GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 43.040

CCS T 35

GB/T 34590.10-2022

Replacing GB/T 34590.10-2017

Road Vehicles - Functional Safety - Part 10: Guideline

道路车辆 功能安全 第 10 部分：指南

(ISO 26262-10:2018, Road Vehicles – Functional Safety – Part 10: Guidelines on ISO 26262, MOD)

Issued on: December 30, 2022 **Implemented on: July 1, 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 is Part 10 of GB/T 34590 *Road Vehicles - Functional Safety*. GB/T 34590 has issued the following parts:

--- Part 1: Vocabulary;

--- Part 2: Management of Functional Safety;

--- Part 3: Concept Phase;

--- Part 4: Product Development at the System Level;

--- Part 5: Product Development at the Hardware Level;

--- Part 6: Product Development at the Software Level;

--- Part 7: Production, Operation, Service and Decommissioning;

--- Part 8: Supporting Processes;

--- Part 9: Automotive Safety Integrity Level (ASIL)-oriented and Safety-oriented Analyses;

--- Part 10: Guideline;

--- Part 11: Guidelines on Applications to Semiconductors;

--- Part 12: Adaptation for Motorcycles.

This Document replaced GB/T 34590.10-2017 *Road vehicles - Functional safety - Part 10: Guideline*. Compared with GB/T 34590.10-2017, the major technical changes of this Document are as follows besides the structural adjustment and editorial modifications:

--- Change the scope of application of the standard from "mass-produced passenger cars" into "mass-produced road vehicles other than mopeds"; and modify the description of the scope (see Clause 1 of this Edition; Clause 1 of 2017 Edition);

--- Add "FTTI and emergency operation fault tolerance time interval" (see 4.4 of this Edition);

--- Change the description of the general provisions of the accreditation measures (see 5.2.1 of this Edition; 5.2.1 of 2017 Edition);

--- Change the description of functional safety assessment (see 5.2.2 of this Edition; 5.2.2 of 2017 Edition);

--- Change the description of the understanding of the safety profile (see 5.3 of this Edition; 5.3 of 2017 Edition);

--- Change the description in Figure 8 (see Figure 8 of this Edition; Figure 7 of 2017 Edition);

--- Change the description in Figure 9 (see Figure 9 of this Edition; Figure 8 of 2017 Edition);

--- Change the description of the consideration of exposure duration in the calculation of the probability measure of random hardware failure (PMHF) (see 8.3.2.2 of this Edition; 8.3.3 of 2017 Edition);

--- Add "typical dual-point failure mode (intended function and safety mechanism)" (see 8.3.2.3 of this Edition);

--- Add "calculation formula" (see 8.3.2.4 of this Edition);

--- Add "PMHF unit --- average probability per hour (see 8.4 of this Edition);

--- Add "Guidelines for the development of systems with safety-related availability requirements" (see Clause 12 of this Edition);

--- Delete Annex A of 2017 edition.

This Document modifies and adopts ISO 26262-10:2018 *Road Vehicles – Functional Safety – Part 10: Guidelines on ISO 26262*.

The technical differences and causes between this Document and ISO 26262-10:2018 are as follows:

--- Change the subclause structure of 13.3 (see 13.3) [Translator Note: here it shall be 12.3]; so that the subclause structure is more rational.

This Document made the following editorial modifications:

--- Change the paragraph sequence of the Scope;

--- Delete the title of 4.3.1.

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 the Ministry of Industry and Information Technology of PRC.

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

Drafting organizations of this Document: China Automotive Technology and Research Center Co., Ltd.; Pan Asia Technical Automotive Center Co., Ltd.; China FAW Group Co., Ltd.; Hella

Road Vehicles - Functional Safety - Part 10: Guideline

1 Scope

This Document provides an overview of the GB/T 34590 series of standards, as well as giving additional explanations, and is intended to enhance the understanding of the other parts of this series of standards. This Document has an informative character only and describes the general concepts of the GB/T 34590 series of standards in order to facilitate comprehension. The explanation expands from general concepts to specific contents.

This Document is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles, excluding mopeds.

This Document does not address unique E/E systems in special vehicles such as E/E systems designed for drivers with disabilities.

NOTE: Other dedicated application-specific safety standards exist and can complement the ISO 26262 series of standards or vice versa.

Systems and their components released for production, or systems and their components already under development prior to the publication date of this document, are exempted from the scope of this edition. This Document addresses alterations to existing systems and their components released for production prior to the publication of this document by tailoring the safety lifecycle depending on the alteration. This Document addresses integration of existing systems not developed according to this document and systems developed according to this Document by tailoring the safety lifecycle.

