ICS 43.040
T 35

中华人民共和国国家标准

GB/T 34590.2—2017

道路车辆　功能安全
第2部分:功能安全管理

Road vehicles—Functional safety—
Part 2:Management of functional safety

(ISO 26262-2:2011,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 2 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 26262-2：2011《道路车辆　功能安全　第 2 部分：功能安全管理》。

本部分与 ISO 26262-2：2011 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”；

——增加了一条(5.4.2.3)，调整了相应的章条编号顺序，本部分的 5.4.2.4～5.4.2.9 条分别对应国际标准的 5.4.2.3～5.4.2.8；

——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 34590.3—2017 代替 ISO 26262-3：2011；
- 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 26262-5：2011；
- 用修改采用国际标准的 GB/T 34590.6—2017 代替 ISO 26262-6：2011；
- 用修改采用国际标准的 GB/T 34590.7—2017 代替 ISO 26262-7：2011；
- 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、泛亚汽车技术中心有限公司、舍弗勒投资(中国)有限公司、上海海拉电子有限公司、北京兴科迪科技有限公司、中国第一汽车股份有限公司、博世汽车部件(苏州)有限公司、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、联合汽车电子有限公司。

本部分参加起草单位：上汽大众汽车有限公司、安徽江淮汽车集团股份有限公司、本田技研工业（中国）投资有限公司、重庆长安汽车股份有限公司、上海汽车集团股份有限公司商用车技术中心。

本部分主要起草人：李波、童菲、尚世亮、薛剑波、曲元宁、蒋军、张立君、史晓密、杨虎、邓湘鸿、范嘉睿、付越、奚忠方、李艳文、冯亚军、李达、陈化荣、李琴、黄嵘、明月、张乐敏、唐小华、刘明华、梁惠、周宏伟、宋锦明。

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2部分:功能安全管理

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、产品开发阶段以及生产发布后的管理)。

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　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 34590.3—2017　道路车辆　功能安全　第3部分:概念阶段(ISO 26262-3:2011,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 34590.6—2017　道路车辆　功能安全　第6部分:产品开发:软件层面(ISO 26262-6:2011,MOD)

GB/T 34590.7—2017　道路车辆　功能安全　第7部分:生产和运行(ISO 26262-7:2011,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。

4 要求

4.1 一般要求

如声明满足 GB/T 34590—2017 的要求时，应满足每一个要求，除非有下列情况之一：

a) 按照本部分的要求，已经计划了安全活动的剪裁并表明这些要求不适用；或

b) 不满足要求的理由存在且是可接受的，并且按照本部分对该理由进行了评估。

标有“注”或“示例”的信息仅用于辅助理解或阐明相关要求，不应作为要求本身且不具备完备性。

将安全活动的结果作为工作成果。应具备上一阶段工作成果作为“前提条件”的信息。如果章条的某些要求是依照 ASIL 定义的或可剪裁的，某些工作成果可不作为前提条件。

“支持信息”是可供参考的信息，但在某些情况下，GB/T 34590—2017 不要求其作为上一阶段的工作成果，并且可以是由不同于负责功能安全活动的人员或组织等外部资源提供的信息。

4.2 表的诠释

表属于规范性表还是资料性表取决于上下文。在实现满足相关要求时，表中列出的不同方法有助于置信度水平。表中的每个方法是：

a) 一个连续的条目(在最左侧列以顺序号标明，如 1，2，3)；或

b) 一个选择的条目(在最左侧列以数字后加字母标明，如 2a，2b，2c)。

对于连续的条目，全部方法应按照 ASIL 等级推荐予以使用。除了所列出的方法外，如果应用所列出方法以外的其他方法，应给出满足相关要求的理由。

对于选择性的条目，应按照指定的 ASIL 等级，对这些方法进行适当的组合，不依赖于这些方法是否在表中列出。如果所列出的方法对于一个 ASIL 等级来说具有不同的推荐等级，宜采用具有较高推荐等级的方法。应给出所选的方法组合满足相关要求的理由。

注：表中所列出的方法的理由是充分的。但是，这并不意味着有倾向性或对未列到表中的方法表示反对。

对于每种方法，应用相关方法的推荐等级取决于 ASIL 等级，分类如下：

——“++”表示对于指定的 ASIL 等级，高度推荐该方法；

——“+”表示对于指定的 ASIL 等级，推荐该方法；

——“o”表示对于指定的 ASIL 等级，不推荐也不反对该方法。

4.3 基于 ASIL 等级的要求和建议

若无其他说明，对于 ASIL A、B、C 和 D 等级，应满足每一子章条的要求或建议。这些要求和建议参照安全目标的 ASIL 等级。如果在项目开发的早期对 ASIL 等级完成了分解，应按照 GB/T 34590.9—2017 第 5 章，遵循分解后的 ASIL 等级。

如果 GB/T 34590—2017 中 ASIL 等级在括号中给出，则对于该 ASIL 等级，相应的子章条应被认为是推荐而非要求。这里的括号与 ASIL 等级分解无关。

