ICS 43.040
CCS T 35

中华人民共和国国家标准

GB/T 34590.5—2022
代替 GB/T 34590.5—2017

道路车辆　功能安全
第5部分：产品开发：硬件层面

Road vehicles—Functional safety—
Part 5：Product development at the hardware level

（ISO 26262-5：2018，MOD）

2022-12-30 发布　　2023-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 34590《道路车辆　功能安全》的第5部分。GB/T 34590已经发布了以下部分：

——第1部分：术语；

——第2部分：功能安全管理；

——第3部分：概念阶段；

——第4部分：产品开发：系统层面；

——第5部分：产品开发：硬件层面；

——第6部分：产品开发：软件层面；

——第7部分：生产、运行、服务和报废；

——第8部分：支持过程；

——第9部分：以汽车安全完整性等级为导向和以安全为导向的分析；

——第10部分：指南；

——第11部分：半导体应用指南；

——第12部分：摩托车的适用性。

本文件代替GB/T 34590.5—2017《道路车辆　功能安全　第5部分：产品开发：硬件层面》，与GB/T 34590.5—2017相比，主要技术变化如下：

——标准适用范围由“量产乘用车”更改为“除轻便摩托车外的量产道路车辆”（见第1章，2017年版的第1章）；

——增加了摩托车的适用性要求（见4.5）；

——增加了载货汽车、客车、专用汽车、挂车的适用性要求（见4.6）；

——更改了第5章的标题（见第5章，2017年版的第5章）；

——更改了关于目的的描述（见5.1，2017年版的5.1）；

——更改了图2（见5.2，2017年版的5.2）；

——删除了5.3、5.4、5.5中关于“本章输入、要求和建议、工作成果”的内容（见2017年版的附录D）；

——删除了“安全计划（细化的）”（见2017年版的6.3.1）；

——增加了硬件规范（来自外部）（见6.3.2）；

——更改了关于目的的描述（见7.1，2017年版的7.1）；

——删除了安全计划（细化的）（见2017年版的7.3.1）；

——增加了非安全相关的硬件需求规范（来自外部）（见7.3.2）；

——表1由“模块化的硬件设计原则”更改为“硬件架构设计原则”（见7.4.1.6，2017年版的7.4.1.6）；

——增加了对噪声因素的要求（见7.4.1.7）；

——增加了对ASIL（A）的要求（见7.4.3.3）；

——增加了对ASIL（A）的要求（见7.4.3.4）；

——增加了关于“按照表3中列出的硬件设计验证方法提供证据证明”的内容（见7.4.4.1）；

——增加了验证SEooC的假设的有效性的要求（见7.4.4.3）；

——增加了硬件设计过程中产生的硬件要素的生产、运行、服务和报废要求（见7.4.5.5）；

——增加了列项 a)、b)中关于“附加的安全机制”的要求(见 8.4.4);
——增加了关于 SPFM 目标值相关公式的示例(见 8.4.7);
——更改了总则的描述(见 9.2,2017 年版的 9.2);
——增加了关于“本要求的 ASIL 适用等级”的内容(见 9.4.1.1);
——增加了“证明单一硬件元器件单点故障发生概率足够低”的论据的内容(见 9.4.1.2);
——增加了“证明一个硬件元器件的残余故障发生概率足够低”的论据的内容(见 9.4.1.3);
——增加了构成相关项的多个系统的要求(见 9.4.2.3);
——删除了关于“失效率组合以及比例因子换算”的内容(见 2017 年版的 9.4.2.7);
——增加了适用的 ASIL 等级(见 9.4.3.4);
——删除了失效率换算的内容(见 2017 年版的 9.4.3.12);
——增加了双点故障可能导致的双点失效可接受的条件的要求(见 9.4.3.12);
——增加了关于“在不能满足 9.4.3.11 或 9.4.3.12 的要求的情况下导致可能的双点失效的条件”的内容(见 9.4.3.13);
——更改了第 10 章的标题(见第 10 章,2017 年版的第 10 章);
——删除了硬件安全需求规范、硬件设计规范(见 2017 年版的 10.3.1);
——删除了项目计划(细化的)(见 2017 年版的 10.3.2);
——增加了示例以及对安全相关硬件元器件的鉴定要求(见 10.4.3);
——更改了表 12 的标题(见 10.4.6,2017 年版的 10.4.6);
——增加了硬件集成和验证规范(见 10.5.1);
——删除了“启动硬件层面产品开发”的内容(见 2017 年版的第 5 章和表 A.1)。

