ICS 43.430
CCS T 35

中华人民共和国国家标准

GB/T 34590.2—XXXX
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

Road vehicles—Functional safety—Part2：Management of functional safety

(ISO 26262-2:2018,MOD)

（征求意见稿）

（本草案完成时间：2021年4月1日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照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》的规定起草。

GB/T 34590-XXXX《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、运行、服务和报废；

——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；

——第 11 部分：半导体应用指南；

——第 12 部分：摩托车的适用性。

本文件为GB/T 34590-XXXX的第2部分。

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 26262-4：2018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。

本文件做了下列编辑性修改：

——将国际标准中的“本国际标准”改为“本文件”；

——删除国际标准的前言；

——修改国际标准的引言及其表述。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会（SAC/TC114）归口。

本文件起草单位：

本文件主要起草人：

本文件所代替文件的历次版本发布情况为：

——GB/T 34590.2,2017 年首次发布。

引　言

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

安全是道路车辆开发的关键问题之一。汽车功能的开发和集成强化了对功能安全的需求，以及对提供证据证明满足功能安全目标的需求。

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，这些都在功能安全的考虑范畴之内。GB/T 34590通过提供适当的要求和流程来降低风险。

为了实现功能安全，GB/T 34590-XXXX（所有部分）：

a) 提供了一个汽车安全生命周期（开发、生产、运行、服务、报废）的参考，并支持在这些生命周期阶段内对执行的活动进行剪裁；

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) 使用 ASIL 等级来定义 GB/T 34590 中适用的要求，以避免不合理的残余风险；

d) 提出了对于功能安全管理、设计、实现、验证、确认和认可措施的要求；及

e) 提出了客户与供应商之间关系的要求。

GB/T 34590针对的是电气/电子系统的功能安全,通过安全措施(包括安全机制)来实现。它也提供了一个框架，在该框架内可考虑基于其它技术（例如，机械、液压、气压）的安全相关系统。

功能安全的实现受开发过程（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-XXXX、GB/T 34590.4-XXXX、GB/T 34590.5-XXXX、GB/T 34590.6-XXXX、GB/T 34590.7-XXXX 之间的相互关系；

——对于摩托车：

- GB/T 34590.12-XXXX的第8章支持GB/T 34590.3-XXXX；
- GB/T 34590.12-XXXX的第9章和第10章支持GB/T 34590.4-XXXX。

——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-XXXX 的第 6 章。

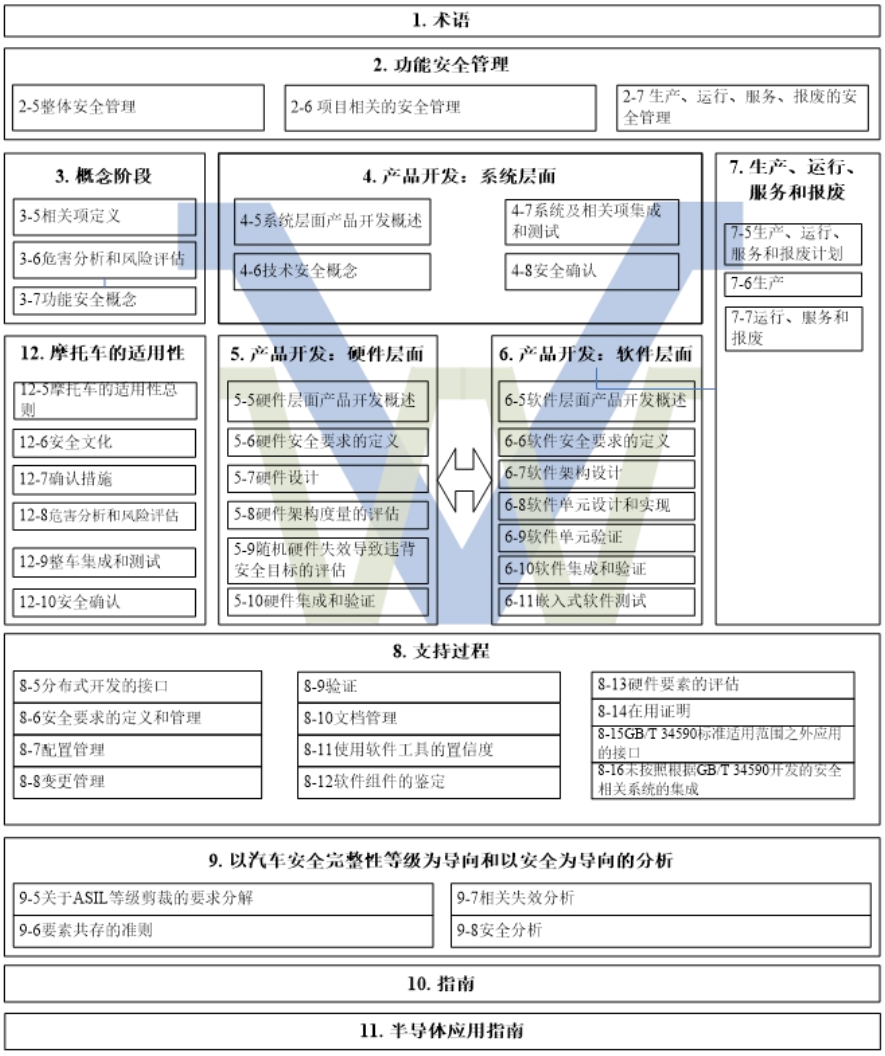

图 1　GB/T 34590-XXXX 概览

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（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。

本文件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电气/电子系统的与安全相关的系统。

本文件不适用于特殊用途车辆上特定的电气/电子系统，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文件发布日期前正在开发的系统及其组件不适用于本文件。对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，本文件基于这些变更对安全生命周期的活动进行剪裁。未按照本文件开发的系统与按照本文件开发的系统进行集成时，需要按照本文件进行安全生命周期的剪裁。

本文件针对由安全相关的电气/电子系统的功能异常表现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，除非危害是直接由安全相关的电气/电子系统的功能异常表现表现而引起的。

本文件提出了安全相关的电气/电子系统进行功能安全开发的框架，该框架旨在将功能安全活动整合到企业特定的开发框架中。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。

本文件不针对电气/电子系统的标称性能。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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-XXXX 道路车辆 功能安全 第1部分：术语(ISO 26262-1:2018,MOD)

GB/T 34590.3-XXXX 道路车辆 功能安全 第3部分：概念阶段(ISO 26262-3:2018,MOD)

GB/T 34590.4-XXXX 道路车辆 功能安全 第4部分：产品开发：系统层面(ISO 26262-4:2018,MOD)

GB/T 34590.5-XXXX 道路车辆 功能安全 第5部分：产品开发：硬件层面(ISO 26262-5:2018,MOD)

GB/T 34590.6-XXXX 道路车辆 功能安全 第6部分：产品开发：软件层面(ISO 26262-6:2018,MOD)

GB/T 34590.7-XXXX 道路车辆 功能安全 第7部分:生产、运行、服务和报废(ISO 26262-7:2018,MOD)

GB/T 34590.8-XXXX 道路车辆 功能安全 第8部分：支持过程(ISO 26262-8:2018,MOD)

GB/T 34590.9-XXXX 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 26262-9:2018,MOD)

3 术语、定义和缩略语

GB/T 34590.1-XXXX界定的术语、定义和缩略语适用于本文件。

4 要求

4.1 目的

本章规定了：

a) 如何符合 GB/T 34590-XXXX；

b) 如何解释 GB/T 34590-XXXX 中所使用的表格；及

c) 如何解释各章条基于不同的 ASIL 等级的适用性。

4.2 一般要求

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

a) 按照本文件的要求，安全活动的剪裁已经实施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，并且按照本文件的要求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。

4.3 表的诠释

本文件中的表是规范性或资料性取决于上下文。在满足相关要求时，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，高度推荐和推荐的方法按照ASIL等级推荐予以使用。高度推荐或推荐的方法允许用未列入表中的其它方法替代,此种情况下，应给出满足相关要求的理由。如果可以给出不选择所有条目也能符合相应要求的理由，则不需要对缺省方法做进一步解释。

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，而与这些方法在表中是否列出无关。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。应给出选择组合方法或选择单一方法满足相应要求的理由。

注：在表中所列出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。

4.4 基于 ASIL 等级的要求和建议

若无其它说明，对于ASIL A、 B、 C和D等级，应满足每一章条的要求或建议。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，按照GB/T 34590.9第5章的要求，应遵循分解后的ASIL等级。

如果GB/T 34590中ASIL等级在括号中给出，则对于该ASIL等级，相应的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。

4.5 摩托车的适用性

对于适用于GB/T 34590.12要求的摩托车的相关项或要素，GB/T 34590.12的要求替代本文件和GB/T 34590.2的相应要求。

4.6 卡车、客车、挂车和半挂车的适用性

对卡车、客车、挂车和半挂车的特殊规定以（T&B）来表示。

5 整体安全管理

5.1 目的

本章旨在确保参与安全生命周期执行的组织,即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，实现以下目标：

a) 建立并维护能够用于支持和鼓励功能安全有效实现，并能够促进与功能安全相关的其他领域有效沟通的安全文化；
b) 建立并维护充分的组织的专门的功能安全规章和流程；
c) 建立并维护可确保能充分解决识别出的安全异常的流程；

建立并维护可确保参与人员的能力与其职责相匹配的能力管理体系；及

建立并维护用以支持功能安全的质量管理体系。

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 34590参考安全生命周期包含了在概念阶段、产品开发、生产、运行、服务和报废期间的主要安全活动。计划、协调和监控安全活动的进度，以及确保认可措施得到执行，是关键的管理任务，并且贯穿整个生命周期。安全生命周期可以被剪裁（本文件第6章）。

注 1：GB/T 34590.3-XXXX、GB/T 34590.4-XXXX、GB/T 34590.5-XXXX、GB/T 34590.6-XXXX 和 GB/T 34590.7-XXX 分别详细描述了在概念阶段、产品开发、生产、运行、服务和报废期间的安全活动。