5 整体安全管理

5.1 目的

本章的目的是定义负责安全生命周期或在安全生命周期内执行安全活动的组织的要求。

本章是 GB/T 34590 安全生命周期内所有活动的前提条件。

5.2 总则

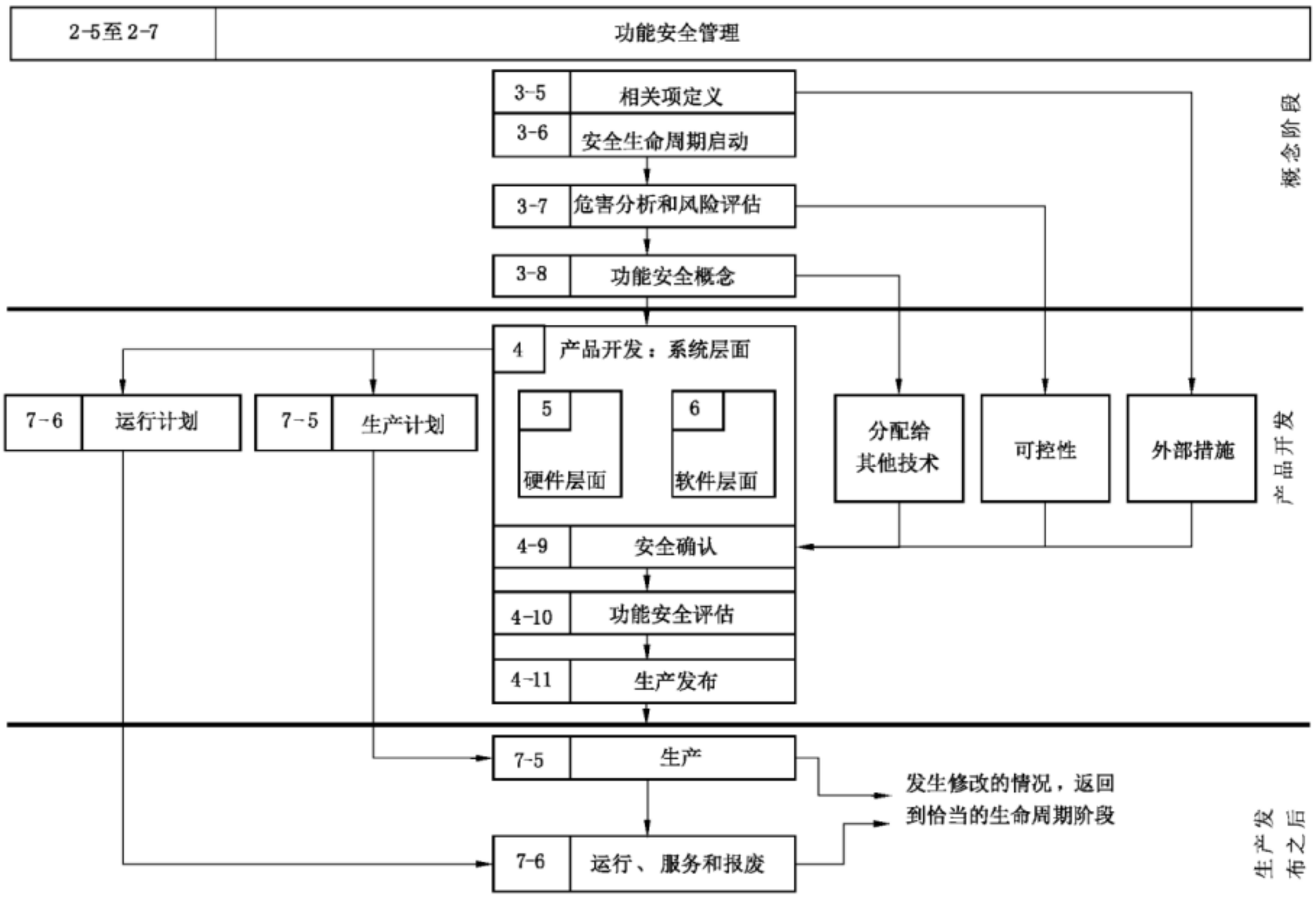
5.2.1 安全生命周期概述

GB/T 34590 安全生命周期(见图 2)包含了在概念阶段、产品开发、生产、运行、服务和报废期间的主要安全活动。计划、协调和记录安全生命周期所有阶段的安全活动是关键的管理任务。

图 2 描述了安全生命周期的参考模型,允许进行安全生命周期的剪裁,包括子阶段迭代。

注 1: GB/T 34590.3—2017(概念阶段)、GB/T 34590.4—2017(产品开发:系统层面)、GB/T 34590.5—2017(产品开发:硬件层面)、GB/T 34590.6—2017(产品开发:软件层面)和 GB/T 34590.7—2017(生产和运行)分别详细描述了在概念阶段、产品开发过程和生产发布后的安全活动。

注 2: 附录 A 中表 A.1 概括了功能安全管理特定阶段的目的、前提条件和工作成果。



注:在图中,GB/T 34590—2017 各部分中的具体条款用以下方式表示:"m-n",m 代表部分的数值,n 代表章的数值。例如:3-6 代表 GB/T 34590.3—2017 的第 6 章。

图 2 安全生命周期

5.2.2 安全生命周期的解释说明

GB/T 34590—2017 不仅定义了针对安全生命周期内特定阶段和特定子阶段的要求,同时也定义了适用于安全生命周期中多个或全部阶段的要求,例如功能安全管理要求。

关键的管理任务是计划、协调和追踪与功能安全相关的活动。这些管理任务适用于安全生命周期的所有阶段。本部分给出了功能安全管理的要求,分别是:

——整体安全管理(见本章);

——概念阶段和产品开发阶段的安全管理(见第 6 章);

——相关项生产发布后的安全管理(见第 7 章)。

安全生命周期中不同阶段和子阶段的定义以及其他关键概念的解释描述如下:

a) 子阶段:相关项定义

安全生命周期的初始任务是对相关项的功能、接口、环境条件、法规要求、已知危害等进行描述。确定相关项的边界及其接口,以及与其他相关项、要素、系统和组件相关的假设(参见 GB/T 34590.3—2017 第 5 章)。

b) 子阶段:安全生命周期启动

在完成相关项定义的基础上,通过确定所开发的相关项是一个全新的开发还是对现有相关项的修改来启动安全生命周期。

如果是对现有相关项的修改,对其所做的影响分析的结果可用于剪裁安全生命周期(参见 GB/T 34590.3—2017 第 6 章)。

c) 子阶段:危害分析和风险评估

安全生命周期启动后,应按照 GB/T 34590.3—2017 第 7 章的要求进行危害分析和风险评估。首先,通过危害分析和风险评估预测与相关项相关的危害事件所处工况的暴露概率、危害事件的可控性和严重度,这些参数共同决定了危害事件的汽车安全完整性等级(ASIL)。然后,通过危害分析和风险评估确定相关项的安全目标,安全目标是相关项的最高层面的安全要求。将所确定的危害事件的 ASIL 等级分配给相应的安全目标。

后续阶段和子阶段中详细的安全要求来自安全目标,这些安全要求继承了相应安全目标的 ASIL 等级。

d) 子阶段:功能安全概念

基于安全目标,同时考虑初步的构架设想以定义功能安全概念(参见 GB/T 34590.3—2017 第 8 章)。功能安全概念是通过分配给相关项要素的功能安全要求来定义的。如果能够对涉及的其他技术或与外部措施接口的期望行为进行确认,功能安全概念可包括其他技术或与外部措施的接口(参见 GB/T 34590.4—2017 第 9 章)。其他技术的实施不在本标准范围内,且外部措施的实施不在相关项开发范围内。

e) 阶段:产品开发:系统层面

在定义了功能安全概念后,应按照 GB/T 34590.4—2017,从系统层面进行相关项的开发。系统开发流程基于 V 模型概念,V 模型左侧包含技术安全要求的定义、系统架构、系统设计和实现,V 模型右侧包含集成、验证、确认和功能安全评估。

在本阶段定义了软硬件接口。

图 1 为系统层面产品开发各个子阶段的概览。

系统层面产品开发包括对发生在安全生命周期内其他阶段活动的确认任务:

——对通过其他技术实现功能安全概念的确认;

——对外部措施有效性的假设的确认和对性能的假设的确认;及

——对人员反应所做假设的确认,包括可控性和操作任务。

生产发布是产品开发的最后子阶段,并提供相关项量产发布(参见 GB/T 34590.4—2017 第 11 章)。

f) 阶段:产品开发:硬件层面

基于系统设计规范,从硬件层面进行相关项的开发(参见 GB/T 34590.5—2017)。硬件开发流程基于 V 模型概念,V 模型左侧包含硬件要求的定义、硬件设计和实现,V 模型右侧包含硬件集成和测试。