本文件修改采用 ISO 26262-5:2018《道路车辆　功能安全　第 5 部分:产品开发:硬件层面》。

本文件与 ISO 26262-5:2018 的技术性差异及其原因如下:

——更改了对 T&B 车辆的描述,由“卡车、客车、挂车和半挂车”更改为“载货汽车、客车、专用汽车、挂车”(见 4.6,ISO 26262-5:2018 的 4.6),与 GB/T 3730.1—2022《汽车、挂车及汽车列车的术语和定义　第 1 部分:类型》中规定的车辆类型保持一致。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会(SAC/TC 114)归口。

本文件起草单位:中国汽车技术研究中心有限公司、中车时代电动汽车股份有限公司、华为技术有限公司、上海海拉电子有限公司、耐世特汽车系统(苏州)有限公司、中国第一汽车集团有限公司、上汽大众汽车有限公司、泛亚汽车技术中心有限公司、法雷奥汽车内部控制(深圳)有限公司、日立安斯泰莫汽车电子(上海)有限公司、英飞凌科技(中国)有限公司、上汽大通汽车有限公司、上海金脉电子科技有限公司、比亚迪汽车工业有限公司、宁德时代新能源科技股份有限公司、联合汽车电子有限公司、知行汽车科技(苏州)有限公司、上海汽车集团股份有限公司技术中心、株洲中车时代电气股份有限公司、长城汽车股份有限公司、宇通客车股份有限公司、舍弗勒(中国)有限公司、戴姆勒大中华区投资有限公司、北京汽车股份有限公司、北京新能源汽车股份有限公司、兴科迪科技(泰州)有限公司、惠州市亿能电子有限公司、北京华特时代电动汽车技术有限公司、合肥巨一动力系统有限公司、蜂巢能源科技有限公司、博世汽车部件(苏州)有限公司、北京宝沃汽车股份有限公司、北京百度智行科技有限公司、力高(山东)新能源技术有限公司、华霆(合肥)动力技术有限公司、爱驰汽车(上海)有限公司、北京经纬恒润科技股份有限公司、纬湃科技投资(中国)有限公司、南京芯驰半导体科技有限公司、吉利汽车研究院(宁波)有限公司、苏州汇川联合动力系统有限公司、潍柴动力股份有限公司。

本文件主要起草人：李波、李勇、魏芳、罗彦、刘航、付越、余建业、邵海贺、李军、张乐敏、尚世亮、李珍珍、杨和全、徐惠忠、李刚、张祥、毛向阳、周东东、熊再辉、赵田丽、王超、张婵、宋炜瑾、李红波、陈磊、刘庆河、李钰锐、姜兆娟、吕明、郭菲菲、李党清、钱秋华、樊耀国、庄萍、张茨、王志鹏、李哲伟、王亚丽、鲍伟、罗欢、章爱琴、王钰、王斌、黄毅、佟子谦、陈小虎、陈皎、刘畅、孙博。