注 2：表 A.1 概括了功能安全管理的目的、前提条件和工作成果。

图2说明了与安全生命周期相关的管理活动。

注 3：在图中，GB/T 34590-XXXX 各部分中的具体条款用以下方式表示：“m-n”,其中 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-XXXX 的第 6 章。

注 4：1)系统层面产品开发的子阶段如 GB/T 34590.4-XXXX 图 2 所示。

注 5：2)硬件层面产品开发的子阶段如 GB/T 34590.5-XXXX 图 2 所示。

注 6：3)软件层面产品开发的子阶段如 GB/T 34590.6-XXXX 图 2 所示。

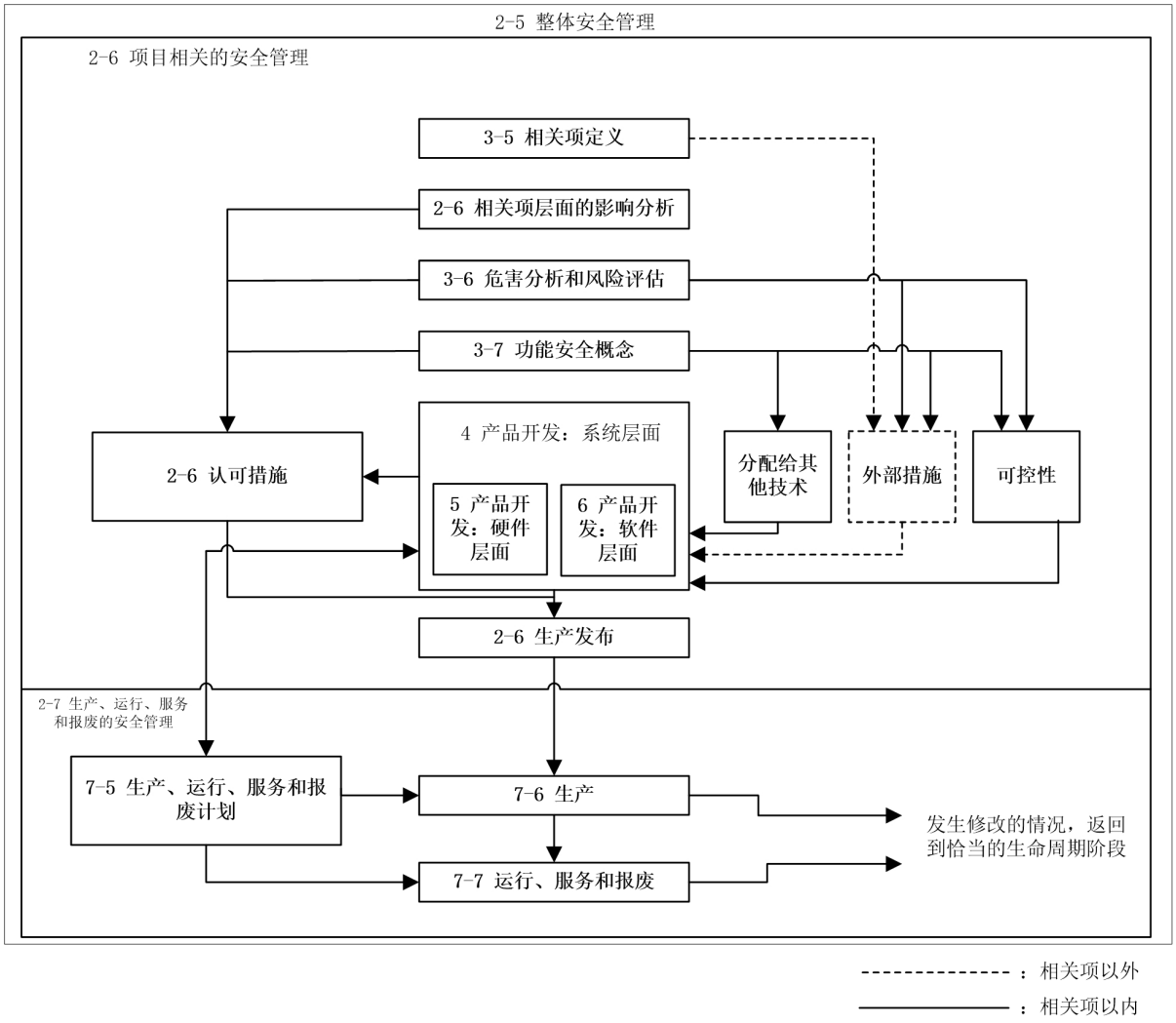

图 2　与安全生命周期相关的管理活动

5.2.2　安全生命周期的解释说明

5.2.2.1　总则

GB/T 34590 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多个或全部阶段的要求，例如功能安全管理的要求。

关键的安全管理任务是计划、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。本文件给出了功能安全管理的要求，分别是：

——整体安全管理（本文件第 5 章）；

——在概念阶段及在系统、硬件和软件层面产品开发阶段的项目相关的安全管理（本文件第 6 章）；及

——生产、运行、服务和报废的安全管理（本文件第 7 章）。

开发相关的安全活动计划在概念阶段启动，并在产品开发阶段（系统、硬件和软件）中进行必需的细化，直到决定对相关项或要素进行生产发布。与生产、运行、服务和报废相关的活动计划在系统层面的产品开发期间启动。

第5.2.2.2条阐述了安全生命周期内不同阶段和子阶段的定义。第5.2.2.3条阐述了在安全生命周期内需要考虑的其他关键概念。

5.2.2.2 安全生命周期的阶段和子阶段

a) 相关项定义（概念阶段的子阶段）：
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，以及对其他相关项、要素或者外部措施的假设（见 GB/T 34590.3-XXXX 第 5 章）。

b) 危害分析和风险评估（概念阶段的子阶段）：
按照 GB/T 34590.3-XXXX,第 6 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 ASIL 等级。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。在危害分析和风险评估、功能安全概念和技术安全概念中，对人员行为的假设（包括可控性和人员反应）以及与 ASIL 分级相关的技术假设是经过确认的。（见 GB/T 34590.3-XXXX 第 6 章，GB/T 34590.3-XXXX 第 7 章和 GB/T 34590.4-XXXX 第 8 章）。
后续阶段和子阶段中详细的安全要求来自安全目标。安全要求继承了相应安全目标的 ASIL 等级，或者在应用了 ASIL 等级剪裁的要求进行分解的情况下，接受分解后的 ASIL 等级。（见 GB/T 34590.9-XXXX 第 5 章）。

c) 功能安全概念（概念阶段的子阶段）：
基于安全目标，同时考虑初步的构架设想以开发功能安全概念（见 GB/T 34590.3-XXXX,第 7 章）。功能安全概念是通过从安全目标中导出功能安全要求，并通过将这些功能安全要求分配给相关项要素来开发的。功能安全概念还可以包括其他技术或依赖于外部措施（见 GB/T 34590.3-XXXX,第 7 章）。在这些情况下，对相应的假设或预期行为进行确认（见 GB/T 34590.4-XXXX,第 8 章）。其他技术的实施不在本文件系列范围内，且外部措施的实施不在相关项开发范围内。

d) 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-XXXX，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、安全确认。
在本阶段定义了软硬件接口。硬件和软件之间的接口在硬件和软件开发期间进行更新。
GB/T 34590.4-XXXX，图 2 提供了系统开发子阶段的概览。
系统开发包括对发生在安全生命周期内其他阶段活动的安全确认任务，包括：
——与 ASIL 等级分类相关的技术假设；
——对人员行为所做假设的确认，包括可控性和人员反应；
——对通过其他技术实现的功能安全概念的确认；及
——对外部措施有效性的假设的确认和对表现性能的假设的确认。

e) 产品开发:硬件层面
基于系统设计规范，开发硬件（见 GB/T 34590.5-XXXX）。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验证。
GB/T 34590.5-XXXX，图 2 提供了硬件开发子阶段的概览。

f) 产品开发:软件层面
基于系统设计规范，开发软件（见 GB/T 34590.6-XXXX）。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和验证。

GB/T 34590.6-XXXX，图 2 提供了软件开发子阶段的概览。

g) 生产、运行、服务和报废

这一阶段的计划（见 GB/T 34590.7-XXXX，第 5 章），以及相关要求的规范，在系统层面的产品开发过程中开始（见 GB/T 34590.4-XXXX），并与系统、硬件和软件开发并行。这样的计划可以通过交换信息或要求来实现，例如提高产品生产能力的安全相关的特殊特性或要求。

这一阶段描述了流程、方法和说明以确保相关项或要素的生产、运行、服务和报废中的功能安全。安全相关的特殊特性，以及相关项或要素的生产、运行、服务（维护和维修）和报废的指导说明的开发和管理是要被考虑的（见 GB/T 34590.7-XXXX，第 6 章和第 7 章）。

5.2.2.3 其他关键概念

a) 认可措施

实施认可措施（本文件第 6 章）以判断相关项实现了功能安全，或对实现功能安全的贡献，例如关于要素的开发。

b) 可控性

在危害分析和风险评估（见 GB/T 34590.3-XXXX，第 6 章）中，驾驶员或其他涉险人员（例如，行人、骑自行车者、乘客、其他车辆的驾驶员）避免特定伤害的能力的可信度，可能受到外部措施的支持。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（见 GB/T 34590.3-XXXX，第 6 章和第 7 章，和 GB/T 34590.4-XXXX，第 8 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，在安全确认过程中进行评估（见GB/T 34590.4-XXXX，第8章）。

c) 外部措施

外部措施是指在相关项边界外（见 GB/T 34590.3-XXXX，第 5 章）减少或减轻相关项故障行为造成的潜在危害的措施。外部措施可以包括额外的车载装置，如动态稳定控制器或防爆轮胎，也可以包括车外装置，如防撞护栏或隧道消防系统。

需确认在相关项定义、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（见 GB/T 34590.4-XXXX，第 8 章）。

可在危害分析和风险评估过程中考虑外部措施（见 GB/T 34590.3-XXXX 中，第 6 章),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（如降低安全目标的 ASIL 等级）,则在功能安全概念中不能再次认为此外部措施是一个减少风险的途径。

