GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 43.040

CCS T 35

GB/T 43267-2023

Road vehicles - Safety of the intended functionality

(ISO 21448:2022, MOD)

道路车辆 预期功能安全

Issued on: November 27, 2023 **Implemented on: November 27, 2023**

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 provided in GB/T 1.1-2020 *Directives for standardization - Part 1: Rules for the structure and drafting of standardizing documents*.

This document modifies using ISO 21448:2022 *Road vehicles - Safety of the intended functionality*.

Compared with ISO 21448:2022, this document makes the following structural adjustments:

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

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

The technical differences between this document and ISO 21448:2022 and their reasons are as follows:

— Replace ISO 26262-1 with the normatively referenced GB/T 34590.1 ~ 34590.12-2022 to adapt to the technical conditions in our country;

— Change the definition of the term “acceptance criterion” (see 3.1) to make it easier to understand the term;

— Add the term “priority subset” and its definition (see 3.35) to help support SOTIF analysis, verification and validation, as well as evaluation activities to deal with a large number of scenarios and use cases;

— Add description about Annex E (see 4.3.1);

— Change methods for deriving verification and validation activities (see Table 6).

This document also makes the following editorial modifications:

— Add Note 2, Example 3, Note 3 and Note 4 to the definition of the term “acceptance criterion” (see 3.1);

— Remove some notes in ISO 21448:2022, i.e., Note of the terms “DDT fallback” and “fallback ready user”; Note 2 of the terms “dynamic driving task; DDT”, “levels of driving automation” and “scenario”; Note 3 of the terms “minimal risk condition; MRC” and “use case”; Note 2 and Note 4 of the term “operational design domain; ODD”; Note 4 of the term “scene”; as well as description of the source of the terms “hazard”, “object and event detection and response; OEDR”, “risk” and “unreasonable risk”;

— Add Note 3 to the specification of the functionality and considerations for the design (see 5.2);

— Add Notes 4 ~ 7 to the risk evaluation (see 6.4) to facilitate understanding of the acceptance criterion;

— Add Note 5 on acceptance criteria in the specification of acceptance criteria for the residual risk (see 6.5), which helps to apply and understand how to define risk acceptance criteria based on traffic data analysis;

— Add Note 3 to the objectives of identification and evaluation of potential functional insufficiencies and potential triggering conditions (see 7.1) to help apply and improve the acceptance criteria;

— Remove the note of the example in A.3 of ISO 21448:2022;

— Add Note 4 regarding the content of D.5 (see 7.3.3);

— Change Note 3 of the specification of integration and testing (see 9.3);

— Add Note 6 to SOFIT issue evaluation and resolution process (see 13.4);

— Add simplified examples of specification and design (see A.4) to facilitate understanding and application;

— Add examples of scenario priority subsets based on quantitative rules (see Table B.6) to facilitate understanding and application;

— Add perception system performance target quantification and examples of common sensor performance limitations (see D.5) to facilitate understanding and application;

— Add SOTIF considerations for OTA updates (see D.6), which helps SOTIF consideration during operation;

— Add examples of risk acceptance criteria for autonomous driving systems (see Annex E) to facilitate the application and improvement of the acceptance criteria.

Please note that some of the contents of this document may involve patents. The issuing organizations of this document are 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).

Drafting organizations of this document: China Automotive Technology and Research Center Co., Ltd., FAW Car Co., Ltd., Huawei Technologies Co., Ltd., Shanghai

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, i.e.:

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

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 in scope of this document when it can lead to safety hazards.

This document does not apply to:

— faults covered by the 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; and

— the mechanism, design and requirements that support risk mitigation abilities during operation.

Note 3: A.4 gives simplified examples of specification and design framework.

5.3 System design and architecture considerations

The specification and design provide an adequate understanding of the system, its elements, its functionality and the performance targets, so that the activities in subsequent phases can be performed. This includes an exhaustive list of known functional insufficiencies, related triggering conditions and, where applicable, their countermeasures. Some potential functional insufficiencies, triggering conditions and countermeasures are known and documented before the SOTIF-related process begins while others are revealed as a result of the SOTIF activities. The system is designed such that countermeasures are implemented to mitigate the effect of known functional insufficiencies on the overall system.

Each iteration of the SOTIF-related activity (see Figure 11) can result in engineering activities which can lead to updates in the specification and design at any relevant level. Each iteration relies on the specification and design being updated at any relevant level, such that it reflects all information discovered in previous iterations.

Cooperation among development parties [Original Equipment Manufacturer (OEM), Tier 1, Tier N] is necessary to discover potential functional insufficiencies of the integrated system, component or element, and to develop countermeasures to these insufficiencies during the development phases (see 4.4). Relevant sections of design and specification are communicated to lower-level system and component developers. Assumptions of use, foreseeable misuse and potential performance insufficiencies are communicated from one tier to the next hierarchical levels, up to and including the OEM, after each development cycle/ iteration.

As the SOTIF activities identify new functional insufficiencies and triggering conditions (see Clause 7), and measures to improve the SOTIF are defined (see Clause 8), the specification and design is updated as part of each development cycle as seen in Figure 11.

SOTIF work products are linked with the specification and design if they impact the specification and design (as defined in 5.2), including pre-existing relevant content. This ensures that all information from previous iterations is captured, and that the specification is ready for the next iteration cycle.

Note: Traceability and completeness of the specification and design (work products 5.5) can be demonstrated by linking to SOTIF measures (work products 8.5) which can be further linked with:

— the relevant design document(s);

This is an excerpt of the PDF (Some pages are marked off intentionally)

Full-copy PDF can be purchased from 1 of 2 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

Accountable person and shareholder: Wayne Zheng

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

------ The End ------