ICS 43.430

CCS T 35

中华人民共和国国家标准

GB/T 34590.8—XXXX

代替 GB/T 34590.8—2017

道路车辆 功能安全

第8部分：支持过程

Road vehicles-Functional safety-

Part 8:Supporting processes

(ISO 26262-8:2018,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8部分。

本文件代替GB/T 34590.8-2017《道路车辆 功能安全 第8部分：支持过程》，与GB/T 34590.8-2017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”，修；

——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；

——新增了软件工具置信度的工具使用方面和工具鉴定方面等两组活动的要求（见 11.2）。

——新增了 III 类硬件要素的评估的要求（见 13.4.4）。

——新增了 GB/T 34590 标准适用范围之外应用的接口相关要求（见 15）和未按照根据 GB/T 34590 开发的安全相关系统的集成的相关要求（见 16）。

——删除了 GB/T 34590.5-2017 中软件工具鉴定的确认评审的要求。

本文件使用重新起草法修改采用了ISO 26262-8：2018 《道路车辆 功能安全 第8部分：支持过程》。

本文件与ISO 26262-8：2018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 34590.2-XXXX代替ISO 26262-2：2018；

用修改采用国际标准的GB/T 34590.3-XXXX代替ISO 26262-2：2018；

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 26262-2：2018；

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 34590.9-XXXX代替ISO 26262-9：2018；

——新增了基于工具用户的要求的示例（见11.2）。

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 34590.8,2017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。

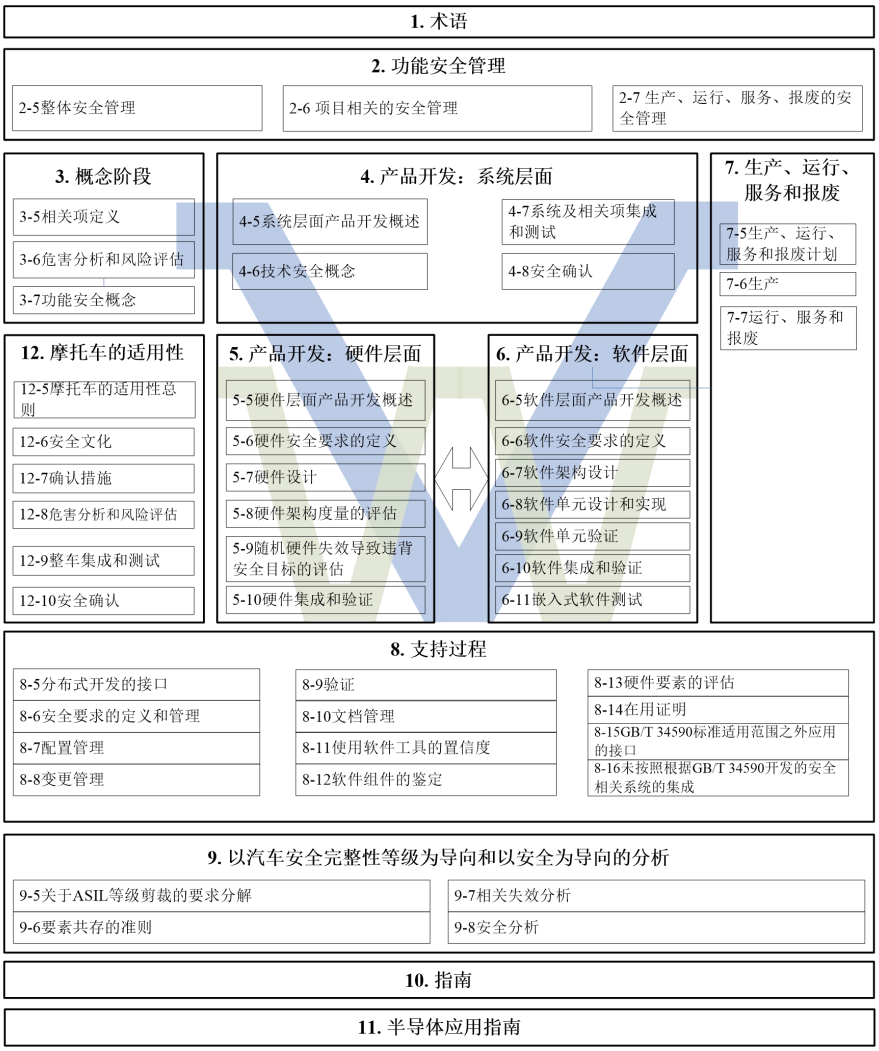


图 1　GB/T 34590-XXXX 概览

道路车辆 功能安全
第8部分：支持过程

1 范围

GB/T 34590的本部分规定了对支持过程的要求，包括：

——分布式开发中的接口；
——安全要求的整体管理；
——配置管理；
——变更管理；
——验证；
——文档化管理；
——使用软件工具的置信度；
——软件组件的鉴定；
——硬件组件的鉴定；
——在用证明；
——接口超出GB/T 34590范围的应用；及
——未根据GB/T 34590开发的安全相关系统的集成。

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裁剪。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裁剪。

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。

本文件不针对电子电气系统的标称性能。

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 34590.2-XXXX 道路车辆 功能安全 第2部分：功能安全管理(ISO 26262-2:2018,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 34590.9-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 XXXXX-1给出的术语、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 GB/T XXXXX.2-XXXX 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 GB/T XXXXX.2-XXXX 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-XXXX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 对表格的诠释

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 XXXXX-9第5章的要求，应遵循分解后的ASIL等级。

如果GB/T 34590-XXXX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 XXXXX.12要求的摩托车的相关项或要素，GB/T 34590.12的要求替代本部分和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 分布式开发的接口

5.1 目的

本章的目的是：

a）定义客户和供应商在进行开发活动时的交互和依赖；

b）描述职责的分配；及

c）识别相关项及其要素在进行分布式开发时需要交换的工作成果。

5.2 总则

相关项或要素开发的客户（如：车辆制造者）和供应商共同遵守 GB/T 34590 定义的分布式开发要求。在安全生命周期中的概念、开发、生产、运行、服务和报废阶段，客户和供应商就责任达成一致。分包的关系是被允许的。客户内部具有关于相关项开发的计划、执行和文档化的安全相关流程，因此，类似的流程适用于与供应商在分布式相关项开发中的合作。这同样也适用于供应商对功能安全负有全部责任的相关项开发。

注 1：开发接口协议（DIA）旨在描述客户和供应商之间的角色和责任。因此，客户和供应商的安全计划符合开发接口协议。

注 2：本章不适用于未对供应商分配任何安全责任的采购，包括标准组件、元器件或委托开发。

注 3：本注释适用于 T&B；本章不适用于向基础车辆集成车辆上装设备的情况。第 15 章适用于把按照 GB/T 34590 开发的车辆上装设备集成到按照另一标准开发的基础车辆中的情况。第 16 章适用于把按照另一标准开发的车辆上装设备集成到按照 GB/T 34590 开发的基础车辆中的情况。

5.3 本章的输入

5.3.1 前提条件

本文件安全生命周期相关阶段（该阶段计划且实施了分布式开发）中适用的前提条件。

5.3.2 支持信息

可考虑如下信息：

——安全生命周期相关阶段（该阶段计划且实施了分布式开发）中适用的支持信息；及

——基于报价需求（RFQ）的供应商投标（来自外部）。

5.4 要求和建议

5.4.1 要求的应用

5.4.1.1 应将本章的要求用于每个按照 GB/T 34590 开发的相关项和要素，但适用下述之一的商业现成的且不是为了满足特定安全要求而定制生产的要素除外：

a) 按照基于质量标准（如：电子组件的 AEC 标准）的公认流程，鉴定商业现成的硬件要素，且按照第 13 章进行评估；

b) 商业现成的软件组件按照第 12 章经鉴定合格的；或

c) 商业现成的硬件要素或软件组件作为 SEooC 来开发。

注 1：非定制生产的商业现成的硬件要素或软件组件可能是独立于客户的 SEooC，其项目特定的修改已被要素规范所覆盖。

示例：通信堆栈、操作系统或软件库是商业现成的要素。

注 2：按照 GB/T 34590.2-XXXX，6.4.5.7，SEooC 的假设在其目标应用中得到确认。

5.4.1.2 应将有关客户-供应商关系（接口和交互）的要求，用于客户-供应商关系的每个层面。

注 1：这包含顶层供应商采取的分包、分包商采取的分包等。

注 2：对内部供应商的管理可以采取与管理外部供应商相同的方法。

5.4.2 供应商选择准则

5.4.2.1 供应商选择准则应包含对供应商开发能力的评估，如果适用，也包含按照 GB/T 34590 对类似复杂度和 ASIL 等级的相关项和要素的生产能力的评估。

注：供应商选择准则包含：

——供应商质量管理体系的证据；

——供应商以往的表现和质量；

——对供应商功能安全能力（作为投标的一部分）的确认；

——以往按照 GB/T 34590.2-XXXX，6.4.12 进行的功能安全评估结果，或

——来自整车厂开发、生产、质量和物流部门（因其影响功能安全）的推荐。

5.4.2.2 客户给候选供应商的报价需求（RFQ）应包含：

a) 符合 GB/T 34590 的正式要求；

b) 供货范围的定义；

注：供货范围规定了需要供应商提供的相关项或要素的功能、特性和边界。

c) 如果已存在，基于供应商报价对象的安全目标或相关功能安全要求（包含其分配的 ASIL 等级）；及

注：如果在选择供应商时 ASIL 等级未知，则可以作出保守的假设。

d) 如果已存在，基于供应商报价对象的要素的失效率目标值和诊断覆盖率目标值（按照 GB/T 34590.4-XXXX，6.4.5.3）

5.4.3 分布式开发的启动和计划

5.4.3.1 客户和供应商应定义开发接口协议，包含以下：

a) 客户和供应商安全经理的任命；

b) 按照 GB/T 34590.2-XXXX，6.4.5 进行安全活动的联合裁剪；

c) 客户需开展的安全生命周期的活动和供应商需开展的安全生命周期的活动；

注 1：活动的联合计划是需要考虑的，包含按照 GB/T 34590.2 给出的功能安全评估和功能安全审核的职责。

d) 需共享的信息和工作成果，包含分配和评审；

注 2：这包括对需提供的文档达成一致，以完成客户及供应商的安全档案；

注 3：交换的信息包含安全相关的特殊特性；

注 4：对所涉及开发方的活动所必须的工作成果相关部分，可进行识别和交换。

e） 每项活动分配给每一方的责任；

注 5：责任可以描述为“负责”、“批准”、“支持”、“通知”、“咨询”。

f） 目标值的沟通或确认（本文件 5.4.2.2d），这些目标值由系统层面的目标导出，再分配给相关方，目的是使这些相关方满足单点故障度量及潜伏故障度量的目标值（按照 GB/T 34590.5 对硬件架构度量的评估和因随机硬件失效导致违背安全目标的评估）；

g） 在客户和供应商合作中所需要的接口相关的流程、方法及工具；

注 6：流程、工具及工具配置的版本和修订可以是相关的。

h） 哪一方（供应商或者客户）按照 GBT 34590.4 执行安全确认所达成的协议；

注 7：如果由供应商执行整车集成和确认，对供应商所需的能力和资源达成一致是重要的，因为安全确认工作需要集成后的车辆（本文件 GB/T 34590.4-XXXX）。

i） 按照 GB/T 34590.2-XXXX，关于由供应商开发的要素或工作成果的功能安全评估活动；

注 8：这些由供应商开发的要素或工作成果的功能安全评估活动，可能是由供应商本身、客户、或供应商/客户指定的组织或个人来执行。

j） 供应商关于功能安全评估报告的计划；及

注 9：开发接口协议包含报告的最低限度内容、版本和里程碑节点；

注 10：附录 B 给出了开发接口协议的一个示例。

k） 客户与供应商之间达成的允许客户指定审核人员在供应商的场所进行功能安全审核的协议。

5.4.3.2 如果供应商执行危害分析和风险评估，那么危害分析和风险评估应提供给客户进行验证和批准。

5.4.3.3 概念阶段的责任方应按照 GB/T 34590.3-XXXX 制定功能安全概念。

5.4.4 分布式开发的执行

5.4.4.1 客户应确保供应商按时收到所需的用于执行开发接口协议中安全活动的信息和数据。

5.4.4.2 供应商应向客户报告可能增加不符合开发接口协议条款的风险的问题。

5.4.4.3 供应商应向客户报告在其责任范围内和其分包商责任范围内的开发活动中发生的安全异常。

5.4.4.4 应分析已识别出的潜在影响供应商交付成果的安全异常，并采取措施予以解决。双方应就谁来执行所需的行动达成协议。

5.4.4.5 供应商应确定客户的安全要求是否可行，以及 6.4.1 和 6.4.2 的要求是否满足。若不可行/不满足，则客户应重新检查安全要求并做适当的修改，以确保安全要求定义的正确性。

5.4.4.6 供应商应向客户传达其职责范围以外但供应商认为为确保实现功能安全所必要的相关项的要素的安全要求。

5.4.4.7 在导出用于当前开发的安全要求时，按照 GB/T 34590.2-XXXX，5.4.2.6，双方都应考虑从之前相似开发中所获得的经验。

5.4.4.8 供应商应向客户报告安全计划中制定的各项任务和里程碑节点上所取得的进展。供应商和客户应就报告的内容和提交的日期达成一致。

5.4.5 分布式开发中的功能安全评估活动

5.4.5.1 对于分配了安全要求的最高 ASIL 等级为 ASIL（B）、C 或 D 的要素，在 DIA 中应指定哪个组织按照 GB/T 34590.2-XXXX 对供应商开发的要素或工作成果执行功能安全评估活动。