外部措施可以在 GB/T 34590 的范围之外（例如，外部措施是由另一技术实现或在车辆以外实施），或在 GBT 34590 的范围内（例如，如果外部措施由与相关项不同的电气/电子系统实现）。

d) 影响分析：相关项层面

在相关项层面执行影响分析（见 6.4.3）以确定相关项是全新开发、或是对现有相关项的修改，还是对现有相关项环境的修改，如果有一个或多个修改，则分析修改对功能安全的影响。

e) 影响分析：要素层面

当现有要素被复用（本文件 6.4.4）时，在要素层面进行影响分析，以评估复用要素是否能够符合分配给该要素的安全要求，分析时要考虑要素被复用时所在的运行环境。

f) 其他技术

其他技术（如机械和液压技术）不同于电子电气技术。这些技术可在安全要求的规范制定中和分配中(见 GB/T 34590.3-XXXX，第 7 章和 GB/T 34590.4-XXXX)被考虑，或作为外部措施被考虑。换言之，由其他技术实现的要素可以在相关项内实施，或者可以定义为外部措施。

g) 生产发布

考虑安全生命周期的成果（包括适用的认可措施的成果），生产发布（本文件 6.4.13）正式决定将相关项或要素用于生产。

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：

符合质量管理标准的证据。

示例 1：IATF 16949 与 ISO 9001 中关于安全生命周期各个阶段的质量管理。

示例 2：ISO/IEC 33000 标准系列，能力成熟度模型集成(CMMI®)或是汽车软件过程改进及能力评定(Automotive SPICE®)[1)]标准系列中关于产品开发的部分。

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该满足第5.4.2～5.4.6条。

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。

注：附件B提供了构建安全文化的更多细节。

5.4.2.2 组织应建立、执行并维护组织的专门的规章和流程，以实现且维护功能安全并符合 GB/T 34590 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计划（例如：通用安全计划）或通用的流程描述。

5.4.2.3 组织应建立并维护功能安全、预期功能安全、信息安全及与实现功能安全相关的其他领域之间的有效沟通渠道。

示例 1：建立功能安全与预期功能安全之间的沟通渠道，以便于两者交互相关信息（例如，在产品开发过程中，功能安全活动和预期功能安全活动是并行开展的，需要针对可能的相互影响进行评估）。

示例 2：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，在识别到信息安全问题可能违背安全目标或安全要求的情况下，或在信息安全要求可能与功能安全要求冲突的情况下）。

示例 3：建立功能安全和非电气/电子系统相关安全（如机械安全）之间的沟通渠道。

示例 4：建立功能安全和质量之间的沟通渠道。

注：关于功能安全与信息安全潜在交互的指导见附录E。

5.4.2.4 在安全生命周期执行期间，组织应执行要求的安全活动，包括文档的创建和管理(按照 GB/34590.8—XXXX，第 10 章的说明)。

5.4.2.5 组织应为功能安全的实现提供所需的资源。

注：资源包括人力资源、工具、数据库、指南和工作说明。

5.4.2.6 基于以下几点，组织应建立、执行并维护持续改进的流程：

---

1) CMMI®和 Automotive SPICE®是适用的商业产品示例。这些信息是为了方便本文件的用户而提供的，并不代表本文件对这些产品的推荐。

——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；及

——将获得的改进应用于后续相关项。

5.4.2.7 组织应确保给予负责实现或维护功能安全、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 关于功能安全的安全异常管理

5.4.3.1 组织应建立、执行并维护流程，以确保将识别出的安全异常明确传达给负责在安全生命周期内实现或维护功能安全的人员。

注：根据安全异常情况，责任人可包括客户安全经理、供应商安全经理、与相关项开发相关的安全经理，或在生产、运行、服务和报废期间实现和维护功能安全的人员。

5.4.3.2 组织应建立、执行和维护安全异常解决流程，以确保及时、有效地分析、评估、解决和管理已识别的安全异常，直至关闭。

注：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。

注：如果安全异常的解决导致变更，则按照GB/T 34590.8-XXXX中，第8章，将该变更纳入变更管理流程。

注：安全经理可以提名负责解决安全异常的人员。

注：安全异常解决流程可以整合进质量管理体系的异常解决流程中（见5.4.5）。

5.4.3.3 只有达成以下条件，安全异常才应认为被关闭：

a) 基于某一依据，实施了充分的安全措施以解决安全异常，且安全措施的有效性得到了验证；或

注1：在设计变更解决了安全异常的情况下，按照ISO 26262-8：2018第8章进行的相应的影响分析可提供依据。

注2：安全异常可以通过其他技术实施的措施或外部措施（例如ISO 26262 范围之外的措施）解决。

b) 基于某一依据，将安全异常评估为不构成不合理风险并将其关闭。

注3：如果没有合理依据，则无法关闭安全异常。

5.4.3.4 应对 5.4.3.3 规定的关闭安全异常的依据进行记录；并应进行评审。

示例：对关闭安全异常的依据的评审可以作为功能安全评估的一部分（见 6.4.12）。

5.4.3.5 未完成关闭的安全异常应上报给负责功能安全的人员，比如将涉及产品开发的安全异常上报给项目经理。

注：如果在开发过程中识别到安全异常，但未完成关闭，而此时进行功能安全评估，则负责功能安全评估的人员是需被明确传达安全异常的人员之一。

5.4.4 能力管理

5.4.4.1 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-XXXX 标准和其他适用的安全标准；

——用于功能安全组织的专门规则；

——用于与功能安全交互专业的组织的专门规则；及

——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-XXXX 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；

——相关项环境方面的专业知识；

——管理经验；及

——生产、运行、服务和报废方面的专业知识。

注 3：组织可以定义技能、能力和资质的充分性的标准。

示例：英国健康与安全执行局在“安全相关系统管理能力”中给出的准则。

5.4.5 质量管理体系

5.4.5.1 组织应具有支持实现功能安全并满足质量管理标准如 IATF 16949，ISO 9001 或等同标准的质量管理体系。

5.4.6 独立于项目的安全生命周期剪裁

5.4.6.1 组织可剪裁安全生命周期，应用于各相关项或要素，即独立于项目的剪裁，仅限于以下情况 ：

a) 合并或分解子阶段、活动或任务；

注：如果所用的方法难以清晰地区分单独的子阶段，那么这些子阶段可以合并。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) 在不同的阶段或子阶段中执行同一活动或任务；

c) 在新增的阶段或子阶段中执行同一活动或任务；

d) 反复进行某个阶段或子阶段；

e) 若符合 6.4.7.1，执行与其他阶段或子阶段的安全活动同时进行的安全活动；或

f) 根据某个理由，省略不适用于组织的阶段或子阶段。

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 到 5.4.6 得出。

5.5.2 能力管理证据，由 5.4.4 得出。

5.5.3 质量管理体系证据，由 5.4.5 和 5.4.6 得出。

5.5.4 已识别的安全异常报告（如果适用），由 5.4.3 得出。

6 项目相关的安全管理

6.1 目的

本章的目的是，确保参与概念阶段或系统、硬件、软件层面开发阶段的组织实现以下目标：

a) 定义与分配安全活动相关的角色和责任；

b) 在相关项层面执行影响分析，以识别相关项是全新的，或是对现有相关项修改，还是对现有相关项的使用环境进行修改；并在有一项或多项修改时，分析所识别出的修改对功能安全的影响；

c) 在现有要素复用的情况下，在要素层面执行影响分析，评估复用的要素是否可以满足分配给它的安全要求，并考虑该要素复用的运行环境；

注：在相关项或要素层面的影响分析能支持安全活动的计划（见6.4.6.7）。

d) 定义所剪裁的安全活动，提供相应的剪裁理由，并评审所提供的理由；

e) 计划安全活动；

f) 按照安全计划协调并追踪安全活动的进度；
g) 规划分布式开发(见 GB/T 34590.8-XXXX，第 5 章)；
h) 在整个安全生命周期内，确保安全活动的正确进程；
i) 创建可理解的安全档案，以提供实现了功能安全的证据；
j) 判断相关项是否实现了功能安全（即功能安全评估），或者判断某一要素（即供应商进行的功能安全评估活动）或工作成果（例如认可评审）对于实现功能安全的贡献；及
k) 在开发结束时，基于支持有信心实现功能安全的证据，决定相关项或要素是否能够生产发布。

6.2 总则

在项目中，定义和分配与安全活动相关的角色和职责。

在相关项层面进行影响分析，以识别相关项是全新的，或是对现有相关项修改，还是对现有相关项的使用环境进行修改；并在有一项或多项修改时，分析所识别出的修改对功能安全的影响。

在现有要素复用的情况下，在要素层面进行影响分析，并考虑该要素复用的运行环境。

安全管理包括计划和协调安全活动、根据相应的计划跟踪活动进度的责任，以及对被剪裁的安全活动进行描述和理由说明的责任。

将安全计划文档化，并参考开发接口协议（见GB/34590.8—XXXX，第5章），该协议定义了在分布式开发中与其他方的安全计划的接口。

安全管理也有责任确保执行认可措施。根据适用的ASIL等级，认可措施的执行要求在资源、管理和发布权限上的充分独立性。

认可措施包括认可评审、功能安全审核和功能安全评估：

——认可评审的目的是评判关键工作成果（见表 1）是否提供了充分和令人信服的证据，证明其对实现功能安全的贡献；

——如果适用，功能安全审核的目的是评估安全活动所要求的流程的执行情况；

——如果适用，功能安全评估的目的是判断相关项是否实现了功能安全，或判断对功能安全实现的贡献（例如要素的开发）。

表1列出了认可措施。

除了认可措施外，还需进行验证活动。按照GB/T 34590-XXXX其他部分的要求，这些验证活动用于验证相关工作成果是否满足项目要求以及技术要求，尤其是与应用案例和失效模式相关的技术要求。

