ICS 43.040
CCS T 35

中华人民共和国国家标准

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 43267-2023

Road Vehicles—Safety of The Intended Functionality

道路车辆 预期功能安全

(ISO 21448:2022, MOD)

Issued on 2023-11-27 **Implemented on 2023-11-27**

Jointly Issued by
State Administration for Market Regulation of the People's Republic of China &
Standardization Administration of the People's Republic of China

CONTENTS

FOREWORD

This document is 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*".

This document is modified in relation to ISO 21448:2022 "Road vehicles - Safety of the intended functionality".

With respect to ISO 21448:2022, the following structural adjustments have been made to this document:

— Figures 2 to 17 correspond to Figures 1 to 16 of ISO 21448:2022;

— Tables B.7 to B.15 correspond to Tables B.6 to B.14 of ISO 21448:2022.

The technical deviations between this document and ISO 21448:2022, together with their justifications, are as follows:

— Replaced ISO 26262 with GB/T 34590.1 ~ 34590.12-2022 in the normative references, so as to adapt to our domestic technical conditions;

— Modified the definition of "acceptance criterion" (See 3.1) to facilitate understanding of this term;

— Added the term "priority subset" and its definition (See 3.35) to facilitate supporting the SOTIF analysis, verification, validation and evaluation activities and addressing a number of scenarios and use cases;

— Added the expressions about Annex E (See 4.3.1);

— Modified the Methods for deriving verification and validation activities (See Table 6).

The following editorial changes have been made to this document:

— Added Note 2, Example 3, Notes 3 and 4 to the definition of "acceptance criterion" (See 3.1);

— Deleted the note to "DDT fallback" and "fallback ready user", Note 2 to "dynamic driving task", "levels of driving automation" and "scenario", Note 3 to "minimal risk condition" and "use case", Notes 2 and 4 to "operational design domain", Note 4 to "scene", and the descriptions about source of terms "hazard", "object and event detection and response", "risk", and "unreasonable risk" contained in ISO 21448:2022;

— Added Note 3 in the "Specification of the functionality and considerations for the design" (See 5.2);

— Added Notes 4 to 7 in the "Risk evaluation" (See 6.4) to facilitate understanding of acceptance criteria;

— Added Note 5 about acceptance criteria in the "Specification of acceptance criteria for the residual risk" (See 6.5) to facilitate applying and understanding how to specify the acceptance criteria for risks based on traffic data analysis;

— Added Note 3 in the "Identification and evaluation of potential functional insufficiencies and potential triggering conditions" to facilitate applying and improving the acceptance criteria;

— Deleted the note to A.3 example in ISO 21448:2022;

— Added Note 4 about Clause D.5 (See 7.3.3);

— Modified Note 3 to "Specification of integration and testing" (See 9.3);

— Added Note 6 in the "SOTIF issue evaluation and resolution process" (See 13.4);

— Added the simplified examples of specification and design (See A.4) to facilitate understanding and application;

— Added the examples of scenario priority subset based on quantity rules (See Table B.6) to facilitate understanding and application;

— Added the examples for quantification of perception system performance targets and common sensor performance insufficiencies (See D.5) to facilitate understanding and application;

— Added the SOTIF considerations for the OTA updates (See D.6) to facilitate the safety considerations

for intended functions during operation;

— Added the examples of acceptance criteria for risks of automated driving system (See Annex E) to facilitate applying and improving the acceptance criteria.

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

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

This document was prepared by SAC/TC 114 (National Technical Committee on Road Vehicles of Standardization Administration of China).

This document was drafted by China Automotive Technology Research Center Co., Ltd., China FAW Motor Corporation Limited, Huawei Technology Co., Ltd., Shanghai Shangtang Lingang Intelligent Technology Co., Ltd., FAW Volkswagen Co., Ltd., Jike Automobile (Ningbo Hangzhou Bay New Area) Co., Ltd., Shanghai Motor Vehicle Testing and Certification Technology Research Center Co., Ltd., NIO Automotive Technology (Anhui) Co., Ltd., Great Wall Motors Co., Ltd., Shanghai Haila Electronics Co., Ltd., Vinier (China) Electronics Co., Ltd., Shenzhen DJI Zhuojian Technology Co., Ltd., Beijing Hangji Technology Co., Ltd., Zhongqi Chuangzhi Technology Co., Ltd., Volkswagen (China) Investment Co., Ltd., Bosch Automotive Parts (Suzhou) Co., Ltd., Zhixing Automotive Technology (Suzhou) Co., Ltd. Company, Beijing Horizon Robotics Technology R&D Co., Ltd., FAW Jiefang Automobile Co., Ltd., Beijing Chehejia Automotive Technology Co., Ltd., Neusoft Ruichi Automotive Technology (Shanghai) Co., Ltd., Beijing Jingwei Hengrun Technology Co., Ltd., Neusoft Group Co., Ltd., Zhima Motor Automobile Co., Ltd Lantu Automobile Technology Co., Ltd., CRRC Times Electric Vehicle Co., Ltd., Shanghai Jidu Automobile Co., Ltd., BYD Automobile Industry Co., Ltd., Pan Asia Automobile Technology Center Co., Ltd., Yutong Bus Co., Ltd., Hezhong New Energy Vehicle Co., Ltd., Xiangyang Da'an Automobile Testing Center Co., Ltd., Beijing New Energy Vehicle Co., Ltd., China Changan Automobile Group Co., Ltd., Guangzhou Automobile Group Co., Ltd., Yikatong (Hubei) Technology Co., Ltd., Suzhou Bowo Innovative Energy Technology Co., Ltd., Chongqing Changan Automobile Software Technology Co., Ltd., Geely Automobile Research Institute (Ningbo) Co., Ltd., Shanghai Hesai Technology Co., Ltd., United Automotive Electronics Co., Ltd., Beijing National New Energy Vehicle Technology Innovation Center Co., Ltd., Beijing Baidu Zhixing Technology Co., Ltd., and Shanghai NIO Automotive Co., Ltd.

