GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 43.040

CCS T 35

GB/T 34590.4-2022

Replacing GB/T 34590.4-2017

Road Vehicles - Functional Safety -

Part 4: Product development at the system level

道路车辆 功能安全 第 4 部分：产品开发：系统层面

(ISO 26262-4:2018, 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 4 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 serves as a replacement of GB/T 34590.4-2017 *Road Vehicles - Functional Safety - Part 4: Product development at the system level*. In comparison with GB/T 34590.4-2017, apart from structural adjustments and editorial modifications, the main technical changes are as follows:

-- MODIFY the Scope, from “series production passenger cars” into “series production road vehicles, excluding mopeds” (see Clause 1; Clause 1 of Version 2017);

-- ADD the adaptation for motorcycles (see 4.5);

-- ADD the adaptation for trucks, buses, trailers and semi-trailers (see 4.6);

-- MODIFY the content of Clause 5, from “Product development at the starting system level” into “General topics for the product development at the system level” (see Clause 5; Clause 5 of Version 2017);

-- MODIFY the objectives of Clause 5 (see 5.1; 5.1 of Version 2017);

-- DELETE the content of "Inputs of this clause", "Requirements and suggestions", "Work products" in Clause 5 (see 5.3, 5.4, 5.5 of Version 2017);

-- MODIFY the content of Clauses 6 and 7 of Version 2017, refining the development objectives of the technical safety concept phase (see 6.1; 6.1, 7.1 of Version 2017);

-- MODIFY the description of the general principles of the technical safety concept (see 6.2; 6.2 of Version 2017);

-- MODIFY the requirements for the specification of the technical safety requirements (see 6.4.1; 6.4.1 of Version 2017);

-- MODIFY the requirements for the specification of the safety mechanism (see 6.4.2; 6.4.2 of Version 2017);

-- DELETE the content corresponding to ASIL decomposition (see 6.4.3 of Version 2017);

-- ADD the objectives of safety analyses on the system architectural design (see 6.4.4.1);

-- DELETE the relevant content and tables of the attributes of the modular system design (see 7.4.3.7 of Version 2017);

-- MODIFY the requirements for production, service, operation and decommissioning (see 6.4.8; 7.4.7 of Version 2017);

-- DELETE the relevant content and tables of the verification of the system design (see 7.4.8 of Version 2017);

-- ADD the relevant content and requirements of the system phase verification (see 6.4.9.2);

-- MODIFY the objectives of the system and item integration and testing (see 7.1; 8.1 of Version 2017);

-- DELETE the description of "the effectiveness of diagnostics or failure coverage of safety mechanisms" in the integration and testing strategy (see 7.4.1.1);

-- MODIFY the content of "the effectiveness of diagnostics or failure coverage of safety mechanisms" at the system level and the vehicle level (see Table 10, Table 14; Table 11, Table 16 of Version 2017);

-- MODIFY the objectives of safety validation (see 8.1; 9.1 of Version 2017);

-- ADD the safety validation environment (see 8.4.1);

-- MODIFY the description of the validated plan, into the "specification of safety validation" (see 8.4.2; 9.4.2 of Version 2017);

-- DELETE the validation of random hardware failure measurement at the item level (see 9.4.3.3 of Version 2017);

-- DELETE the relevant content of functional safety assessment and production release (see Clause 10 and Clause 11 of Version 2017).

This document has been modified using ISO 26262-4:2018 *Road Vehicles - Functional Safety - Part 4: Product development at the system level*.

The technical differences between this document and ISO 26262-4:2018, and the causes for these differences are as follows:

-- MODIFY the description of T&B vehicles, from “trucks, buses, trailers and semi-trailers” into “goods vehicles, buses, special vehicles and trailers” (see 4.6; 4.6 of ISO 26262-4:2018), so as to maintain the consistency with the vehicle types specified GB/T 3730.1-2022 *Terms and Definitions of Motor Vehicles, Trailers and Combination vehicle - Part 1: Types*.