最后，相关项或相关项中各要素的发布责任人，基于支持有信心实现功能安全的证据，判断相关项或要素是否已做好了批量生产和运行的准备。

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；

能力管理证据，按照5.5.2；及

质量管理体系证据，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；及

——其他用于进行影响分析的现有信息（见 6.4.3 和 6.4.4）。

示例：产品概念、修改请求、实施计划或在用证明。

6.4 要求和建议

6.4.1 总则

第6.4.2～6.4.13条适用于参与相关项或相关项的一个或多个要素的概念阶段或产品开发阶段（系统、硬件或软件）的组织。

示例：供应商开发了一个要由客户集成的要素（见 GB/T 34590.8:XXXX，第 5 章），该要素根据 4.4 的要求，实施一个或多个 ASIL 等级为 A、B、C 或 D 的安全要求。

6.4.2 安全管理的角色和职责

6.4.2.1 在相关项产品开发的启动阶段应指定一名项目经理。

注：在分布式开发的情况下（见GB/T 34590.8:XXXX，第5章），客户和开发一个或多个将被集成的要素的供应商，均需任命项目经理。

6.4.2.2 应按照 5.4.2.7 的要求赋予项目经理责任和权限，以确保：

a) 执行实现功能安全所需的安全活动；及
b) 满足 GB/T 34590-XXXX 的要求。

6.4.2.3 项目经理应确认组织提供了符合 5.4.2.5 要求的功能安全活动所需的资源。

注：在计划阶段预估、确定并分配足够的资源。

6.4.2.4 项目经理应确保已指定了符合 5.4.4 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：因术语“安全经理”被定义为角色（见GB/T 34590.1-XXXX），其任务可以根据组织的形式分配给不同的人。

注3：在分布式开发的情况下（见GB/T 34590.8-XXXX，第5章），在客户处和开发一个或多个要集成的要素的供应商处任命安全经理。

6.4.3 相关项层面的影响分析

6.4.3.1 在安全生命周期开始时，应进行相关项层面的影响分析，以确定相关项是全新开发，或是对现有相关项修改，还是对现有相关项的使用环境进行修改。

注：在用证在用证明可适用于修改的情况（见GB/T 34590.8-XXXX，第14章）。

6.4.3.2 在对相关项或其环境修改的情况下，按照 6.4.3.1 执行的相关项层面的影响分析应识别并描述应用于相关项的修改，包括：

注 1：本章考虑的影响分析关注计划阶段相关项的修改。在开发执行过程中的设计修改是通过变更管理流程实现的（见 GB/T 34590.8-XXXX，第 8 章）。

a) 设计的修改；

注 2：设计的修改可来自需求的修改。

注 3：设计的修改可以影响相关项的行为。

示例 1：设计的修改可来自标定数据的修改。

示例 2：设计的修改可来自相关项运行模式的更改。

a) 实现方式的修改；及

注 4：实现方式的修改不影响相关项的规格或性能。

注 5：对于相关项实现方式的修改，可能会影响相关项的行为。

注 6：实现方式的修改可来自软件的修正。

b) 与环境相关的修改。

示例 3：温度、海拔、湿度、振动、电磁干扰（EMI）和燃料类型。

注 7：修改包括：

——将相关项安装于新的目标环境（如车辆变型）；

——运行场景的变更；及

——相关项在车内的不同位置。

6.4.3.3 按照 6.4.3.2，相关项层面的影响分析应：

a) 评估修改对功能安全的影响；及
b) 基于修改的影响，识别并描述要开展的安全活动。

6.4.4 现有要素的复用

在复用现有要素的情况下，应执行要素层面的影响分析，包括：

a) 识别运行环境的修改，包括其导致的对要素的修改；
b) 无论复用的要素是否进行修改，都需要评估其能否符合分配给其的安全要求，这些安全要求来自集成该要素的相关项或要素；

注1：无论是否计划对现有要素进行修改，它都可以被复用。例如，可以计划对要素进行修改，以实现现有要素的集成。

c) 基于修改影响（包括先前假设有效性的影响）进行评估，识别要执行的安全活动；及
d) 评估与复用要素有关的现有安全相关文档，并判断其是否支持将要素集成到相关项，或将要素集成到另一个要素。

注2：本章中考虑的影响分析涉及在计划阶段考虑的要素运行环境的修改。开发过程中考虑的设计修改通过变更管理流程执行。（见GB/T 34590.8，第8章）。

注3：现有要素的复用需：

a) 基于硬件要素的评估（见 GB/T 34590.8-XXXX，第 13 章）；
b) 基于软件组件的鉴定（见 GB/T 34590.8-XXXX，第 12 章）；
c) 基于在用证明（见 GB/T 34590.8-XXXX，第 14 章）；或
d) 作为独立于环境的安全要素（见 GB/T 34590.10-XXXX）。

6.4.5 安全活动的剪裁

6.4.5.1 可以对特定相关项开发的安全活动进行剪裁，即省略或以不同于 GB/T 34590 所参考的生命周期中规定的方式执行。如果安全活动被剪裁，那么

a) 应在安全计划中定义该剪裁（见 6.4.6.5，b）；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的认可评审（见 6.4.9）或功能安全评估（见 6.4.12）过程中进行评审。

注 3：本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 5.4.6 适用。

6.4.5.2 如果是按照影响分析结果（按照 6.4.3 或 6.4.4）对某一安全活动按照 6.4.5.1 进行剪裁，则应满足 6.4.6.7 的要求。

6.4.5.3 如果由于在用证明结果而按照 6.4.5.1 对某一安全活动进行剪裁，则剪裁应满足 GB/T 34590.8-XXXX，第 14 章的要求。

6.4.5.4 如果由于硬件要素评估而按照 6.4.5.1 对某一安全活动进行剪裁，则剪裁应满足 GB/T 34590.8-XXXX，第 13 章的要求。

6.4.5.5 如果是由于软件组件鉴定而按照 6.4.5.1 对某一安全活动进行剪裁，则剪裁应满足 GB/T 34590.8-XXXX，第 12 章的要求。

6.4.5.6 如果基于考虑所使用软件工具的置信度的依据而按照 6.4.5.1 对某一安全活动进行剪裁，则应满足 GB/T 34590.8-XXXX，第 11 章的要求。

6.4.5.7 如果由于要素被开发为独立于环境的安全要素（“SEooC”）而按照 6.4.5.1 对某一安全活动进行剪裁，那么

a) 独立于环境的安全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环境的假设，包括其外部接口；及
b) 当安全要素被集成到其目标应用中时，应验证对独立于环境的安全要素的预期用途和应用环境的假设。

注 1：本文件作为一个整体不能应用于独立于环境的安全要素的开发，因为功能安全不是一个要素属性（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通过功能安全评估方法来评价的相关项的属性。

示例：微控制器作为独立于环境的安全要素开发。

注 2：了解更多独立于环境的安全要素的开发见 GB/T 34590.10。

6.4.5.8 本要求适用于 T&B 的相关项的开发：如果某个应用超出了 GB/T 34590 的范围，且该应用正在与已根据这些标准开发的基础车辆或相关项进行对接，则应按照 GB/T 34590.8-XXXX，第 15 章的要求对相应的安全活动进行剪裁。

6.4.5.9 本要求适用于 T&B 的相关项的开发：如果开展安全活动，以确保未按照 GB/T 34590 开发的系统或组件，满足集成到按照这些标准开发的相关项中所需的功能安全水平，则应按照 GB/T 34590.8-XXXX，第 16 章的要求对这类安全活动进行剪裁。

6.4.6 安全活动的计划和协调

6.4.6.1 按照 5.4.2.7 的要求，安全经理应负责计划和协调组织所参与的功能安全活动。

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 （见 5.4.4）。

注 2：根据相关项是全新开发、对现有相关项的修改或是对现有相关项环境的修改（见 6.4.3），又或者要素是全新的还是复用的（见 6.4.4），安全活动范围可以不同，并据此计划相应的安全活动。

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

6.4.6.3 在组织内部应按照 5.4.2.7 和 5.4.4 的要求,分配并沟通关于执行安全活动的责任。

注：安全经理负责计划和协调安全活动。其他人员可以负责细化计划（见6.4.6.8）或执行安全活动（例如，计划或执行集成和验证活动以及配置管理）。

6.4.6.4 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（见GB/T 34590.8-XXXX，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。

6.4.6.5 安全计划应规定实现功能安全的活动计划和流程计划，包括：

a) 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；
b) 如果适用，所剪裁的安全活动的定义，按照 6.4.5；

注 1：例如，依据相关项层面（见 6.4.3）或要素层面（见 6.4.4）的影响分析结果进行剪裁。另参考 6.4.6.7。

c) 安全活动的计划需要满足 GB/T 34590.3-XXXX，GB/T 34590.4-XXXX，GB/T 34590.5-XXXX，GB/T 34590.6-XXXX 的要求；
d) 按照 GB/T 34590.8-XXXX，在适用的情况下，支持过程的计划，包括按照 GB/T 34590.8-XXXX，第 5 章，对定义与分布式开发中其他方的安全计划接口的开发接口协议（“DIA”）的引用；
e) 集成和验证活动计划，按照 GB/T 34590.3-XXXX、GB/T 34590.4-XXXX、GB/T 34590.5-XXXX、GB/T 34590.6-XXXX 和 GB/T 34590.8-XXXX，第 9 章；安全确认活动计划，按照 GB/T 34590.4-XXXX，第 8 章；

注 2：作为工作成果，安全计划包括详细的集成，验证和安全确认计划，然而这些计划也可包含在其他文档中（见 GB/T 34590.8-XXXX，第 10 章）。

f) 按照第 6.4.9～6.4.12 条的认可评审、功能安全审核和功能安全评估的日程安排；

注 3：6.4.9 给出的执行认可措施的人员的独立性水平在安全计划中定义。

注 4：安全经理负责认可措施的日程安排。详细的认可措施计划由相应认可措施的负责人制定。

g) 相关失效分析的计划，如果适用，按照 GB/T 34590.3-XXXX，GB/T 34590.4-XXXX，GB/T 34590.5-XXXX，GB/T 34590.6-XXXX，GB/T 34590.9-XXXX，第 7 章，GB/T 34590.9-XXXX，第 8 章；

