推荐性国家标准

《道路车辆 功能安全 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》

（征求意见稿）编制说明

一、工作简况

1、任务来源

本项目是根据国标委发【2020】37号文《国家标准化管理委员会关于下达2020年第二批推荐性国家标准计划的通知》（计划项目编号：20202465-T-339），修改采用ISO 26262-9：2018，对GB/T 34590.9-2017《道路车辆 功能安全 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》进行修订。

2、项目背景

GB/T 34590-2017《道路车辆 功能安全》修改采用国际标准ISO 26262-2011，该项标准针对汽车电子电气安全相关系统，为避免车辆电控系统因故障而导致车辆失控、人员伤亡等事故风险，提出了电控系统在全生命周期（设计、开发、生产、运行、报废）内的功能安全要求，可有效的降低由于汽车电子电气系统的随机硬件失效和系统性失效所带来的风险，对汽车安全性的提高有重要作用。该项标准发布后，受到了国内整车、零部件企业的高度重视，并积极导入该项标准，在企业技术研发和流程体系上提出功能安全的要求。满足功能安全要求已成为保证汽车电控系统和整车安全运行的行业共识。

国际标准化组织ISO于2018年12月发布了ISO 26262-2018（共12个部分），与第1版相比，标准适用范围由乘用车扩展到除轻便摩托车之外的所有道路车辆，并新增了第11部分：半导体应用指南和第12部分：摩托车的适用性。ISO 26262第二版相较第一版，ISO结合当前汽车技术国际水平的发展情况和变化，增加了很多新的要求，也对很多具体条款进行了修订。在促进我国跟进经济全球化的步伐，与国际接轨，同时符合我国国情和技术发展水平的原则下，修改采用国际标准ISO 26262-2018的基础上，对GB/T 34590-2017系列标准进行修订，为提高国内汽车整车和零部件企业的安全和管理水平、满足相关出口要求，提升产品竞争力方面有重要的必要性和意义。

3、主要工作过程

本项目任务下达后，全国汽车标准化技术委员会组织行业相关单位成立标准起草组，确定中国汽车技术研究中心有限公司为牵头单位。其他参与单位包括：舍弗勒贸易（上海）有限公司、北京兴科迪科技有限公司等30余家企业。主要工作过程如下：

2019年10月31，项目起草组启动预研，明确了项目分工和计划。完成国际标准ISO 26262-9:2018《Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level(ASIL)-oriented and safety-oriented analyses》翻译稿，在此基础上

形成立项草案。

2019年11月8日，全国汽车标准化技术委员会电子与电磁兼容分技术委员会（TC114/SC29）年会上正式提交了立项申请，并通过了委员立项投票。

2019年11月～2020年4月，共召开起草组及专家审核组网络会议6次，形成起草组草案。

2020年5月28日，召开“道路车辆功能安全标准研究制定工作组第十三次会议”网络会议，来自国内外整车生产企业、零部件供应商、汽车电子软件和硬件开发企业、检测机构和科研院所等71家单位的130名代表参加会议。会上介绍了GB/T 34590-2017标准修订进展情况，并将起草组草案发送至工作组征集修改意见。

2020年5月～11月，起草组对来着12家单位的82条修改意见进行了讨论，其中采纳36条，不采纳46条。并于11月2日将起草组草案发送至工作组继续征集修改意见。

2020年11月～2021年1月，共收到来着3家单位的工作组意见27条，其中采纳12条，不采纳15条。起草组根据修改意见更新并形成了社会公开征求意见稿。

4、主要参加单位和起草组成员及所做的工作

本标准由中国汽车技术研究中心有限公司、舍弗勒贸易（上海）有限公司、北京兴科迪科技有限公司等30余家企业参与起草，在标准制定过程中，召开了多次标准草案会议、调研，查阅了国内外相关标准和资料。

二、国家标准编制原则和确定国家标准主要内容

1、标准编制原则

本标准编制过程中遵循以下原则：

1） 规范性

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》和GB/T 20000.2-2009《标准化工作指南 第2部分：采用国际标准》的要求进行编制。

2） 一致性

本标准修改采用ISO 26262-2018，与国际标准在技术内容和文本结构上保持一致，并尽量与现行有效的国家法律、法规、标准保持一致并符合国家在语言文字方面的规定。

2、标准主要技术内容

本标准主要由范围、规范性引用文件、术语和定义、要求、关于ASIL等级剪裁的要求分解、要素共存的准则、相关失效分析、安全分析等组成，主要内容如下：

1） 范围

GB/T 34590的本部分规定了以汽车安全完整性等级为导向和以安全为导向的分析的要求，包括：

——关于 ASIL 剪裁的要求分解；

——要素共存的准则；

——相关失效分析；及

——安全分析。

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。

本文件不适用于特殊用途车辆上特定的电气/电子系统，例如，为残疾驾驶者设计的车辆。

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，也规定了组织应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。

2） 通用要求

规定了标准的一般要求、表的诠释、基于 ASIL 等级的要求和建议、摩托车的适用性、卡车、客车、挂车和半挂车的适用性等内容。

3） 关于ASIL等级剪裁的要求分解

规定了如果使用了ASIL等级分解，则要确保安全要求在下一个更细层面上分解成冗余的安全要求，并将这些要求分配给了充分独立的设计要素；根据允许的ASIL等级分解方案应用ASIL等级分解等相关要求，包括：目的、总则、前提条件、支持信息、要求和建议、工作成果。

4） 要素共存的准则

规定了安全相关的子要素与非安全相关的子要素、分配了不同ASIL等级的安全相关子要素在同一要素内共存的准则等相关要求，包括：目的、总则、前提条件、支持信息、要求和建议、工作成果。