This document also makes the following editorial modifications:

-- MODIFY the introduction and expression of the international standard.

Please be noted that certain content of this document may involve patents. The institution issuing this document does not undertake the responsibility of identifying these 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 114 on Auto of Standardization Administration of China (SAC/TC 114).

The drafting organizations of this document: China Automotive Technology and Research Center Co., Ltd.; BYD Auto Industry Co., Ltd.; Nexteer Automotive (Suzhou) Co., Ltd.; Huawei Technologies Co., Ltd.; Schaeffler (China) Co., Ltd.; NIO Automobile (Anhui) Co., Ltd.; SAIC VOLKSWAGEN Co., Ltd.; NIO Inc.; Pan Asia Technical Automotive Center Co., Ltd.; United Automotive Electronic Systems; FAW Jiefang Automotive Company; JTEKT Research and Development Center (Wuxi) Co., Ltd.; Beijing Borgward Automotive Co., Ltd.; Beijing Horizon Robotics Technology R&D Co., Ltd.; Infineon Technology (China) Co., Ltd.; Shanghai G-PULSE Electronics Technology Co., Ltd.; iMotion Automotive Technology (Suzhou) Co., Ltd.; Hitachi Astemo Automotive Systems (Shanghai) Co., Ltd.; SINCODE Technology (Taizhou) Co., Ltd.; Shanghai SenseTime Lingang Intelligent Technology Co., Ltd.; Hella Shanghai Electronics Co., Ltd.; Hubei ECARX Technologies Co., Ltd.; Dongfeng Motor Group Co., Ltd.; Technology Center of SAIC Motor Co., Ltd.; SAIC GM Wuling Automobile Co., Ltd.; Shanghai NIO Automobile Co., Ltd.; Daimler Greater China Ltd.; BOSCH Auto Parts (Suzhou) Co., Ltd.; China FAW Group Co., Ltd.; Shanghai Hesai Technology Co., Ltd.; Dongfeng Liuzhou Automobile Co. Ltd.; Neusoft (Dalian) Corporation; Great Wall Motor Co., Ltd.; Suzhou Inovance United Power System Co., Ltd.; BAIC BJEV Co., Ltd.; YUTONG

Road vehicles - Functional safety -

Part 4: Product development at the system level

1 Scope

This document specifies the requirements for product development at the system level for automotive applications, including the following:

-- general topics for the initiation of product development at the system level;

-- specification of the technical safety requirements;

-- the technical safety concept;

-- system architectural design;

-- item integration and testing; and

-- safety validation.

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 this document 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 behaviour 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 behaviour 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.

Annex A provides an overview on objectives, prerequisites and work products of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 34590.1-2022 *Road vehicles - Functional safety - Part 1: Vocabulary* (ISO 26262-1:2018, MOD)

NOTE: There is no technical difference between the referenced content of GB/T 34590.1-2022 and the referenced content of ISO 26262-1:2018.

GB/T 34590.2-2022 *Road vehicles - Functional safety - Part 2: Management of functional safety* (ISO 26262-2:2018, MOD)

NOTE: There is no technical difference between the referenced content of GB/T 34590.2-2022 and the referenced content of ISO 26262-2:2018.

GB/T 34590.3-2022 *Road vehicles - Functional safety - Part 3: Concept phase* (ISO 26262-3:2018, MOD)

NOTE: There is no technical difference between the referenced content of GB/T 34590.3-2022 and the referenced content of ISO 26262-3:2018.

GB/T 34590.5-2022 *Road vehicles - Functional safety - Part 5: Product development at the hardware level* (ISO 26262-5:2018, MOD)

NOTE: There is no technical difference between the referenced content of GB/T 34590.5-2022 and the referenced content of ISO 26262-5:2018.

GB/T 34590.6-2022 *Road vehicles - Functional safety - Part 6: Product development at the software level* (ISO 26262-6:2018, MOD)

NOTE: There is no technical difference between the referenced content of GB/T 34590.6-2022 and the referenced content of ISO 26262-6:2018.

