ICS

T

中华人民共和国国家标准

GB/T XXXXX—XXXX

道路车辆 功能安全

第8部分：支持过程

Road vehicles — Functional safety — Part 8: Supporting processes

（征求意见稿）

2016.01.15

YYYY－YY－YY 发布　　YYYY－YY－YY 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

前　言

GB/T XXXXX《道路车辆 功能安全》包括十个部分：

——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 XXXXX的第8部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分修改采用国际标准ISO 26262-8：2011 《道路车辆 功能安全 第8部分：支持过程》（英文版）。

本部分的附录A、B为资料性附录

本部分由国家标准化管理委员会提出。

本部分由全国汽车标准化技术委员会（SAC/TC114）归口。

本部分起草单位：

本部分主要起草人：

引　言

ISO 26262 是以 IEC61508 为基础，为满足道路车辆上特定电子电气系统的需求而编写。

ISO 26262 适用于道路车辆上特定的由电子、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、软件内容和机电一体化应用不断增加，来自系统性失效和硬件随机失效的风险逐渐增加。ISO 26262 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 ISO 26262 针对的是电子电气系统的功能安全，但是它也提供了一个基于其它技术的与安全相关系统的框架。ISO 26262：

a) 提供了一个汽车安全生命周期(管理、开发、生产、运行、维护、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；

c) 应用汽车安全完整性等级规定 ISO 26262 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、维护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和工作成果相互关联。ISO 26262 涉及与安全相关的开发活动和工作成果。

图1为ISO 26262的整体架构。ISO 26262基于V模型为产品开发不同阶段提供过程参考：

— 阴影"V"表示标准中第 3、4、5、6 和 7 部分之间的关系；

— 以“m-n”方式表示的具体条款中，“m”代表特定部分的编号，“n”代表该部分章条的编号。

示例：“2-6”代表 GB/TXXXX-2 的第六章

图1 GB/T XXXXX概览

道路车辆 功能安全

第8部分：支持过程

1 范围

GB/T XXXXX适用于安装在最大总质量不超过3.5吨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的系统。

GB/T XXXXX不适用于安装在特殊用途车辆上的特定的电子电气系统，例如为残疾驾驶者设计的车辆。

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不适用于本标准。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、制动系统、自适应巡航系统）有专用的功能性能标准。

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，

— 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。

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，仅所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 XXXXX-1:201X，道路车辆 功能安全 第1部分：术语；

GB/T XXXXX-2:201X，道路车辆 功能安全 第2部分：功能安全管理；

GB/T XXXXX-3:201X，道路车辆 功能安全 第3部分：概念阶段；

GB/T XXXXX-4:201X，道路车辆 功能安全 第4部分：产品开发：系统层面；

GB/T XXXXX-5:201X，道路车辆 功能安全 第5部分：产品开发：硬件层面；

GB/T XXXXX-6:201X，道路车辆 功能安全 第6部分：产品开发：软件层面；

GB/T XXXXX-7:201X，道路车辆 功能安全 第7部分：生产和运行；

GB/T XXXXX-9:201X，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/IEC 12207, 系统和软件工程 软件生命周期过程

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部分。

4 要求

4.1 一般要求

如声明满足GB/T XXXXX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 的要求，已经计划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可接受的，并且按照 GB/T XXXXX-2 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。

安全活动的结果以工作成果的形式给出。“前提条件”是那些作为前一阶段的工作成果而应在本阶段提供的信息。如果条款的某些要求是依照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，但在某些案例中，GB/T XXXXX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 对表格的诠释

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（在最左侧栏以顺序号标明，如 1,2,3），或

b) 一个选择的条目（在最左侧栏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。如果应用所列出方法以外的其它方法，应给出满足相关要求的理由。

对于选择性的条目，按照ASIL等级指示的要求，应采用适当的方法组合，不依赖于组合的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，则应采用具有更高推荐等级的方法。应给出组合方法满足相关要求的理由。

注：在表中所列出的方法的理由是充分的。但是，这并不表示着有偏袒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，未推荐或反对该方法。

4.3 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，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 XXXXX中ASIL等级在括号中给出，则对于该ASIL等级，相应的子章节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 分布式开发的接口

5.1 目的

本章目的是描述相关项和要素进行分布式开发的流程及相关责任的分配。

5.2 总则

相关项开发的客户（如：车辆制造者）和供应商共同遵守 GB/T XXXXX 中定义的要求。客户和供应商就责任达成一致。分包的关系是被允许的。类似于客户对内部相关项开发的计划、执行和文档的安全相关定义，在与分布式相关项开发供应商或负责相关项开发全部安全责任的供应商合作中，类似的流程需要得到同意。

