ICS 43.040
T 35

中华人民共和国国家标准

GB/T 34590.1—2017

道路车辆　功能安全
第1部分:术语

Road vehicles—Functional safety—
Part 1: Vocabulary

(ISO 26262-1:2011, 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1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 26262-1:2011《道路车辆　功能安全　第1部分：术语》。

本部分与ISO 26262-1:2011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”；

——2.3　架构　architecture，修改原文中的functions(功能)为requirements(要求)，因为术语“分配”是指将要求指定给架构要素，而不是功能；

——2.32　要素　element，修改原文中的定义内容，明确要素所包含的范围；

——2.55　硬件元器件　hardware part，修改原文中的定义并增加示例内容，便于理解；

——2.66　初始的ASIL等级　initial ASIL，修改原文中的定义内容，ASIL等级是危害分析和风险评估得出的；

——2.69　相关项　item，修改原文中的定义内容，使其定义完整化；

——2.76　多点失效　multiple-point failure，删除原文中的注释，该注释导致过定义和重复定义；

——2.86　乘用车　passenger car，修改原文中的定义内容，与GB 7258—2012《机动车运行安全技术条件》中的定义保持一致；

——2.110　安全措施　safety measure，将原文中的注1内容修改为示例；

——2.117　半形式记法　semi-formal notation，修改原文中的示例内容，SADT指代Structured Analysis and Design Techniques的缩写，而非原文的System Analysis and Design Techniques；

——2.126　特殊用途车辆　special-purpose vehicle，删除原文中的注；

——2.138　验证评审　verification review，修改原文注释2中的内容，明确验证评审的目的。

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、泛亚汽车技术中心有限公司、上海海拉电子有限公

司、舍弗勒投资(中国)有限公司、中国第一汽车股份有限公司、博世汽车部件(苏州)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、大陆汽车投资(上海)有限公司、上海汽车集团股份有限公司技术中心、东风汽车公司技术中心。

本部分参加起草单位:湖南中车时代电动汽车股份有限公司、上汽大众汽车有限公司、郑州宇通客车股份有限公司、东软集团股份有限公司、宁德时代新能源科技有限公司。

本部分主要起草人:李波、尚世亮、薛剑波、蒋军、童菲、曲元宁、杨虎、张立君、史晓密、明月、还宏生、付越、邓湘鸿、范嘉睿、冯亚军、付艳玲、张红霞、李琴、易茂明、张乐敏、卢长军、李春林、邱冬。

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来避免风险。

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1部分:术语

1　范围

GB/T 34590的本部分规定了本标准所有部分所应用的术语和定义,以及缩略语。

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、自适应巡航控制系统)有专用的功能性能标准。

2　术语和定义

2.1

分配　allocation

将要求指定给架构**要素**(2.32)。

注:目的不是将一个不可分割的要求分割成多个要求。从一个不可分割的**系统**(2.129)层面的要求到多个较低层面的不可分割的要求的追溯是允许的。

2.2

异常　anomaly

与预期(例如,基于要求、规范、设计文档、用户文档、标准或者经验的预期)偏离的情况。

注:异常可在除**评审**(2.98)、**测试**(2.134)、分析、编译、**组件**(2.15)的使用、或适用文档的使用等过程中被发现,也可在过程中被发现。

2.3

架构　architecture

相关项(2.69)、功能、**系统**(2.129)或**要素**(2.32)的结构的表征,用于识别结构模块及其边界和接口,并包括硬件和软件要素的要求**分配**(2.1)。

2.4

评估　assessment

对**相关项**(2.69)或**要素**(2.32)的特性的检查。

注:执行评估的一方或多方的**独立性**(2.61)水平与每一次评估相关。

2.5

审核　audit

对已实施流程的检查。