5） 相关失效分析

规定了通过分析其潜在原因或引发因素，确认设计中充分实现了要求的独立性或免于干扰；定义安全措施，以减轻可能的相关失效等相关要求，包括：目的、总则、前提条件、支持信息、要求和建议、工作成果。

6） 安全分析

规定了通过开展安全分析确保由于系统性故障或随机硬件故障而导致违背安全目标的风险足够低的相关要求，包括：目的、总则、前提条件、支持信息、要求和建议、工作成果。

7） 附录

附录A提供了以汽车安全完整性等级为导向和以安全为导向的分析的目的、前提条件和工作成果的概览。附录B提供了要素共存和要求分解的架构示例。附录C提供了识别相关失效的框架。

本文件代替GB/T 34590.9-2017《道路车辆 功能安全 第9部分：以汽车安全完整性等级为导向和安全为导向的分析》,与GB/T 34590.9-2017相比，除结构调整和编辑性改动外，主要技术变化如下：

——修改了标准适用范围,由“量产乘用车”扩大到“除轻便摩托车外的量产道路车辆”;

——修改了关于 ASIL 等级剪裁的要求分解目的（见 5.1）；

——修改了关于 ASIL 等级剪裁的要求分解总则（见 5.2）；

——修改了初始安全需求应分解为冗余安全需求的内容（见 5.4.3）；

——修改了每个分解初始安全要求自身应符合初始安全要求的内容（见 5.4.4）；

——删除了“如果不能通过将要素关闭来阻止对初始安全要求的违背，则应展示执行分解后安全要求的充分独立要素具备足够的可用性”内容（见 2017 版的 5.4.8）；

——修改了要素共存准则的总则内容（见 6.2）；

——删除了“应用本章之前应将安全要求分配给要素的子要素”内容（见 2017 版的 6.4.2）；

——修改了如果同一要素中存在执行不同 ASIL 等级要求的内容（见 6.4.4）；

——修改了相关失效分析的目的（见 7.1）；

——修改了相关失效分析的总则（见 7.2）；

——修改了相关失效分析的前提条件（见 7.3.1）；

——修改了“维修错误”为“服务错误”（见 7.4.4 e））；

——增加了“老化和磨损”（见 7.4.4 i））；

——增加了相关失效分析的细节程度和严格程度的内容（见 7.4.8）；

——增加了相关失效分析的验证依据条款（见 7.4.9）；

——增加了相关失效分析验证报告（见 7.5.2）；

——修改了安全分析目的内容（见 8.1）；

——修改了安全分析的要求和建议内容（见 8.4.1）；

——增加了安全分析验证报告（见 8.5.2）；

——增加了附录 B 要素共存和要求分解的架构示例（见附录 B）；

——增加了附录 C 识别相关失效的框架（见附录 C）。

本文件使用重新起草法修改采用了ISO 26262-9：2018 《道路车辆 功能安全 第9部分：术语》。

本文件与ISO 26262-9：2018的技术性差异及其原因如下：

——关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第 2 章“规范性引用文件”中，具体调整如下：用修改采用国际标准的 GB/T 34590-XXXX（所有部分）代替 ISO 26262：2018（所有部分）；

本文件做了下列编辑性修改：

——将国际标准中的“本国际标准”改为“本文件”；

——删除国际标准的前言；

——修改国际标准的引言及其表述。

三、主要试验（或验证）情况分析

本标准的技术内容应在充分理解ISO 26262内涵的基础上，根据我国汽车行业的特点和实际情况，加入自身的理解和要求，制定出符合我国汽车电子产业发展需求的标准，提升车辆系统或产品的可靠性，避免过当设计而增加成本以及避免因系统失效、随机硬件失效、软件故障所带来的风险，使电子系统的安全功能在各种严酷条件下保持正常运作，确保驾乘人员及路人的安全，从而提高国内车企的设计开发、流程和管理水平。

为了做好此项工作，道路车辆功能安全标准研究制定工作组广泛地收集了国内、外有关标准及资料，调研国内外整车和零部件企业以及通过开展起草组会议、工作组会议、研讨交流的形式吸取有益建议和意见，逐步完善标准草案。

四、标准中涉及专利情况

本标准不涉及专利问题。

五、预期达到的社会效益、对产业发展的作用

本标准将推动汽车行业通过建立和完善汽车电子电气产品的功能安全流程开发体系，按照标准的技术要求进行产品开发，从而提升企业的整体技术和管理水平。同时在促进我国跟进经济全球化的步伐，与国际接轨，同时符合我国国情和技术发展水平的原则下，修改采用国际标准 ISO 26262-2018 的基础上，对 GB/T 34590-2017 系列标准进行修订，为提高国内汽车整车和零部件企业的安全和管理水平、满足相关出口要求，提升产品竞争力方面有重要的必要性和意义。

六、采用国际标准和国外先进标准情况

本标准修改采用ISO国际标准：ISO 26262-9：2018，Road vehicles — Functional safety —Part 9: Automotive Safety Integrity Level(ASIL)-oriented and safety-oriented analyses。

七、在标准体系中的位置，与现行相关法律、法规、规章及相关标准，特别是强制性标准的协调性：

无。

八、重大分歧意见的处理经过和依据：

无。

九、标准性质的建议说明：

由于本标准规定的是针对汽车安全的方法论要求。根据标准化法和有关规定，建议本标准的性质为推荐性国家标准。

十贯彻标准的要求和措施建议（包括组织措施、技术措施、过渡办法、实施日期等）：

无。

十一、废止现行相关标准的建议：

无。

十二、其他应予说明的事项：

无。