注 1：这些由供应商开发的要素或工作成果的功能安全评估活动，可能由供应商本身、客户、或者客户/供应商指定的组织或人员执行。

注 2：在 DIA 审批过程中，所有这些都需要与客户达成一致。

5.4.5.2 对于分配了安全要求的最高 ASIL 等级为 ASIL（B）、C 或 D 的要素，在 DIA 中应规定供应商

功能安全评估活动的计划。

注：计划包括报告的最低限度内容和里程碑节点。

5.4.5.3 对于分配了安全要求的最高 ASIL 等级为 ASIL（B）、C 或 D 的要素，供应商应向客户提供功能安全评估报告，包括供应商对所开发的要素是否符合来自客户的安全要求的评估，以及所实施的流程是否满足实现功能安全的准则。

5.4.5.4 对于分配了安全要求的最高 ASIL 等级为 ASIL（B）、C 或 D 的要素，应将供应商的功能安全评估活动的结果提供给客户和供应商。

5.4.6 生产、运行、服务和报废的协议

5.4.6.1 供应商应向客户提供证据，证明能具备并保持 GB/T 34590.2-XXXX 第 7 章和 GB/T 34590.7-XXXX 第 5 章和第 6 章所要求的生产过程能力。

注：关于半导体生产的指南，本文件 GB/T 34590.11-XXXX，4.9。

5.4.6.2 客户和供应商间的供应协议应依据 GB/T 34590.2-XXXX，7.4.2.1 明确功能安全责任，并应定义各方的安全活动。

注：关于半导体分布式开发的指南，本文件 GB/T 34590.11-XXXX，4.10。

5.4.6.3 供应协议应规定各方间关于安全相关特殊特性的生产监控记录和从客户退回部件的失效分析结果的访问和交换。

注：这些事项能由质量管理协议充分覆盖。

5.4.6.4 供应协议应规定关于交换安全相关事件和所需分析的及时的沟通渠道。对于现场问题，就按照已建立的现场监控过程对这些事件进行分析。

注：该分析包括类似相关项和潜在受类似事件影响的其他方。

5.5 工作成果

5.5.1 **供应商选择报告**，由 5.4.2.1 和 5.4.2.2 的要求得出。

5.5.2 **开发接口协议（DIA）**，由 5.4.3，5.4.5.1 和 5.4.5.2 的要求得出。

5.5.3 **供应商安全计划**，由 5.4.3 和 5.4.4 的要求得出。

5.5.4 **功能安全评估报告**，由 5.4.5.3 和 5.4.5.4 的要求得出。

5.5.5 **供应协议**，供应协议，由 5.4.6.1～5.4.6.4 的要求得出。

6 安全要求的定义和管理

6.1 目的

本章的目的是：

a) 确保正确的定义安全要求及其属性和特性；及

b) 确保在整个安全生命周期内对安全要求的一致管理。

6.2 总则

安全要求是旨在达到并确保所需功能安全等级的要求。

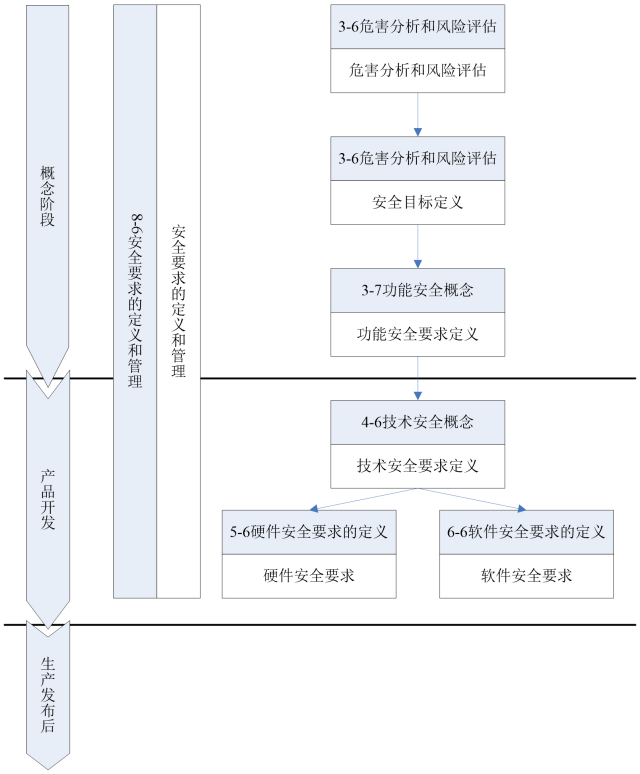
在安全生命周期过程中，安全要求通过分层结构进行定义和细化。图 2 给出了 GB/T 34590-XXXX 中用到的安全要求的结构和相关性。安全要求被分配给要素或在要素间分布。

安全要求的管理包括：对要求达成一致、从安全要求的执行方取得承诺和保持追溯性。

为了支持对安全要求的管理，推荐使用合适的需求管理工具。

“GB/T 34590.3、GB/T 34590.4、GB/T 34590.5”列出了有关安全要求内容在不同层面的特定要

求。



注：图中 GB/T 34590-XXXX 每部分的特定章用以下方式标示：“m-n”，“m”代表部分号，“n”代表章号，例如“3-7”代表 GB/T 34590.3-XXX 的第 7 章。

图 2 安全要求的结构

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GB/T 34590.2-XXXX,5.5.1；及

—安全生命周期相关阶段（该阶段定义或管理了安全要求）中适用的前提条件。

6.3.2 支持信息

本文件安全生命周期相关阶段（该阶段定义或管理了安全要求）中适用的支持信息。

6.4 要求和建议

6.4.1 安全要求的定义

为了达到 6.4.2.4 所列安全要求的特性，应使用以下恰当的组合来定义安全要求：

a) 自然语言；及

b) 表 1 所列的方法。

表 1 定义安全要求

方法	ASIL 等级			
	A	B	C	D

1a	用于要求定义的非形式记法[a,b]	++	++	+	+
1b	用于要求定义的半形式记法[a,b,c,d]	+	+	++	++
1c	用于要求定义的形式标记法[a]	+	+	+	+

[a] 安全要求定义方法的恰当选择考虑：针对特定问题待定义的安全要求，方法是否足够准确以具备 6.4.2 规定的安全要求的特性；方法的复杂性；定义或管理安全要求的人员的背景知识。示例包括使用状态图或关系图来定义软件或硬件的复杂行为，包括许多状态或/和复杂转换。

[b] 对于较高层面的安全要求（如安全目标、功能安全要求和技术安全要求），自然语言和其他类型的非形式记法是最恰当的形式，然而有些要求可能用半形式记法更好处理。

[c] 半形式记法使用数学或图形要素【如方程、图形、图表、流程图、时序图和许多其他形式的表示(例如 UML®和 SysML™)】补充的自然语言来表达需求。示例包括基于模型的技术，以及在自然语言中为要求描述语句应用模板和受控词汇表。

[d] 对于较低层面的安全要求，其可能定义了精确的硬件和软件行为和能力，由于半形式记法更清晰所以更合适。然而，即使这样，也难以或没有必要对每条要求都使用半形式技术。

6.4.2 安全要求的属性和特性

6.4.2.1 安全要求应能被明确的识别为安全要求。

注：为了符合该要求，可将安全要求列在一个单独的文件中。如果在同一文件中管理安全要求和其他要求，可通过使用 6.4.2.5 中给出的特殊属性而明确的识别出安全要求。

6.4.2.2 安全要求应继承将其导出的原安全要求的 ASIL 等级，但运用了按照 GB/T 34590.9-XXXX 的 ASIL 分解除外。

注：因安全目标是顶层的安全要求，故 ASIL 等级的继承始于安全目标层。

6.4.2.3 应将安全要求分配给实施这些要求的相关项或要素。

6.4.2.4 安全要求应具有如下特性:

注 1：安全要求的特性能够使相关人员进行清晰地沟通。这些特性是向必须执行安全要求的人传达安全要求的主要手段。下面引用的特性与 ISO/IEC/IEEE 29148(参考文献【8】）中引用的特性一致。

a) 明确的；

注 2：如果对要求的意思存在共同的理解，那么要求是明确的。

b) 可理解的；

注 3：如果要求的相关人员或要求的使用者理解要求的意思，那么要求是可理解的。

c) 不可分割的（单一的）；

注4：当一个层面的安全要求在所考虑的层面上不能被分解为至少两个独立的安全要求，那么这些要求是不可分割的。此特性的实现可能与安全要求的其他基本特性的实现相矛盾。在这种情况下，不可分割的重要性可以降低。

d) 内部一致的；

注 5：如果要求不包含自相矛盾的内容，则要求是内部一致的。

e) 可行和可实现的；

注 6：如果某个要求在相关项的开发限制（资源、当前技术水平等）内可被实现，则其是可行的。

注 7：一项要求在技术上可以实现，它不需要重大的技术进步，并且在可接受范围内符合相关项限制（如成本、进度、技术、法律、法规等）”；

f) 可验证的

注 8：如果在定义要求的层面上有方法检查这些要求是否得到了满足，则要求是可验证的。

注 9：收集到有关相关项的证据表明相应的要求已得到满足。如果要求是可测量的，可验证性会更强。

g) 必要的

注 10：要求中定义了基本能力、特性、约束和/或质量因素。如果移除或删除，则将存在产品的其他能力或流程无法满足的缺陷。

注 11：要求在当前是适用的，且没有随着时间的推移而改变。对于具有计划失效日期或适用日期的要求进行了清晰的识别。

h) 实施自由的

注 12：要求定义的是对于相关项必要和充分的内容，避免对架构设计施加不必要的限制。该属性的目的是独立实施要求。要求描述的是需要什么，而不是如何满足。

i) 完整的，及

注 13：所描述的要求是可测量的，并且充分描述了要求相关者所关注的能力和特性，因此要求是清晰的，不需要进一步扩充。

j) 合规的

注 14：所述要求符合相关适用的且应满足来自政府、汽车工业及产品的标准、规范和接口要求。

6.4.2.5 安全要求应具有如下属性：

a) 在整个安全生命周期中，具有唯一识别并保持不变；

示例 1：可通过不同的方法实现对要求的唯一识别，如对每个词"应"标注下脚标，例如："系统应 9782 检查…"；或者对含有词"应"的每个句子进行连续的编号，例如："9782 在…情况下，系统应检查…"。

b) 状态；及

示例 2：安全要求的状态可以是"已建议"、"已假设"、"已接受"、"已评审"、"已交付"或"已验证"。

c) ASIL 等级。

6.4.3 安全要求的管理

6.4.3.1 从一个或多个安全目标导出的相关项或要素的安全要求集应具备以下特性：

a) 分层结构；

注 1：如图 2 所示，分层结构是指安全要求是由几个连续层面构建而成的。这些层面总是与相应的设计阶段保持一致。图 2 中的任何设计阶段都可能存在多个层面的分层。

b) 按照适当分组原则建立的组织结构；

注 2：安全要求的组织意味着每个层面的安全要求被分组在一起，通常与架构相对应。

c) 完整性；

注 3：完整性表示一个层面的安全要求完全的实施了上一层面的全部安全要求。

d) 外部一致性；

注 4：不同于内部一致性，即每个单独的安全要求不包含与自身相矛盾的内容，外部一致性表示多个安全要求不互相矛盾。

e) 分层结构中任意一层的信息不重复；及

注 5：信息不重复表示安全要求的内容不重复出现在分层结构同一层面的其他安全要求中，并且在每个分层层面均有此要求。

f) 可维护性。

注 6：可维护性表示要求集可被修改或扩展，例如引入要求的新版本或增加/去掉要求集内的要求。

注 7：当每个要求满足 6.4.2.4 的所有要点，并且要求集满足 6.4.3.1 时，可维护性得到了提高。

6.4.3.2 安全要求应是可追溯的，与以下内容相关联：

a) 安全要求在下一个更高分层层面的每个来源；

b) 导出到下一个更低分层层面的每个安全要求，或各安全要求在设计中的实现；及

c） 按照 9.4.2 的验证规范。

注 1：可使用各种追溯记录类型，如需求管理系统、电子材料等。

注 2：可追溯性支持：

——要求、其实现及验证间的一致性；

——对特定的安全要求更改后，影响分析的有效性；及

——认可措施(如功能安全评估，以评估功能安全实现与否)的执行。

6.4.3.3 应将表 2 所列验证方法的恰当组合用于验证安全要求是否符合本章的要求，及是否符合得出安全要求的 GB/T 34590-XXXX 相关部分中关于验证安全要求的特定要求。

表 2 验证安全要求的方法

方法		ASIL 等级			
		A	B	C	D
1a	通过走查验证	++	+	o	o
1b	通过检查验证	+	++	++	++
1c	半形式验证[a]	+	+	++	++
1d	形式验证[a]	o	+	+	+
[a] 可执行模型可以支持验证。					

6.4.3.4 按照第 7 章，安全要求应置于配置管理下来维护整个安全生命周期的一致性。

示例：当较低层面的安全要求与较高层面的安全要求相符合时，配置管理可以定义一个基线作为安全生命周期后续阶段的基础。

6.5 工作成果

无。

7 配置管理

7.1 目的

本章的目的是：

a）确保工作成果、相关项、要素及其生产的原理和一般条件，在任何时间以可控的方式可被唯一识别和重生成；及

b）确保当前版本和较早版本的关系及区别是可追溯的。

7.2 总则

配置管理是汽车工业中的成熟实践，可依据如 ISO 10007、Automotive SPICE®、ISO/IEC 33000 、ISO/IEC/IEEE 15288[4]和 ISO/IEC/IEEE 12207 进行应用。

