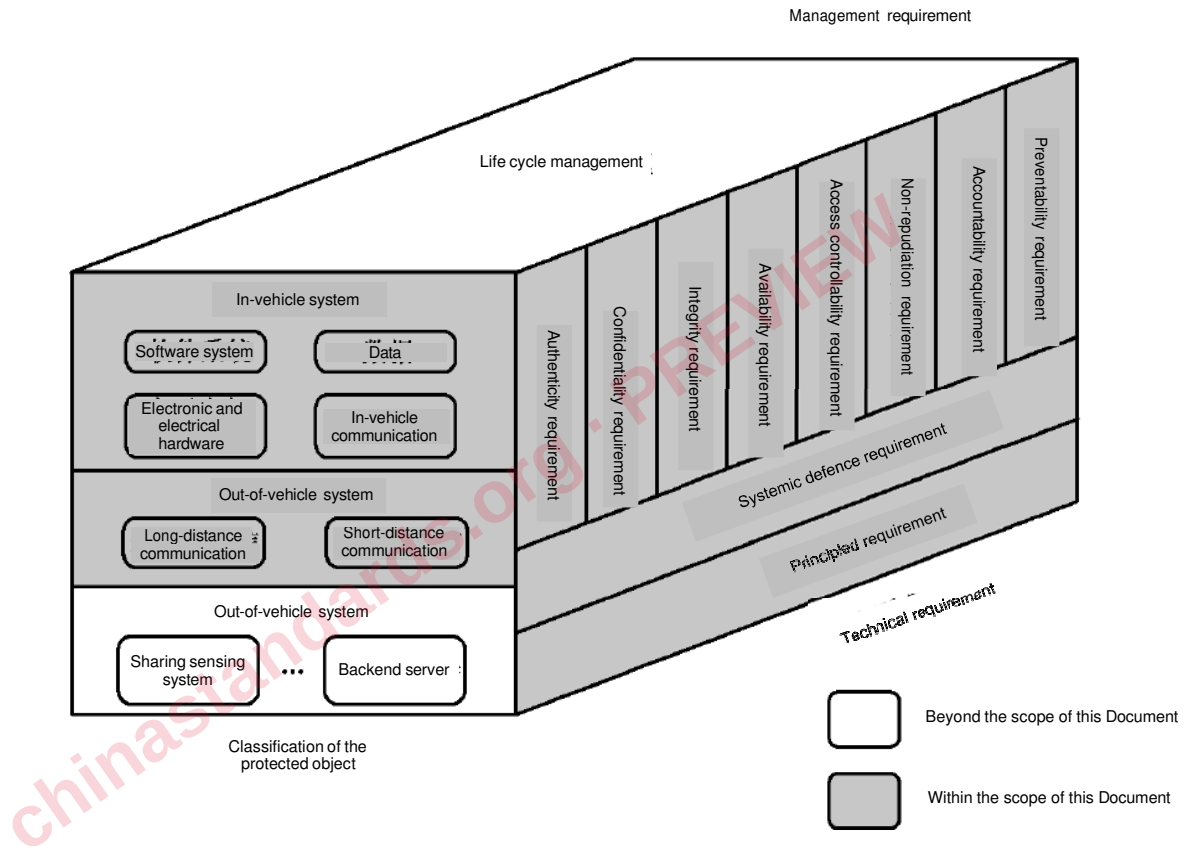


Figure 1 – Standard Framework