Chief drafters of this document are Li Bo, Shang Shiliang, Liu Hang, Bai Xiaoyu, Liu Yu, Fu Yue, Zhou Lin, Wang Yu, Wang Xiaoyi, Zhang Weiqian, Wang Jiahao, Wu Yuecui, Ma Ting, Yu Jianye, Han Wenhao, Liu Hui, Fu Chaoying, Chen Rui, Zhang Liuyang, Rong Hui, Ma Kai, Qu Yuanning, Song Weijin, Yang Hu, Yu Bo, Zhang Lijun, Wang Fangfang, Wen Jiwei, Chen Wei, Gao Jianyong, Li Chunlin, Qian Kun, Xie Yuliu, Li Yong Li Hongpeng, Zheng Tong, Xia Xianzhao, Zhang Hongwei, Chen Yili, Zhang Li, Li Zhenzhen, Liu Fabiao, Li Guilan, Gao Hailong, Wang Haichuan, Shao Haihe, Fu Yuhan, Guo Kuiyuan, Shi Juan, Liang Yu, Guo Xiaodong, Zhao Jinfu, Chen Yong, Zhou Hongwei, Wang Jianbin, Ren Xianan, Zhao Xin, Zheng Yan, Li Zhaolin, Jia Yuanhui, Xu Dawei, and Huang Yi.

INTRODUCTION

The safety of road vehicles is a concern of paramount importance for the road vehicle industry. The number of automated driving functionalities included in vehicles is increasing. These rely on sensing, processing of complex algorithms and actuation implemented by electrical and/or electronic (E/E) systems.

An acceptable level of safety for road vehicles refers to the absence of unreasonable risk caused by any hazard associated with the intended functionality and its implementation, including both hazards due to failures and due to insufficiencies of specification or performance insufficiencies.

For the achievement of functional safety, GB/T 34590.1-2022 defines functional safety as the absence of unreasonable risk due to hazards caused by malfunctioning behavior of the E/E system. GB/T 34590.3-2022 describes how to conduct a hazard analysis and risk assessment (HARA) to determine vehicle-level hazards and associated safety goals. The other parts of GB/T 34590 provide the requirements and recommendations to avoid and control random hardware failures and systematic failures that could violate safety goals.

For some E/E systems, e.g., systems which rely on sensing the external or internal vehicle environment to build situational awareness, the intended functionality and its implementation can cause hazardous behavior, despite these systems being free from the faults addressed in GB/T 34590 (all parts). Example causes of such potentially hazardous behavior include:

— the inability of the function to correctly perceive the environment;

— the lack of robustness of the function, system, or algorithm with respect to sensor input variations, heuristics used for fusion, or diverse environmental conditions;

— the unexpected behavior due to decision making algorithm and/or divergent human expectations.

In particular, these factors are relevant to functions, systems or algorithms that use machine learning.

The absence of unreasonable risk resulting from hazardous behaviors related to functional insufficiencies is defined as the safety of the intended functionality (SOTIF). Functional safety [addressed by GB/T 34590 (all parts)] and the SOTIF are complementary aspects of safety (see A.2 for a better understanding of the respective scopes of GB/T 34590 (all parts) and this document).

To address the SOTIF, measures to eliminate hazards or reduce risks are implemented during the following phases:

— the specification and design phase;

Example 1: Modification of vehicle functionality or of sensor performance requirements, driven by identified system insufficiencies or by hazardous scenarios identified during the SOTIF activities.

— the verification and validation phase;

Example 2: Technical reviews, test cases with a high coverage of relevant scenarios, injection of potential triggering conditions, In-the-loop testing [e.g., software in the loop (SIL), hardware in the loop (HIL), model in the loop (MIL) of selected SOTIF-relevant scenarios.

Example 3: Long-term vehicle road testing, test-track vehicle testing, simulation testing.

— the operation phase.

Example 4: Field monitoring of SOTIF incidents.

These hazards can be triggered by specific conditions (i.e., triggering conditions) of a scenario, which can include reasonably foreseeable misuse of the intended functionality. Additionally, the interaction with other functions at the vehicle level can lead to hazards (e.g., activation of the parking brake while the automated driving function is active).