GB/T 34590 的每个工作成果要服从于配置管理。

7.3 本章的输入

7.3.1 前提条件

应具备如下信息：

——安全计划，按照GB/T 34590.2-XXXX，6.5.3；

——组织专门的功能安全规章和流程，按照GB/T 34590.2-XXXX，5.5.1；及

——安全生命周期相关阶段（该阶段对配置管理进行了计划或管理）中适用的前提条件；及

7.3.2 支持信息

无。

7.4 要求和建议

7.4.1 应计划配置管理。

注：配置管理计划可以包括职责和资源、工具和存储库、配置项的识别和命名规范、访问权限、基线计划、发布/批准程序。

7.4.2 配置管理过程应符合：

a) 质量管理体系标准的相关要求；及

b) 软件开发的特定要求。

注 1：软件开发的软件配置管理的特定要求，本文件 ISO/IEC/IEEE12207。

注 2：配置管理过程可以适应开发的相应阶段。

7.4.3 安全计划要求的工作成果及再次生成相关项和要素所需要的工作成果，应按照配置管理策略，生成基线并存放。

7.4.4 在整个安全生命周期中，需要被唯一识别和重生成的工作成果、相关项和要素，在配置管理策略中应定义其条件或目的。

示例：作为客户-供应商关系里安全活动的一部分，在其交换之前需要创建工作成果、相关项和要素的配置条件或目的。

7.4.5 在整个安全生命周期中，应对配置管理进行维护。

7.5 工作成果

7.5.1 配置管理计划，由 7.4.1～7.4.5 的要求得出。

8 变更管理

8.1 目的

变更管理的目的是在整个安全生命周期中，分析和控制安全相关工作成果、相关项和要素的变更。

8.2 总则

变更管理确保对变更进行系统性计划、控制、监测、实施和记录，同时在整个安全生命周期内维护工作成果、相关项和要素的相关功能和特性。

注：变更理解为因组件或元器件的异常、移除、增添、加强、报废等导致的修改。

变更管理是汽车行业中的成熟实践，可根据 ISO 10007、Automotive Spice®、ISO/IEC 33000、ISO/IEC/IEEE 15288[4]或 ISO/IEC/IEEE 12207 等进行应用。

8.3 本章的输入

8.3.1 前提条件

应具备如下信息：

——配置管理计划，按照7.5.1；

——安全计划，按照GB/T 34590.2-XXXX，6.5.3；及

——组织专门的功能安全规章和流程，按照GB/T 34590.2-XXXX，5.5.1。

8.3.2 支持信息

无。

8.4 要求和建议

8.4.1 计划和启动变更管理

8.4.1.1 在对工作成果进行变更前，应计划和启动变更管理流程。

注：配置管理和变更管理是相互关联的，定义并维护两个流程间的接口，以确保变更管理的有效性。

8.4.1.2 应在变更管理计划中识别要进行变更管理的工作成果、相关项和要素，这些工作成果、相关项和要素也要满足 7.4.3 的要求。

8.4.1.3 应为已识别出的工作成果、相关项和要素定义实施变更管理流程的日程表。

8.4.1.4 变更管理流程应包括：

a) 变更需求，按照 8.4.2；

b) 变更需求分析，按照 8.4.3；

c) 变更需求的决策和依据，按照 8.4.4；

d) 已接受的变更的实施和验证，按照 8.4.5；及

e) 文档化，按照 8.4.5。

注 1：变更管理流程可适用于开发过程中的相应阶段；

注 2：可在一个变更需求中处理多个变更。

8.4.2 变更需求

8.4.2.1 应为每个变更需求分配唯一的识别码。

8.4.2.2 每个变更需求应至少包含以下信息：

a) 日期；

b) 所需变更的理由；

c) 所需变更的准确描述；及

d) 所需变更基于的配置。

8.4.3 变更需求分析

8.4.3.1 对于每个变更需求,应针对以下信息,对所涉及的相关项或要素、接口及关联相关项或要素进行影响分析：

a) 变更需求的类型；

示例：可能的变更类型有：解决错误、调整、消除、加强、预防。

b) 对需更改的工作成果、相关项和要素及受影响的工作成果、相关项和要素进行的识别；

c) 在分布式开发的情况下，所涉及的相关方的识别及其责任；

d) 变更对功能安全的潜在影响；及

e) 变更的实现和验证的日程表。

8.4.3.2 对工作成果的每次变更，应重新启动安全生命周期的适用阶段。后续阶段的开展应符合 GB/T 34590-XXXX。

8.4.4 变更需求评估

8.4.4.1 应使用按照 8.4.3.1 进行的影响分析的结果,对变更需求进行评估,并且应由授权人员决定是否接受、拒绝或推迟变更。

示例：典型的授权的人员包括：

——项目经理；

——安全经理；

——负责质量保证的人员；及

——涉及的开发人员。

注：已接受的变更需求可按优先级排序，并与已接受的相关变更需求合并。

8.4.4.2 对于每个已接受的变更需求，应决定由谁来开展变更及变更的最晚时间。该决定应考虑开展变更时所涉及到的接口。

8.4.5 变更的实施和记录

8.4.5.1 应按计划实施变更和验证变更。

8.4.5.2 如果变更影响了安全相关功能或特性，则应在发布相关项前，对按照 GB/T 34590.2-XXXX 的 6.4.9 和 6.4.10 的功能安全评估和适用的确认评审进行更新。

8.4.5.3 变更的记录应包含以下信息：

a) 按照第 7 章，在合适的层面下，变更的工作成果、相关项和要素的清单，包括：配置和版本。

b) 开展的变更细节；及

c) 变更部署的计划日期。

注 1：对临时变更需求，应明确指出该变更需求的理由和变更持续的时间（如已知）。

注 2：对被拒绝的变更需求，记录变更需求和拒绝的理由。

8.5 工作成果

8.5.1 **变更管理计划**，由 8.4.1 的要求得出。

8.5.2 **变更需求**，由 8.4.2 的要求得出。

8.5.3 **影响分析和变更需求计划**，由 8.4.3 和 8.4.4 的要求得出。

8.5.4 **变更报告**，由 8.4.5 的要求得出。

9 验证

9.1 目的

验证的目的是确保工作成果符合它们相应的要求。

9.2 总则

验证适用于以下安全生命周期阶段：

a）在概念阶段，验证确保了概念是正确的、完整的、并符合相关项的边界条件，同时确保了定义的边界条件本身是正确的、完整的和一致的，以使概念可以得到实现。

b）在产品开发阶段，以不同的方式执行验证，描述如下：

——在设计阶段，验证是对工作成果的评估，例如：需求规范、架构设计、模型或软件编码，从而确保它们与之前建立的要求在正确性、完整性和一致性方面相符合。评估可通过评审、模拟或分析技术开展，并以系统化方式计划、定义、执行和记录。

注：设计阶段是指 GB/T 34590.4-XXXX 第 6 章、GB/T 34590.5-XXXX 第 7 章、GB/T 34590.6-XXXX 第 7 章和 GB/T 34590.6-XXXX 第 8 章。

——在测试阶段，验证是在测试环境下对工作成果、相关项和要素的评估，以确保其满足要求。测试以系统化的方式进行计划、定义、执行、评估和记录。

c）在生产和运行阶段，验证确保了：

——生产过程中恰当地满足安全相关的特殊特性

——在用户手册、维修和维护指导中恰当地提供了安全相关的信息；及

——通过在生产流程中应用控制措施，相关项的安全相关特性得到了满足。

注：这是一般性的验证流程，GB/T 34590.3、GB/T 34590.4、GB/T 34590.5、GB/T 34590.6 和 GB/T 34590.7 中的安全生命周期的各阶段给出了示例。该流程并不针对安全确认。本文件 GB/T 34590.4-XXXX 第 8 章，以获取更多细节。

9.3 本章的输入

9.3.1 前提条件

应具备如下信息：

——组织专门的功能安全规章和流程，按照 GB/T 34590.2-XXXX,5.5.1；及

——安全生命周期相关阶段（该阶段计划和执行验证）中适用的前提条件。

9.3.2 支持信息

本文件安全生命周期相关阶段（该阶段计划和执行验证）中适用的支持信息。

9.4 要求和建议

9.4.1 验证计划

9.4.1.1 对安全生命周期的每个阶段及子阶段，应制定验证计划，并应涵盖以下方面：

a）需验证的工作成果内容；

b）验证的目的；

c）用于验证的方法；

d）验证通过和不通过的准则；

e）如果适用，验证环境；

注：验证环境可以是测试环境或模拟环境。

f）如果适用，用于验证的设备；

示例：测试工具或者测量设备。

g）如果适用，用于验证的资源；

h）当探测出异常时需采取的行动；及

i）回归策略。

注：回归策略定义了在相关项或要素变更后如何重复进行验证。验证可以被全部或部分重复，并可包含其他能影响验证结果的相关项或要素。

9.4.1.2 制定验证计划宜考虑以下方面：

a）所使用验证方法的充分性；

b）需验证的工作成果的复杂性；

c）与验证目标材料相关的前期经验；及

注：这包括维修历史及在用证明达到的程度。

d）所使用技术的成熟度，或使用这些技术的风险。

9.4.2 验证规范

9.4.2.1 验证规范应对用于验证的方法进行细化，并应包含：

a）评审或分析的检查清单；或

b）模拟场景；或

c）测试用例、测试数据和测试目标。

9.4.2.2 对于测试，每条测试用例的定义应包含以下内容：

a）唯一的识别；

b）需验证的相关工作成果的版本的参考；

c）前提条件和配置；

注：如果对工作成果的可能配置（例如：系统变型）进行完整验证是不可行的，可选择一个合理的子集（例如：系统的最小或最大功能性配置）。

d）如果适用，环境条件；

注：环境条件与周围物理属性（例如：温度）有关，测试在该环境进行或模拟部分测试。

e）输入数据，数据时序及其值；

f）期望的表现，包括：输出数据、输出值的可接受范围、时间表现和公差表现；及

注 1：当定义期望的表现时，对初始输出数据的定义可能是必要的，以探测变化。

注 2：为避免重复定义和存储不同测试用例用到的前提条件、配置及环境条件，有必要使用明确的参考。

g）确定测试用例通过和不通过的准则。

9.4.2.3 对于测试，应按使用的测试方法对测试用例进行分组，从以下几个方面考虑：

a）所需的测试设备或测试环境；

b）逻辑和时间的依赖性；及

c）资源。

示例：将测试用例分成回归测试用例和完整测试用例。

9.4.2.4 对于测试，测试用例宜由与待验证的工作成果的完成人不同的人进行评审。

9.4.3 验证的执行和评估

9.4.3.1 应按照 9.4.1 所做的计划及按照 9.4.2 所做的规范，执行验证。

9.4.3.2 验证宜由与待验证的工作成果的完成人不同的人执行。

9.4.3.3 对验证结果的评估应包含以下信息：

a）所验证工作成果的唯一识别；

b）验证计划和验证规范的参考；

c）如果适用，评估中用到的验证环境配置、验证工具及标定数据；

d）验证结果与期望结果的一致性水平；

e）验证通过或不通过的明确的陈述，如果验证不通过，陈述应包含不通过的理由和对所验证工作成果进行修改的建议；及

注：按照验证的完成和结束准则[本文件 9.4.1.1 d)]和预期的验证结果，对验证进行评估。

f）每个验证步骤未执行的理由。

9.4.3.4 用于验证的测试设备应能提供有效的和可重复的结果，并应按照所采用的质量管理体系进行管控。

9.5 工作成果

9.5.1 **验证计划，**由 9.4.1.1 和 9.4.1.2 的要求得出。

9.5.2 **验证规范，**由 9.4.2.1～9.4.2.4 的要求得出。

9.5.3 验证报告， 由 9.4.3.1 ～ 9.4.3.4 的要求得出。

10 文档管理

10.1 目的

目的是开发用于整个安全生命周期的文档管理策略，以促进有效的和可重复的文档管理过程。

10.2 总则

文档管理是汽车工业中的一个成熟的实践,可依据质量管理体系（例如IATF16949 [6]或ISO9001[3]）或相关标准（例如 ISO/IEC/IEEE 12207 或 ISO/IEC/IEEE 15288[4]）进行应用。

GB/T 34590-XXXX 中对文档的要求主要关注内容，而非排版和外观。

信息不必一定呈现在物理文档中。文档可采取不同的形式和结构，并可使用工具自动生成文档。

示例：可能的形式有：纸张、电子媒体、数据库。

信息是否充分取决于很多因素，包括:复杂性、安全相关系统/子系统的范围和与特殊应用相关的要求。

宜避免一个文档中信息的重复及不同文档间信息的重复，以助于可维护性。

注：在一个文档中，使用交叉引用以代替信息的重复，将读者引向信息的源文件。

10.3 本章的输入

10.3.1 前提条件

应具备如下信息：

——组织专门的功能安全规章和流程，按照GB/T 34590.2-XXXX,5.5.1；及

——安全计划，按照GB/T 34590.2-XXXX，6.5.3。

10.3.2 支持信息

无。

10.4 要求和建议

10.4.1 应计划文档管理过程，以获得文档：

a) 用于在整个生命周期的每个阶段中有效完成各阶段及验证活动；

b) 用于功能安全的管理；及

c) 作为认可措施的输入。

10.4.2 应将对 GB/T 34590 中工作成果的识别理解为文档化要求，文档应包含相关要求的结果信息。

注：文档可以是单个文档的形式，该文档包含工作成果的完整信息；也可以是一组文档的形式，这些文档合起来包含工作成果的完整信息。

10.4.3 文档宜是：

a) 准确的和简明的；

b) 结构清晰的；

c) 目标使用者容易理解的；

d) 可验证的；及

e) 可维护的。

10.4.4 整个文档的结构宜考虑内部流程和工作实践。应对文档进行组织以助于搜索相关信息。

示例：文档树。

10.4.5 每个工作成果或文档应包含下面的正式要素：

a) 题目，参照内容的范围；

b) 作者和批准者；

c) 文档每个不同修订（版本）的唯一标识；

d) 变更历史；及

注：变更历史包含：每次变更的作者姓名、日期和简要描述。

e) 状态。

注：“草稿”、“已发布”、“有效”、“废止”。

10.4.6 按照第 7 章，应能识别当前适用的文档修订（版本）或信息项。

10.5 工作成果

10.5.1 **文档管理计划**，由 10.4.1 和 10.4.2 的要求得出。

10.5.2 **文档指南要求**，由 10.4.3~10.4.6 的要求得出。

11 所使用软件工具的置信度

11.1 目的

本章的目的是：

a）提供准则，以确定在适用时所要求的软件工具置信度水平；及

b）在适用时提供鉴定软件工具的方法，以建立证据证明软件工具适合用于支持 GB/T 34590-XXXX 要求的活动或任务（即，对那些 GB/T 34590-XXXX 要求的活动或任务，使用者可依靠软件工具的正确功能）。