注 5：安全分析的目标和范围是在其计划中定义的，且取决于相应的子阶段和应用环境。

h) 如果适用，提供候选项的在用证明，按照 GB/T 34590.8-XXXX，第 14 章；及
i) 如果适用，提供软件工具置信度，按照 GB/T 34590.8-XXXX，第 11 章。

6.4.6.6 安全活动的计划应包括：

a) 目标；
b) 对其他活动或信息的依赖性；
c) 负责执行活动的人员；

d) 执行活动所需的资源；
e) 起始时间、结束时间和持续时间；及
f) 相应工作成果的识别。

6.4.6.7 当修改相关项和现有相关项环境时，按照 6.4.3，或当复用要素时，按照 6.4.4：

a) GB/T 34590 标准的参考安全生命周期应根据相应影响分析的结果进行剪裁；

注 1：在安全计划中定义了剪裁后的安全活动，该过程考虑了适用的生命周期阶段和子阶段（见 6.4.5）。

b) 应相应地识别、描述和返工需要创建或更新的受影响的工作成果；及

注 2：受影响的工作成果包括安全确认规范（见 GB/T 34590.4-XXXX，第 8 章）。

c) 如果安全文档不符合 GB/T 34590 ，则应确定必要的活动以符合标准中的相应要求。

示例 1：按照不同于 GB/T 34590 的安全标准开发的要素，相应的安全文档不完全符合 GB/T 34590。

示例 2：缺少安全文档或安全文档不完全符合 GB/T 34590 的现有要素。

6.4.6.8 安全计划应逐步更新，至少在每个阶段开始时更新。

注：至少在每个阶段的开始，安全计划都需更新，目的是细化该阶段的安全活动计划。安全计划可以在子阶段中进一步细化。

6.4.6.9 安全计划要求的工作成果应在开发阶段保持最新状态，目的是在生产发布前和发布时保持对相关项或要素具有足够的代表性。

6.4.6.10 如果是分布式开发，则客户和供应商均应针对各自的安全活动制定安全计划。

注：定义相应的开发接口协议，按照GB/T 34590.2-XXXX，第5章。

6.4.7 安全生命周期进程

6.4.7.1 如果缺乏来自相关先前子阶段的信息，只有在即使缺乏信息也不会导致功能安全方面的不合理风险的情况下，才能开始后续子阶段。

注：对于缺乏信息可能危及项目的情况，需进行问题升级。

6.4.7.2 按照 GB/T 34590.8-XXXX，第 7、8 和 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（见 GB/T 34590.4-XXXX）。

6.4.8 安全档案

6.4.8.1 应按照安全计划建立安全档案，为实现功能安全提供论据。

6.4.8.2 安全档案宜逐步收录安全生命周期内的工作成果，以支持安全论证。

注 1：在分布式开发的情况下，相关项的安全档案可以是客户和供应商的安全档案的结合，这些档案参考了相关方生成的工作成果的证据。然后相关项的整体论据由各方的论据支持。客户和供应商之间的接口在开发接口协议中定义（见 GB/T 34590.8-XXXX，第 5 章）。

注 2：按照 6.4.6，为了支持安全计划，可在工作成果可用之前确定预期的安全论证。为了支持按照 6.4.12.3 进行的逐步的功能安全评估，随着工作成果的产生，安全档案可以逐步发布，为安全论证提供证据。

6.4.9 认可措施

6.4.9.1 相关项及其要素的功能安全应被认可，基于：

a) 按照表 1 和 6.4.10 的要求，认可评审判断关键工作成果，即表 1 所列工作成果，能否提供充足并令人信服的证据，证明其对实现功能安全的贡献，此过程应考虑 GB/T 34590 相应的目标和要求。

注 1：对表 1 中规定的和安全计划中要求的工作成果进行认可评审。

b) 按照表 1 和 6.4.11，功能安全审核判断功能安全所需的流程的实施情况；及

注 2：GB/T 34590 中定义了功能安全所需的参考流程。与相关项或要素有关的流程通过安全计划中引用或规定的活动来定义。

c) 按照表 1 和 6.4.12，功能安全评估判断相关项实现的功能安全，或所开发的要素对实现功能安全的贡献。

注 3：表 1 中定义的独立性的目的是确保客观、公正的观点，避免利益冲突。本文中所用的“独立性”一词指的是组织独立性。

注 4：认可措施指南见附录 C。

注 5：认可措施的结果报告包括所分析的工作成果或流程文档的名称和版本号（见 GB/T 34590.8-XXXX，第 10 章）。

注 6：如果在认可措施完成后，相关项发生变更，则需要重新进行或补充相关的认可措施（见 GB/T 34590.8-XXXX，8.4.5.2）。

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	应用于以下的独立性程度[a]					范围
	QM	ASIL A	ASIL B	ASIL C	ASIL D	
相关项层面对于影响分析的认可评审（见 6.5.1）； 独立于影响分析的责任者和项目管理。	I3	I3	I3	I3	I3	判断按照 6.4.3 进行的影响分析是否正确识别了相关项是新相关项、对现有相关项的修改或是环境变化的现有相关项。 判断按照 6.4.3 进行的影响分析是否充分地识别了各种变化引发的功能安全影响；以及要执行的安全活动。
危害分析和风险评估的认可评审（见 GBT 34590.3-XXXX 第 6 章）； 独立于相关项开发人员、项目管理和工作成果责任者。	I3	I3	I3	I3	I3	判断与危害事件相关的运行场景的选择和危害事件定义是否适当。 判断已确定的 ASILs、对于相关项识别的危害事件的质量管理（“QM”）评级和导致没有 ASIL 的参数(例如 CO/SO/EO)是否正确。

						判断定义的安全目标是否涵盖已识别的危害事件。
安全计划的认可评审（见 6.5.3）； 独立于该相关项的开发人员、项目管理和工作成果责任者。 注 1:安全计划的认可评审包括由于现有要素复用而执行的要素层面影响分析的评审（见 6.5.2）。 注 2:安全计划包含候选项在用证明（分析、数据和可信度）及相应的剪裁，若适用（见 6.4.6 和 GB/T 34590.8-XXXX 第 14 章）。 注 3:安全计划包括因使用软件工具而引起的剪裁，若适用（见 6.4.6 和 GB/T 34590.8:XXXX 第 11 章））。	—	I1	I1	I2	I3	依照全部安全需求中的最高 ASIL 等级执行。
功能安全概念的认可评审（见 GB/T 34590.3-XXXX 第 7 章），由相应安全分析和相关失效分析的结果支持（见 GB/T 34590.9-XXXX 第 8 章和 GB/T 34590.9-XXXX 第 7 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。
技术安全概念的认可评审（见 GB/T 34590.4-XXXX 第 6 章），由相应安全分析和相关失效分析的结果支持（见 GB/T 34590.9-XXXX 第 8 章和 GB/T 34590.9-XXXX 第 7 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	依照导出技术安全需求的全部功能安全需求的最高 ASIL 等级执行。 如果已对功能安全概念执行了 ASIL 分解，则应考虑分解的 ASIL 结果。
集成和测试策略的认可评审（见 GB/T 34590.4-XXXX 第 7 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。	—	I0	I1	I2	I2	依照全部安全需求中的最高 ASIL 等级执行。
安全确认规范的认可评审（见 GB/T 34590.4-XXXX 第 8 章）；	—	I0	I1	I2	I2	依照全部安全需求中的最高 ASIL 等级执行。

独立于该相关项的开发人员、项目管理和工作成果责任者。						
安全分析和相关失效分析的认可评审（见GB/T 34590.9-XXXX 第 8 章和 GB/T 34590.9-XXXX 第 7 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	依照全部安全需求中的最高 ASIL 等级执行。
安全档案的认可评审（见 6.5.4） 独立于安全档案的责任者。	—	I1	I1	I2	I3	依照全部安全需求中的最高 ASIL 等级执行。
按照 6.4.11，进行功能安全审核； 独立于相关项开发人员和项目管理。	—	—	I0	I2	I3	依照全部安全需求中的最高 ASIL 等级执行。
按照 6.4.12，进行功能安全评估； 独立于相关项开发人员和项目管理。	—	—	I0	I2	I3	依照全部安全需求中的最高 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，应由与负责创建工作成果的人员不同的人员执行； ——I1：认可措施应由与负责创建工作成果的人员不同的人员执行； ——I2：认可措施应由独立于负责创建工作成果的团队的人员执行，即由不向同一个直接上级报告的人员执行； ——I3：认可措施应由在管理、资源和发布权限方面与负责创建对应工作产品的部门独立的人员执行。						

6.4.9.2 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。

6.4.9.3 实施认可措施的人员应有权限获取相关信息和工具。

6.4.10 认可评审

6.4.10.1 应按照 5.4.4 和 5.4.2.7 的要求，为表 1 所列和安全计划中要求的各项认可评审指定负责人。该人员应提供一份报告，其中包含工作成果对功能安全所做贡献的判断。

6.4.10.2 认可评审应在生产发布前完成。

6.4.10.3 认可评审可基于对是否实现 GB/T 34590 的相应目标来做判断。

注：为增加实现评审目标的置信度，评审员应对照GB/T 34590 的相应要求，检查工作成果的正确性、完整性、一致性、充分性和内容。

6.4.10.4 按照 6.4.9.2 和 5.4.4，可指定一名或多名助理支持认可评审的执行。这些人员可能缺乏与相应相关项、要素或工作成果有关的开发人员的独立性，但其独立性至少应为表 1 中定义的 I1，并且评审人员应评价其输入，以确保给出公正的意见。