本文件及其所代替文件的历次版本发布情况为：

——2017年首次发布为GB/T 34590.5—2017；

——本次为第一次修订。

引　言

ISO 26262 是以 IEC 61508 为基础，为满足道路车辆上电气/电子系统的特定需求而编写。

GB/T 34590 修改采用 ISO 26262，适用于道路车辆上由电子、电气和软件组件组成的安全相关系统在安全生命周期内的所有活动。

安全是道路车辆开发的关键问题之一。汽车功能的开发和集成强化了对功能安全的需求，以及对提供证据证明满足功能安全目标的需求。

随着技术日益复杂、软件和机电一体化的广泛应用，来自系统性失效和随机硬件失效的风险逐渐增加，这些都在功能安全的考虑范畴之内。GB/T 34590 通过提供适当的要求和流程来降低风险。

为了实现功能安全，GB/T 34590：

a) 提供了一个汽车安全生命周期（开发、生产、运行、服务、报废）的参考，并支持在这些生命周期阶段内对执行的活动进行剪裁；

b) 提供了一种汽车特定的基于风险的分析方法，以确定汽车安全完整性等级（ASIL）；

c) 使用 ASIL 等级来定义 GB/T 34590 中适用的要求，以避免不合理的残余风险；

d) 提出了对于功能安全管理、设计、实现、验证、确认和认可措施的要求；

e) 提出了客户与供应商之间关系的要求。

GB/T 34590 针对的是电气/电子系统的功能安全，通过安全措施（包括安全机制）来实现。GB/T 34590 也提供了一个框架，在该框架内可考虑基于其他技术（例如，机械、液压、气压）的安全相关系统。

功能安全的实现受开发过程（例如，需求规范、设计、实现、集成、验证、确认和配置）、生产过程、服务过程和管理过程的影响。

安全问题与常规的以功能为导向和以质量为导向的活动及工作成果相互关联。GB/T 34590 涉及与安全相关的开发活动和工作成果。GB/T 34590 包含 12 个部分。

——第 1 部分：术语。界定了 GB/T 34590 所应用的术语和定义。

——第 2 部分：功能安全管理。描述了应用于汽车领域的功能安全管理的要求，包括独立于项目的关于所涉及组织的要求（整体安全管理）以及项目特定的在安全生命周期内关于管理活动的要求。

——第 3 部分：概念阶段。描述了车辆在概念阶段进行相关项定义、危害分析和风险评估、功能安全概念的要求。

——第 4 部分：产品开发：系统层面。描述了车辆在系统层面产品开发的要求，包括启动系统层面产品开发总则、技术安全要求的定义、技术安全概念、系统架构设计、相关项集成和测试、安全确认。

——第 5 部分：产品开发：硬件层面。描述了车辆在硬件层面产品开发的要求，包括硬件层面产品开发的概述、硬件安全要求的定义、硬件设计、硬件架构度量的评估、因随机硬件故障而导致违背安全目标的评估、硬件集成和验证。

——第 6 部分：产品开发：软件层面。描述了车辆在软件层面产品开发的要求，包括软件层面产品开发的概述、软件安全要求的定义、软件架构设计、软件单元设计和实现、软件单元验证、软件集成和验证、嵌入式软件测试、可配置软件。

——第 7 部分：生产、运行、服务和报废。描述了车辆在生产、运行、服务和报废的要求，包括生产、运行、服务和报废计划及具体要求。

——第 8 部分：支持过程。描述了对支持过程的要求，包括分布式开发的接口、安全要求的定义和管理、配置管理、变更管理、验证、文档管理、使用软件工具的置信度、软件组件的鉴定、硬件要素评估、在用证明、GB/T 34590 适用范围之外应用的接口、未按照 GB/T 34590 开发的安全相关系统的集成。

——第 9 部分：以汽车安全完整性等级为导向和以安全为导向的分析。描述了关于 ASIL 剪裁的要求分解、要素共存的准则、相关失效分析、安全分析等活动的要求。

——第 10 部分：指南。目的是增强对 GB/T 34590 其他部分的理解，提供了 GB/T 34590 中的关键概念、安全管理的精选话题、概念阶段和系统开发、安全过程的要求结构（流程和顺序）、硬件开发、独立于环境的安全要素、在用证明的示例、ASIL 的分解、带安全相关可用性要求的系统、关于“所使用软件工具的置信度”的分析、安全相关的特殊特性、故障树的构建和应用等方面的指南。