11.2 总则

在系统或其软件要素、硬件要素开发中使用的软件工具，可以支持 GB/T 34590-XXXX 要求的活动或任务。在这些情况下，需要具备软件工具有效达到下述目标的置信度：

a) 在开发产品中，将因软件工具功能异常导致错误输出的系统性故障的风险减小到最低；及

b) 如果 GB/T 34590-XXXX 要求的活动或任务依赖于所使用软件工具的正确功能，软件工具的开发流程充分符合 GB/T 34590-XXXX。

注 1：“软件工具”，可以是独立软件包，也可以是由一套软件工具集成的工具链。

示例 1：商业工具、开源工具、免费工具、共享工具或使用者自己开发的工具。

为了制定上述条件下开发的软件工具的置信度水平要求，对以下准则进行评估：

——软件工具功能异常及其相应的错误输出，可导致或无法探测出正在开发的安全相关项或要素中的错误的可能性；及

——防止或探测软件工具相应输出中的这些错误的置信度。

基于工具用户的要求，工具可以是已有的，也可以是按照要求开发的。

示例： 软件开发工具、需求管理工具、系统设计工具、测试工具、静态分析工具等。

使用软件工具的置信度由两组活动组成，详见图 3：

a) 工具使用方面

——基于工具所需功能和特性进行软件工具使用评估。相应工具置信度（TCL）的确定是基于分析等级，包括工具影响（TI）、工具错误探测（TD）。TI和TD的确定取决于使用该工具进行要素开发和/或验证的开发过程。

——按照评估和鉴定的结果，将软件工具集成进用户环境（见11.4.2和11.4.3）。

示例 2：工具可能需要与配置管理工具、编辑工具或编译器进行集成。

——验证该工具在用户环境下正常工作。检查预定的工具置信度水平或鉴定（11.4.2）的有效性，如果需要，在用户环境下执行鉴定过程。

示例 3：为有代表性的使用案例测试用户环境下的工具的执行情况。

示例 4：运行工具确认测试套件。

——工具的适当使用：在用户环境下，操作工具按照定义的程序自动执行开发/验证任务。（本文件11.4.3）。

b) 工具鉴定方面

——基于对工具使用给定的或假设的信息（例如：使用案例、用户要求、TCL、ASIL等级）进行工具鉴定。

对工具要求的严格性，不宜因工具是已有的或者定制的而有倾向性。相反，要求取决于工具的作用、工具失效相关的风险和相关项或要素的最高ASIL等级。

注 2：此方法的目的是避免对专门为电子电气系统开发的低影响的工具提出过度要求。另外，此方法也降低了由以下假设所带来的倾向性：不需要对已有工具提出适当严格的要求。

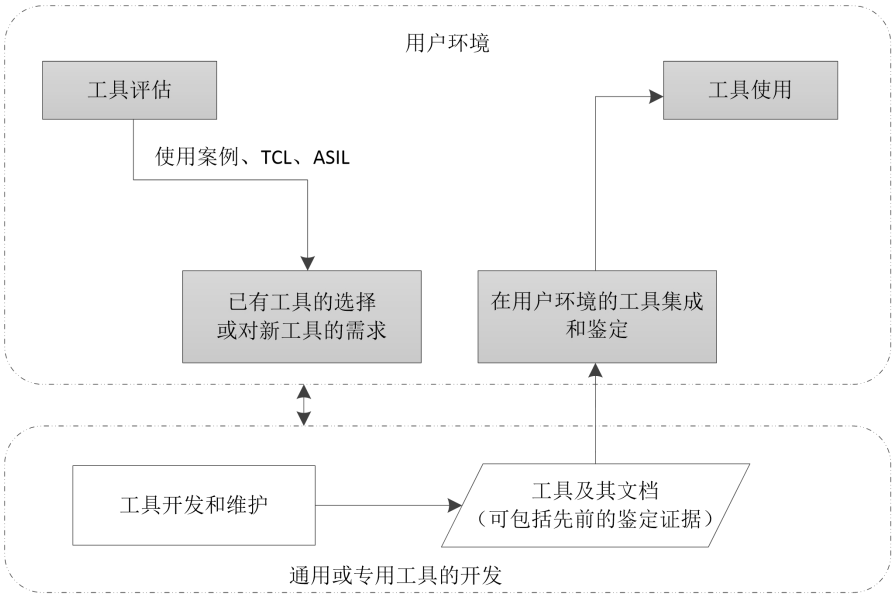


图 3-工具置信度活动的概览

为评估预防或探测措施的置信度，考虑并可评估在安全相关项或要素开发过程中实施的软件工具内部措施（如：监控）及软件工具外部措施（如：指南、测试、评审）。工具评估流程、工具置信度水平（TCL）的确定和相应的鉴定如图 4 所示。

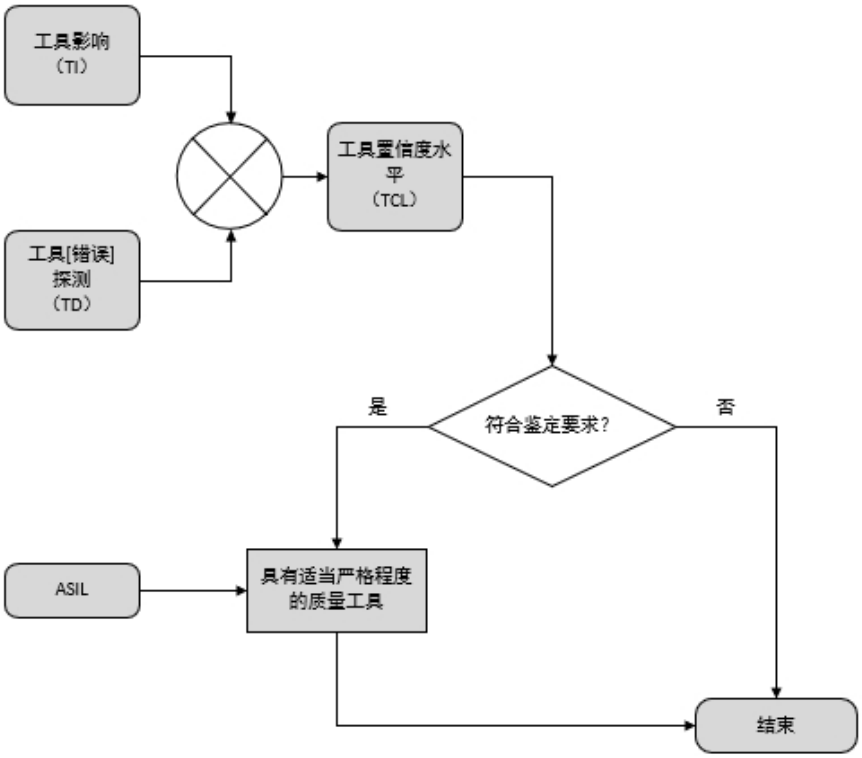


图 4-工具评估与鉴定流程

如果受工具置信度水平要求，则使用恰当的鉴定方法以符合此工具置信度水平，并符合分配给将使用此软件工具开发的相关项或要素的安全要求中最高 ASIL 等级。

11.3 本章的输入

11.3.1 前提条件

应具备如下信息：

——安全计划，按照GB/T 34590.2-XXXX，6.5.3；

——组织专门的功能安全规章和流程，按照GB/T 34590.2-XXXX，5.5.1；及

——安全生命周期相关阶段（该阶段使用了软件工具）中适用的前提条件。

11.3.2 支持信息

可考虑如下信息：

——预先确定的最大ASIL等级；

——软件工具的用户手册（来自外部）；及，

——软件工具的环境和约束（来自外部）。

11.4 要求和建议

11.4.1 一般要求

11.4.1.1 如果安全生命周期包含使用软件工具用于系统、硬件要素或软件要素的开发，使得 GB/T 34590-XXXX 要求的活动或任务依赖于软件工具的正确功能，与此同时未按照适用的流程步骤对工具的相关输出进行检查或验证，那么该软件工具应符合本章的要求。

11.4.2 预先确定的工具置信度水平的有效性或鉴定的有效性

如果对软件工具的置信度水平评估或鉴定的执行，独立于特定安全相关项或要素的开发，那么应在软件工具用于特定安全相关项或要素开发之前，对预先确定的工具置信度水平的有效性或鉴定的有效性进行验证。

注：关于软件工具、置信度水平评估和鉴定的信息的搜集可以是跨组织的活动，这样有助于减少每个开发项目的难度。

11.4.3 软件工具与其评估准则或鉴定的一致性

当使用软件工具时，应确保工具的使用、工具定义的环境和功能约束及其一般运行条件，与工具评估准则或鉴定相符合。

示例：使用案例和实施的预防或探测功能异常及其相应的错误输出的措施，应与软件工具鉴定报告中记录的版本和配置设置一致。

11.4.4 对软件工具使用的计划

11.4.4.1 应计划软件工具的使用，包括制定：

a) 软件工具的识别码和版本号；

b) 软件工具的配置；

示例 1：通过设定编译器开关和 C 源文件中“#pragma”声明，定义编译器的配置。

c) 软件工具的使用案例；

注 1：在开展安全生命周期活动时，使用案例可以描述用户与软件工具的配合和软件工具功能的应用子集。

注 2：使用案例可包含对软件工具配置及软件工具执行环境的要求。

d) 软件工具执行的环境；

示例 2：执行软件工具所需的资源、基础设施或运行时环境，应用软件工具所需的流程活动或与软件工具输出结果验证相关的后续流程活动。

e) 当软件工具功能异常并产生相应的错误输出时，会直接违背分配给相关项或要素的全部安全要求的最高 ASIL 等级；及

注 3：可根据特定开发确定最高 ASIL 等级，或可根据软件工具通用的用法确定最高 ASIL 等级。在预先假定 ASIL 等级的情况下，对该假设进行验证。

f) 如需要，基于确定的置信度水平和 ASIL 等级的软件工具的鉴定方法。

11.4.4.2 为确保恰当的评估或使用软件工具，应具备以下信息：

a) 软件工具的特征、功能和技术属性的描述；

b) 如果适用，用户手册或其他使用指南；

c) 工具运行要求的环境描述；

d) 如果适用，对异常运行条件下期望的软件工具表现的描述；

示例 1：异常运行条件可以是禁止的编译开关组合、不符合用户手册的环境或不正确的安装。

示例 2：异常运行条件下期望的表现可以是对输出生成的阻止、用户提示或用户报告。

e) 如果适用，对已知软件工具功能异常，及恰当的安全保护、避免或应急措施的描述；及

示例 3：针对已知的功能异常、编译器编码优化局限或建模中使用受限制的一组构件的使用指南或应急措施。

示例 4：安全保护包括通过使用约束防止全部已知的功能异常和问题、探测和报告全部已知的功能异常和问题，也包括提供安全替代技术以开展相应的活动。

f) 在制定软件工具要求的置信度水平过程中，识别出的对软件工具功能异常和相应错误输出的预防或探测措施。

注 1：相应错误输出的预防或探测措施可针对软件工具输出中的已知和潜在错误。

示例 5：冗余软件工具输出的对比、执行的测试、静态分析或评审、软件工具日志文件的分析、具有已知问题的功能的避免。

11.4.5 通过分析对软件工具进行评估

11.4.5.1 对软件工具使用的描述应包含下述信息：

a) 预期的目的；

示例 1：功能的模拟、源代码的生成、嵌入式软件的测试、安全生命周期的裁剪、GB/T 34590 要求的活动和任务的简单化或自动化。

b) 输入和期望的输出；及

示例 2：后续开发活动输入所需的数据、源代码、模拟结果、测试结果、或 GB/T 34590 的其他工作成果。

c) 如果适用，使用过程、环境的和功能的约束。

示例 3：软件工具嵌入到开发过程、不同软件工具使用共享数据及其他使用条件、预防或探测软件工具的功能异常的流程措施。

11.4.5.2 应分析和评估软件工具的预期使用，以确定：

a) 特定软件工具功能异常可引入或不能探测开发中安全相关项或要素中错误的可能性。这是通过工具影响（TI）等级表示的：

——当有论据表明没有这样的可能性时，应选择TI1;

——在所有其他情况下应选择TI2。

b) 用于预防软件工具功能异常并产生相应错误输出的措施的置信度，或用于探测软件工具存在功能异常并已产生相应错误输出的措施的置信度。这是通过工具错误探测（TD）等级表示的：

——当对预防或探测出功能异常及其相应错误输出具有高置信度时，应选择TD1；

——当对预防或探测出功能异常及其相应错误输出具有中等置信度时，应选择TD2；

——在所有其他情况下应选择TD3。

注 1：预防或探测可通过流程步骤、任务或软件工具的冗余、或软件工具自身的合理性检查完成。

注 2：如果具备的开发流程中没有系统性措施，则典型适用 TD3，为此，仅能随机探测出软件工具的功能异常及其相应错误输出。

注 3：如果用一个软件工具验证另一软件工具的输出，当评估这一软件工具时，考虑软件工具间的相互依赖性，为该软件工具选择一个充分的 TD。例如，工具之间可能因使用了公共组件或者共享资源而存在相互依赖性。

注 4：此使用分析的详细程度仅需要允许恰当的确定 TI 和 TD 的等级。

示例 1：在按照 GB/T 34590 对产生的源代码进行验证的情况下，为代码生成器选择 TD1。当不对产生的源代码进行验证时，为代码生成器选择 TD3。

示例 2：使用指南防止功能异常，例如编译器对代码构成的错误或不清晰的理解。

示例 3：针对用于静态验证源代码中不存在潜在的除零情况的工具，如果为此目的也同时进行了测试，则可为该工具选择 TD2。如果仅通过工具验证不存在除零的情况，可为该工具选择 TD3。