This Document addresses possible hazards caused by malfunctioning behavior of safety-related E/E systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behavior of safety-related E/E systems.

This Document describes a framework for functional safety to assist the development of safety-related E/E systems. This framework is intended to be used to integrate functional safety activities into a company-specific development framework. Some requirements have a clear technical focus to implement functional safety into a product; others address the development process and can therefore be seen as process requirements in order to demonstrate the capability of an organization with respect to functional safety.

This document does not address the nominal performance of E/E systems.

In the case of inconsistencies between this Document and another part of the GB/T 34590 series of standards, the requirements, recommendations and information specified in the other part of the GB/T 34590 series of standards apply.

2 Normative References

The provisions in following documents become the essential 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.

GB/T 34590.1-2022 Road Vehicles - Functional Safety - Part 1: Vocabulary (ISO 26262-1:2018, MOD)

NOTE: The contents quoted from GB/T 34590.1-2022 have no technical differences with the contents quoted from ISO 26262-1:2018.

3 Terms and Definitions

For the purposes of this Document, the terms and definitions given in GB/T 34590.1-2022 apply.

4 Key Concepts of GB/T 34590

4.1 Functional safety for automotive systems (relationship with GB/T 20438)

GB/T 20438, Functional Safety of electrical/electronic/programmable electronic safety-related systems, is designated by IEC as a generic standard and a basic safety publication. This means that industry sectors will base their own standards for functional safety on the requirements of GB/T 20438.

In the automotive industry, there are a number of issues with applying GB/T 20438 directly. Some of these issues and corresponding differences in the GB/T 34590 series of standards are described below.

GB/T 20438 is based upon the model of “equipment under control”, for example an industrial plant that has an associated control system as follows:

a) A hazard analysis identifies the hazards associated with the equipment under control (including the equipment control system), to which risk reduction measures will be applied. This can be achieved through electrical/electronic/programmable electronic (E/E/PE) systems, or other technology safety-related systems (e.g., a safety valve), or external measures (e.g. a physical containment of the plant). The GB/T 34590 series of standards contains a normative automotive scheme for hazard classification based on

5.2.2 Functional safety assessment

If the highest ASIL of the item's safety goals is ASIL C or D, a functional safety assessment is performed to evaluate an item's achievement of functional safety. In GB/T 34590.2-2022, certain aspects of a functional safety assessment are described as well as further aspects of confirmation measures.

The scope of the functional safety assessment is defined in GB/T 34590.2-2022, Clause 6.

In the case a functional safety assessment is performed, the results of the functional safety audit and of the confirmation reviews are an input for the functional safety assessment. The person responsible for the assessment can perform the assessment according to his/her discretion, including how to make use of the results of the functional safety audit and confirmation reviews.

EXAMPLE 1: If the results of the functional safety audit are satisfactory, the person responsible for the functional safety assessment can decide to rely on the results of the audit, without making a further judgement of the implementation of the processes required for functional safety.

EXAMPLE 2: Based on the confirmation review report of a particular work product, the person responsible for the assessment can decide to perform, or to request, a more in-depth review of certain aspects of that work product, or can check whether the confirmation review sufficiently considered the interplay between that work product and related work products.

NOTE 1: It is possible that the person responsible for the functional safety assessment performs a particular confirmation review i.e., a confirmation review is not necessarily performed by a person different from the person responsible for the assessment.

The assessment on functional safety may be repeated or updated.

EXAMPLE 3: A functional safety assessment update because of a change of the item, or element(s) of the item, which is identified by the change management as having an impact on the functional safety of the item (see GB/T 34590.8-2022, Clause 8).

EXAMPLE 4: A functional safety re-assessment that is triggered by a functional safety assessment report that recommends a conditional acceptance or a rejection of the item's functional safety. In this case, the iteration includes a follow-up of the recommendations resulting from the previous functional safety assessment(s), including an evaluation of the performed corrective actions, if applicable.

If the highest ASIL of the item's safety goals is ASIL A or ASIL B, a functional safety assessment can be omitted or performed less rigorously. However, even if the functional safety assessment is not performed, other confirmation measures are still performed (see GB/T 34590.2-2022, Table 1).

In the case of a distributed development, the scope of a functional safety assessment includes the work products generated, and the processes and safety measures implemented, by a vehicle manufacturer and the suppliers in the item's supply chain (see GB/T 34590.2-2022 and GB/T 34590.8-2022, Clause 5).

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

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