图 1 提供了硬件层面产品开发的概览。

g) 阶段:产品开发:软件层面

基于系统设计规范,从软件层面进行相关项的开发(参见 GB/T 34590.6—2017)。软件开发流程基于 V 模型概念,V 模型左侧包含软件要求的定义、软件架构设计和实现,V 模型右侧包含软件集成、测试和软件要求验证。

图 1 提供了软件层面产品开发的概览。

h) 生产计划和运行计划

生产计划和运行计划以及相关要求的定义在系统层面产品开发过程中启动(参见 GB/T 34590.4—2017)。GB/T 34590.7—2017 第 5 章和第 6 章中给出了生产和运行的要求。

i) 阶段:生产和运行,服务和报废

该阶段描述了与相关项的功能安全目标相关的生产过程,即与安全相关的特殊特性,以及对相关项的维护、维修、报废的指导说明的开发和管理,以确保相关项在生产发布后的功能安全(参见 GB/T 34590.7—2017 第 5 和第 6 章)。

j) 可控性

在危害分析和风险评估中(参见 GB/T 34590.3—2017 第 7 章),驾驶员或其他涉险人员控制危害情况能力的可信度。在安全确认过程中,需要确认在危害分析和风险评估、功能安全概念和技术安全概念中关于可控性的假设(参见图 2 和 GB/T 34590.4—2017 第 9 章)。

注:暴露概率和严重度依赖于场景,通过人为干预的最终可控性受相关项设计的影响,因此,在确认过程中进行评估(参见 GB/T 34590.4—2017 的 9.4.3.2)。

k) 外部措施

外部措施指相关项外部的措施,在相关项定义里对其进行了规定(参见图 2 和 GB/T 34590.3—2017 第 5 章),用于减少或减轻来自相关项的风险。外部措施不仅包括附加的车载装置如动态稳定控制器或防爆轮胎,而且也可包括车辆以外的装置如防撞栏或隧道消防系统。

在安全确认过程中,需要确认在相关项定义、危害分析和风险评估、功能安全概念和技术安全概念中关于外部措施的假设(参见图 2 和 GB/T 34590.4—2017 第 9 章)。

可在危害分析和风险评估过程中考虑外部措施,然而,如果可信度来自危害分析和风险评估过程中的外部措施,则在功能安全概念中不能认为此外部措施是一个减少风险的途径。

GB/T 34590—2017 同样适用于其范围内的那些外部措施。

l) 其他技术

其他技术,如机械和液压技术,不同于本标准适用范围内的电子电气技术。这些技术可在功能安全概念制定中(参见图 2 及 GB/T 34590.3—2017 第 8 章)、安全要求分配中(参见 GB/T 34590.3—2017 及 GB/T 34590.4—2017)或作为外部措施被考虑。

注:如果其他技术被定义为外部措施,则考虑到降低相关风险而重新进行危害分析和风险评估是有益的,这样做可能会降低相关安全目标的 ASIL 等级。

5.3 本章的输入

5.3.1 前提条件

无。

5.3.2 支持信息

可考虑如下信息:

质量管理体系符合质量管理标准(如:ISO/TS 16949、ISO 9001 或等同要求)的证据。

5.4 要求和建议

5.4.1 总则

执行安全生命周期活动的组织应满足 5.4.2～5.4.5。

5.4.2 安全文化

5.4.2.1 组织应创造、培育并保持一种安全文化，以支持并鼓励有效地实现功能安全。

示例：附录 B 中给出了评估安全文化的例子。

5.4.2.2 组织应建立、执行并维护专门的规章和流程，以符合 GB/T 34590—2017 的要求。

注：组织的专门的规章和流程可包括创建并维护通用的安全计划和流程描述。

5.4.2.3 组织应建立并维护功能安全领域与功能安全相关的其他领域之间的有效沟通渠道。

示例 1：建立功能安全与信息安全之间的沟通渠道，以便于两者交互相关信息，例如，功能安全危害分析和风险评估的结果、信息安全威胁分析和风险评估的结果、功能安全目标、信息安全目标、功能安全概念、信息安全策略等。

注：功能安全针对的是由电子电气系统的内部故障行为而导致的问题，而信息安全针对的是外部恶意事件(攻击)导致的问题。在开发过程中，一些功能安全活动和信息安全活动是相类似的。为了达到产品的整体安全，功能安全和信息安全之间是有协作的，功能安全活动的输出可关系到或影响到信息安全活动，反之亦然。两者之间的交互和融合能促进产品更好的达到整体上的安全性。

