推荐性国家标准

《道路车辆 功能安全 第10部分：指南》

（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】48号文《国家标准化管理委员会关于下达2020年第三批推荐性国家标准计划的通知》（计划项目编号：20203944-T-339），修改采用ISO 26262-10：2018，对GB/T 34590.10-2017《道路车辆 功能安全 第10部分：指南》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：泛亚汽车技术中心有限公司、中国第一汽车集团有限公司等30余家企业。主要工作过程如下：

2019年9月～11月，项目启动预研，完成国际标准ISO 26262-10:2018《Road vehicles — Functional safety — Part 10: Guidelines on ISO26262》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20日，召开起草组启动会，明确了项目分工和计划。

2019年11月～2020年5月，共召开起草组网络会议5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23家单位的187条修改意见进行了讨论，其中采纳168条，不采纳11条，部分采纳8条。并于11月4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2家单位的工作组意见56条，起草组共召开起草组网络会议2次，逐条进行了讨论和处理，其中采纳39条，不采纳11条，部分采纳6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、泛亚汽车技术中心有限公司、中国第一汽车集团有限公司等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

本文件规定了范围、规范性引用文件、术语和定义、GB/T 34590中的关键概念、关于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 - 安全要求的流程和顺序、关于硬件开发、独立于环境的安全要素、在用证明的示例、关于ASIL的分解、带安全相关可用性需求的系统的开发指南等内容，主要技术内容如下：

1） 范围

GB/T 34590的本部分提供了GB/T 34590的概览，也给出了额外的解释，目的是增强对本文件其它部分的理解。本文件只具有资料性特性，描述了GB/T 34590的一般概念以便于理解。该解释将一般概念扩展到特定的内容。

本文件适用于安装在量产道路车辆（轻便摩托车除外）上的包含一个或多个电子电气系统的与安全相关的系统。本文件不适用于安装在特殊用途车辆上的特定的电子电气系统，例如为残疾驾驶者设计的车辆。

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开发的系统及其组件不适用于本文件。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，仅修改的部分需要按照本文件开发并进行安全生命周期的裁剪。未按照和按照本文件正在进行开发的系统进行变更时，仅修改的部分需要按照本文件开发并进行安全生命周期的裁剪。

本文件针对由电子电气安全相关系统的故障行为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，除非危害是直接由电子电气安全相关系统的故障行为而引起的。

本文件提出了安全相关的电子电气系统进行功能安全开发的框架，应将此框架内的功能安全活动整合到企业的整体开发体系中。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。

如果本文件与GB/T 34590其它部分存在不一致时，以GB/T 34590其它部分中定义的要求、建议和信息为准。

2） GB/T 34590 中的关键概念

针对汽车系统的功能安全（与GB/T 20438的关系）；相关项、系统、要素、组件、硬件元器件和软件单元；故障、错误和失效之间的关系；FTTI和紧急运行容错时间间隔等概念给出了指南。

3） 关于安全管理的精选话题

对于工作成果、认可措施、安全档案的理解等安全管理的内容给出了阐述和说明。

4） 概念阶段和系统开发

通过使用简单的示例，为概念阶段提供了危害分析和风险评估的原理概览。包括：总则、危害分析和风险评估示例、关于可控性分级的论述、外部措施、合并安全目标的示例。

5） 安全过程的要求结构-安全要求的流程和顺序

展示了符合GB/T 34590的安全要求开发流程和顺序，给出了GB/T 34590硬件要求与设计阶段之间的关系。

6） 关于硬件开发

给出了随机硬件故障的分类、残余失效率和局部单点故障度量评估的示例、关于硬件的进一步解释、PMHF单位—每小时平均概率等内容的指导。

7） 独立于环境的安全要素

提供了独立于环境的安全要素的开发的总体说明及使用案例。

8） 在用证明的示例

给出了在用证明的概述、相关项定义和在用证明候选项的定义、变更分析、在用证明的目标价值等内容。

9） 关于 ASIL 的分解

针对ASIL分解的目的、ASIL分解的描述、ASIL分解的示例给出了指导。

10) 带安全相关可用性需求的系统的开发指南

给出了带安全相关可用性需求的系统的开发指南，包括：概念阶段指定故障容错时间的说明、硬件设计阶段的可用性考虑、软件开发阶段的相关说明。

11) 关于“所使用软件工具的置信度”的分析

提供了GB/T 34590.8-XXXX第11章中描述的确定软件工具使用置信度的过程示例，包括工具使用案例的评估和软件工具的鉴定。

12) 安全相关的特殊特性指南

从产品开发阶段的安全相关特性的鉴别到生产阶段的监控提供指导，包括：总则、安全相关的特殊特性的确定、与安全相关的特殊特性控制措施规范、安全相关的特殊特性的监测。

13) 附录

附录A提供了故障树的构建和应用示例。

本文件代替GB/T 34590.10-2017《道路车辆 功能安全 第10部分：指南》，与GB/T 34590.10-2017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”；

——新增了对商用车辆的相关要求和示例、对摩托车的适应性要求等；

——新增了“容错时间间隔和紧急运行容许时间间隔”（见 4.4）；

——新增了“典型的双点失效模式（预期功能以及安全机制）”（见 8.3.2.3）；

——新增了“PMHF 单位——每小时平均概率”（见 8.4）；

——新增了“带安全相关可用性需求的系统的开发指南”（见第 12 章）；

——删除了 2017 版的附录 A。

本文件使用重新起草法修改采用了ISO 26262-10：2018 《道路车辆 功能安全 第10部分：指南》。

本文件与ISO 26262-10：2018的技术性差异及其原因如下：

——关于规范性引用文件，本文件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 34590.1-XXXX 代替 ISO 26262-1：2018；

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 26262-10: 2018，Road vehicles-Functional safety-Part10:Guideline on ISO 26262。

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。