GB/T 34590.7-2022 *Road vehicles - Functional safety - Part 7: Production, operation, service and decommissioning* (ISO 26262-7:2018, MOD)

NOTE: There is no technical difference between the referenced content of GB/T 34590.7-2022 and the referenced content of ISO 26262-7:2018.

GB/T 34590.8-2022 *Road vehicles - Functional safety - Part 8: Supporting processes* (ISO 26262-8:2018, MOD)

NOTE: There is no technical difference between the referenced content of GB/T 34590.8-2022 and the referenced content of ISO 26262-8:2018.

GB/T 34590.9-2022 *Road vehicles - Functional safety - Part 9: Automotive Safety Integrity Level (ASIL) -oriented and safety-oriented analyses* (ISO 26262-9:2018, MOD)

NOTE: There is no technical difference between the referenced content of GB/T 34590.9-2022 and the referenced content of ISO 26262-9:2018.

3 Terms and definitions

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

4 Requirements

4.1 Purpose

This clause describes how:

a) to achieve compliance with the GB/T 34590 series of standards;

b) to interpret the tables used in the GB/T 34590 series of standards; and

c) to interpret the applicability of each clause, depending on the relevant ASIL(s).

4.2 General requirements

When claiming compliance with the GB/T 34590 series of standards, each requirement shall be met, unless one of the following applies:

a) tailoring of the safety activities in accordance with GB/T 34590.2-2022 has been performed that shows that the requirement does not apply; or

b) a rationale is available that the non-compliance is acceptable and the rationale has been evaluated in accordance with GB/T 34590.2-2022.

Informative content, including notes and examples, is only for guidance in understanding, or

a) the target values of the metrics in GB/T 34590.5-2022, Clause 8; and

b) the procedures in GB/T 34590.5-2022, Clause 9.

6.4.5.4 This requirement applies to ASILs (B), C, and D. For distributed developments (see GB/T 34590.8-2022, Clause 5) the derived target values shall be communicated to each relevant party.

NOTE: Architectural constraints described in GB/T 34590.5-2022, Clauses 8 and 9, are not necessarily applicable to COTS parts and components. This is because suppliers usually cannot foresee the usage of their products in the end-item and the potential safety implications. In such a case, basic data such as failure rate, failure modes, failure rate distribution per failure modes, built-in diagnostics, etc. are made available by the supplier in order to allow the estimation of architectural constraints at overall hardware architecture level.

6.4.6 Allocation to hardware and software

6.4.6.1 The technical safety requirements shall be allocated to the system architectural design elements with system, hardware or software as the implementing technology.

NOTE: If the requirements are allocated to system as implementing technology, GB/T 34590.4-2022 is used again for further development of these requirements until they can be allocated to hardware and software.

6.4.6.2 The allocation and partitioning decisions shall comply with the system architectural design.

NOTE: To achieve independence and to avoid propagation of failures, the system architectural design can implement the partitioning of functions and components.

6.4.6.3 Each system architectural design element shall inherit the highest ASIL from the technical safety requirements that it implements.

6.4.6.4 If a system architectural design element is comprised of sub-elements with different ASILs assigned, or of safety-related and non-safety-related sub-elements, then each of these shall be treated in accordance with the highest ASIL, unless the criteria for coexistence (in accordance with GB/T 34590.9-2022, Clause 6) are met.

6.4.6.5 If technical safety requirements are allocated to custom hardware elements that incorporate programmable behaviour (such as ASICs, FPGA or other forms of digital hardware) an adequate development process, combining requirements from GB/T 34590.5-2022 and GB/T 34590.6-2022, shall be defined and implemented.

NOTE 1: The evidence of compliance with an allocated safety requirement for some of those hardware elements can be provided through evaluation methods in accordance with GB/T 34590.8-2022, Clause 13, if the criteria for applying this clause are met.

NOTE 2: Guidance can be found in GB/T 34590.11-2022.

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

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