示例 2：建立功能安全与机械安全之间的信息沟通渠道。

5.4.2.4 组织应建立、执行并维护流程以确保识别出的功能安全异常能够明确地通报给安全经理和其他责任者。

示例：安全经理和其他责任者可以是客户安全经理、供应商安全经理，以及与相关项开发相关的安全经理。

5.4.2.5 组织应建立、执行并维护解决安全异常的流程，以确保及时、有效地对功能安全异常进行分析、评估、解决和处理。

注：功能安全异常的解决流程可包括根本原因分析，由该根本原因分析得出对以后的修正行动。

5.4.2.6 在安全生命周期内，组织应执行所需的功能安全活动，包括相关文档的生成和管理(按照 GB/T 34590.8—2017 第 10 章的说明)。

5.4.2.7 组织应为功能安全的实现提供所需的资源。

注：人力资源、工具、数据库和模板。

5.4.2.8 基于以下几点，组织应建立、执行并维护持续改进的流程：

——从其他相关项安全生命周期的执行过程中学习经验，包括现场经验；

——将获得的改进应用于后续相关项。

5.4.2.9 组织应确保给予执行或支持安全活动的人员以足够的权限来履行他们的职责。

5.4.3 能力管理

组织应确保执行安全生命周期活动的人员具有与其职责相匹配的技能水平、能力和资质。

注 1：在开发过程中，达到足够的技能水平和能力的方法之一是考虑以下知识领域的培训和资质培养：

——常规的安全实践、概念和设计；

——GB/T 34590—2017 和其他适用的安全标准；

——用于功能安全组织的专门规则；

——组织所建立的功能安全流程。

注 2：为了评估执行满足 GB/T 34590—2017 的活动所需的技能、能力和资质，可以考量以往的专业活动经验，如：

——相关项专业领域的知识；

——相关项相关领域的专业知识；

——管理经验。

5.4.4 安全生命周期中的质量管理

执行安全生命周期活动的组织应具有满足质量标准如 ISO/TS 16949、ISO 9001 或等同标准的质量管理体系。

5.4.5 独立于项目的安全生命周期剪裁

组织可剪裁安全生命周期，应用于各相关项的开发，即独立于项目的剪裁，但仅限于以下的一种或多种方式：

a) 合并或分解子阶段、活动或任务；或

注：如果所用的方法难以清晰地区分单独的子阶段，则可以合并单独的子阶段。例如，计算机辅助开发工具能在一个步骤中支持多个子阶段的活动。

b) 同一活动或任务可在不同的阶段或子阶段中执行；或

c) 同一活动或任务可在新增的阶段或子阶段中执行；或

d) 反复进行某个阶段或子阶段。

5.5 工作成果

5.5.1 组织的专门的功能安全规章和流程，由 5.4.2 和 5.4.5 得出。

5.5.2 能力证据，由 5.4.3 得出。

5.5.3 质量管理证据，由 5.4.4 得出。

6 概念阶段和产品开发过程中的安全管理

6.1 目的

本章的第一个目的是定义关于安全生命周期(见图 1 和图 2)内，概念阶段和开发阶段的安全管理角色和职责。

本章的第二个目的是定义在概念阶段和开发阶段中的安全管理要求，包括安全活动的计划和协调、安全生命周期的推进、安全档案的创建和认可措施的执行。

6.2 总则

安全管理有责任确保认可措施得到执行。根据适当的 ASIL 等级，一些认可措施要求在资源、管理和发布权限上有独立性(参见 6.4.7)。

认可措施包括认可评审、功能安全审核和功能安全评估：

——认可评审的目的是核查工作成果是否符合 GB/T 34590—2017 的要求；

——功能安全审核的目的是评价功能安全活动所需要的流程的执行情况；

——功能安全评估的目的是评价相关项是否实现了功能安全。

除了认可措施外，还需进行验证评审。GB/T 34590—2017 的其他部分也要求这些评审，目的是验证相关的工作成果满足项目的要求，以及与应用案例和失效模式相关的技术要求。

表 1 列出了所需的认可措施。附录 D 列出了关于验证的评审，及所参考的本标准的适用部分。

安全管理有责任对所有剪裁的安全活动(参见 6.4.5)进行描述和理由说明。

6.3 本章的输入

6.3.1 前提条件

应具备如下信息：

——组织的专门的功能安全规章和流程，按照 5.5.1；
——能力证据，按照 5.5.2；
——质量管理证据，按照 5.5.3。

6.3.2 支持信息

如果有，可以考虑如下信息：
——项目计划（来自外部）；
——其他活动，包括其他安全活动。

6.4 要求和建议

6.4.1 总则

对于至少有一个安全目标为 ASIL A、B、C 或 D 的相关项，执行安全生命周期活动的组织应满足 6.4.2～6.4.9 的要求，除非有其他说明。

6.4.2 安全管理的角色和职责

6.4.2.1 在相关项开发的启动阶段应指定一名项目经理。

6.4.2.2 应赋予项目经理责任和权限，按照 5.4.2.9 的要求，确保：

a) 执行实现功能安全所需的安全活动；

b) 满足 GB/T 34590—2017 的要求。

6.4.2.3 项目经理应确认组织提供了符合 5.4.2.7 要求的功能安全活动所需的资源。

注：通常在计划阶段对足够的资源进行预估、确定和分配。

6.4.2.4 项目经理应确保已指定了符合 5.4.3 要求的安全经理。

注 1：安全经理的角色可以由项目经理承担。

注 2：GB/T 34590.1—2017 定义了“安全经理”，在矩阵式组织里，安全经理的任务可以分配给不同的人。

6.4.3 安全活动的计划和协调

6.4.3.1 按照 5.4.2.9 的要求，在安全生命周期的开发阶段，安全经理应负责计划和协调功能安全活动。

注 1：安全经理可将任务分配给具有所需技术、能力和资质的人员。

注 2：安全活动的计划包含在安全计划（参见 6.4.3.5）中。某些已纳入安全计划中的安全活动在 GB/T 34590—2017 的其他工作成果（参见 6.4.3.3）中进一步细化。

注 3：基于相关项是一个全新开发还是一个对既有相关项的修改（参见 GB/T 34590.3—2017 第 6 章），安全活动可以不同，并据此计划相应的安全活动。

6.4.3.2 安全经理应负责维护安全计划并监督安全活动的进度是否按照安全计划进行。

6.4.3.3 在组织内部应按照 5.4.2.9 和 5.4.3 的要求，分配并通报关于细化和协调如下计划中安全活动的责任：

——相关项的集成和测试计划，按照 GB/T 34590.4—2017；
——确认计划，按照 GB/T 34590.4—2017；
——软件验证计划，按照 GB/T 34590.6—2017；及
——功能安全评估计划，按照 6.4.9。

责任人应负责维护各自的安全计划并监督安全活动的进度是否按照各自的安全计划进行。

6.4.3.4 安全计划应：

a) 在项目计划中被引用；或

b) 包含在项目计划中，并使安全活动是可区分的。

注：在配置管理下，安全计划可交叉引用其他信息(参见 GB/T 34590.8—2017 第 7 章)。交叉引用通常优于在不同工作成果或在配置管理下的其他文档里对活动的重复描述。

6.4.3.5 安全计划应包括：

a) 实现功能安全的活动计划和流程计划；

b) 将独立于项目的安全活动应用到项目特定的安全管理中，按照第 5 章；

c) 如果适用，所剪裁的安全活动的定义，按照 6.4.5；

d) 危害分析和风险评估计划，按照 GB/T 34590.3—2017 第 7 章；

e) 开发活动计划，包括按照 GB/T 34590.3—2017 第 8 章进行功能安全概念的开发和实施、按照 GB/T 34590.4—2017 进行产品系统层面的开发和实施、按照 GB/T 34590.5—2017 进行产品硬件层面的开发和实施、按照 GB/T 34590.6—2017 进行产品软件层面的开发和实施；

f) 如果适用，开发接口协议计划，按照 GB/T 34590.8—2017 第 5 章；

g) 支持过程计划，按照 GB/T 34590.8—2017；

h) 验证活动计划，按照 GB/T 34590.3—2017、GB/T 34590.4—2017、GB/T 34590.5—2017、GB/T 34590.6—2017 和 GB/T 34590.8—2017 第 9 章；安全确认活动计划，按照 GB/T 34590.4—2017 第 9 章；