Therefore, a proper understanding by the user of the functionality, its behavior and its limitations (including the human/machine interface) is essential to ensure safety.

Example 5: Lack of driver attention while using a L2 automated driving system.

Example 6: Mode confusion (e.g., the driver thinks the function is activated when it is deactivated) can directly lead to a hazard.

Note 1: Reasonably foreseeable misuse excludes intentional alterations made to the system's operation.

Information provided by the infrastructure [e.g., Vehicle2Everything (V2X), maps) is also part of the evaluation of functional insufficiencies if it can have an impact on the SOTIF. See D.4 for guidance on V2X features.

Example 7: For automated valet parking systems, the functionalities of route planning and object detection could be achieved jointly by the infrastructure and the vehicle.

Note 2: Depending on the application, elements of other technologies can be relevant when evaluating the SOTIF.

Example 8: The location and mounting of a sensor on the vehicle can be relevant to avoid noisy sensor output resulting from vibration.

Example 9: The windshield optical properties can be relevant when evaluating the SOTIF of a camera sensor.

With respect to the random hardware faults and systematic faults (including hardware and software faults) of the E/E system, GB/T 34590 (all parts) gives the guidance on reducing risks.

The functional insufficiencies mentioned in this document may be considered as systematic faults. However, the measures to address these functional insufficiencies are specific to this document and complementary to those described in GB/T 34590 (all parts). Specifically, GB/T 34590 (all parts) assumes that the intended functionality is safe, and addresses E/E system faults that can cause hazards due to a deviation from the intended functionality. The requirement-elicitation process for the system and its elements can include aspects of both standards.

Table 1 illustrates the mapping relation between the possible causes of hazardous events and existing standards.

Table 1 Overview of safety relevant topics addressed by different standards

Source of hazard	Cause of hazardous events	Corresponding standard
System	E/E system faults	GB/T 34590 (all parts)
	Functional insufficiencies	This document
	Incorrect and inadequate Human-Machine Interface (HMI) design (inappropriate user situational awareness, e.g., user confusion, user overload, user inattentiveness)	This document European Statement of Principles on human-machine interface [26]
	Functional insufficiencies of artificial intelligence-based algorithms	This document
	System technologies Example: Eye damage from the beam of a lidar.	Specific standards Example: IEC 60825
External factor	Reasonably foreseeable misuse by the user or by other road participants	This document GB/T 34590 (all parts)
	Attack exploiting vehicle cybersecurity vulnerabilities	ISO/SAE 21434
	Impact from intelligent infrastructure and/or vehicle to vehicle communication, and external systems	This document ISO 20077, GB/T 34590 (all parts), GB/T 20438
	Impact from vehicle surroundings (e.g., other users, nonintelligent infrastructure, weather, electromagnetic interference)	This document GB/T 34590 (all parts), ISO 7637-2, ISO 7537-3, ISO 11452-2, ISO 11452-4, ISO 10605 and other standards

Road Vehicles—Safety of The Intended Functionality

1 SCOPE

This document provides a general argument framework and guidance on measures to ensure the safety of the intended functionality (SOTIF), which is the absence of unreasonable risk due to a hazard caused by functional insufficiencies, including:

a) the insufficiencies of specification of the intended functionality at the vehicle level;

b) the insufficiencies of specification or performance insufficiencies in the implementation of electric and/or electronic (E/E) elements in the system.

This document provides guidance on the applicable design, verification and validation measures, as well as activities during the operation phase, that are needed to achieve and maintain the SOTIF.

This document is applicable to intended functionalities where proper situational awareness is essential to safety and where such situational awareness is derived from complex sensors and processing algorithms, especially functionalities of emergency intervention systems and systems having levels of driving automation from L1 to L5.

This document is applicable to intended functionalities that include one or more E/E systems installed in series production road vehicles, excluding mopeds.

Reasonably foreseeable misuse is in the scope of this document. In addition, operation or assistance of a vehicle by a remote user or communication with a back office that can affect vehicle decision making is also in scope of this document when it can lead to safety hazards.

This document does not apply to:

— faults covered by GB/T 34590 (all parts);

— cybersecurity threats;

— hazards directly caused by the system technology (e.g., eye damage from the beam of a lidar);

— hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, release of energy and similar hazards, unless directly caused by the intended functionality of E/E systems;

— deliberate actions that clearly violate the system's intended use (which are considered feature abuse).

2 NORMATIVE REFERENCES

The following normative documents contain provisions which, through normative reference in this text, constitute essential provision of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendment) applies.

GB/T 34590 (all parts) Road vehicles - Functional safety

GB/T 34590.1-2022 Road vehicles - Functional safety - Part 1: Vocabulary

3 TERMS AND DEFINITIONS

For the purpose of this document, the terms and definitions given in GB/T 34590.1-2022 and the following apply.

3.1 acceptance criterion

criterion representing the absence of an unreasonable level of risk (3.23)

Note 1: The acceptance criterion can be of qualitative as well as quantitative nature, e.g., physical parameters that define when a specific behavior is considered as hazardous behavior, maximum

The following pages are left blank intentionally.