推荐性国家标准

《道路车辆 功能安全 第2部分：功能安全管理》

（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：20203810-T-339），修改采用ISO 26262-2：2018，对GB/T 34590.2-2017《道路车辆 功能安全 第2部分：功能安全管理》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：博世汽车部件（苏州）有限公司、上海蔚来汽车有限公司等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 26262-2:2018《Road vehicles — Functional safety — Part 2: Management of functional safety》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14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11家单位的128条修改意见进行了讨论，其中采纳64条，不采纳55条，部分采纳9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，共收到来着1家单位的工作组意见5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0条，不采纳5条，部分采纳0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、博世汽车部件（苏州）有限公司、上海蔚来汽车有限公司等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

本标准主要包括范围、规范性引用文件、术语和定义、要求、整体安全管理、项目相关的安全管理和生产、运行、服务、报废的安全管理等，主要技术内容包括：

1） 范围

GB/T 34590的本部分规定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）；及

——项目特定的在安全生命周期内关于管理活动的要求，例如在概念阶段、产品开发阶段（系统层面、硬件层面、软件层面）以及生产、运行、服务和报废的管理。

本标准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与安全相关的电子电气系统。

本标准不适用于特殊用途车辆上特定的电子电气系统，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标准发布日期前开发的系统及其组件不适用于本标准。于在本标准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标准开发并进行安全生命周期的裁剪。未按照和按照本标准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标准开发并进行安全生命周期的裁剪。

本标准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。本标准不针对与触电、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。

本标准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。本标准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。

2） 通用要求

规定了如何确保GB/T 34590的符合性、标准中所使用表格的解释，以及各条款基于不同ASIL等级的适用性的解释。同时对于摩托车，卡车公共汽车、挂车和半挂车的适用性也做了说明。

3） 整体安全管理

规定了整体安全管理的目的、总则、输入、要求及工作成果。总则主要围绕生命安全周期的概述（生命周期相关管理阶段图）、解释说明（各阶段/子阶段的定义，关键概念的说明）进行了说明；有关要求的章节，对于安全声明周期中的安全文化、安全异常管理、能力管理、质量管理体系、裁剪做了说明。整体安全管理需考虑质量管理标准，如IATF 16949,ISO9001等。通过整体安全管理，形成组织专门的功能安全规章和流程，管理证据及报告等。

4） 项目相关的安全管理

本章规定了项目相关的安全管理的目的、总则、输入、要求及工作成果。项目的安全管理需确保相关组织在概念阶段、系统/硬件/软件层面开发阶段，定义与安全活动相关的角色和责任，进行相关项/要素的影响分析，活动裁剪，活动计划，活动追踪，规划分布式开发，确保活动进程，创建维护安全档案，评估功能安全活动以及是否生产发布。本章节输入包括整体安全管理的工作成果，还需考虑项目计划、其他活动（包括其他安全活动）及其他用于影响分析的现有信息。具体要求如下：

- ✓ 定义了安全管理的角色和职责，说明了项目经理和安全经理的区别；
- ✓ 相关项层面的影响分析，确定是全新开发还是现有相关项的修改（设计、实现方式/环境的修改）
- ✓ 现有要素的复用，需分析识别运行环境的修改，评估安全要求的符合性，识别安全活动，以及是否支持集成到相关项或另一个要素中。
- ✓ 安全活动的裁剪，需明确哪些裁剪及裁剪的理由。不同裁剪活动应满足相应的要求。

- ✓ 安全活动的计划和协调，安全经理需计划和协调相应活动，维护安全计划和监控进度，完成分配和沟通等责任，安全计划应被引用或包含在项目计划中，并规定了满足 GBT 34590 相应要求的活动计划和流程计划。且安全计划需逐步更新。
- ✓ 安全生命周期进程，要求如果缺失前一阶段信息缺失时在没有不合理风险情况下，才能开始后续子阶段。所要求的工作成果满足配置管理、变更管理及文档管理且在系统层面阶段启动之前纳入。
- ✓ 安全档案。
- ✓ 认可措施，包括认可评审、功能安全审核及功能安全评估。
- ✓ 生产发布。

本章的工作成果包括影响分析报告、安全计划、安全档案、认可措施报告、生产发布报告等。

5) 生产、运行、服务、报废的安全管理

本章规定了生产、运行、服务、报废阶段安全管理的目的、总则、输入、要求及工作成果。本章节定义了实现和维护生产、运行、服务和报废相关功能安全的组织和人员的职责、生产、运行、服务和报废阶段的计划和流程、以及变更管理。工作成果为该阶段的安全管理证据。