注：在相关项集成和测试计划(参见 GB/T 34590.4—2017)、软件验证计划(参见 GB/T 34590.6—2017)中详细说明了验证活动。在确认计划(参见 GB/T 34590.4—2017)中详细说明了确认活动。同时参见 6.4.3.3。

i) 认可评审的计划、功能安全审核的启动和功能安全评估的启动，按照 6.4.7～6.4.9。

注：在安全计划中规定了实施认可措施的人员的独立性级别(参见 6.4.7)和资质(参见 5.4.3)。

j) 相关失效分析的计划，如果适用，按照 GB/T 34590.9—2017 第 7 章；以及安全分析计划，按照 GB/T 34590.9—2017 第 8 章；

k) 如果适用，提供候选项的在用证明，按照 GB/T 34590.8—2017 第 14 章；及

l) 如果适用，提供软件工具的可信度，按照 GB/T 34590.8—2017 第 11 章。

6.4.3.6 安全活动的计划应包括：

a) 目的；

b) 对其他活动或信息的依赖性；

c) 负责执行活动的资源；

d) 执行活动所需的资源；

e) 起点时间和持续时间；及

f) 相应工作成果的识别。

6.4.3.7 对于至少有一个安全目标为 ASIL B、C 或 D 的相关项，应满足如下要求：按照 6.4.3.1～6.4.3.6 的要求制定的安全计划，应由授权人批准，该授权人应考虑按照 6.4.7 的要求对安全计划进行认可评审。

6.4.3.8 按照 5.4.2.4 的要求，对识别出的安全异常应向安全经理以及其他责任人员汇报。

注：安全异常解决方案导致的变更应纳入变更管理流程(参见 GB/T 34590.8—2017 第 8 章)。

6.4.4 安全生命周期进程

6.4.4.1 只有来自相关子阶段的信息足够充分时，才应启动安全生命周期后续子阶段的安全活动。

注：对于相关项安全目标的实现来说，如果缺失的信息不会导致不可接受的风险，则信息可以被认为是充分的。

6.4.4.2 按照 GB/T 34590.8—2017 第 7 章、第 8 章和第 10 章的要求，每一项安全计划所要求的工作成果应分别服从配置管理、变更管理以及文档化管理，且纳入管理的时间不迟于“产品开发：系统层面”阶段的启动时间(参见图 1)。

6.4.5 安全活动剪裁

6.4.5.1 可以对特定相关项开发的安全活动进行剪裁，如省略或以不同的方式执行。如果对安全活动进行剪裁，则：

a) 应在安全计划中定义该剪裁[参见 6.4.3.5c)]；及

b) 应给出理由说明为什么剪裁对于实现功能安全来说是恰当且充分的。

注 1：该理由应考虑相关要求的 ASIL 等级。

注 2：剪裁的理由包含在安全计划中且在安全计划认可评审(参见 6.4.7)或功能安全评估(参见 6.4.9)过程中进行评审。

注 3：该要求适用于特定相关项的安全活动的剪裁。关于组织层面相关项开发的安全生命周期的剪裁，仅 5.4.5 适用。

6.4.5.2 如果是因为对现有相关项的修改而按照 6.4.5.1 对某一安全活动进行剪裁，应满足 GB/T 34590.3—2017 第 6 章的要求。

6.4.5.3 如果存在在用证明而按照 6.4.5.1 对某一安全活动进行剪裁时，则应满足 GB/T 34590.8—2017 第 14 章的要求。

6.4.5.4 如果由于 ASIL 分解而按照 6.4.5.1 的要求不采用某一安全活动，则应满足 GB/T 34590.9—2017 第 5 章的要求。

6.4.5.5 如果是基于考虑所使用软件工具的置信度而按照 6.4.5.1 对某一安全活动进行剪裁，则应满足 GB/T 34590.8—2017 第 11 章的要求。

6.4.5.6 如果是因为要素独立于相关项开发而按照 6.4.5.1 的要求对安全活动进行剪裁，则：

a) 独立于相关项的要素的开发应基于一个需求规范，该需求规范来自对预期用途和应用环境的假设，包括其外部接口；及

b) 应确认独立于相关项而开发的要素的预期用途和应用环境的假设的有效性。

注：本标准作为一个整体不能应用于独立于相关项的要素开发，因为功能安全不是一个要素的属性(然而一个相关项中的某一个要素可以认为是与安全相关的)。功能安全是一个可以用功能安全评估方法来评价的相关项的属性。

示例：微控制器独立于相关项开发。

6.4.6 安全档案

6.4.6.1 对于至少有一个安全目标为 ASIL(A)、B、C 或 D 的相关项：应按照安全计划建立安全档案。

6.4.6.2 安全档案宜逐步收录安全生命周期内的工作成果。

6.4.7 认可措施：类型、独立性和权限

6.4.7.1 应按照所要求的独立性等级、表 2、6.4.3.5i)、6.4.8 和 6.4.9 的要求，执行表 1 所定义的认可措施。

注 1：对表 1 中定义的且被安全计划所要求的工作成果进行认可评审。

注 2：认可评审包括按照本标准对形式、内容、充分性、完整性方面的要求进行正确性检查。

注 3：表 1 包括认可措施，附录 D 中给出了验证评审的概述。

注 4：认可措施的结果报告包括已分析的工作成果或流程文档的名称和版本号(参见 GB/T 34590.8—2017 的 10.4.5)。

注 5：如果在认可评审或功能安全评估完成后，还有相关项的变更，则需要重复或补充所有这些工作。

注 6：在附录 C 中给出了每个认可措施的目标。

注 7：认可措施，如认可评审和功能安全审核，可以与功能安全评估合并、联合，以支持相关项类似变型的处理。

表 1　要求的认可措施(包括独立性等级要求)

认可措施	应用于 ASIL 的独立性程度[a]				范围
	A	B	C	D	
对于相关项的危害分析和风险评估的认可评审(参见 GB/T 34590.3—2017 第 5 章和第 7 章,若适用也可参见 GB/T 34590.8—2017 第 5 章); 独立于该相关项的开发人员、项目管理和工作成果责任者	I3	I3	I3	I3	评审的范围应包括该相关项已识别危害的 ASIL/QM 等级的正确性,以及对安全目标的评审
安全计划的认可评审(参见 6.5.1); 独立于该相关项的开发人员、项目管理和工作成果责任者	—	I1	I2	I3	依照相关项全部安全目标中的最高 ASIL 等级执行
相关项集成和测试计划的认可评审(参见 GB/T 34590.4—2017); 独立于该相关项的开发人员、项目管理和工作成果责任者	I0	I1	I2	I2	依照相关项全部安全目标中的最高 ASIL 等级执行
确认计划的认可评审(参见 GB/T 34590.4—2017); 独立于该相关项的开发人员、项目管理和工作成果责任者	I0	I1	I2	I2	依照相关项全部安全目标中的最高 ASIL 等级执行
安全分析的认可评审(参见 GB/T 34590.9—2017 第 8 章); 独立于该相关项的开发人员、项目管理和工作成果责任者	I1	I1	I2	I3	依照相关项全部安全目标中的最高 ASIL 等级执行
软件工具标准评估报告和软件工具鉴定报告[b] 的认可评审(参见 GB/T 34590.8—2017 第 11 章); 独立于该软件工具鉴定的审核人员	—	I0	I1	I1	依照因该软件工具的使用而可能违背的全部安全要求中的最高 ASIL 等级执行
候选项在用证明(分析、数据和可信度)的认可评审(参见 GB/T 34590.8—2017 第 14 章); 独立于该证明的作者	I0	I1	I2	I3	依照与所考虑的候选项的行为、功能等相关的安全目标或者要求的 ASIL 等级执行
安全档案完整性的认可评审(参见 6.5.3) 独立于安全档案的制定者	I0	I1	I2	I3	依照相关项全部安全目标中的最高 ASIL 等级执行
按照 6.4.8,进行功能安全审核; 独立于相关项开发人员和项目管理人员	—	I0	I2	I3	依照相关项全部安全目标中的最高 ASIL 等级执行
按照 6.4.9,进行功能安全评估; 独立于相关项开发人员和项目管理人员	—	I0	I2	I3	依照相关项全部安全目标中的最高 ASIL 等级执行