注：本章不适用于采购的标准组件及元器件、或未对供应商分配任何安全责任的开发委托。

5.3 本章的输入

5.3.1 前提条件

参见计划和开展了分布式开发的安全生命周期相关阶段的适用前提条件。

5.3.2 支持信息

可考虑如下信息：

— 开发接口协议（DIA）的草拟版本（来自外部）；

— 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 应将第 5 章的要求用于每个按照 GB/T XXXXX 开发的相关项和要素，但适用下述之一的商业现成硬件元器件除外：

a) 无特定硬件安全要求分配给硬件元器件，或

b) 按照基于全球质量标准（如：电子组件的 AEC 标准）的公认流程，鉴定商业现成硬件元器件，且对商业现成硬件元器件的鉴定涵盖了预期应用的参数范围。

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按照 GB/T XXXXX 开发和生产同等复杂度和 ASIL 等级的相关项及要素能力的评估。

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 XXXXX-2，6.4.9 进行的安全评估结果；

— 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 XXXXX的正式要求，

b) 相关项定义或要素的功能定义，及

c) 基于供应商报价对象的安全目标、功能安全要求或技术安全要求（如果已存在，需包含其相应ASIL等级）。

注：如果在选择供应商时 ASIL 等级未知，则做保守的假设。

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：

注：附录 B 给出了开发接口协议的示例。

a) 客户和供应商安全经理的任命，

b) 按照GB/T XXXXX，6.4.5进行安全生命周期的联合剪裁，

c) 客户需开展的活动及流程和供应商需开展的活动及流程，

d) 需交换的信息和工作成果，

注 1：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 2：交换的信息包括安全相关的特殊特性。

注 3：在分布式开发的情况下，对所涉及开发方的活动所必须的工作成果的相关部分，可进行识别和交换。

e) 活动的责任方或责任人，

f) 目标值的沟通。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能满足单点故障度量及潜伏故障度量的目标值（通过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，参见GB/T XXXXX-5），及

g) 支持过程和工具，含接口，以确保客户和供应商间的兼容性。

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作验证。

5.4.3.3 相关项开发的责任方应按照 GB/T XXXXX-3 制定功能安全概念。客户和供应商应就功能安全要求达成一致。

5.4.4 分布式开发的执行

5.4.4.1 供应商应向客户报告每个可能增加不符合项目计划、安全计划、集成和测试计划（按照 GB/T XXXXX-4）、软件验证计划（按照 GB/T XXXXX-6）或开发接口协议中其它条款的风险的问题。

5.4.4.2 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（如有）的开发活动中发生的每个异常。

5.4.4.3 供应商应确定每个安全要求是否能得到满足。如果不能，应重新检查安全概念，同时如果必要，应修改安全概念以产生安全要求。

5.4.4.4 对相关项安全产生潜在影响的每个变更，或对证明满足 GB/T XXXXX 的计划活动产生潜在影响的每个变更，都应与支持影响分析（按照第 8 章）的另一方进行沟通。

5.4.4.5 在导出用于当前开发的安全要求时，按照 GB/T XXXXX-2，5.4.2.7，双方都宜考虑从之前相似开发中获得的经验。

5.4.4.6 供应商应向客户的安全经理报告安全计划中制定的任务和重要阶段上取得的进展。供应商和客户应就报告的形式和提交的日期达成一致。

示例：在周期性间隔或在日程框架中定义的重要阶段时，客户对供应商编制发布的质量管理报告进行检查。

5.4.4.7 应就由哪一方（供应商或客户）按照 GB/T XXXXX-4 执行安全确认达成一致。

注：如果由供应商执行集成和确认，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（参见 GB/T XXXXX-4）。

5.4.4.8 按照 4.3，此要求适用于 ASIL D 等级。客户应被允许在任何恰当的时间、在供应商场所内开展额外的功能安全审核。

5.4.5 在供应商场所的功能安全评估

5.4.5.1 按照 4.3，此要求适用于 ASIL (B)、C、D 等级。当接近已定义的重要阶段时，应执行一次或多次功能安全评估，这些评估应包含相关项开发的每个阶段。应在合适的详细程度(对相关项的复杂性及其安全目标的 ASIL 等级)开展功能安全评估，并按照 GB/T XXXXX-2，6.4.9 执行功能安全评估。

5.4.5.2 按照 4.3，此要求适用于 ASIL B 等级。应开展功能安全评估。

注：这可由客户、其它组织或供应商自己完成。

5.4.5.3 按照 4.3，此要求适用于 ASIL C 和 D 等级。应由客户、其授权的组织或人员在供应商场所开展符合 GB/T XXXXX-2，6.4.9 的功能安全评估。

注：这可由供应商自己完成。

5.4.5.4 按照 4.3，此要求适用于 ASIL (B)、C 和 D 等级。客户和供应商应有功能安全评估报告。

5.4.5.5 按照 4.3，此要求适用于 ASIL (B)、C 和 D 等级。对识别出的每个潜在影响供应商交付物的异常，应进行分析并应得出解决它们的行动。双方应就由谁执行所要求的行动达成一致。

5.4.6 生产发布后

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 XXXXX-2 第 7 章和 GB/T XXXXX-7 第 5 章所要求的过程能力。