6) 附录A提供了功能安全管理的概览（包括特定阶段的目标、前提条件和工作成果）和工作流。附录B提供了安全文化评估示例。附录C提供了认可措施在每个层面的评审要求。附录D提供了功能安全评估安排示例。附录E提供了功能安全与信息安全的潜在交互作用指南。

本文件代替GB/T 34590.2-2017《道路车辆 功能安全 第2部分：功能安全管理》,与GB/T 34590.2-2017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；

——修改了整体安全管理的目的，明确执行安全活动的组织实现的目标（见 5.1）；

——修改了安全生命周期内不同阶段及子阶段的定义（见 5.2.2.2，2017 版，5.2.2）；

——新增了在安全生命周期内需要考虑的其他关键概念中的认可措施、相关项层面的影响分析、要素层面的影响分析、生产发布等概念（见 5.2.2.3）；

——修改了条中功能安全、信息安全、预期功能安全及与功能安全实现相关的其他领域之间的沟通，增加示例（见 5.4.2.3）；

——修改了中功能安全的安全异常管理内容，新增加安全异常关闭的条件以及异常的处理（见 5.4.3，2017 版，5.4.2.5）；

——修改了整体安全管理的工作成果，增加了质量管理体系证据和已识别的安全异常报告（见 5.5）；

——修改了项目相关的功能安全管理的目的和 6.2 中的项目安全管理相关的总则（见 6.1）；

——修改了功能安全管理的总则的要求（见 6.2）；

——修改了项目相关的功能安全管理的要求（见 6.4.1），增加了分布式开发下的项目经理角色任命的注（见 6.4.2）；

——新增了项目相关的功能安全管理中的相关项层面的影响分析（见 6.4.3）和现有要素的复用（见 6.4.4）；

——新增了硬件要素评估和软件组件鉴定的裁剪要求以及 T&B 的相关项开发裁剪的要求（见 6.4.5）；

——增加修改相关项和现有相关项环境时以及复用要素时的安全计划及协调要求，增加安全计划在开发阶段持续更新的要求，以及分布式开发时的安全计划要求（见 6.4.6，2017 版，6.4.3）；

——修改了安全档案的要求，增加分布式开发时安全档案要求和安全声明周期中逐步发布安全档案以提供安全论证证据的要求（见 6.4.8，2017 版，6.4.6）；

——修改了认可措施的要求，增加了功能安全审核判断流程的实施情况和判断相关项实现的功能安全或贡献的要求（见 6.4.9，2017 版，6.4.7）；

——新增了认可评审的要求（见 6.4.10）；

——修改了功能安全审核的要求，新增了评估报告的要求（见 6.4.11，2017 版，6.4.8）；

——修改了功能安全评估的要求，增加了功能安全评估的阶段、范围、人员要求，修订了评估的接受条件等（见 6.4.12，2017 版，6.4.9）；

——新增了生产发布的条件和要求（见 6.4.13）；

——修改了项目相关功能安全开发的工作成果（见 6.5）；

——修改了生产、运行、服务、报废的安全管理的要求。将生产发布后的阶段调整为生产、运行、服务和报废阶段的描述（见第 7 章）；

——修改了功能安全管理概览的要求（见附录 A）；

——修改了安全文化（见附录 B）；

——删除了认可措施的目标，新增了认可措施指南（见附录 C）；

——删除了 2017 版标准中附录 D 验证评审概览（见 2017 版，附录 D）；

——修改了附录中功能安全评估安排举例（见附录 D）；

——新增了附录 E 功能安全与信息安全的潜在交互作用指南。新增功能安全与信息安全的潜在交互作用指南（见附录 E）。

本文件使用重新起草法修改采用了ISO 26262-2：2018 《道路车辆 功能安全第2部分：功能安全管理》。

本文件与ISO 26262-2：2018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；
- 用修改采用国际标准的GB/T 34590.3-XXXX代替ISO 26262-3：2018；
- 用修改采用国际标准的GB/T 34590.4-XXXX代替ISO 26262-4：2018；
- 用修改采用国际标准的GB/T 34590.5-XXXX代替ISO 26262-5：2018；
- 用修改采用国际标准的GB/T 34590.6-XXXX代替ISO 26262-6：2018；
- 用修改采用国际标准的GB/T 34590.7-XXXX代替ISO 26262-7：2018；
- 用修改采用国际标准的GB/T 34590.8-XXXX代替ISO 26262-8：2018；
- 用修改采用国际标准的GB/T 34590.9-XXXX代替ISO 26262-9：2018。

——修改了 5.2.3 条的描述，增加示例 1。

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 26262-2: 2018，Road vehicles-Functional safety-Part2: Management of functional safety。

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：

自本标准实施之日起废止 GB/T 34590.2-2017。

十二、其他应予说明的事项：

无。