[a] 注释解释如下:

—— —:对于认可措施无要求和建议;

——I0:宜执行认可措施;但如果执行,应由不同的人员执行;

——I1:认可措施应由不同的人员执行;

——I2:认可措施应由来自不同团队的人员执行,即不向同一个直接上级报告;

——I3:认可措施应由来自不同的部门或组织的人员执行,即在管理、资源和发布权限方面与负责相关工作成果的部门是独立的。

[b] 软件工具开发本身不在相关项安全生命周期范围内,但是该工具鉴定的审核属于安全生命周期内的活动。

表 2　认可措施的流程要求

要点	认可评审	功能安全审核	功能安全评估
评估的内容	工作成果	功能安全所需流程的实施情况	按照 GB/T 34590.3—2017 第 5 章相关项定义所描述的相关项
结果	认可评审报告[a]	按照 6.4.8，功能安全审核报告[a]	按照 6.4.9，功能安全评估报告
执行认可措施的人员的责任	评估工作成果与 GB/T 34590 要求的符合性	评估所需流程执行情况	评估已实现的功能安全； 按照 6.4.9.6，提供接受、有条件接受或拒绝的建议
安全生命周期中的时间节点	相关安全活动完成后； 在生产发布前完成	所需流程的实施期间	在开发过程中或单一时间段里逐步开展 在生产发布前完成
广度和深度	按照安全计划	实施基于安全计划中参考或定义的活动的流程	安全计划所要求的工作成果、所需流程的实施情况、及对所实施的安全措施（在相关项开发过程可以评估的）的评审

[a] 报告可以包含在功能安全评估报告中。

6.4.7.2　在相关项开发过程中，实施认可措施的人员应能接触开展安全活动的人员和组织机构，并应得到其支持。

6.4.7.3　实施认可措施的人员应有权限获取相关信息和工具。

6.4.8　功能安全审核

6.4.8.1　当相关项安全目标的最高 ASIL 等级是 ASIL(B)、C 或 D 时，应按照 6.4.7、6.4.3.5i)和 6.4.8.2 的要求进行相关项的功能安全审核。

6.4.8.2　按照 5.4.3 的要求，应委派一名或多名人员开展一次或多次功能安全审核。所委派的人员应提供包含对功能安全所要求的过程实施情况的评估报告。

注 1：如果由 SPICE(Software Process Improvement and Capability Etermination 软件过程改进和能力测定)评估人员开展功能安全审核，则可以同时开展功能安全审核和 SPICE 评估(参见 ISO/IEC 15504)GB/T 34590—2017 和 SPICE 在内容上有足够的共通内容来支持计划的同步，如果同步，SPICE 评估人员能向功能安全审核员提供反馈。但是，SPICE 评估仅能同步检查在 GB/T 34590.8—2017 中规定的某些支持过程，不足以对功能安全进行评估(参见 6.4.9)。

注 2：组织的流程定义可以同时符合多种标准，如 GB/T 34590 和 SPICE 的配置管理流程要求。这种流程的协调有助于避免重复工作或流程的不一致。对于协调后的流程，可给出组织专门流程对 GB/T 34590 中要求和对 SPICE 要求的交叉引用。

6.4.9　功能安全评估

6.4.9.1　当相关项安全目标的最高 ASIL 等级为(B)、C 或 D 时，应按照 6.4.7 和 6.4.9.2～6.4.9.8 的要求开展功能安全评估。

6.4.9.2　应按照 6.4.3.3 和 6.4.3.5i)的要求，制定功能安全评估计划。

示例：附录 E 给出了功能安全评估的计划安排。

6.4.9.3　按照 5.4.3 的要求，应委派一名或多名人员开展功能安全评估，被委派的人员应提供一份包含对功能安全实现程度的评判报告。

6.4.9.4 功能安全评估范围应包括：

——安全计划要求的工作成果；

——功能安全要求的流程；及

注 1：流程的评估可基于功能安全审核的结果。

——对在相关项开发过程中已实施的且可评估的安全措施进行适宜性和有效性评审。

注 2：对于在产品生产子阶段实施的但不能在相关项开发过程中进行评估的安全措施，可与生产过程能力结合在一起进行评估(参见 GB/T 34590.7—2017 的 5.4.2.2)。

6.4.9.5 功能安全评估应考虑：

a) 其他认可措施的计划[参见 6.4.3.5i)]；

b) 认可评审和功能安全审核的结果；

c) 如果适用，来自先前的功能安全评估的建议(参见 6.4.9.7、6.4.9.8 和 GB/T 34590.8—2017 的 8.4.5.2)。

6.4.9.6 按照 6.4.9.3 的要求制定的功能安全评估报告应包含对相关项的功能安全接受、有条件接受或拒绝的建议。对于有条件接受的情况：

a) 如果相关项的功能安全被认为是明显的，尽管存在已识别的未解决的问题，应为有条件接受；及

b) 有条件接受的建议应包含与功能安全评估标准的偏差以及这些偏差可被接受的依据。

6.4.9.7 按照 6.4.9.6，如果功能安全评估报告建议对已实现的功能安全是有条件接受，则宜实施在功能安全评估报告中提供的修正措施。

6.4.9.8 按照 6.4.9.6，如果功能安全评估报告建议对已实现的功能安全是拒绝，则：

a) 应启动充分的修正行动；及

b) 应重新进行功能安全评估。

6.5 工作成果

6.5.1 安全计划，由 6.4.3～6.4.5 得出。

6.5.2 项目计划(细化的)，由 6.4.3.4 得出。

6.5.3 安全档案，由 6.4.6 得出。

6.5.4 功能安全评估计划，由 6.4.9 得出。

6.5.5 认可措施报告，由 6.4.7～6.4.9 得出。

7 相关项生产发布后的安全管理

7.1 目的

本章的目的是定义相关项生产发布后，负责功能安全的组织和人员的职责。这与确保在生产发布后的生命周期子阶段内，相关项所需的功能安全的常规活动相关。

7.2 总则

见 5.2。

7.3 本章的输入

7.3.1 前提条件

应提供如下信息：

——按照 5.5.3，满足质量管理的证据。

7.3.2 支持信息

无。

7.4 要求和建议

7.4.1 总则

对于至少存在一个等级为 ASIL A、B、C 或 D 的安全目标的相关项，与执行安全生命周期活动相关的组织应满足 7.4.2 的要求。

7.4.2 责任、计划和所要求的流程

7.4.2.1 组织应按照 5.4.2.9 的要求指定具有相关责任和权限的人员，以维护相关项在生产发布后的功能安全。

7.4.2.2 应按照 GB/T 34590.7—2017 对确保相关项生产发布后的功能安全的活动进行计划，并应按照 GB/T 34590.4—2017 在系统层面产品开发过程中启动该活动。