注：由于认可评审是为了支持功能安全评估而进行的，如果适用，该任命和评价也可以在功能安全评估中进行评估。

6.4.10.5 只要评审根据按照表 1 以足够的独立性进行，认可评审和验证评审就可以合并进行。

6.4.11 功能安全审核

6.4.11.1 当相关项和要素的安全要求的最高 ASIL 等级是 ASIL (B)、C 或 D 时，应按照 6.4.9 开展并在生产发布前完成功能安全审核。

6.4.11.2 按照 5.4.4 和 5.4.2.7 的要求，应委派负责进行功能安全审核的人员。

6.4.11.3 功能安全审核可基于是否达到 GB/T 34590 中流程相关的目标来判断。

注： GB/T 34590-XXXX 目标的实现与标准中相应要求相对应。

示例： 6.1 规定了第 6 章中要求的目标。

6.4.11.4 负责执行功能安全审核的人员应提供包含对功能安全所要求的流程实施情况判断的评估报告，基于以下内容：

a) 根据安全计划中定义或参考的活动定义，评估过程实施情况；
b) 基于组织的专门的规则和流程（见 5.5.1）对安全计划成果的评估；
c) 如果提供论证，对其为什么实现了 GB/T 34590 中流程相关目标进行评估；

注 1： 考虑到 6.4.11.3，为了便于功能安全审核，负责安全活动的人员可以提供论证来证明为何 GB/T 34590 相应目标已实现。

注 2： 符合 GB/T 34590 所有相应的要求是已实现 GB/T 34590 目标的一个充分理由。

d) 对安全计划要求的工作成果是否可用的评估；
e) 对安全计划要求的工作成果是否符合 GB/T 34590.8-XXXX 的 10.4.3 以及工作成果彼此间的一致性的评估，及
f) 如果适用，按照 5.4.2.6 的改善建议，例如，存在不符合项的情况。

注 3： 功能安全审核可以与汽车软件过程改进及能力评定 ASPICE（见 ISO/IEC 33000 ）一起或同步进行，但是，按照 6.4.12.2，汽车软件过程改进及能力评定 ASPICE ®[2])的评估不足以执行功能安全评估。

注 4： 组织的流程定义可以同时符合多种标准，如 GB/T 34590 和 ASPICE 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，可给出组织的专门的流程对 GB/T 34590 中要求和对 ASPICE 要求的交叉引用。

注 5： 在项目早期阶段执行的功能安全审核对于识别流程中的不足是有益的。

6.4.12 功能安全评估

6.4.12.1 当相关项或要素安全要求的最高 ASIL 等级为(B)、C 或 D 时，应按照 6.4.9 的要求开展功能安全评估。以判断相关项已实现的功能安全，或已开发要素对实现功能安全的贡献。

6.4.12.2 功能安全评估可基于对 GB/T 34590 的各项目标是否达到来判断。

注： GB/T 34590的目标实现是根据开发时这些标准的相应要求、技术解决方案的技术现状和适用的工程领域知识来判断的。

示例： 6.1 中规定了第 6 章要求的目标。

6.4.12.3 功能安全评估:

a) 按照 6.4.6.5 f)进行计划;
b) 最迟宜在系统级产品开发之初进行规划;
c) 宜在产品开发过程中逐步执行;

---

2) Automotive SPICE®是适用的商业产品示例。这些信息是为了方便本文件的用户而提供的，并不代表本文件对该产品的推荐。

d) 应在生产发布前完成。

示例：功能安全评估的示例议程见附件 D。

6.4.12.4 按照 5.4.2.7 和 5.4.4 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的报告。

6.4.12.5 负责进行功能安全评估的人员应被授予权力，根据他们的自由裁量权进行功能安全评估，包括:

a) 按照 6.4.12.7 要求在功能安全评估范围内，安全活动及其结果的广度和深度需被评估；
b) 按照 6.4.9.3 提供的信息;及
c) 按照 6.4.9.2 的要求，实施功能安全评估的必需支持，例如负责相关工作成果的人员要在场。

6.4.12.6 按照 6.4.9.2 和 5.4.4 的要求，功能安全评估员可以委派一名或多名助理来支持功能安全评估的执行。 这些人员可能缺乏与相应相关项、要素或工作成果的开发人员之间的独立性，但其独立性至少应达到表 1 所定义的 I1，评估人员应对其输入进行评估，以确保给出的意见是公正的。

注：功能安全评估员应对功能安全评估的结果负责。

6.4.12.7 功能安全评估范围应包括：

a) 安全计划及安全计划要求的所有工作成果；

注 1：功能安全评估员可以剪裁被评审的特定工作成果的详细程度。 但是，表 1 中列出的安全计划要求的那些工作成果值得特别注意。

注 2：功能安全评估员考虑包含双向可追溯性的需求管理（见 GB/T 34590.8-XXXX，第 6 章）是否已被充分实施。

注 3：对相应工作成果的检查为判断是否实现某一 GB/T 34590 目标（见 6.4.12.2）提供了支持。

b) 功能安全要求的流程；

注 4：对已实施的流程的评估可基于功能安全审核的结果以及由此所产生的纠正措施（如有）。

c) 在相关项或要素开发过程中，可评估已执行或实施的安全措施的恰当性和有效性；

注 5：功能安全评估检查与生产、运行、服务和报废有关的需求的适应性。关于生产，在生产过程能力分析期间检查此类要求的正确实施（见 GB/T 34590.7-XXXX, 5.4.2.2 和 GB/T 34590.7-XXXX，6.4.1.3）。

d) 考虑到 GB/T 34590 的相关目标的实现，关于为什么实现功能安全的论证（如果可以提供）；

注 6：考虑到 6.4.12.2，负责创建工作成果的人员可以提供论据来证明为何 GB/T 34590 的相应目标已实现，从而促进功能安全评估的进行。

注 7：符合所有相应的 GB/T 34590 要求是实现 GB/T 34590 目标的充分理由。

e) 安全档案中提供的论据，及
f) 安全异常关闭的理由，按照 5.4.3。

注 8：在分布式开发的情况下，在客户及其供应商处执行功能安全评估活动（见 GB/T 34590.8-XXXX，第 5 章）。供应商进行的功能安全评估可判断是否满足客户的安全要求，并判断已开发的要素或工作成果对实现功能安全的贡献。供应商按里程碑节点并以开发接口协议中定义的形式向客户提供功能安全评估报告（见 GB/T 34590.8-XXXX，5.4.5）。客户进行的功能安全评估会考虑供应商的安全评估报告（本文件 6.4.12.8）。最后，如果客户是车辆制造商，则功能安全评估包括对集成在目标车辆中的相关项已实现功能安全的判断。

6.4.12.8 功能安全评估应考虑：

a) 其他认可措施的计划（见 6.4.6.5 f）；
b) 认可评审和功能安全审核的结果；

c) 如果适用，先前的功能安全评估的建议和采取的纠正措施（见 6.4.12.9～6.4.12.13 和 GB/T 34590.8-XXXX, 8.4.5.2）；及

d) 如果适用，供应商按照 GB/T 34590.8-XXXX,第 5 章的开发接口协议，开发的要素或工作成果的功能安全评估活动的结果。

6.4.12.9 功能安全评估报告应包括对相关项的功能安全接受、有条件接受或拒绝的建议，或所开发的要素/工作成果对相关项功能安全的贡献。

6.4.12.10 按照 6.4.12.9 的要求，功能安全评估报告可包括对相关项的功能安全、或所开发的要素或工作成果对功能安全的贡献做出有条件接受的建议，以所确定的接受条件的决议为准。

注：在分布式开发的情况下（见GB/T 34590.8-XXXX，第5章），供应商的功能安全评估报告应包括关于已开发要素或工作成果的接受、有条件接受或拒绝的建议。

6.4.12.11 按照 6.4.12.10，如果功能安全评估报告建议是对已实现的功能安全有条件接受，功能安全评估报告中应包括接受条件。

6.4.12.12 按照 6.4.12.10，如果功能安全评估报告建议是对已实现的功能安全有条件接受，则应采取必要的纠正措施，以解决功能安全评估报告中记录的接受条件。

6.4.12.13 按照 6.4.12.9，如果功能安全评估报告建议是对已实现的功能安全拒绝,则：

a) 应采取充分的纠正措施；及

b) 应重新进行功能安全评估。

6.4.13 生产发布

6.4.13.1 在生产发布之前，应按照第 6.4.8 节提供安全档案。

6.4.13.2 在生产发布之前，应按照第 6.4.9～6.4.12 节提供适用的认可措施报告。

6.4.13.3 仅当有足够证据证明对功能安全实现有信心时，才可批准相关项或要素的生产发布。

注：可以通过以下方式提供实现功能安全的信心证据：
——认可措施的结果，特别是包含在功能安全评估报告中的建议，如果适用，按照6.4.12.9；及
——安全档案。

6.4.13.4 生产发布的功能安全文档应包括以下信息：

a) 负责发布的人员的名字和签名；

b) 发布相关项或要素的版本；

c) 发布相关项或要素的配置；及

d) 发布日期。

6.4.13.5 在生产发布时，应提供嵌入式软件的基线（包括标定数据）和硬件的基线，并应按照 GB/T 34590.8-XXXX，第 10 章的规定进行记录。

6.5 工作成果

6.5.1 相关项层面的影响分析，由 6.4.3 得出。

6.5.2 要素层面的影响分析，如果适用，由 6.4.4 得出。

6.5.3 安全计划，由 6.4.5～6.4.13 得出。

6.5.4 安全档案，由 6.4.8 得出。

6.5.5 认可措施报告，由 6.4.9～6.4.12 得出。

6.5.6 生产发布报告，由 6.4.13 得出。

7 生产、运行、服务、报废的安全管理

7.1 目的

本章的目的是定义实现和维护生产、运行、服务和报废相关功能安全的组织和人员的职责。

7.2 总则

见5.2。

7.3 本章的输入

7.3.1 前提条件

应具备如下信息:
——组织的专门的功能安全规则和流程，按照 5.5.1；
——能力证据，按照 5.5.2；
——质量管理体系的证据，按照 5.5.3；及
——生产发布报告，按照 6.5.6。

