ICS 43.040
T 35

中华人民共和国国家标准

GB/T 34590.6—2017

道路车辆　功能安全
第6部分:产品开发:软件层面

Road vehicles—Functional safety—
Part 6:Product development at the software level

(ISO 26262-6:2011,MOD)

2017-10-14 发布　　2018-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 34590《道路车辆　功能安全》分为以下部分：

——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：生产和运行；

——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。

本部分为GB/T 34590的第6部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用重新起草法修改采用ISO 26262-6:2011《道路车辆　功能安全　第6部分：产品开发：软件层面》。

本部分与ISO 26262-6:2011的技术性差异及其原因如下：

——修改了本部分的适用范围，由原文的“适用于安装在最大总质量不超过3.5 t的量产乘用车上的包含一个或多个电子电气系统的与安全相关系统”改为“适用于安装在量产乘用车上的包含一个或多个电子电气系统的与安全相关的系统”；

——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 34590.1—2017代替ISO 26262-1:2011；
- 用修改采用国际标准的GB/T 34590.2—2017代替ISO 26262-2:2011；
- 用修改采用国际标准的GB/T 34590.4—2017代替ISO 26262-4:2011；
- 用修改采用国际标准的GB/T 34590.5—2017代替ISO 26262-6:2011引用的ISO 26262-5:2011；
- 用修改采用国际标准的GB/T 34590.8—2017代替ISO 26262-8:2011；
- 用修改采用国际标准的GB/T 34590.9—2017代替ISO 26262-9:2011。

本部分还做了下列编辑性修改：

——修改了国际标准的引言及其表述和图1的内容。

本部分由全国汽车标准化技术委员会(SAC/TC 114)提出并归口。

本部分负责起草单位：中国汽车技术研究中心、上海海拉电子有限公司、舍弗勒投资(中国)有限公司、泛亚汽车技术中心有限公司、博世汽车部件(苏州)有限公司、中国第一汽车股份有限公司、北京兴科迪科技有限公司、联合汽车电子有限公司、东软集团股份有限公司、北京经纬恒润科技有限公司、上汽大众汽车有限公司、上海汽车集团股份有限公司商用车技术中心。

本部分参加起草单位：重庆长安汽车股份有限公司、浙江尤奈特电机有限公司、上汽通用五菱汽车股份有限责任公司、本田技研工业(中国)投资有限公司、碧智三维公司、东风汽车有限公司东风日产乘用车公司、爱德克斯(常州)管理有限公司、AW(杭州)信息技术有限公司、京滨电子装置研究开发(上

海)有限公司。

本部分主要起草人:李波、蒋军、薛剑波、杨虎、尚世亮、童菲、曲元宁、张立君、蒋云、史晓密、刘北、常平、陈伟、明月、付越、吴含冰、张乐敏、宋锦明、周宏伟、刘姿汝、褚静娟、匡小军、盛一芝、王轶群、韩子凯、张小帆、徐寅、李钟、储小勤、徐惠忠。

引　言

ISO 26262 是以 IEC 61508 为基础，为满足道路车辆上电子电气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。

安全是未来汽车发展的关键问题之一，不仅在驾驶辅助和动力驱动领域，而且在车辆动态控制和主被动安全系统领域，新的功能越来越多地触及到系统安全工程领域。这些功能的开发和集成将强化对安全相关系统开发流程的需求，并且要求提供满足所有合理的系统安全目标的证明。

随着技术日益复杂、软件和机电一体化应用不断增加，来自系统性失效和随机硬件失效的风险逐渐增加。GB/T 34590 通过提供适当的要求和流程给出了避免风险的指导。

系统安全是通过一系列安全措施实现的。安全措施通过各种技术（例如，机械、液压、气压、电子、电气、可编程电子等）实现且应用于开发过程中的不同层面。尽管 GB/T 34590 针对的是电子电气系统的功能安全，但是它也提供了一个框架，在该框架内可考虑基于其他技术的与安全相关系统。GB/T 34590：

a) 提供了一个汽车安全生命周期（管理、开发、生产、运行、服务、报废），并支持在这些生命周期阶段内对必要活动的剪裁；

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) 应用汽车安全完整性等级（ASIL）定义 GB/T 34590 中适用的要求，以避免不合理的残余风险；

d) 提供了对于确认和认可措施的要求，以确保达到一个充分、可接受的安全等级；

e) 提供了与供应商相关的要求。

功能安全受开发过程（例如，包括需求规范、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开发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。

图 1 为 GB/T 34590 的整体架构。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：

——阴影“V”表示 GB/T 34590.3—2017、GB/T 34590.4—2017、GB/T 34590.5—2017、GB/T 34590.6—2017、GB/T 34590.7—2017 之间的相互关系；

——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—2017 第 6 章。

图 1　GB/T 34590—2017 概览

道路车辆　功能安全
第6部分：产品开发：软件层面

1　范围

GB/T 34590的本部分规定了车辆在软件层面产品开发的要求，包括：

——启动软件层面产品开发；

——软件安全要求的定义；

——软件架构设计；

——软件单元设计及实现；

——软件单元测试；

——软件集成和测试；及

——软件安全要求的验证。

本标准适用于安装在量产乘用车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。

本标准不适用于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。对于在本标准发布前完成生产发布的系统及其组件进行进一步的开发或变更时，仅修改的部分需要按照本标准开发。

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。

本标准不针对电子电气系统的标称性能，即使这些系统（例如，主动和被动安全系统、制动系统、自适应巡航系统）有专用的功能性能标准。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2017　道路车辆 功能安全　第1部分：术语（ISO 26262-1：2011，MOD）

GB/T 34590.2—2017　道路车辆功能安全　第2部分：功能安全管理（ISO 26262-2：2011，MOD）

GB/T 34590.4—2017　道路车辆功能安全　第4部分：产品开发：系统层面（ISO 26262-4：2011，MOD）

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（ISO 26262-5：2011，MOD）

GB/T 34590.8—2017　道路车辆功能安全　第8部分：支持过程（ISO 26262-8：2011，MOD）

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（ISO 26262-9：2011，MOD）

3　术语、定义和缩略语

GB/T 34590.1—2017界定的术语、定义和缩略语适用于本文件。