11.4.5.3 如果对 TI 或 TD 选择的正确性是不清楚的或可疑的，宜对 TI 和 TD 进行保守评估。

11.4.5.4 基于为 TI 和 TD 等级确定的值（按照 11.4.5.2 或 11.4.5.3），应按照表 3 来确定所要求的软件工具的置信度水平。

表 3 工具置信度水平的确定

		工具错误探测		
		TD1	TD2	TD3
工具影响	TI1	TCL1	TCL1	TCL1
	TI2	TCL1	TCL2	TCL3

11.4.6 软件工具的鉴定

11.4.6.1 对鉴定等级为 TCL3 的软件工具，应使用表 4 列出的方法。对鉴定等级为 TCL2 的软件工具，

应使用表 5 列出的方法。等级为 TCL1 的软件工具无需鉴定方法。

表 4 TCL3 等级的软件工具的鉴定

方法		ASIL等级			
		A	B	C	D
1a	使用中积累置信度，按照11.4.7	++	++	+	+
1b	工具开发流程评估，按照11.4.8	++	++	+	+
1c	软件工具确认，按照11.4.9	+	+	++	++
1d	按照安全标准开发[a]	+	+	++	++

[a] 没有安全标准完全适用于软件工具的开发。相反，可选择安全标准中相关的一组安全要求。

示例：按照GB/T 34590-XXXX、GB/T 20438、EN50128或RTCA DO-178开发软件工具。

表 5 TCL2 等级的软件工具的鉴定

方法		ASIL等级			
		A	B	C	D
1a	使用中积累置信度，按照11.4.7	++	++	++	+
1b	工具开发流程评估，按照11.4.8	++	++	++	+
1c	软件工具确认，按照11.4.9	+	+	+	++
1d	按照安全标准开发[a]	+	+	+	+

[a] 没有安全标准完全适用于软件工具的开发。相反，可选择安全标准中相关的一组安全要求。

示例：按照GB/T 34590-XXXX、GB/T 20438、EN50128或RTCA DO-178开发软件工具。

11.4.6.2 应对软件工具的鉴定进行文档化，包含以下信息：

a) 软件工具的唯一识别码和版本号；

b) 软件工具划分的最高工具置信度等级，及其评估分析参考；

c) 对于考虑的使用案例，当软件工具功能异常并产生相应的错误输出时，可能直接违背任何安全要求的预定义最高 ASIL 等级或特定 ASIL 等级；

d) 软件工具被鉴定的配置和环境；

e) 执行鉴定的人员或组织；

f) 鉴定使用的方法，按照 11.4.6.1；

g) 用于鉴定软件工具的措施结果；及，

h) 如果适用，在鉴定过程中识别出的使用约束和功能异常。

11.4.7 使用中积累置信度

11.4.7.1 如果按照表 4 或表 5，将“使用中积累置信度”的方法用于软件工具的鉴定，则应满足此条的要求。

11.4.7.2 仅当具备以下方面的证据时，才应论证软件工具在使用中积累了置信度：

注：第 14 章中在用证明的要求不适用于本条。

a) 此前，已经将该软件工具用于相同的目的，具有相似的使用案例、相似的预定运行环境和相似的功能约束中；

b) 使用中积累置信度的理由是基于充分适当的数据；

注：可从累计使用量中获得数据（例如：时间长度或频率）。

c) 软件工具的定义未改变；及

d) 在之前开发中获得的软件工具功能异常和相应错误输出的发生案例是以系统化方式累计的。

11.4.7.3 应通过考虑以下信息，对给定开发活动中软件工具的先前使用经验进行分析和评估：

a) 软件工具唯一的识别码和版本号；

b) 软件工具的配置；

c) 使用周期和使用相关数据的细节；

示例 1：软件工具相关使用案例中，使用的软件工具特征及使用频率。

d) 软件工具的功能异常和相应错误输出的详细文档化记录，其中包含引起功能异常和错误输出的条件；

e) 所监控的先前版本清单，其中列出每个相关版本中解决的功能异常；及

f) 如果适用，对已知缺陷的安全保护、避免措施、应急措施或相应错误输出的探测措施

示例 2：使用报告的来源可以是日志、供应商提供的软件工具版本历史、已发布的勘误表。

11.4.7.4 使用中积累置信度的论证应仅对所评估的软件工具版本有效。

11.4.8 工具开发流程评估

11.4.8.1 如果按照表 4 或表 5，将“工具开发流程评估”的方法用于软件工具的鉴定，则应满足此条的要求。

11.4.8.2 用于软件工具开发的流程应满足适当的标准。

注：对于开源开发，那些团体使用的某些标准也可能是适当的。

11.4.8.3 应基于恰当的国内或国际标准对软件工具开发流程进行评估，同时提供恰当的软件开发流程被应用的证据。

注：该评估涵盖了对软件工具的一个恰当且相关的特征子集的开发。

示例：使用基于 Automotive SPICE®、ISO/IEC 33000 或 CMMI 的评估方法。

11.4.9 软件工具确认

11.4.9.1 如果按照表 4 或表 5，将“软件工具确认”的方法用于软件工具的鉴定，则应满足此条的要求。

11.4.9.2 软件工具的确认应满足以下准则：

a) 确认措施应提供软件工具符合分类中指定用途的特定要求的证据；

注 1：确认提供了评估的工具错误不会发生或将被检测到的证据；

注 2：确认可通过使用用户开发的或工具供应商（如果供应商的测试套件包括用户的工具使用案例）开发的自定义测试套件来实施。

示例 1：编程语言标准有助于定义相关编译器的确认要求。

b) 应对确认中发生的软件工具功能异常及其相应错误输出、其可能的后果信息、及避免或探测它们的措施进行分析；及

c） 应检查软件工具对异常运行条件的响应。

示例 2：可预见的误用、不完整的输入数据、不完整的软件工具升级、使用被禁止的配置设置组合。

11.5 工作成果

11.5.1 软件工具准则评估报告，由 11.4.1~11.4.5 的要求得出。

11.5.2 软件工具鉴定报告，由 11.4.6~11.4.9 的要求得出。

12 软件组件的鉴定

12.1 目的

软件组件鉴定的目的是提供证据，以证明在符合GB/T 34590开发的相关项中对它们的重复使用是合适的。

12.2 总则

使用已鉴定的组件避免了对具有相同功能或特性的现有软件组件的重复开发或者促进了商业现成软件的使用。

注：软件组件可包括源代码、模型、预编译代码，或已编译及链接的软件。

示例：本章所指的软件组件包括：

——来自第三方供应商的软件库（商业现成（COTS）软件）；

——现有的未按照 GB/T 34590 开发的软件组件；

——已经用于电控单元的内部开发组件。

12.3 本章的输入

12.3.1 前提条件

应具备如下信息：

——组织专门的功能安全规章和流程，按照GB/T 34590.2-XXXX，5.5.1；及

——对软件组件的要求（来自外部）。

12.3.2 支持信息

可考虑下列信息：

——软件组件的设计规范（来自外部）；

——先前对软件组件采用的验证措施的结果（来自外部）。

12.4 要求和建议

12.4.1 总则

为了能认定软件组件是经鉴定的，应具备：

a） 软件组件的定义，按照 12.4.2.1；

b） 表明软件组件符合 12.4.2.2、12.4.2.3 和 12.4.2.4 相关要求的证据；

c） 软件组件适合其用途的证据，按照 12.4.3；

d） 组件的软件开发过程是基于适当的国家或国际标准的证据（如 ISO/IEC/IEEE 12207）；及

e） 软件组件鉴定计划

注：对之前开发的软件组件，可执行某些二次开发活动，以满足本条的要求。

12.4.2 软件组件鉴定的定义

12.4.2.1 **软件组件鉴定的定义应包括：**

a) 软件组件的唯一识别；

b) 当软件组件错误执行时，可能违背的所有安全要求的最高 ASIL 等级；

c) 为鉴定软件组件所应执行的活动；

d) 软件组件的要求；

示例：要求可包括：

——功能要求；

——已知的安全要求；

——算法精度或数值精度，算法精度考虑仅提供近似解的程序误差，数值精度考虑由计算误差导致的取整误差，以及在电控单元中函数的近似表达所引起的截断误差；

——失效情况下的表现；

——响应时间；

——资源使用；

——运行环境的要求；及

——过载情况下的表现（鲁棒性）。

e) 软件组件预期用途的要求；

f) 配置描述；

注：对于包含多个软件单元的软件组件，配置描述包括每个软件单元的唯一识别和配置。

g) 如有，所需接口的描述、供给接口的描述、共享资源的描述；

h) 应用手册（在适当的地方）；

i) 正确集成与使用软件组件所需的开发工具。

注：描述包括正确集成与使用软件组件所需的开发工具的配置参数。

j) 异常运行条件下，所执行的功能的反应；及

示例：对非重入软件功能的重入调用的反应。

k) 对已知异常及相应应急措施的描述。

12.4.2.2 **为提供证据表明软件组件符合其要求，软件组件的验证应：**

a) 展示对要求的覆盖率，按照 GB/T 34590.6-XXXX 第 9 章；

注：该验证是主要基于要求的测试，可使用软件组件开发过程中或在之前的集成测试中执行的基于要求的测试结果。

示例：专用鉴定测试套件的应用，对软件组件实施和全部集成期间的所有已执行测试的分析。

b) 既覆盖正常运行条件，也覆盖失效情况下的表现；及

c) 显示可能会导致违背分配给该软件组件安全要求的非已知错误

12.4.2.3 **本要求适用于ASIL D，按照4.4：结构覆盖率应按照GB/T 34590.6-XXXX第9章来测量，以评估测试用例的完整性。**

12.4.2.4 **按照12.4.2.2的验证，应仅对软件组件未经改变的实现有效。**

12.4.2.5 **应对软件组件的鉴定进行记录，包括下述信息：**

a) 软件组件的唯一识别；

b) 软件组件的唯一配置；

c) 执行鉴定的人员或组织；

d） 用于鉴定的环境；

e） 用于鉴定软件组件的验证措施的结果；及

f） 分配给软件组件的安全要求的最高 ASIL 等级。

12.4.3 软件组件鉴定的验证

应按照第 9 章验证软件组件的鉴定结果连同这些结果对软件组件预期使用的有效性。

12.5 工作成果

12.5.1 软件组件的文档，由 12.4.2.1 的要求得出。

12.5.2 软件组件鉴定报告，由 12.4.2.2~12.4.2.5 的要求得出。

12.5.3 软件组件鉴定的验证报告，由 12.4.3 的要求得出。

13 硬件要素评估

13.1 目的

本章的目的是确保硬件要素的功能表现足以满足分配的安全要求，因此，由于硬件要素的系统性故障而违背安全目标或安全要求的风险是足够低的。基于随机故障管理的硬件要素的适用性，由被评估硬件要素的集成者在设计集成的下一个更高层面进行确定。

注1：满足安全概念的要求包括提供适用于硬件失效分析的硬件要素的失效模式和失效模式分布的信息

注2：本章的目的不是考虑硬件要素在预期环境条件下的鲁棒性或硬件要素的可靠性时确保其适用性。针对所有硬件要素的这部分内容，在GB/T 34590.5-XXXX第10章中描述。

本章中用到的“硬件要素”术语指的是商业现成硬件组件或元器件，或指定制的硬件组件或元器件，即:

——最初不是按照GB/T 34590开发或设计的；及

——集成到符合GB/T 34590的相关项或要素中时，被认为是与安全相关的。

更准确地说，硬件要素的评估是符合GB/T 34590.5的可选的方法。符合评估条件的硬件要素可以是特定于应用的要素或是标准要素。这些要素通常被开发用于多个行业，包括汽车应用或非汽车应用。

13.2 总则

硬件要素的评估将实现以下目标：

a）提供证据证明硬件具备足够的功能性能，因此可以按照硬件设计的需求提供预期功能；

b）通过使用适当的测试（例如超限测试、加速测试等）或分析，来识别新的或认可已知的失效模式及模型（包括对它们分布的量化）；

c）识别新的或认可已知的硬件要素的使用限制；及

d）提供论据证明由于系统性故障而导致的某个安全目标被违背或某条安全要求被违背的风险是足够低的。

硬件要素的评估是基于特定的应用背景完成的。

在硬件要素的评估中，所考虑的硬件要素根据其特性分为 I 类要素、II 类要素或 III 类要素。这些类别反映了安全相关功能验证的难度，以及硬件要素在安全概念中的作用。

根据类别的不同，给出了不同的硬件要素评估要求。首先第一步，应规定硬件要素的相关要求并识别其安全相关的失效模式。

对于 I 类要素的评估，按照 GB/T 34590.5-XXXX 第 10 章对集成了所评估硬件要素后的硬件要素进行测试是充分的。

对于 II 类要素的评估，可以通过测试与分析相结合的方式来完成。

对于III类要素的评估，除了II类要素所必需的评估活动之外，还需增加论证来证明安全目标被违背的风险或安全要求被违背的风险是足够低的。

13.3 本章的输入

13.3.1 前提条件

应具备下列信息：

——组织专门的功能安全规章和流程，按照GB/T 34590.2-XXXX, 5.5.1；

——与所考虑的硬件要素相关的安全要求；

——设计验证准则（分析和测试），按照GB/T 34590.5-XXXX第6章；及

——生产商的硬件要素规范，如果没有，或硬件要素规范的假设（来自外部）。

13.3.2 支持信息

可考虑下列信息：

——安全生命周期相关阶段（该阶段应用了硬件要素评估）中适用的支持信息；及

13.4 要求和建议

13.4.1 总则

13.4.1.1 被评估硬件要素的分类

硬件要素应被分为以下类别之一：

a） I类要素，如果：

——该要素最多有几种状态，且这几种状态可以从安全的视角被充分地表征、测试和分析；

——可以在不了解该要素的实现细节和生产过程的情况下，识别并评估该要素的安全相关的失效模式；及

——该要素没有与安全概念相关的控制或探测其内部失效的内部安全机制。

注：这并不包含监控要素外部特性的安全机制。

示例：电阻，电容，晶体管，二极管，晶振，谐振器。

b） II类要素，如果：

——该要素具有，例如：较少的运行模式，较小的取值范围，较少的参数，并且可以在不了解实现细节的情况下从安全的角度对其进行分析；

——现有的文档可以提供有效的假设，以支持通过测试和分析评估系统性故障，而无需了解该要素的实现细节和生产过程； 及

示例：数据表，用户手册，应用说明。

——该要素没有与安全概念相关的控制或探测其内部失效的内部安全机制。

注：这并不包含监控要素外部特性的安全机制。

示例：燃油压力传感器，温度传感器，没有与安全概念相关的内部安全机制的独立模数转换器（ADC）。

c）III类要素，如果：

——该要素具有，例如：较多的运行模式，较大的取值范围或较多的参数，并且在不了解实现细节的情况下，不能进行分析；

——系统性故障的来源只能通过实现细节、开发过程和/或生产过程的方式来理解和分析；或

——该要素具有与安全概念相关的控制或探测其内部失效的内部安全机制。

示例：微处理器，微控制器，数字信号处理器（DSP）。

13.4.1.2 应定义由分配的安全要求和安全概念产生的对硬件要素的要求。

注：对于I类要素，这通常与硬件要素规范一致，例如：电阻的标称值和公差值。

13.4.1.3 应识别硬件要素的失效模式或故障，及其随机硬件故障的分布。

13.4.1.4 应识别与硬件要素的安全相关的失效模式或故障。该分析应提供证据证明GB/T 34590.5-XXXX, 7.4.3、第8章、第9章的相关要求得到了满足。