——第 11 部分：半导体应用指南。提供了 GB/T 34590 其他部分针对半导体开发的参考，包括半导体组件及其分区、特定半导体技术和应用案例、如何使用数字失效模式进行诊断覆盖率评估、相关失效分析、数字组件定量分析、模拟组件的定量分析、PLD 组件定量分析等方面的指南。

——第 12 部分：摩托车的适用性。描述了 GB/T 34590 其他部分对摩托车适用性的要求，包括对摩托车适用性的一般要求、安全文化、认可措施、危害分析和风险评估、整车集成与测试、安全确认。

GB/T 34590 基于 V 模型为产品开发的不同阶段提供参考过程模型，图 1 为 GB/T 34590 的整体架构。

注 1：阴影“V”表示 GB/T 34590.3—2022、GB/T 34590.4—2022、GB/T 34590.5—2022、GB/T 34590.6—2022、GB/T 34590.7—2022 之间的相互关系；

注 2：对于摩托车：

——GB/T 34590.12—2022 的第 8 章支持 GB/T 34590.3—2022；

——GB/T 34590.12—2022 的第 9 章和第 10 章支持 GB/T 34590.4—2022。

注 3：以“*m*-*n*”方式表示的具体章条中，“*m*”代表特定部分的编号，“*n*”代表该部分章的编号。

示例：“2-6”代表 GB/T 34590.2—2022 的第 6 章。

图 1　GB/T 34590 概览

道路车辆　功能安全
第5部分：产品开发：硬件层面

1　范围

本文件规定了车辆在硬件层面产品开发的要求，包括：

——硬件层面产品开发的概述；

——硬件安全要求的定义；

——硬件设计；

——硬件架构度量的评估；

——因随机硬件故障而导致违背安全目标的评估；

——硬件集成和验证。

本文件适用于安装在除轻便摩托车外的量产道路车辆上的包含一个或多个电气/电子系统的与安全相关的系统。

注：其他专用的安全标准可作为本文件的补充，反之亦然。

已经完成生产发布的系统及其组件或在本文件发布日期前正在开发的系统及其组件不适用于本文件。对于在本文件发布前完成生产发布的系统及其组件进行变更时，本文件基于这些变更对安全生命周期的活动进行裁剪。未按照本文件开发的系统与按照本文件开发的系统进行集成时，需要按照本文件进行安全生命周期的裁剪。

本文件针对由安全相关的电气/电子系统的功能异常表现而引起的可能的危害，包括这些系统相互作用而引起的可能的危害。本文件不针对与触电、火灾、烟雾、热、辐射、毒性、易燃性、反应性、腐蚀性、能量释放等相关的危害和类似的危害，除非危害是直接由安全相关的电气/电子系统的功能异常表现而引起的。

本文件提出了安全相关的电气/电子系统进行功能安全开发的框架，该框架旨在将功能安全活动整合到企业特定的开发框架中。本文件规定了为实现产品功能安全的技术开发要求，也规定了组织具备相应功能安全能力的开发流程要求。

本文件不针对电气/电子系统的标称性能。

本文件中对硬件要素的要求适用于非可编程和可编程硬件要素，如ASIC、FPGA和PLD，更多指南见GB/T 34590.10—2022和GB/T 34590.11—2022。

附录A概述了本文件的目标、前提条件和工作成果。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 34590.1—2022　道路车辆　功能安全　第1部分：术语（ISO 26262-1：2018，MOD）

注：GB/T 34590.1—2022被引用的内容与ISO 26262-1：2018被引用的内容没有技术上的差异。

GB/T 34590.2—2022　道路车辆　功能安全　第2部分：功能安全管理（ISO 26262-2：2018，MOD）