5.4.6.2 客户和供应商间的供应协议应依据 GB/T XXXXX-2，7.4.2.1 明确功能安全责任，并应定义各方的安全活动。

5.4.6.3 供应协议应规定描述、声明、阐明各方间关于安全相关特殊特性的生产监控记录的访问和交换。

5.4.6.4 发现安全相关事件的各方应及时依照供应协议报告此事件。如果发生了安全相关事件，应对事件开展分析。该分析应包括类似相关项和受类似事件潜在影响的相关方。

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 的要求得出。

5.5.3 供应商项目计划，由 5.4.3 的要求得出。

5.5.4 供应商安全计划，由 5.4.3 的要求得出。

5.5.5 功能安全评估报告，由 5.4.5.1 至 5.4.5.5 的要求得出。

5.5.6 供应协议，由 5.4.6.2 至 5.4.6.3 的要求得出。

6 安全要求的定义和管理

6.1 目的

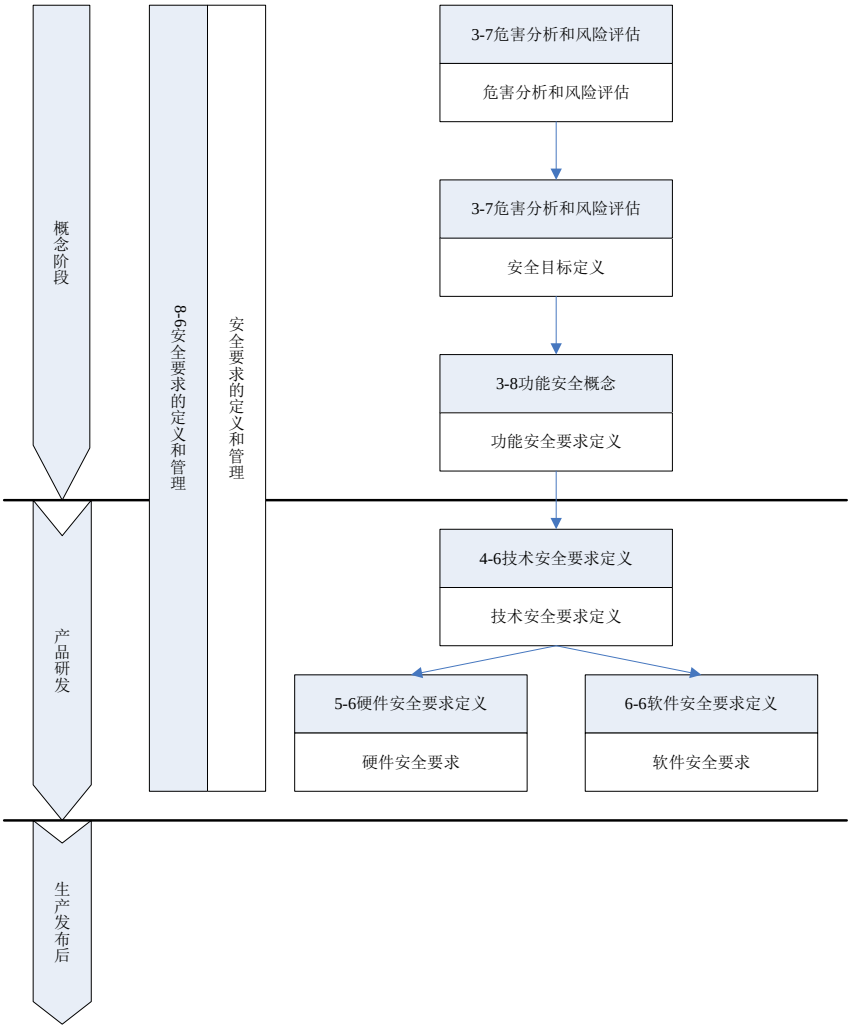
第一个目的是确保正确的定义安全要求及其属性和特性。

第二个目的是确保在整个安全生命周期内一致的管理安全要求。

6.2 总则

安全要求包含旨在达到并确保所要求的 ASIL 等级的全部要求。

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 XXXXX 中用到的安全要求的结构和相依性。安全要求被分配给要素或在要素间分布。



注：图中 GB/T XXXXX 每部分的特定章节用以下方式标示：“m-n”，“m”代表部分号，“n”代表章节号，例如“3-7”代表 GB/T XXXXX-3 的第 7 章。