13.4.2 I 类硬件要素的评估

由于I类要素的功能较为简单，因此不需要对其本身进行评估；集成了I类硬件要素的硬件开发应按照GB/T 34590进行。

13.4.3 II 类硬件要素的评估

13.4.3.1 评估方法

II类硬件要素的评估应使用恰当的分析和测试选择进行。

13.4.3.2 评估计划

应开发评估计划，并应描述：

a）硬件要素的唯一识别及版本；

b）硬件要素预期使用环境的定义；

c）评估策略和依据；

注：策略包括：分析、必要的测试和逐步的描述。

d）该策略所必需的工具和设备；

e）实施该评估的责任方；及

f）用于评估硬件要素通过和不通过的准则。

13.4.3.3 评估论证

13.4.3.3.1 应按照硬件设计，对硬件要素的功能性能符合其规范且足以满足其预期用途进行全面论证。

注：所要求的性能，包括在已制定的正常环境条件下的行为，及与假定失效触发事件组合的环境条件下的行为。

13.4.3.3.2 对13.4.3.3.1的全面论证应基于与下述类型信息的组合：

a）使用的分析方法和假设；

b） 来自运行经验的数据；及

c） 现有测试结果。

13.4.3.3.3 应给出每一个假设（包括推断）的理由。

13.4.3.4 分析评估

13.4.3.4.1 分析的结果应以全面的形式提供，且可以由具有相关工程学科或科学学科资质的人员加以验证。

注：可用的分析方法包括设计验证方法，例如：外推法、数学模型、损伤分析或类似方法，以及过程差距分析，以显示可避免系统性失效的足够的证据。

13.4.3.4.2 分析应考虑硬件要素所暴露的全部环境条件，这些条件的限制及其他额外的运行压力（例如：预期的开关周期、充电和放电、长时间关闭）。

13.4.3.5 测试评估

13.4.3.5.1 应制定测试计划，且测试计划应包含下列信息：

a）硬件要素的功能描述；

b）所分配的安全要求；

c）需要进行的测试规范和顺序；

d）测试与安全要求之间的追溯性；

e）组装和连接的要求；

f）需要模拟的运行条件和环境条件；

g）被测要素的数量；

h）测试通过/不通过的准则；

i）需要测量的环境参数；及

j）对测试设备的要求，包括精度。

13.4.3.5.2 应按照GB/T 34590.5-XXXXX,10.4.6完成被评估硬件要素对外部压力的鲁棒性测试。

示例：该规范可以基于GB/T 28046或等效的企业标准。

13.4.3.5.3 应按照计划进行测试，并应具备测试结果数据。

13.4.3.5.4 集成到符合GB/T 34590的要素时，应符合GB/T 34590.5-XXXX第10章或GB/T 34590.4-XXXX第7章的要求。

13.4.3.6 评估报告

评估报告应说明，基于所执行的分析和测试，针对定义并分配给该硬件要素的安全要求（包括其工作范围和条件），硬件要素是否通过了评估。

注：评估报告可由包括调查报告和解释记录在内的一系列文件组成。

13.4.3.6.1 应按照第9章对评估报告进行验证。

13.4.4 III 类硬件要素的评估

13.4.4.1 III 类硬件要素宜按照 GB/T 34590 进行开发。

注：这意味着 “III类要素的评估” 并非首选方法，因此下一版本的硬件要素计划按照 GB/T 34590开发。

13.4.4.2 对 III 类硬件要素的评估，应满足 13.4.3 中规定的要求。

13.4.4.2.1 应提供额外措施，证明由于系统性故障而违背安全目标或违背安全要求的风险足够低。

注1：根据提供的论证组合，硬件评估的结果表明在给定应用的情况下使用III类要素是安全的。但是该论证并非对所有应用都有效。

注 2：措施可以包括但不限于：

a）安全相关功能的可验证性；

b）现场经验/“值得信赖的组件”；

注：现场经验可以作为硬件评价的一部分支持性论证。对于完整的在用证明论证，则遵循GB/T 34590.8- XXXXX,第14章，而非本章。

c）由具备安全相关失效模式检测能力的、独立的多样化要素进行监控；及

注：独立性可通过符合GB/T 34590.9 -XXXXX,第7章的相关失效分析来显示。

d）符合不同安全标准但具有同等完整性等级的开发。

13.5 工作成果

13.5.1 硬件要素评估计划，由 13.4.3.2 的要求得出；

13.5.2 如果适用，硬件要素测试计划，由 13.4.3.5.1 的要求得出；

13.5.3 如果适用，硬件要素评估报告，由 13.4.1.1，13.4.3.6 和 13.4.4.3 的要求得出。

14 在用证明

14.1 目的

本章的目的是提供对在用证明的指导。当现场数据可用时，对已有相关项或要素的复用，可以使用在用证明，作为符合GB/T 34590的替代方法。

14.2 总则

在用证明可用于与已发布并投入使用的产品的定义及使用条件具有相同或高度通用性的任何类型的产品。它也可用于与这类产品相关的任何工作成果。

注 1：在用证明不是指互换性：即为取代在用产品而具有替换设计或替换实现的产品，不能因为其满足原有功能要求而被认为是在用证明，除非该产品符合本章定义的准则。

相关项或要素，如系统、功能、硬件或完整的软件产品，可作为在用证明的候选项。

候选项也可针对工作成果，如技术安全概念。

使用在用证明的动机包括：

a) 意图将商业使用的“汽车应用”部分的或完全的沿用到另一个目标；或

b) 意图使运行中的电控单元（ECU）执行一个附加功能；或

c) 在 GB/T 34590 发布前已在现场使用的候选项；或

d) 在其他安全相关工业中使用的候选项；或

e) 候选项是广泛使用的商业现成产品（COTS），不一定必须用于汽车应用。

在用证明是通过候选项适当的文件、配置管理和变更管理的记录、及安全相关事故的现场数据来证实的。

一旦定义了具有预期在用证明可信度（本文件14.4.2）的候选项（本文件14.4.3），在准备在用证明时，需考虑两个重要准则：

——在候选项上一评估期内的现场数据的相关性（本文件14.4.5）；及

——如有，从候选项上一评估期开始可能对候选项产生影响的变更（本文件14.4.4）。

注 2：关于现场数据的相关性，在用证明是为了指出候选项的系统性失效和随机失效，它并不指出与候选项老化相关的失效。

使用在用相关项或要素并不能使这些相关项或要素免除下述项目相关的安全管理活动：

——在安全计划中描述在用证明可信度；及

——由在用证明得出的数据和工作成果是安全档案的一部分，并符合认可措施。

14.3 本章的输入

14.3.1 前提条件

应具备下列信息：

——关于候选项的预期使用：

候选项定义；

适用的安全目标或安全要求及相应的ASIL等级；及

可预见的运行场景和预期的运行模式及接口。

——关于候选项之前的使用：

来自服务期的现场数据（来自外部）。

14.3.2 支持信息

关于候选项之前的使用应考虑下列信息：

——安全档案，按照GB/T 34590.2-XXXX，6.5.4。

注：对于未按照 GB/T 34590 开发的候选项（例如商业现成产品（COTS）、基于 GB/T 34590 之外的其他安全标准（如 IEC61508 或 RTCA DO-178 C）所开发的候选项），可能不具备安全档案中的某些工作成果，在这种情况下，这些成果将被候选项开发中得到的可用数据所替代。

14.4 要求和建议

14.4.1 总则

下述条基于候选项未来使用时适用的 ASIL 等级；

14.4.2 在用证明可信度

14.4.2.1 只有当候选项符合 14.4.2～14.4.5 时才应使用在用证明可信度。

14.4.2.2 应按照 GB/T 34590.2-XXXX，6.4. 5 计划由在用证明得出在用证明可信度。

14.4.2.3 在用证明可信度应仅来自于被候选项在用证明覆盖的安全生命周期子阶段和活动；

14.4.2.4 应按照 GB/T 34590.4-XXXX 第 8 章在适当层面执行对相关项或要素中的在用证明要素的集成措施。

示例：某个电控单元的硬件有令人满意的现场记录，且将被 100%沿用到某个新的应用。在用证明可信度可被用于该硬件要素开发的子阶段及活动。同样，如果具有令人满意的服役记录的软件 100%被沿用，那么在用证明可信度也可被用于软件子阶段及活动。

14.4.2.5 应按照 GB/T 34590.4-XXXX 第 9 章执行对嵌入了在用证明要素的相关项的安全确认。

14.4.2.6 对嵌入了在用证明的要素的相关项,其认可措施应按照 GB/T 34590.2-XXXX,6.4.9 和 6.4.10 考虑在用证明及相关数据。

14.4.2.7 对在用证明的相关项或要素进行任何修改，都应符合 14.4.4，以保持相应的在用证明可信度。

注：本章适用于任何类型的修改，包括那些由于安全相关事件而启动的修改。

14.4.3 候选项的最低限度信息

应具备对候选项及其之前使用的描述，以及包括：

a) 如有，候选项的识别和追溯，及内部要素或组件的目录；

b) 相应的配合要求、形式要求和功能要求，若适用，并描述候选项的接口和环境特性、物理和尺寸特性、功能和性能特性；及

c) 如果适用，候选项之前使用时的安全要求及相应的 ASIL 等级。

14.4.4 候选项修改分析

14.4.4.1 在用证明的候选项

应按照14.4.4.2～14.4.4.3识别出对候选项及其环境的修改。

注 1：候选项的修改是指设计变更和实施变更。要求更改、功能性加强或性能加强可导致设计变更。实施变更不影响候选项的定义或其性能，仅影响其实施特性。软件更正、使用新的开发工具或生产工具可导致实施变更。

注 2：配置数据或标定数据的更改如果影响了候选项的表现并与违背安全目标相关，则认为这些更改是对候选项的修改。

注 3：将候选项用于具有不同安全目标或要求的新型应用、将候选项安装于新的目标环境（如车辆变型、环境条件范围）、与候选项存在相互作用的组件升级或位于候选项附近的组件升级都可导致候选项环境的变更。

14.4.4.2 为未来应用引入的相关项修改

以未来应用为目的而引入的相关项及其环境的修改，应符合GB/T 34590.2-XXXX，6.4.3。

14.4.4.3 为未来应用引入的要素修改

以未来在不同相关项中进行应用为目的而引入的要素及其环境的修改，应符合GB/T 34590.2-XXXX，6.4.4。

14.4.4.4 独立于未来应用的候选项修改

在候选项评估期后引入的、独立于未来应用的候选项修改，应提供在用证明状态仍然有效的证据。

14.4.5 现场数据的分析

14.4.5.1 配置管理和变更管理

应提供候选项在其服务期内及评估期结束后处于配置管理和变更管理管辖下的证据，以便于建立候选项的当前状态。

14.4.5.2 在用证明的目标值

注：如果还没有分配任何 ASIL 等级给候选项，可保守的选取 ASIL D 等级。

14.4.5.2.1 应具备候选项评估期的计算依据。

14.4.5.2.2 候选项的评估期应按照14.4.5.2.3，由所参考全部样本的观察期的累加得出。

14.4.5.2.3 对每个与候选项具有相同定义和实现、并在车辆上运行的样本的观察期，应超过年平均车辆运行时间，才能在候选项评估期的分析中考虑。

14.4.5.2.4 为了使候选项达到在用证明状态，候选项应在评估期内证明对每个可能被候选项违背的安全目标的符合性，符合表6，且具备单侧置信下线为70%（使用卡方分布）。

注 1：为了在用证明的目的，可观察到的事件意味着报告给制造商的失效和由候选项导致的潜在违背安全目标的失效。

表6 可观察到的事故率的限制

ASIL	可观察到的事故率
D	$<10^{-9}$/h
C	$<10^{-8}$/h
B	$<10^{-8}$/h
A	$<10^{-7}$/h

表 6 可观察到的事故率的限制

ASIL	可观察到的事故率
D	$<10^{-9}$/h
C	$<10^{-8}$/h
B	$<10^{-8}$/h
A	$<10^{-7}$/h

注 2：在分析现场安全目标的潜在违背时，解释了可观察到的事件的特征和发生率。

注 3：表 7 给出了无可观察到的事件的最短评估周期的示例，这是达到 70%置信度所必需的。

注 4：如果在样本的采集数据中发现可观察到的事件，必需的最短评估期 $t_{service}$ 可进行如下调整：

$$t_{service} = t_{MTTF} \times \frac{(\chi_{CL;\ 2f+2})^2}{2}$$

式中：

CL ——置信度的绝对值（例如，0.7 对应了 70%）；

t_{MTTF} ——平均失效间隔（1/失效率）；

f ——安全相关事件的数量；

$(X_{\alpha,\gamma})^2$ ——误差概率α和自由度γ的卡方分布。

14.4.5.2.5 在获得在用证明状态（按照14.4.5.2.4）前，可暂时预计所用的在用证明可信度。在这种情况下，对每个可能被候选项违背的安全目标，候选项评估期应证明对其符合性，并应满足表8且具备单边置信下限为70%（使用卡方分布）。