7.3.2 支持信息

无。

7.4 要求和建议

7.4.1 总则

第7.4.2条适用于参与相关项或相关项要素的生产、运行、服务和报废的组织。

7.4.2 责任、计划和所要求的流程

7.4.2.1 组织应按照 5.4.2.7 的要求指定具有相关责任和权限的人员，以实现并维护相关项在生产、运行、服务和报废阶段的功能安全。

7.4.2.2 在相关项及其要素的生产、运行、服务和报废过程中，确保相关项的功能安全活动:

a) 应按照 GB/T 34590.7-XXXX，第 5 章进行计划；
b) 应按照 GB/T 34590.4-XXXX 在系统层面的产品开发期间启动；及
c) 应按照 GB/T 34590.7-XXXX，第 6 章和第 7 章执行。

7.4.2.3 组织应建立、执行并维护流程以实现和保持相关项在生产、运行、服务和报废阶段的功能安全。

注：这包括与相关项功能安全相关的现场监控流程。参考GB/T 34590.7-XXXX。

7.4.2.4 如果在生产、运行、服务或报废期间相关项有变更，应按照 6.4.13 对生产发布进行相应变更。

注：变更需符合变更管理的要求（见GB/T 34590.8-XXXX第8章）。

7.5 工作成果

关于生产、运行、服务和报废的安全管理证据，由7.4.2得出。

附 录 A

（资料性）

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	本章旨在确保参与安全生命周期执行的组织，即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，实现以下目标： a) 建立并维护能够用于支持和鼓励功能安全有效实现，并能够促进与功能安全相关的其他领域有效沟通的安全文化； b) 建立并维护充分的组织的专门的功能安全规章和流程； c) 建立并维护可确保能充分解决识别出的安全异常的流程； d) 建立并维护可确保参与人员的能力与其职责相匹配的能力管理体系；及 e) 建立并维护用以支持功能安全的质量管理体系。 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 能力管理证据； 5.5.3 质量管理体系证据； 5.5.4 已识别的安全异常报告（如果适用）。
6 基于项目的安全管理	本章的目的是，确保参与概念阶段或系统、硬件、软件层面开发阶段的组织实现以下目标： a)定义与分配安全活动相关的角色和责任； b)在相关项层面执行影响分析，以识别相关项是全新的，或是对现有相关项修改，还是对现有相关项的使用环境进行修改；并在有一项或多项修改时，分析所识别出的修改对功能安全的影响； c)在现有要素复用的情况下，在要素层面执行影响分析，评估复用的要素是否可以满足分配给它的安全要求，并考虑该要素复用的运行环境； d)定义所剪裁的安全活动，提供相应的剪裁理由，并评审所提供的理由； e)计划安全活动； f)按照安全计划协调并追踪安全活动的进度； g)规划分布式开发(参考 GB/T 34590.8-XXXX，第 5 章)； h)在整个安全生命周期内，确保安全活动的正确进程； i)创建可理解的安全档案，以提供实现了功能安全的证据； j)判断相关项是否实现了功能安全（即功能安全评估），或者判断某一要素（即供应商进行的功能安全评估活动）或工作成果（例如认可评审）对于实现功能安全的贡献；及 k)在开发结束时，基于支持有信心实现功能安全的证据，决定相关项或要素是否能够生产发布。	组织的专门的功能安全规章和流程（本文件 5.5.1）； 能力管理的证据（本文件 5.5.2）； 质量管理体系的证据（本文件 5.5.3）；	6.5.1 相关项层面的影响分析； 6.5.2 要素层面的影响分析（如果适用）； 6.5.3 安全计划； 6.5.4 安全档案； 6.5.5 认可措施报告； 6.5.6 生产发布报告。
7	本章的目的是定义实现和维护生产、运行、服务和报废相关功能安全的组	组织的专门的	7.5.1 关于生产、运

关于生产、运行、服务和报废的安全管理	织和人员的职责。	功能安全规则和流程（本文件5.5.1）； 能力管理的证据（本文件5.5.2）； 质量管理体系的证据（本文件5.5.3）； 生产发布报告（本文件6.5.6）。	行、服务和报废的安全管理证据。

附 录 B
（资料性）
安全文化

安全文化包括：

a) 负责实现或维护功能安全的人员，以及在组织中执行或支持安全活动的人员，需正直且具有奉献精神；

b) 对于安全事项，组织需秉持安全思维，允许质疑、避免自满、追求卓越、鼓励担当和公司自律。

注：参考Safety Series No. 75-INSAG-4, International Atomic Energy Agency, Vienna, 1991。

表 B.1 安全文化评估示例

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、质量的人员及其管理流程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。	流程采用多样性以获得优势： ——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； ——安全确认； ——功能安全审核； ——功能安全评估。

附 录 C
（资料性）
认可措施指南

C.1 总则

本附录包括认可措施的指南，可以作为判断对相关工作成果功能安全的预期贡献的依据。

C.2 相关项层面影响分析的认可评审（见 6.5.1）

目标是判断影响分析是否正确和完整地识别修改，并评估其对功能安全的影响。

C.3 危害分析和风险评估的认可评审（见GB/T 34590.3-XXXX，第 6 章）

C.3.1 目标是判断危害分析和风险评估的结果以及所使用的方法是否有说服力，是否有合理的依据，以及判断安全目标是否涵盖所有已识别、具有汽车ASIL等级的危害事件。该判断可以基于C.3.2到C.3.7。

C.3.2 评估场景分析，以确保运行场景的选择是适当的，并符合GB/T 34590.3:XXXX，6.4.2.7。

C.3.3 评估危害识别，以确保定义的危害事件是适当的，并符合GB/T 34590.3-XXXX，6.4.2。

C.3.4 评估确定E、C、S参数（包括E0、C0和S0以及那些导出QM的参数）的依据，以确保这些依据是充分且合理的。

C.3.5 评估危害分析和风险评估中作出的假设（例如考虑预期用途、车辆环境和外部措施）是否有明确的文档记录，以确保没有任何假设被忽略或无效。

注：记录假设有助于安全确认。

C.3.6 评估相关项之间可比较的危害事件的一致性，包括ASIL等级，不考虑功能异常，以确保组织中各个相关项之间风险评估的一致性。

C.3.7 评估一组安全目标是否避免了所有已识别的危害事件的不合理风险。

C.4 安全计划的认可评审

C.4.1 目标是评判将要执行的各项安全活动是否定义清晰，是否充分实现功能安全。该判断可以基于C.4.2～C.4.5。

C.4.2 评估安全计划是否与影响分析一致。

C.4.3 评估安全计划是否与项目计划和资源规划一致，以确保项目中包含必需的安全活动。

C.4.4 如果适用，评估所应用的剪裁（即，用不同于GB/T 34590所参考的安全生命周期的方式省略或执行安全活动），包括相应的依据（见6.4.5），以确保项目中适当的包含了必需的安全活动。

如果剪裁是基于在用证明开展的（见GB/T 34590.8-XXXX，第14章）：

a) 评估在用证明的结果是否能够证明所声称的在用证明置信度，以确保在用证明的正确性；
b) 评估在用证明的结果是否能够证明所声称的在用证明置信度，以确保在用证明的正确性；
c) 评估在用证明的候选项变更，以确保变更不影响候选项实现功能安全。

C.4.5 对于分布式开发，评估开发接口协议（见GB/T 34590.8-XXXX，第5章）中所定义的职责划分、安全活动以及交付物，以确保项目中包含了必需的安全活动。

C.5 功能安全概念的认可评审（见GB/T 34590.3-XXXX，第 7 章）

C.5.1 目标是在考虑初步架构的情况下，判断功能安全概念是否提供了充分和令人信服的证据，证明功能安全要求符合安全目标。该判断可以基于C.5.2～C.5.9。

C.5.2 评估功能安全概念的可行性，以确保功能安全概念是充分合理的并能够实现。

C.5.3 考虑到安全分析（见GB/T 34590.9-XXXX，第8章）和对应于初步架构要素的相关失效分析（见GB/T 34590.9-XXXX，第7章）的结果，评估功能安全概念是否适当，以确保功能安全要求的有效性和完整性。

C.5.4 考虑初步架构的要素，评估所定义的安全机制是否充分考虑了功能异常表现，以确保安全机制充分覆盖故障。

C.5.5 评估所定义的安全机制是否对故障作出充分反应，以确保失效得到充分减轻。

C.5.6 评估报警和降级策略，以启动相关人员的适当人为操作，确保对降级模式的适当参与和可控性。

C.5.7 评估ASIL等级分解结果的有效性，以确保：

——分解的功能安全要求的正确性和冗余性；
——所需独立性的可行性；及
——分解的 ASIL 等级符合 GB/T 34590.9-XXXX，第 5 章的要求。

C.5.8 评估功能安全概念中的假设（例如，考虑车辆环境）是否被明确记录，以确保没有任何假设被忽略、隐含或无效。

注：记录上述假设有助于安全确认。

C.5.9 评估功能安全要求分配到初步架构要素（包括其他技术要素）或外部措施的完整性，以确保没有任何功能安全要求被忽略。

C.6 技术安全概念认可评审（见GB/T 34590.4-XXXX，第 6 章）

C.6.1 目标是在考虑系统设计要素的情况下，判断技术安全概念是否提供了充分和令人信服的证据，证明技术安全要求符合功能安全要求。可根据C.6.2～C.6.9作出判断。

C.6.2 评估技术安全概念的可行性，以确保技术安全概念能够在系统设计中实现。

C.6.3 考虑到与系统设计要素相对应的安全分析（见GB/T 34590.9-XXXX，第8章）和相关失效分析（见GB/T 34590.9-XXXX，第7章）的结果，评估技术安全概念是否适当，确保技术安全要求的有效性和完整性。

C.6.4 考虑系统设计的要素，评估所定义的安全机制是否充分考虑了功能异常表现，以确保安全机制充分覆盖故障。

C.6.5 评估所定义的安全机制是否对故障作出充分反应，以确保失效得到充分减轻。

C.6.6 评估警告和降级策略的实施与功能安全概念的一致性。

C.6.7 评估ASIL等级分解结果的有效性，以确保：

——分解后的技术安全要求的正确性和冗余性；
——所需独立性的可行性；及
——分解的 ASIL 等级符合 GB/T 34590-9:XXXX，第 5 章的要求。

C.6.8 评估技术安全概念中所作假设（例如，考虑到车辆环境）是否被明确记录，以确保没有任何假设被忽略、隐含或无效。

注：记录上述假设有助于安全确认。

C.6.9 评估将技术安全要求分配到系统设计要素的完整性，以确保没有任何技术安全要求被忽略。

C.7 集成和测试策略的认可评审（见GB/T 34590.4-XXXX，第 7 章）

C.7.1 目标是判断集成和测试策略中描述的集成和测试活动、方法和技术是否能够提供足够的证据，证明相关项或要素符合系统设计以及相应的安全要求。该评估可基于C.7.2～C.7.4。