图 2-安全要求的结构

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

为了支持对安全要求的管理，推荐使用合适的要求管理工具。

此章节包括对安全要求进行定义和管理的要求（参见图 3）。

GB/T XXXXX-3、GB/T XXXXX-4、GB/T XXXXX-5 和 GB/T XXXXX-6 列出了有关安全要求内容在不同层面的特定要求。

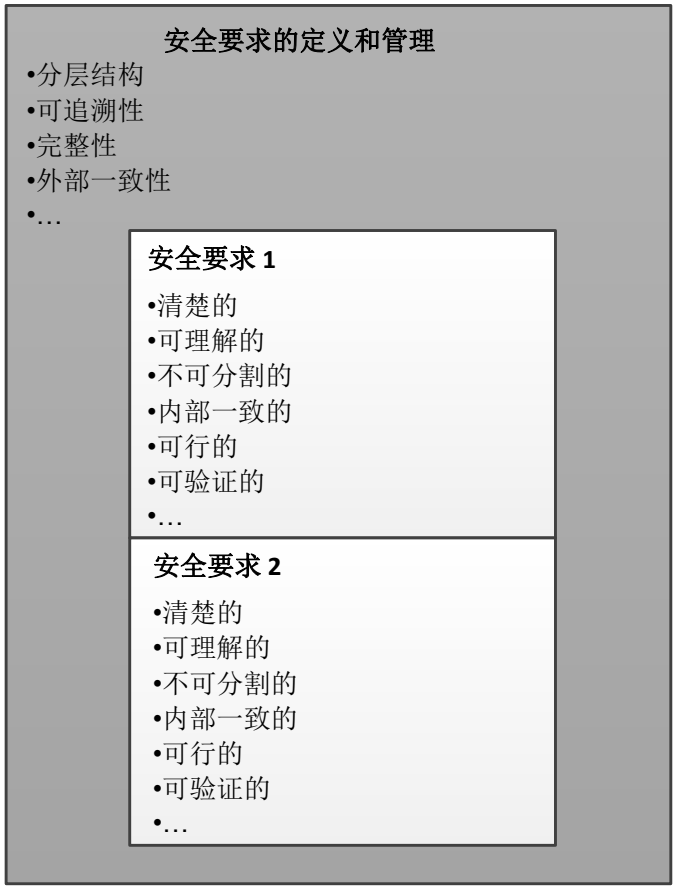


图 3-安全要求管理和特定安全要求间的关系

6.3 本章的输入

6.3.1 前提条件

参见定义或管理安全要求的安全生命周期相关阶段的适用前提条件。

6.3.2 支持信息

参见定义或管理安全要求的安全生命周期相关阶段的适用支持信息。

6.4 要求和建议

6.4.1 安全要求的定义

6.4.1.1 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所列方法。

注：对较高层面的安全要求（如：功能和技术安全要求），自然语言更合适；而对于较低层面的安全要求（如：软件和硬件安全要求），表 1 所列比标记法更合适。

表 1 定义安全要求

方法		ASIL			
		A	B	C	D
1a	用于要求定义的非正式标记法	++	++	+	+
1b	用于要求定义的半正式标记法	+	+	++	++
1c	用于要求定义的正式标记法	+	+	+	+

6.4.2 安全要求的属性和特性

6.4.2.1 安全要求应能被无歧义的识别为安全要求。

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它要求，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，除非运用了按照 GB/T XXXXX-9 的 ASIL 分解。

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（参见 GB/T XXXXX-1，定义 1.108）。

6.4.2.3 应将安全要求分配给相关项或要素。

6.4.2.4 安全要求应具有如下特性：

a) 无歧义并可理解的，

注 1：如果对要求的意思存在共通的理解，那么要求是无歧义的。

注 2：如果相邻抽象层面的读者（即：要求的利益相关者或要求的使用者）理解要求的意思，那么要求是可理解的。

b) 不可分割的，

注：当一个层面的安全要求在所考虑的层面上不能被分解为一个以上的安全要求，那么这些要求是不可分割的。

c) 内部一致的，

注：不同于外部一致性（多个安全要求不互相抵触），内部一致性表示每个单独的安全要求不包含自相矛盾的内容。

d) 可行的，及

注：如果在相关项的开发限制（资源、使用最先进技术等）内，要求可被实施，则它是可行的。

e) 可验证的。

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：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：安全要求的状态可以是“建议的”、“假设的”、“接受的”或“经评审的”。

c) ASIL等级。

6.4.3 安全要求的管理

6.4.3.1 安全要求集应具有如下特性：

a) 分层结构

注：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。这些层面与相应的设计阶段始终保持一致。

b) 依据恰当编组原则建立的有组织的结构，

注：安全要求的组织，表示通常依据架构将每个层面的要求组合在一起。

c) 完整性，

注：完整性表示一个层面的安全要求完整的实施了前一层面的全部安全要求。

d) 外部一致性，

注：不同于内部一致性（每个单独的安全要求不包含自相矛盾的内容），外部一致性表示多个安全要求不互相抵触。

e) 分层结构中任意一层的信息不重复，及

注：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它安全要求中，并且在每个分层层面都得以实现。

f) 可维护性。

注：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。

6.4.3.2 安全要求应是可追溯的（通过参照以下）：

a) 安全要求在更高分层层面的每个来源，

b) 导出到更低分层层面的每个安全要求，或各安全要求在设计中实现，及

c) 按照9.4.2，验证的定义。

注：此外，可追溯性支持了：

— 当对特定安全要求进行更改时的影响分析，及

— 功能安全评估。

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 XXXXX 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			
		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	o	+	+	+
[a] 可执行模型可以支持方法 1c					