表 8 可观察到的事故率的限制（过渡期）

ASIL	可观察到的事故率
D	$<3 \times 10^{-9}$/h
C	$<3 \times 10^{-8}$/h
B	$<3 \times 10^{-8}$/h
A	$<3 \times 10^{-7}$/h

14.4.5.2.6 在14.4.5.2.5描述的临时期内，对任何现场观察到的事件，应遵循以下方面：

——对可观察到的事件率停止使用表8，而对候选项使用表6，或反之；

——提供证据证明已完全识别出观察到的事件的根本原因并按照GB/T 34590进行了排除，同时，继续对候选项累计小时进行计数，重置该特定根本原因的累计小时计数，并将这条证据记录到安全档案中。

14.4.5.2.7 当候选项的失效率是非恒定值时，在用证明应采用额外的措施，例如因疲劳导致损坏的情况。

注：这些措施适用于其失效率显著依赖于某些因素（诸如与相关项生命周期相关的磨损、老化或运行时间）的候选项。措施可包括专用的耐久测试，或更长的观察期。

14.4.5.3 现场问题

问题报告系统应确保获取并记录了候选项运行期间，现场中任何由候选项引起的、具有潜在安全影响的可观察到的事件（本文件GB/T 34590.2-XXXX，7.4.2.3）。

14.5 工作成果

14.5.1 用于在用证明的候选项描述，由 14.4.3 的要求得出。

14.5.2 在用证明分析报告，由 14.4.4～14.4.5 的要求得出。

15 GB/T 34590 标准适用范围之外应用的接口

15.1 目的

本章适用于 T&B，其目的是确保 GB/T 34590 适用范围之外的应用，不会违背按照 GB/T 34590 开发的基础车辆或相关项的安全目标。

15.2 总则

本章适用于商用车辆的商业模式，该模式下由公司组装或集成的整车不属于 GB/T 34590 范围但适用其他标准。图 5 表明了该应用与按照 GB/T 34590 开发的相关项之间的关系。

图 5 按照 GB/T 34590 开发的相关项在其他标准范围内使用

示例 1： 车身制造商作为集成方，将按照 GB/T 34590 开发的基础车辆与按照机械指令开发的车身设备集成并组装成整车。

示例 2： 一家农业设备制造商将根据 GB/T 34590 开发的制动系统集成到根据农林机械标准开发的农业设备中。

15.3 本章的输入

15.3.1 前提条件

应具备以下信息：

——相关项定义，按照 GB/T 34590.3-XXXX5.5.1

15.3.2 支持信息

无。

15.4 要求和建议

15.4.1 15.4 中的要求应适用于 T&B。

15.4.2 基础车辆制造商、相关项或要素的供应商应向集成方沟通信息，识别可修改的系统和组件以及允许的系统安全限制/修改的要求。

15.4.3 基础车辆制造商或相关项的供应商应针对要求集成方采取的安全措施进行沟通。

注 1：假设集成方具备实现安全措施的必要能力。

示例 1：集成方的能力准则可以是：

——符合其他安全标准；

——适当的安全文化；及

——已建立的质量管理体系。

注 2：基础车辆制造商、相关项或要素的供应商对预期的集成用例及其安全要求做出假设。如有例外情况，集成方应针对安全要求与基础车辆制造商、相关项或要素的供应商进行沟通。

示例 2：在驾驶过程中，车身制造商联系基础车辆制造商请求开启 PTO 功能。车身制造商使用 ISO 13849 开发，双方针对在 ISO 13849 基础上增加的 ASIL 等级达成一致。基础车辆制造商沟通关于 PTO 功能相关的带有 ASIL 等级的安全要求，车身制造商(以商定的性能等级)符合这些要求。基础车辆制造商启用车身制造商所请求的 PTO 功能。

15.5 工作成果

15.5.1 基础车辆制造商或供应商指南，由 15.4.2 和 15.4.3 的要求得出。

16 未按照根据 GB/T 34590 开发的安全相关系统的集成

16.1 目的

本章适用于 T&B，其目的是确保未按照 GB/T 34590 开发的系统或组件满足将其集成到按照 GB/T 34590 开发的相关项中所需的功能安全要求的等级。

16.2 总则

本章适用于遵循 GB/T 34590 的公司集成未按照 GB/T 34590 而是按照其他标准开发的系统或组件的商用车辆的商业模式。图 6 表明了该应用与按照 GB/T 34590 开发的相关项之间的关系。

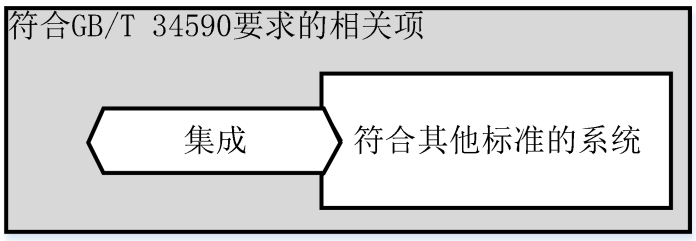


图 6　集成一个按照其他标准开发的系统

注 1：由于额外的安全活动，此商业模式可能要求系统集成方付出更多的投入和开发成本，因此，遵循 GB/T 34590 的开发流程更为推荐。

注 2：商用车商业模式可以是小批量生产。

注 3：另一个标准可以是机械指令，包括 IEC 61508、ISO 13849 和 ISO 25119。

公司特定的流程也可以用于集成。

16.3　本章的输入

16.3.1　前提条件

应具备如下信息：

——相关项定义，按照 GB/T 34590.3-XXXX，5.5.1

注 1：相关项定义与系统集成方的系统或系统组相关，包括未按照 GB/T 34590 开发的系统或组件。

注 2：此类系统或组件的集成方可以是基础车辆制造商。

16.3.2　支持信息

无。

16.4　要求和建议

16.4.1　应将 16.4 中的要求用于 T&B。

16.4.2　在集成方安全档案中应给出依据，以证明本章应用的合理性。

示例：供应商遵循安全标准 ISO 13849。

16.4.3　集成方应定义准则，以论证按照另一安全标准开发的安全相关系统符合所需的功能安全要求的等级。

示例 1：ASIL 等级和 PL 等级（ISO 13849 中使用的性能等级）之间的映射。

注：该准则应涉及设计流程、产品设计、认证措施和审批流程。

示例 2：不同安全标准之间，对于应用方法要求和所需失效率要求的对比。

16.4.4　集成方和供应商应就相关的一系列措施达成一致，以验证是否满足准则。

示例：一系列措施可以是：

——待集成系统规范的可用性；
——通过测试报告证明待集成系统符合其要求的证据；
——通过 FMEA、FTA、既定设计模式/配置的应用，对系统性设计故障进行结构化设计分析；
——待集成系统适合其预期用途的证据；
——基于充分的 PPAP（生产件批准程序）审批流程，对组件进行产品发布的证据；
——通过高加速寿命测试、环境测试、超出规范限制的测试、鲁棒性测试进行的设计验证与设计确认测试；及
——现场数据分析。

16.5　工作成果

16.5.1　安全依据，由 16.4.2~16.4.4 的要求得出。

附录 A

（资料性）

支持过程的概览和文件流

表A.1提供了对支持过程的目的、前提条件和工作成果的概览。

表 A.1　支持过程概览

章	目的	前提条件	工作成果
5 分布式开发的接口	本章的目的： a) 定义客户和供应商在进行开发活动时的交互和依赖； b) 描述相关责任的分配；及 c) 识别相关项及其要素在进行分布式开发时需要交换的工作成果。	本文件安全生命周期相关阶段（该阶段计划且实施了分布式开发）中适用的前提条件。	5 5.5.1 供应商选择报告，由5.4.2.1和5.4.2.2的要求得出； 5.5.2 开发接口协议（DIA），由5.4.3，5.4.5.1和5.4.4.2的要求得出； 5.5.3 供应商安全计划，由5.4.3和5.4.4的要求得出； 5.5.4 功能安全评估报告，由5.4.5.3和5.4.5.4的要求得出； 5.5.5 供应协议，由5.4.6.1~5.4.6.4的要求得出。
6 安全要求的定义和管理	本章的目的： a)确保正确的定义安全要求及其属性和特性；及 b)确保在整个安全生命周期内对安全要求的一致管理。	组织专门的功能安全规章和流程，按照GB/T 34590.2-XXXX,5.5.1。 安全生命周期相关阶段（该阶段定义或管理了安全要求）中适用的前提条件。	无。
7 配置管理	本章的目的： a) 确保工作成果、相关项、要素及其生产的原理和一般条件，在任何时间以可控的方式可被唯一识别和重生成；及 b) 确保可追溯较早版本和当前版本的关系及区别。	安全计划，按照GB/T 34590.2-XXXX的6.5.3； 组织专门的功能安全规章和流程，按照GB/T 34590.2-XXXX的5.5.1；及 安全生命周期相关阶段（该阶段对配置管理进行了计划或管理）中适用的前提条件。	7.5.1 配置管理计划，由7.4.1～7.4.5的要求得出。
8 变更管理	变更管理的目的是在整个安全生命周期中，分析和控制安全相关的工作成果、相关项和要素的变更。	配置管理计划，按照7.5.1； 安全计划，按照GB/T 34590.2-XXXX，6.5.3；及 组织专门的功能安全规章和流程，按照GB/T 34590.2-XXXX，5.5.1。	8.5.1 变更管理计划，由8.4.1的要求得出； 8.5.2 变更需求，由8.4.2的要求得出； 8.5.3 影响分析和变更需求计划，由8.4.3和8.4.4的要求得出； 8.5.4 变更报告，由8.4.5的要求得出。

9 验证	验证的目的是确保工作成果符合它们相应的要求。	组织专门的功能安全规章和流程，按照 GB/T 34590.2-XXXX，5.5.1；及 安全生命周期相关阶段（该阶段计划和执行验证）中适用的前提条件。	9.5.1 验证计划，由 9.4.1.1 和 9.4.1.2 的要求得出； 9.5.2 验证规范，由 9.4.2.1～9.4.2.4 的要求得出； 9.5.3 验证报告，由 9.4.3.1～9.4.3.4 的要求得出。
10 文档管理	目的是开发用于整个安全生命周期的文档管理策略，以促进有效的和可重复的文档管理过程。	组织专门的功能安全规章和流程，按照 GB/T 34590.2-XXXX，5.5.1；及 安全计划，按照 GB/T 34590.2-XXXX，6.5.3。	10.4.3 to 10.4.6. 10.5.1 文档管理计划，由 10.4.1 和 10.4.2 的要求得出； 10.5.2 文档指南要求，由 10.4.3～10.4.6 的要求得出。
11 所使用软件工具的置信度	本章的目的： a）提供准则，以确定在适用时所要求的软件工具置信度水平；及 b）在适用时提供鉴定软件工具的方法，以建立证据证明软件工具适合用于支持 GB/T 34590 要求的活动或任务（即，对那些 GB/T 34590 要求的活动或任务，使用者可依靠软件工具的正确功能）。	安全计划，按照 GB/T 34590.2-XXXX，6.5.3； 组织专门的功能安全规章和流程，按照 GB/T 34590.2-XXXX，5.5.1；及 安全生命周期相关阶段（该阶段使用了软件工具）中适用的前提条件。	11.5.1 软件工具准则评估报告，由 11.4.1～11.4.5 的要求得出； 11.5.2 软件工具鉴定报告，由 11.4.6～11.4.9 的要求得出。
12 软件组件的鉴定	软件组件鉴定的目的是提供证据，以证明在符合 GB/T 34590 开发的相关项中对它们的重复使用是合适的。	组织专门的功能安全规章和流程，按照 GB/T 34590.2-XXXX, 5.5.1； 对软件组件的要求。	12.4.3. 12.5.1 软件组件的文档，由 12.4.2.1 的要求得出。 12.5.2 软件组件鉴定报告，由 12.4.2.2～12.4.2.5 的要求得出。 12.5.3 软件组件鉴定的验证报告，由 12.4.3 的要求得出。
13 硬件要素的评估	本章的目的是确保硬件要素的功能表现足以满足分配的安全要求，因此，由于硬件要素的系统性故障而违背安全目标或安全要求的风险是足够低的。基于随机故障管理的硬件要素的适用性，由被评估硬件要素的集成者在设计集成的下一个更高层面进行确定。基于随机故障管理的硬件要素的适用性，由被评估硬件要素的集成者在设计集成的下一个更高层面进行确定。	组织专门的功能安全规章和流程，按照 GB/T 34590.2-XXXX, 5.5.1； 与所考虑的硬件要素相关的安全要求； 设计验证准则（分析和测试），按照 GB/T 34590.5-XXXX,第 6 章；及 生产商的硬件要素规范，如果没有，或硬件要素规范的假设。	13.5.1 硬件要素评估计划，由 13.4.3.2 的要求得出。 13.5.2 硬件要素测试计划，由 13.4.3.5.1 的要求得出。 13.5.3 硬件要素的评估报告，由 13.4.1.1,13.4.3.6 和 13.4.4.3 的要求得出（如果适用）。