7.4.2.3 组织应建立、执行并维护流程以保持相关项在生产发布后的各生命周期阶段的功能安全。

7.4.2.4 组织应建立、执行并维护与相关项功能安全相关的现场监控流程。

注 1：安全事故的现场监控流程包含报告事故、修正措施，例如召回以及相应的处理过程。

注 2：从现场监控收集的数据可用做在用证明（参见 GB/T 34590.8—2017 第 14 章）。

7.4.2.5 如果生产发布后相关项有变更，应重新按照 GB/T 34590.4—2017 第 11 章的要求进行生产发布。

注：变更应符合变更管理的要求（参见 GB/T 34590.8—2017 第 8 章）。

7.5 工作成果

7.5.1 现场监控的证据，参见 7.4.2.4。

附 录 A
（资料性附录）
功能安全管理的概览和工作流

表 A.1 提供了功能安全管理特定阶段的目标、前提条件和工作成果概览。

表 A.1 功能安全管理概览

章	目的	前提条件	工作成果
5 整体安全管理	本章的目的是定义负责安全生命周期或在安全生命周期内执行安全活动的组织的要求。 本章是 GB/T 34590 安全生命周期内所有活动的前提条件	无	5.5.1 组织的专门的功能安全规章和流程； 5.5.2 能力证据； 5.5.3 质量管理证据
6 概念阶段和产品开发过程中的安全管理	本章的第一个目标是定义关于安全生命周期内，概念阶段和开发阶段的安全管理角色和职责。 本章的第二个目的是定义在概念阶段和开发阶段中的安全管理要求，包括安全活动的计划和协调、安全生命周期的推进、安全档案的创建和认可措施的执行	组织的专门的功能安全规章和流程(参见 5.5.1)； 能力证据(参见 5.5.2)； 质量管理证据(参见 5.5.3)	6.5.1 安全计划； 6.5.2 项目计划(细化的)； 6.5.3 安全档案； 6.5.4 功能安全评估计划； 6.5.5 认可措施报告
7 相关项生产发布后的安全管理	本章的目的是定义相关项生产发布后，负责功能安全的组织和人员的职责。这与确保在生产发布后的生命周期子阶段内，相关项所需的功能安全的常规活动相关	质量管理证据(参见 5.5.3)	7.5 现场监控的证据

附 录 B
（资料性附录）
评估安全文化的示例

表 B.1 给出了评估安全文化的示例。

表 B.1 评估安全文化的示例

缺乏安全文化的例子	良好安全文化的例子
责任不具备可追溯性	流程确保了与功能安全相关的决策责任是可追溯的
成本和进度总是优先于安全和质量	安全是最高优先级
与安全和质量相比，奖励制度更有利于成本和进度	奖励制度支持并激励有效地实现功能安全； 奖励制度惩罚那些走捷径而危及安全或质量的人
评估安全、质量以及管理流程的人员过度地受到负责执行流程人员的影响	流程提供了足够的相互制衡，例如：集成过程中适当的独立程度（安全、质量、验证、确认以及配置管理）
对于安全的消极态度，例如： ——严重依赖于产品开发周期后期的测试； ——管理仅当现场出现问题时才有应对	对于安全的积极态度，例如： ——安全和质量问题在产品生命周期的最初阶段发现并得到解决
所要求的资源没有以一种及时的方式进行计划或分配	所要求的资源被分配； 技术资源具有与所分配的活动相匹配的能力
群体思维； 形成审查小组时“暗中布局”； 异议者被排斥或认定为“不是团队成员”； 反对意见对绩效考核有消极的影响； 少数异议者被认为是“麻烦制造者”，“不是团队成员”或“告密者”； 有质疑的员工害怕后果	流程采用多样性优势： ——在所有的流程中探寻、评价和综合多样性； ——不鼓励并惩罚反对采用多样性的行为。 存在支持交流和决策的渠道，并鼓励下列管理做法： ——鼓励自我披露； ——鼓励其他任何人进行披露； ——发现和解决问题的过程持续进行
没有系统的持续改进流程、学习循环或其他形式的经验总结	持续改进集成到所有的流程中
流程是临时的或不明确的	在所有层面执行一个明确的、可追踪的和受控的流程，包括： ——管理； ——工程； ——开发接口； ——验证； ——确认； ——功能安全审核； ——功能安全评估

附 录 C
（资料性附录）
认可措施的目标

C.1 安全计划评审（参见 6.5.1）

C.1.1 评估安全计划与 GB/T 34590—2017 中安全生命周期的符合性。如果适用，评估安全活动的剪裁，即相比于参考安全生命周期，省略的或以不同的方式执行的安全活动，包括相应的理由（参见 6.4.5）。

C.1.2 评估安全计划与 GB/T 34590—2017 中关于安全活动计划的要求的符合性（参见 6.4.3～6.4.5）。

C.2 安全档案完整性评审（参见 6.5.3）

C.2.1 确认在安全档案中参考的工作成果存在并完整，以便能充分地评估相关项功能安全的实现情况。

注：参考的工作成果可以是与支持安全档案相关的工作成果。

C.2.2 确认在安全档案中参考的工作成果：

——可追溯性；

——工作成果内部或成果之间没有矛盾；及

——既没有导致违背安全目标的问题，或存在的问题是可控的并且有计划得到解决。

C.3 功能安全审核（参见 6.4.8 和 6.5.5）

基于在安全计划中参考的或特定的安全活动的定义，在流程的执行过程中，评估功能安全流程的实施。

C.4 功能安全评估（参见 6.4.9 和 6.5.5）

C.4.1 按照 GB/T 34590—2017 相关要求评估安全计划所要求的工作成果的符合性，包括但不限于需要认可评审的工作成果。对于后者，应考虑认可评审的结果。