6.4.3.4 安全要求应置于配置管理（按照第 7 章）下。

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

第一个目的是确保工作成果及其产生的原理和一般条件，在任何时间以可控的方式可被唯一识别和重生成。

第二个目的是确保可追溯较早版本和当前版本的关系及区别。

7.2 总则

配置管理是汽车工业中的成熟实践，可依据 ISO/TS 16949、ISO 10007 和 ISO/IEC 12207 进行应用。

配置管理对 GB/T XXXXX 的每个工作成果进行管理。

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 XXXXX-2，6.5.1。

— 在配置管理计划和管理的安全生命周期的相关阶段中适用的前提条件。

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。

7.4.2 配置管理过程应符合：

a) 质量管理系统（如ISO/TS 16949或ISO 9001）的相关要求，及

b) 依照ISO/IEC 12207中配置管理章节的软件开发特定要求。

7.4.3 按照 GB/T XXXXX-2 安全计划要求的工作成果，应置于配置管理下，并应依照配置管理策略生成基线。

7.4.4 在配置管理计划中，应对置于配置管理下的工作成果进行文档化。

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

7.5.1.1 配置管理计划，由 7.4.1、7.4.2 和 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，同时确保工作产品的一致性。在进行变更前，评估对功能安全的潜在影响。为此，引入并建立变更决策流程，并将责任分配给相关方。

注：此处，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。

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 XXXXX-2，6.5.2。

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 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同时启动，定义并维护两个流程间的接口，以确保对变更的可追溯性。

8.4.1.2 识别出需符合变更管理的工作成果，并应包括 GB/T XXXXX 要求的、需在配置管理下的那些工作成果。

8.4.1.3 应为每个工作成果定义应用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) 变更需求的决策和理由，按照8.4.4，

d) 已接受的变更的实施，按照8.4.5，及

e) 文档，按照8.4.5。

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 最低程度上，每个变更需求应包含以下信息：

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，应对所涉及的相关项、接口及关联相关项进行影响分析。应针对以下：

a) 变更需求的类型，

注：变更的可能类型有：解决错误、调整、加强、预防。

b) 对需更改的工作成果和受影响的工作成果进行的识别，

c) 在分布式开发的情况下，对受影响方的识别和引入，

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 对工作成果的每个变更，应返回到安全生命周期的恰当阶段，后续阶段的开展应符合 GB/T XXXXX。

8.4.4 变更需求的评估

8.4.4.1 应使用依照 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涉及到的接口。

8.4.5 变更的开展和记录

8.4.5.1 应按计划开展和验证变更。

8.4.5.2 如果变更影响了安全相关功能，那么应在发布相关项前，对按照 GB/T XXXXX-2，6.4.7 和 6.4.9 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) 适度水平的变更工作成果清单，包括：配置和版本，按照第7章（配置管理），

b) 开展的变更细节，及

c) 变更部署的计划日期。

注：对被拒绝的变更需求，变更需求和拒绝的理由也需被记录。

8.5 工作成果

8.5.1 变更管理计划，由 8.4.1.1 至 8.4.1.3 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 8.4.3.1、8.4.4.1 和 8.4.4.2 的要求得出。

8.5.4 变更报告，由 8.4.5.3 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的阶段：

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：

1) 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 XXXXX-4 第 7 章（系统设计）、GB/T XXXXX-5 第 7 章（硬件设计）、GB/T XXXXX-6 第 7 章（软件架构设计）和 GB/T XXXXX-6 第 8 章（软件单元设计和实现）。

2) 在测试阶段，验证是在测试环境下对工作成果的评估，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：

1) 安全要求在生产流程、用户手册、维修和维护指导中得到了恰当发布；及

2) 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：这是一般性验证流程，GB/T XXXXX-3、GB/T XXXXX-4、GB/T XXXXX-5、GB/T XXXXX-6和GB/T XXXXX-7中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。参见GB/T XXXXX-4第9章（安全确认），以获取更多细节。

9.3 本章的输入

9.3.1 前提条件

参见计划和执行验证的安全生命周期的相关阶段中适用的前提条件。

9.3.2 支持信息

参见计划和执行验证的安全生命周期的相关阶段中适用的支持信息。

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) 用于验证的方法，

注：验证方法包括：评审、走查、检查、模型检查、模拟、工程分析、证明和测试。典型的，验证会使用这些方法和其它方法的组合。

c) 验证的通过和不通过准则，

d) 验证环境（如果适用），

注：验证环境可以是测试或模拟环境。

e) 用于验证的工具（如果适用），

f) 当探测出异常时需采取的行动，及

g) 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，并可包含其它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选择和定义，并应包含：

a) 评审或分析的检查清单；或

b) 模拟场景；或

c) 测试案例、测试数据和测试目标。

9.4.2.2 对于测试，每个测试案例的定义应包含：

a) 唯一的识别码，

b) 需验证的相关工作成果的参考版本，

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) 环境条件（如果适用），

注：环境条件关乎执行测试的周围物理属性（例如：温度）或作为测试的一部分进行模拟的物理属性。

e) 输入数据及其时序、量值，及

f) 期望的表现，包括：输出数据、输出量值的可接受范围、时间表现和公差表现。

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案例用到的前提条件、配置及环境条件，推荐使用这些数据的无歧义参考。