	本章中用到的“硬件要素”术语指的是商业现成（COTS）硬件组件或元器件，或指定制的硬件组件或元器件，即:最初不是按照GB/T 34590开发或设计的，被集成到符合GB/T 34590的相关项或要素中时，被认为是与安全相关的。 更准确地说，硬件要素的评估是符合GB/T 34590.5的可选的方法。符合评估条件的硬件要素可以是特定于应用的要素或是标准要素。这些要素通常被开发用于多个行业，包括汽车应用或非汽车应用。		
14 在用证明	本章的目的是提供对在用证明的指导。当现场数据可用时，对已有相关项或要素的复用，可以使用在用证明，作为符合GB/T 34590的替代方法。	关于候选项的预期使用： ——候选项定义； ——适用的安全目标或安全要求及相应的ASIL等级； ——可预见的运行场景和预期的运行模式及接口。 关于候选项之前的使用： ——来自服务期的现场数据。	14.5.1 用于在用证明的候选项描述,由14.4.3的要求得出。 14.5.2 在用证明分析报告，由14.4.4～14.4.5的要求得出。
15 GB/T 34590标准范围之外应用的接口	本章适用于T&B，其目的是确保GB/T 34590适用范围之外的应用，不会违背按照GB/T 34590开发的基础车辆或相关项的安全目标。	相关项定义，按照GB/T 34590.3-XXXX，5.5.1。	15.5.1 基础车辆制造商或供应商指南，由15.4.2和15.4.3的要求得出。
16 未按照GB/T 34590开发的安全相关系统的集成。	本章适用于T&B，其目的是确保未按照GB/T 34590开发的系统或组件满足将其集成到按照GB/T 34590开发的相关项中所需的功能安全要求的等级。	相关项定义，按照GB/T 34590.3-XXXX，5.5.1。	16.5.1 安全依据，由16.4.2～16.4.4的要求得出。

附录 B

（资料性）

开发接口协议(DIA)示例

B.1 目的

本附录按照第5章的要求（特别是5.4.3.1 c）到k）的要求），提供了开发接口协议的一个说明性示例，并提供了符合GB/T 34590.2-XXXX，5.4.6和5.5.1中要求和建议的组织专门的调整（如有），还可应用按照GB/T 34590.2-XXXX，6.4.5的项目专门的剪裁。

B.2 总则

许多因素会影响客户与供应商交互的类型和数量，本示例是一个被简化的、基于表B.3中所描述的应用场景和表B.4中所列的一系列前提的例子。

表B.1至B.3构成一个如下的DIA例子：

——表B.1大致对应5.4.2的要求，增加了某些组织专门的内容，以避免或消除供应商能力不足带来的风险。

——表B.2大致对应5.4.3的要求，增加了某些组织专门的内容，以避免或消除由于对组件C的边界及其与环境相互作用的错误理解或错误定义带来的风险。

——表B.3大致对应5.4.4的要求，应用于硬件组件C。

注：在每个表中，相应的 GB/T 34590-XXXX 章在括号内表示。

B.3 应用场景

表B.1至B.3所示的DIA示例基于下述应用场景：

a) 客户负责车辆的工程和制造。

b) 客户负责系统工程开发，该系统由多个硬件和软件组件构成，其中某个硬件组件 C 由供应商提供。

c) 组件 C 被分配了具有 ASIL D 等级的要求。

d) 组件 C 之前未被开发过，即：它还不是一个商业现成产品（COTS）。它所涉及的新技术没有充足的可靠的供应商供选择。

e) 多个供应商对供应组件 C 感兴趣，但其足以支持项目的能力并不明显。

f) 使用基于模型开发的流程。

B.4 前提

本示例的开发基于下述前提：

a) 项目管理和工程开发需要的资源得到充分满足。

b) 每个参与的组织都有被评定为“独立的”评估团队，并用在需要的地方。

c) 全部参与组织都使用相同的流程和架构性框架，并经过独立评估以评定其达到最高完整性等级。

——可复用的资产符合流程和架构性框架，并经过独立评估以评定其达到所需的完整性等级。

——其他资源，例如工具，符合流程和架构性框架，并经过独立评估以评定其达到所需的完整性等级。

——参与的组织选择特定的、可兼容的流程和工具，并致力于相同的架构。

——明确的元模型或规范，对工具的语义、建模语言、编程语言以及生产模型进行明确的定义。

——外部可见的行为模型、性能（含最坏情况）模型、失效模式及后果模型对硬件组件（包括

输入/输出设备）是可用的。 这些模型处于一种可被正确集成以创建（子）系统模型的形式。

d) 还有其他高质量执行的客户-供应商交互方式，并不限于高完整性的工程，也未包含在本示例中，例如：商务流程的交互、项目管理的交互和质量管理的交互。

假如不支持上述前提，将需要额外的客户-供应商互动及工作，本示例并未包含。

表 B.1 用于供应商资质评审和选择的客户与供应商的数据交互

ID	活动	由客户提供给供应商的数据	由供应商提供给客户的数据
A.1	供应商资质预审[a]； 项目独立的准则； 提供给 5.4.2。	能力评估调查问卷： ——安全文化（GB/T 34590.2-XXXX，5.4.2）； ——能力的证据（GB/T 34590.2-XXXX，5.4.4）； ——质量管理的证据（GB/T 34590.2-XXXX，5.4.5）； ——GB/T 34590-XXXX。 准许条件，例如： ——独立评估（5.4.5）； ——DIA 模板。	—
A.2		—	条件的接受[a]。
A.3		—	能力评估[a] （GB/T 34590.2-XXXX 第 5 章）； 披露[a]； 建议的整改措施[a]。
A.4		评估：未经鉴定的 ASIL 等级[a]。	—
A.5	评定供应商（通过预审的）[a]。	客户组织专门的对 GB/T 34590.2-XXXX，5.4.6 的流程调整，包括方法、语言、工具及使用限制/指导书。	—
		—	第一方符合性评估； 披露[a] 记录（5.4.2.1）； 建议的整改措施[a]； 为达到目标的替代方法或建议[a]。
		迭代评估与查找不足，以及替代方案[a]。	计划和替代方案的迭代修正[a]。
		评估：未经鉴定的 ASIL 等级[a]。	—
A.6	5.4.2.2 请求建议	RFP/RFQ，包括项目特定的流程剪裁（5.4.3.1 b)），产品概念，即相关项定义（GB/T 34590.3-XXXX，5.5.1）和安全目标（GB/T 34590.3-XXXX，6.5.1）。	—
A.7	—	—	报价；

			符合性声明； 之前递交信息的更新[a]。
A.8	5.4.2 选择供应商	建议的 DIA（项目特定的）5.4.3。	—
A.9		—	选定的项目资源及其能力评估，例如：安全团队成员的技能、能力和资质（GB/T 34590.2-XXXX，5.5.2）； 组织专门的规章和流程（GB/T 34590.2-XXXX，5.5.1），包括工具、库； 初步计划，例如：安全计划（GB/T 34590.2-XXXX，6.5.3）。
A.10		迭代评估和询问，例如关于技能的差距[a]。	迭代修改，解决客户的关注点[a]
A.11		DIA 的接受： （5.5.2）； 选择报告（5.5.1）。	DIA 的接受 （5.5.2）。
A.12		概念（GB/T 34590.3-XXXX；GB/T 34590.4-XXXX）和计划阶段（GB/T 34590.2-XXXX）的合同，包括开发工作的声明。	接受。
[a] 活动或数据为组织专门的，GB/T 34590 未作要求。			

表 B.2 在项目启动和系统概念阶段客户与供应商的数据交互

ID	活动	客户提供给供应商的数据	供应商提供给客户的数据
B.1	启动项目（5.4.3）； 创建功能安全概念（GB/T 34590.3-XXXX，第 5 至 7 章）。	系统层面的计划； 相关项定义(GB/T 34590.3-XXXX，5.5.1)及其生命周期(图 1、GB/T 34590.2-XXXX，5.2.2；GB/T 34590.2-XXXX，图 2 和 GB/T 34590.2-XXXX，6.4.5）； 功能安全概念（GB/T 34590.3-XXXX，第 7 章）。	—
B.2	—	—	安全计划（5.5.3）； HARA（5.4.3.2）； 硬件组件的行为模型，包括故障度量[5.4.3.1 f)、GB/T 34590.5-XXXX，附录 B 和 GB/T 34590.5-XXXX，第 9 章]； 计划的独立评估，包括：保证流程和资源（含技能集合）的配置与分配，以匹配所需完成的工作成果[5.4.3.1 c) e)，g)，j)，5.4.5]。
B.3	—	接受	—
B.4	对已用于类似项目的组件、工具、库的在用证明经验的考量，以及	初步的安全计划（GB/T 34590.2-XXXX，第 5 章），包括	—

	可能的候选项的在用证明数据和分析（第 14 章）。	系统安全档案结构。	
B.5	—	—	具有在用证明的要素（第 14 章），包含项目合适性的独立评估（5.4.5）。
B.6	—	接受。	—
B.7	系统开发生命周期[5.4.3.1.c)]。	技术安全概念（GB/T 34590.4-XXXX，6.5.2）、系统设计规范的相关部分、硬件规范、设计和实施（D&I）约束、软硬件接口（HSI）规范（GB/T 34590.4-XXXX，6.5.4）。	迭代的评估，问题澄清及关于冲突、完整性、一致性等反馈；技术的局限性（若有）；变更需求（若有）（5.4.4）。 更新的行为模型，包括故障模型。
B.8		迭代的澄清、响应和修正，包括更新与组件 C、HSI、分配等相关的系统架构设计和验证规范（GB/T 34590.4-XXXX，6.5.3，GB/T 34590.4-XXXX，6.5.6）、硬件规范（GB/T 34590.5-XXXX，7.5.1）。	关于组件 C 与其环境边界的反馈。
B.9	—	—	接受。

表 B.3 在硬件开发生命周期中客户与供应商的数据交互

ID	活动	客户提供给供应商的数据	供应商提供给客户的数据
C.1	计划 (5.4.3)	硬件开发的授权	—
C.2		—	计划：安全计划（5.5.3 和 GB/T 34590.5-XXXX，6.5.3），DIA 的计划（5.4.3）等。 计划符合性的独立评审（5.4.5）。
C.3		接受。授权开始要求定义。	—
C.4	要求 (5.4.5 和 GB/T 34590.5)。	—	得出和细化硬件规范；D&I 限制（GB/T 34590.5-XXXX，6.5.1）； 验证计划的延伸 a； 软硬件接口的变更请求，如果有（GB/T 34590.5-XXXX，6.5.2）； 独立的安全审核（5.4.3.1）； 独立的认可（5.4.5 和 5.5.4）。
C.5	—	接受。授权开始设计。	—
C.6	设计 (5.4.5 和 GB/T 34590.5-XXXX)	—	设计规范（GB/T 34590.5-XXXX，7.5.1）；实施限制，包括架构的限制（GB/T 34590.5-XXXX 第 8 章）。 HARA 的扩展或修改（GB/T 34590-XXXX 第 6 章），如果有。 相关项集成和测试计划的扩展（GB/T 34590.5-XXXX，10.5）。 软硬件接口的变更请求，如果有（GB/T

			34590.5-XXXX，6.5.2）。 独立的安全审核（5.4.3.1，5.5.4）。
C.7	5.4.4 和 5.4.5	对系统层面发现的冲突进行迭代评估和反馈。	针对客户反馈和询问的迭代澄清、修改及其他响应。 独立的评估（5.4.5 和 5.5.4）。
C.8	5.4.4 和 5.4.5	组件设计的接受。 授权开始实施。	实施。 来自环境的要求。 独立的评估（5.4.5 和 5.5.4）。
C.9	—	接受	—
C.10	—	—	原型件； 集成验证（GB/T 34590.5-XXXX，10.5）； 独立的评估（5.4.5）。
C.11	—	集成的评估（GB/T 34590.4-XXXX 第 7 章）。 变更要求（若有）。	—
C.12	—	—	对处理过的变更进行的评审和审核。 独立的评估（5.4.5 和 5.5.4）。
C.13	—	接受	—
C.14	—	—	批量生产的样品。 独立的评估（5.4.5 和 5.5.4）。
C.15	—	集成的评价（GB/T 34590.4-XXXX 第 7 章）； 变更要求（若有）。	—
C.16	—	—	对处理过的变更进行的评审和审核； 独立的评估（5.4.4、5.4.5 和 5.5.4）。
C.17	—	授权开始生产阶段。	—
C.18	—	—	量产后的报告（5.4.6、5.5.5 和 GB/T 34590.2-XXXX，7.5.1）。
[a] 活动或数据为组织专门的，GB/T 34590-XXXX 未作要求。			

参 考 文 献

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

[2] ISO 26262-12:2018, Road vehicles — Functional safety — Part 12: Adaptation of ISO 26262 for motorcycles.

[3] GB/T 19001-2016 质量管理体系-要求.

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

[5] GB/T 28046-2011（所有部分）道路车辆 电气及电子设备的环境条件和试验.

[6] IATF 16949, Quality management system requirements for automotive production and relevant service parts organizations.

[7] ISO 25119 (all parts), Tractors and machinery for agriculture and forestry — Safety-related parts of control systems.

[8] ISO/IEC/IEEE 29148, Systems and software engineering — Life cycle processes — Requirements engineering.

[9] GB/T 16855-2015（所有部分） 机械安全-控制系统安全相关部件.

[10] GB/T 20438—2017(所有部分) 电气/电子/可编程电子安全相关系统的功能安全 .

[11] RTCA DO-178C, Software Considerations in Airborne Systems and Equipment Certification.

[12] CMMI for Development, CMMI-DEV, Carnegie Mellon University Software Engineering Institute.

[13] German V-Model - Available at: http: //www.v-modell-xt.de/[viewed 2018-09-27].

[14] AEC Q100. Failure Mechanism Based Stress Test Qualification For Integrated Circuits.

[15] AEC Q101. Failure Mechanism Based Stress Test Qualification For Discrete Semiconductors.

[16] AEC Q200. Stress Test Qualification For Passive Components.

[17] Automotive SPICE® - Available at: http: //www.automotivespice.com [viewed 2018-09-27].

[18] ISO 10007, Quality management — Guidelines for configuration management.

[19] ISO/IEC/IEEE 12207, Systems and software engineering — Software life cycle processes.

[20] ISO/IEC 33000 (series), Information Technology — Process Assessment.