C.4.2 考虑功能安全审核的结果的同时，评估功能安全流程的实施（参见 6.4.8）。

C.4.3 对于在相关项开发期间可评估的、所用安全措施的适宜性和有效性进行评审。

C.4.4 如果适用，跟踪先前功能安全评估结果的建议，包括任何已执行的修正行为（参见 6.4.9.7 和 6.4.9.8）。

C.5 危害分析和风险评估的评审（参见 GB/T 34590.3—2017 第 7 章，以及如果适用，GB/T 34590.8—2017 第 5 章）

按照 GB/T 34590—2017 危害分析和风险评估流程，评估危害分析和风险评估的完整性，以及所确定的 ASIL 等级（含 QM）和安全目标的正确性。

C.6 相关项集成和测试计划评审(参见 GB/T 34590.4—2017)

按照 GB/T 34590 关于集成和测试活动的要求,评估相关项集成和测试计划的符合性。

C.7 确认计划评审(参见 GB/T 34590.4—2017)

按照 GB/T 34590—2017 关于安全确认活动的要求,评估确认计划的符合性。

C.8 如果适用,候选项在用证明的评审(参见 GB/T 34590.8—2017 第 14 章)

C.8.1 评估确定在用证明分析的结果是否证明了候选项声明的在用证明可信度(关于任何相关的安全活动的剪裁)。

C.8.2 评估现场监控流程的有效性。

C.8.3 评估在用证明考虑到的候选项更改。

C.9 评审软件工具准则评估报告和软件工具鉴定报告(参见 GB/T 34590.8—2017 第 11 章)

C.9.1 确认正确评估了在相关项或安全相关要素开发中所应用的软件工具的置信度。

C.9.2 按照所需的软件置信度,对软件工具鉴定进行评估。

C.10 安全分析评审(参见 GB/T 34590.9—2017 第 8 章)

评估正确执行了安全分析,且该安全分析可识别出能导致违背安全目标的故障或不充分的安全机制。

附 录 D
（资料性附录）
验证评审概览

表 D.1 提供了 GB/T 34590 其他部分要求的验证评审概览（也可参见 GB/T 34590.8—2017 第 9 章）。

表 D.1 验证评审概览

验证评审的内容	相关项安全目标中最高的 ASIL 等级				要求或推荐的条目
	A	B	C	D	
相关项的危害分析和风险评估（参见 GB/T 34590.3—2017 第 5 章和第 7 章，如果适用，GB/T 34590.8—2017 第 5 章）	要求[a]				GB/T 34590.3—2017 第 7 章
安全目标	要求				GB/T 34590.3—2017 第 7 章
功能安全概念	要求				GB/T 34590.3—2017 第 8 章
技术安全需求规范	要求				GB/T 34590.4—2017 第 6 章
系统设计	要求				GB/T 34590.4—2017 第 7 章
硬件安全要求	要求				GB/T 34590.5—2017 第 6 章
硬件设计	要求				GB/T 34590.5—2017 第 7 章
对于硬件架构评估的结果	[b]	推荐	要求	要求	GB/T 34590.5—2017 第 8 章
按照应用的评估方法，分析由于随机硬件失效造成的对安全目标的潜在违背	[b]	推荐	要求	要求	GB/T 34590.5—2017 第 9 章
软件安全要求和细化的软硬件接口要求	要求				GB/T 34590.6—2017 第 6 章和第 11 章
软件架构设计	要求				GB/T 34590.6—2017 第 7 章
软件单元的设计和实现	要求				GB/T 34590.6—2017 第 8 章
软件组件鉴定报告	对于有鉴定要求的软件模块有要求				GB/T 34590.8—2017 第 12 章
硬件组件鉴定报告	对于有鉴定要求的硬件模块有要求				GB/T 34590.8—2017 第 13 章
安全分析	要求				GB/T 34590.9—2017 第 8 章

[a] 评审范围也包括等级为 QM 的危害事件。

[b] 无要求和建议。

附 录 E
（资料性附录）
功能安全评估安排举例（用于具有 ASIL D 等级的安全目标的相关项）

E.1 安全管理

E.1.1 所评估项目中的组织的安全文化和支持过程的应用。

E.1.2 所评估项目中的能力管理和持续改进的应用。

E.1.3 所评估项目中的角色和责任。

E.1.4 所评估项目的安全计划和分布式开发计划。

E.1.5 所评估项目的安全生命周期的剪裁，包括候选项的在用证明。

E.1.6 功能安全审核、安全档案和可用文档。

E.2 概念阶段期间的安全活动

E.2.1 相关项定义。

E.2.2 危害分析和风险评估。

E.2.3 功能安全概念。

E.2.4 相关项及其安全概念与其他系统/功能的依赖关系。

E.2.5 功能安全要求分配到：

——电气电子要素；

——应用其他技术的要素；

——与外部措施的接口。

E.2.6 功能安全概念验证。

E.3 系统开发阶段的安全活动

E.3.1 系统开发、集成和确认计划。

E.3.2 技术安全概念及其验证。

E.3.3 系统设计和系统失效的避免。

E.3.4 软硬件要素的技术安全要求分配和软硬件接口评审。

E.3.5 系统设计验证。

E.4 硬件开发

E.4.1 硬件开发、鉴定和集成计划。

E.4.2 硬件安全要求、硬件设计和验证。

E.4.3 硬件架构的约束。

E.4.4 评估因随机硬件失效而违背安全目标的可能性。

E.4.5 硬件集成和测试。

E.5 软件开发

E.5.1 软件开发、鉴定和集成计划。

E.5.2 软件安全要求、软件架构设计、软件单元设计和实现。

E.5.3 软件单元测试。

E.5.4 软件集成和测试。

E.5.5 软件安全要求验证。

E.6 相关项集成

E.6.1 集成测试的计划。

E.6.2 软硬件集成和测试。

E.6.3 系统/相关项集成。

E.6.4 整车集成。

E.7 安全确认和生产发布

E.7.1 确认活动。

E.7.2 确认文档和生产发布。

E.8 生产和维护计划

E.8.1 生产阶段与安全相关的特性。

E.8.2 运行、服务和报废阶段与安全相关的特性。

E.9 总结

功能安全评估的文档、建议和功能安全评估后采取的行动。

参 考 文 献

[1] GB/T 20438—2006(所有部分) 电气/电子/可编程电子安全相关系统的功能安全

[2] ISO 9001 Quality management systems—Requirements

[3] ISO/IEC 15504 (all parts) Information technology—Process assessment

[4] ISO/TS 16949 Quality management systems—Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations

中 华 人 民 共 和 国
国 家 标 准
道路车辆 功能安全
第 2 部分：功能安全管理
GB/T 34590.2—2017
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址：www.spc.org.cn
服务热线：400-168-0010
2017 年 10 月第一版
*
书号：155066 · 1-57767

GB/T 34590.2-2017