9.4.2.3 对于测试，应按使用的测试方法对测试案例进行分组。对每种测试方法，作为测试案例的补充，应定义以下内容：

a) 测试环境，

b) 逻辑和时间的依赖性，及

c) 资源。

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 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) 评估中用到的验证环境配置、验证工具及标定数据（如果适用），

d) 验证结果与期望结果的一致性水平，

e) 验证是否通过或不通过的无歧义陈述，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[参见 9.4.1.1 c)]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。

9.5 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 至 9.4.2.3 的要求得出。

9.5.3 验证报告，由 9.4.3.1 和 9.4.3.2 的要求得出。

10 文档

10.1 目的

主要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

GB/T XXXXX 中对文档的要求主要关注其内容，而非版面编排和外观。

除非 GB/T XXXXX 有明确的定义，否则信息不需要呈现在物理文档中。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。

应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：

— 安全计划，按照GB/T XXXXX-2，6.5.1。

10.3.2 支持信息

无。

10.4 要求和建议

10.4.1 应计划文档制定和管理过程，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) 作为功能安全评估的输入。

10.4.2 应将对 GB/T XXXXX 中工作成果的识别理解为文档要求，包括关于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，及

d) 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与下面的正式要素相关：

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）的唯一标识码，

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。

示例：“草稿”、“已发布”。

10.4.6 应能识别当前适用的文档修订（版本）或信息项，按照第 7 章。

10.5 工作成果

10.5.1 文档管理计划，由 10.4.1 的要求得出。

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

11 使用软件工具的置信度

11.1 目的

本章的第一个目的是，在适用时提供制定软件工具置信度水平要求的准则。

本章的第二个目的是，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剪裁 GB/T XXXXX 要求的活动或任务（即，对那些 GB/T XXXXX 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、软件要素、或其硬件要素开发中使用的软件工具，可以通过剪裁 GB/T XXXXX 要求的活动或任务，而支持或使能对安全生命周期的剪裁。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) 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 XXXXX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符合GB/T XXXXX是恰当的。

注：对“软件工具”的理解，可从单独使用的标准软件工具变化到由一组软件工具集成的工具链。

示例：该软件工具可以是商业工具、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。

为评估防止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）。

如果受已确定的工具置信度水平要求，则使用合适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全部安全要求中最高 ASIL 等级。否则，无需使用该鉴定方法。

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 XXXXX-4，5.5.2；

— 使用了软件工具的各安全生命周期阶段的适用前提条件。

11.3.2 支持信息

可考虑以下信息：

— 预先确定的最大ASIL等级；

— 软件工具的用户手册（来自外部）；

— 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 XXXXX 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 预先选定的工具置信度水平的有效性或鉴定的有效性

11.4.2.1 如果对软件工具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前，按照 GB/T XXXXX-2 中表 1 对预先选定的工具置信度水平的有效性或鉴定的有效性进行确认。

注：关于软件工具的信息搜集可以是跨组织的活动，这样有助于减少分级或鉴定的难度。

11.4.3 软件工具与其评估准则或鉴定的一致性

11.4.3.1 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操作条件，与工具评估准则或鉴定相符合。

示例：如软件工具鉴定报告中描述的，对相同使用案例及相同应用措施，使用同一版本和配置设置，以预防或探测功能异常及其相应的错误输出。

11.4.4 计划软件工具的使用

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

c) 软件工具的使用案例，

注 1：使用案例可描述用户与软件工具的配合，或软件工具功能的一个应用子集。

注 2：使用案例可包含对工具配置及工具执行环境的要求。

d) 软件工具执行的环境，

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

注：可制定关于特定开发的最高 ASIL 等级，或可假设关于软件工具一般使用的最高 ASIL 等级。在预先假定 ASIL 等级的情况下，该假设得以验证。

f) 软件工具的鉴定方法（如果基于确定的置信度水平要求）。

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) 用户手册或其它使用指南（如果适用），

c) 工具运行要求的环境描述，

d) 对异常运行条件下期望的软件工具表现的描述（如果适用），

示例 1：异常运行条件可以是禁止的编译器开关组合、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) 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（如果适用），及

示例 1：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 2：安全保护包括防止（通过使用限制）、探测、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探测措施。

注：相应错误输出的探测措施可针对软件工具输出中的已知和潜在错误。

示例：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。

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：功能的模拟、源代码的生成、嵌入式软件的测试、安全生命周期的剪裁、GB/T XXXXX 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：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 XXXXX 的其它工作成果。

c) 环境的和功能的约束（如果适用），

示例：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它使用条件、防止或探测围绕软件工具的功能异常的措施。