C.7.2 考虑开发项目的环境、具体应用、产品领域以及分布式开发和责任，评估集成和测试策略，以确保制定针对安全相关验证方面的充分且合理的计划。

C.7.3 考虑应用的方法和现有经验，评估集成和测试策略，以确保选择充分且合理的验证技术。

C.7.4 如果适用，评估验证方法和技术充分实现GB/T 34590 相应的目标或要求的依据。

C.8 安全确认规范的认可评审，包括安全确认环境描述（见GB/T 34590.4-XXXX，第 8 章）

C.8.1 目标是判断安全确认规范中描述的活动是否能够提供充分和令人信服的证据，以证明安全目标和功能安全概念在整车层面是适当、正确、完整和完全实现的。可根据C.8.2～C.8.4做出判断。

C.8.2 评估定义的安全确认活动的能力，以确认在危害分析和风险评估、功能安全概念以及系统、硬件和软件开发过程中所作的假设。

C.8.3 考虑已实施的安全措施、相关外部措施和其他技术相关要素的有效性，评估定义的安全确认活动为充分减轻失效提供证据的能力。

C.8.4 评估所定义的安全确认活动提供驾驶员或其他可能处于风险中的人员预期避免伤害（即可控性）的证据的能力。

C.9 安全分析和相关失效分析的认可评审（见GB/T 34590.9-XXXX，第 7 章和第 8 章）

目标是判断安全分析和相关失效分析是否正确执行，以确保相关已识别的故障和安全措施得到充分解决。

C.10 安全档案的认可评审（见 6.5.4）

C.10.1 目标是判断安全档案中提供的论证是否有说服力。判断可以基于章节C.10.2～C.10.4。

C.10.2 评估安全档案中提供的论证能否合理且充分的用以证明功能安全已经实现。

C.10.3 评估参考的工作成果是否存在且充分完整，以便能充分地论证功能安全的实现情况。

C.10.4 确认在安全档案中参考的工作成果是否：

——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（见 5.4.3）。

C.11 功能安全审核（见 6.4.11）

目标是基于在安全计划中参考的或规定的安全活动的定义,判断功能安全要求实施的流程是否达到GB/T 34590中流程相关的目标。

C.12 功能安全评估（见 6.4.12）

C.12.1 目标是判断相关项的功能安全或已开发要素对功能安全的预期贡献是否实现，并为功能安全的实现提供接受、有条件接受或拒绝建议。该判断和建议可以基于C.12.2～C.12.8。

C.12.2 按照GB/T 34590 的目标，并考虑标准中的相应要求，评估安全计划及安全计划要求的所有工作成果，以判断工作成果是否提供了充分和令人信服的证据证明其对实现功能安全的贡献。对于需要认可评审的工作成果（见表1），应考虑认可评审的结果。

C.12.3 考虑功能安全审核结果（见6.4.11）的同时，评估功能安全流程的实施，以判断流程相关的方面是否达到GB/T 34590 的目标。

C.12.4 可在相关项开发过程中确定已实施安全措施的评估，以判断这些安全措施的适宜性和有效性。

C.12.5 考虑到GB/T 34590 目标的实现，如果提供了功能安全被实现了的论证，则应考虑这些标准的相应要求来判断这些论证是否令人信服。

C.12.6 考虑安全档案的认可评审，评估安全档案中提供的论据，以判断这些论据是否具有足够的说服力。

C.12.7 按照5.4.3对安全异常关闭的依据进行评估，以判断这些依据是否令人信服。

C.12.8 如果适用，跟踪先前功能安全评估结果的建议，包括任何已执行的纠正措施（见6.4.12.9～6.4.12.13）。

附 录 D

（资料性）

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）

D.1 安全管理

D.1.1 所评估项目中的组织的安全文化和支持过程的应用。

D.1.2 所评估项目中的能力管理和持续改进的应用。

D.1.3 所评估项目中的角色和责任。

D.1.4 所评估项目的安全计划和分布式开发计划。

D.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。

D.1.6 功能安全审核、安全档案和可用文档。

D.2 概念阶段的安全活动

D.2.1 相关项定义的开发。

D.2.2 危害分析和风险评估。

D.2.3 功能安全概念。

D.2.4 相关项及其安全概念与其他系统/功能的依赖关系。

D.2.5 功能安全要求分配到：

——电气/电子系统要素；
——应用其他技术的要素；及
——与外部措施的接口。

D.2.6 功能安全概念验证。

D.3 系统开发阶段的安全活动

D.3.1 系统开发、集成和确认计划。

D.3.2 技术安全概念及其验证。

D.3.3 系统设计和系统失效的避免。

D.3.4 软硬件要素的技术安全要求分配和软硬件接口评审。

D.3.5 系统设计验证。

D.4 硬件开发

D.4.1 硬件开发、鉴定和集成计划。

D.4.2 硬件安全要求、硬件设计和验证。

D.4.3 硬件架构的约束。

D.4.4 评估因随机硬件失效而违背安全目标的可能性。

D.4.5 硬件集成和测试。

D.5 软件开发

D.5.1 软件开发、鉴定和集成计划。

D.5.2 软件安全要求、软件架构设计、软件单元设计和实现。

D.5.3 软件单元测试。

D.5.4 软件集成和测试。

D.5.5 软件安全要求验证。

D.6 相关项集成

D.6.1 集成测试的计划。

D.6.2 软硬件集成和测试。

D.6.3 系统/相关项集成和测试。

D.6.4 整车集成和测试。

D.7 安全确认

D.7.1 安全确认活动。

D.7.2 安全确认文档。

D.8 供应商功能安全评估

供应商功能安全评估报告的考虑。

D.9 安全相关特殊特性

D.9.1 生产中安全相关的特殊特性。

D.9.2 运行、服务和报废中安全相关的特殊特性。

D.10 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。

附 录 E
（资料性）
功能安全与信息安全的潜在交互作用指南

E.1 目标

为解决信息安全对实现功能安全的潜在不利影响，本附录提供了有关功能安全和信息安全活动之间可能交互的指南，这两者均有助于整体实现电气/电子系统的安全。

本指南的目的是从功能安全的角度提供指导，而不是为实现信息安全提供指导。功能安全和信息安全的开发过程之间的关系取决于组织和项目范围，因此本指南未描述交互的方法或技术内容。组织可以确定最适合此交互的方法。

E.2 概述

功能安全解决了导致电气/电子系统出现功能异常表现的系统性和随机性故障，信息安全解决了电气/电子系统外部恶意意图导致的问题。

了解可能会对功能安全产生负面影响或支持功能安全实现的信息安全相关信息，对实现功能安全是有利的。

注：参考SAE J3061、ISO/IEC 27001和ISO/IEC 15408。

E.3 功能安全与信息安全之间的潜在交互

E.3.1 功能安全管理

功能安全管理与信息安全管理的交互可以包括：

——信息安全活动的计划和里程碑节点，以便考虑可能影响安全活动计划的依赖关系，例如软件的开发方面，工具、编程语言和指南的选择；

——信息安全和功能安全的现场监视活动的协调管理，包括事件的报告、跟踪和解决，以便将与安全相关的信息安全现场事件通知给功能安全。

E.3.2 概念阶段

在概念阶段，交互可以包括：

——从功能安全角度将信息安全威胁作为危害进行分析，以支持危害分析和风险评估以及安全目标的完整性；

——功能安全可以提供诸如危害和相关风险之类的信息，以支持对信息安全威胁的识别；

——与电气/电子系统行为相关的信息安全策略或对策，在检测到攻击的情况下以确定对安全目标或安全概念的潜在影响。

E.3.3 产品开发

在产品开发阶段，交互可以包括：

——与电气/电子系统的信息安全策略或对策的设计和实施有关的技术信息，以确定对技术安全概念和系统设计的潜在影响；

——信息安全软件和硬件设计考虑因素，以确定对实现软件和硬件安全要求以及设计约束（例如独立性）的潜在影响；

——功能安全可以提供与安全措施的设计和实施有关的信息，以便传达可能与信息安全相关的功能安全约束；

——可以协调功能安全和信息安全分析活动，以发现信息安全对功能安全的潜在影响。功能安全分析还可以考虑信息安全策略和对策的影响；及

——为解决系统性故障而确定的信息安全对策，以便确定对功能安全的潜在影响，例如，开发与信息安全共享的安全措施所需的方法。

E.3.4 生产和运行

在生产和运行期间，交互可以包括：

——信息安全事件解决策略，以考虑由于信息安全事件响应而导致的设计变更对功能安全的潜在影响。

参 考 文 献

[1] ISO/IEC/IEEE 15288, Systems and software engineering — System life cycle processes.

[2] ISO/IEC/IEEE 16326, Systems and software engineering — Life cycle processes — Project management.

[3] ISO 26262-11:2018, Road Vehicles — Functional safety — Part 11: Guideline on application of ISO 26262 on semiconductors.

[4] ISO 11451 (all parts), Road vehicles — Vehicle test methods for electrical disturbances from narrowband radiated electromagnetic energy.

[5] ISO 11452 (all parts), Road vehicles — Component test methods for electrical disturbances from narrowband radiated electromagnetic energy.

[6] ISO 7637 (all parts), Road vehicles — Electrical disturbances from conduction and coupling.

[7] ISO 10605, Road vehicles — Test methods for electrical disturbances from electrostatic discharge.

[8] ISO 26262-12:2018, Road Vehicles — Functional safety — Part 12: Adaptation of ISO 26262 for Motorcycles.