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：

1) 当有论据表明没有这样的可能性时，应选择 TI1；

2) 在所有其它情况下应选择 TI2；

b) 用于防止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：

1) 当对防止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；

2) 当对防止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；

3) 在所有其它情况下应选择 TD3。

注 1：防止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，当评估后一软件工具时，考虑这些软件工具间的相互依赖性，为后一使用的软件工具选择一个充分的 TD。

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 XXXXX 对产生的源代码进行验证的情况下，可为代码生成器选择 TD1。

示例 2：使用指南可防止功能异常，例如编译器对代码构成的错误或不清晰的理解。

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 如果软件工具用于对开发过程的剪裁，类似省略 GB/T XXXXX 所要求的活动或任务，则不应选择 TD2。

11.4.5.5 基于为 TI 和 TD 等级确定的值（按照 11.4.5.2、11.4.5.3 或 11.4.5.4），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			
		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 XXXXX、GB/T 20438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			
		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 XXXXX、GB/T 20438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) 当软件工具功能异常并产生相应的错误输出时，预定义的、可能违背的任何安全要求的最高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) 在鉴定过程中识别出的使用约束和功能异常（如果适用）。

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，则应满足此子章节的要求。

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子章节。

a) 此前，已经将该软件工具用于相同的目的、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的和适当的数据，

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，以系统化方式累计。

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之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：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) 对软件工具的功能异常和相应错误输出及导致它们的条件细节进行文档化，

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) 对已知功能异常的安全保护、避免措施或应急措施，或相应错误输出的探测措施（如果适用）。

示例：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、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考虑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，则应满足此子章节的要求。

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，提供对软件工具开发使用流程的评估，同时应对经过评估的开发流程的恰当应用进行论证。

注：该评估涵盖了开发一个恰当且相关的软件工具特征子集。

示例：使用基于 A-SPICE、CMMI、ISO 15504 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，则应满足此子章节的要求。

11.4.9.2 软件工具的确认应满足以下准则：

a) 验证措施应说明软件工具符合其特定要求，

注：设计的用于评估软件工具功能和非功能质量方面的测试，可用于验证。

示例：编程语言标准有助于定义相关编译器的验证要求。

b) 应对验证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：可预见的误用、不完整的输入数据、软件工具的不完整升级、使用被禁止的配置设置组合。

11.4.10 软件工具鉴定的确认评审

此子章节适用于 ASIL (B)、C、D 等级，按照 4.3。

应按照 GB/T XXXXX-2 中表 1，对使用软件工具的置信度进行评估，以确保：

a) 对要求的软件工具置信度水平进行正确的评估，及

b) 按照软件工具所要求的置信度水平，对其进行恰当的鉴定。

11.5 工作成果

11.5.1 软件工具准则评估报告，由 11.4.1、11.4.2、11.4.3、11.4.4、11.4.5 和 11.4.10 的要求得出。

11.5.2 软件工具鉴定报告，由 11.4.1 至 11.4.10 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 XXXXX开发的相关项中对它们的重复使用是合适的。

12.2 总则

对已鉴定的软件组件的复用避免了对具有类似或相同功能的软件组件的重复开发。

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（商用现成（COTS）软件）；

— 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

应具备下列信息：

— 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

为了能认为软件组件是经鉴定的，应具备：

a) 软件组件的定义，按照12.4.3.1，

b) 表明软件组件符合按照12.4.3.2，12.4.3.3，以及12.4.3.4相关要求的证据，

c) 软件组件适合其用途的证据，按照12.4.4，及

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。

注：对之前开发的软件组件，可执行某些再开发活动，以满足本子章节的要求。

12.4.2 软件组件鉴定计划

12.4.2.1 软件组件鉴定计划应确定：

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，及

c) 为鉴定软件组件所应执行的活动。

12.4.3 **软件组件的鉴定**

12.4.3.1 软件组件的定义应包括：

a) 对软件组件的要求，

示例：下述要求：

— 功能要求，

— 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，以及在电控单元中许多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）。

b) 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。

c) 接口描述，

d) 应用手册（在适当的地方），

e) 软件组件集成的描述，

注：描述可包括集成和使用软件组件所需的开发工具。

f) 异常运行条件下的功能反应，

示例：非重入软件组件功能的重入调用。

g) 与其它软件组件的相关性，及

h) 对已知异常及相应应急措施的描述。

12.4.3.2 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 XXXXX-6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，在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) 无导致违背安全要求的已知错误。

12.4.3.3 本子章节适用于 ASIL D，按照 4.3

结构覆盖率应按照GB/T XXXXX-6第9章来测量，以评估测试案例的完整性。如有必要，应定义额外的测试案例或提供理由。

12.4.3.4 按照 12.4.3.2 的验证，应仅对软件组件未经改变的实现有效。

12.4.3.5 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，以及

f) 当软件组件错误执行时，可能违反的全部安全要求的最大目标ASIL等级。

12.4.4 软件组件鉴定的验证

12.4.4.1 应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。如有必要，应采用额外的措施。

注：鉴定的有效性可能限定于执行鉴定的工业领域或汽车领域环境。

示例：发动机控制、车身控制以及底盘控制是不同的汽车领域。铁路和民航是不同的工业领域。

12.4.4.2 软件组件的定义应符合该软件组件的预期使用要求。

12.5 工作成果

12.5.1 软件组件文档，由 12.4.3.1 的要求得出。

12.5.2 软件组件鉴定报告，由 12.4.3.5 的要求得出。

12.5.3 安全计划（细化的），由 12.4.2 的要求得出。

13 硬件组件的鉴定

13.1 目的

硬件组件鉴定的第一个目的是为中等复杂性的硬件组件及元器件作为按照GB/T XXXXX开发的相关项、系统或要素的一部分来使用的合适性（考虑安全概念所关注的功能表现和运行限制）提供证据。

硬件组件鉴定的第二个目的是提供关于以下方面的有关信息：

— 它们的失效模式，

— 它们的失效模式分布，以及

— 它们与相关项安全概念相关的诊断能力。

13.2 总则

在GB/T XXXXX的范围内使用的每一个安全相关硬件组件及元器件都须遵守针对整体功能性能、生产一致性、环境耐久和鲁棒性的标准鉴定。

示例 1：对于电子元器件鉴定按照 ISO16750，或按照 AEC-Q100 或 AEC-Q200 标准，或等效企业标准。

对于基础元器件（无源组件、分离式半导体），标准鉴定是足够的。这些基础元器件其后可被用于按照GB/T XXXXX-5的硬件设计。

本章的要求适用于向系统提供专用功能的中等复杂性硬件组件或元器件。

示例 2：传感器、执行器、带专用功能的特定用途集成电路（ASIC）（如协议适配器）。

如果中等复杂性硬件组件或元器件是安全相关的，依其等级，除按照本章对其进行鉴定外，还按照 GB/T XXXXX-4 或 GB/T XXXXX-5 或两者对其进行集成和测试。

通常本章中所描述的鉴定可适用于其失效模式或故障已知、且其可能失效是充分可测的组件或元器件。

示例 3：在燃油压力传感器的开发过程中，传感器的正确功能在高至 200bar 油压和 140°C 温度运行范围内得到准许。如果用于相同或更低的运行范围，该燃油压力传感器的鉴定使该传感器用于与其功能性能及其故障相适合的、特定安全相关项的实现成为可能。在这种情况下，可以省略按照 GB/T XXXXX-5 的传感器基础硬件设计分析、集成和测试，同时可直接按照 GB/T XXXXX-4 进行关于分配给传感器的技术安全要求的集成活动。

对于基础元器件、硬件元器件和组件的鉴定和集成的总结如表6所示。

表 6 — 依据硬件元器件或组件等级开展的鉴定、集成和测试活动

活动	硬件元器件或组件			
	安全相关基础硬件元器件	安全相关中等复杂性硬件元器件	安全相关中等复杂性硬件组件	安全相关复杂硬件组件
	（例如电阻、晶体管）	（例如格雷码解码器）	（例如燃料压力传感器）	（例如 ECU）
标准鉴定	适用的	适用的	—	—
按照第 13 章的鉴定	—	适用的	适用的	—

按照 GB/T XXXXX-5 的集成或测试	—	适用的 [a]	适用的 [a]	适用的
按照 GB/T XXXXX-4 的集成或测试	—			适用的
[a] 基于硬件元器件或组件的等级，按照 GB/T XXXXX-4、或 GB/T XXXXX-5、或 GB/T XXXXX-4 及 GB/T XXXXX-5 两者，对其进行集成。				

硬件组件或元器件的鉴定可用两个不同的方法来完成：测试或分析。这些方法可根据硬件组件或元器件单独使用，或组合使用。

— 测试时，硬件组件或元器件暴露在预期环境和运行条件下，并对其功能要求的符合性进行评估。精确的再现环境条件是困难的，并且所有推断取决于错误，因此在解释测试结果的时候，要考虑这些测试条件的局限性。

— 通过分析的鉴定，依赖于所用分析方法和假设的合理性。一般来说，硬件组件太复杂难以仅通过分析来进行鉴定。然而，分析可有效的用于测试数据的外推，及确定已测试硬件组件中较小改变的影响。

即使用了不同的鉴定方法，最终结果都将体现在一份鉴定报告中（可包括调查报告和解释记录等在内的一系列文件）。该报告给出了假设、条件、测试案例及其结果等证据。如果可能，最好用便于独立检查的方式来制定组合方法；它通常包括性能数据、鉴定过程、结果和理由。

ISO16750 中给出的方法有助于定义鉴定测试的类型和顺序。

13.3 本章的输入

13.3.1 前提条件

应具备下列信息：

— 相关安全要求，

— 鉴定准则（分析和测试），按照GB/T XXXXX-5第6章，及

— 生产商的硬件组件或元器件定义，如果没有，或硬件组件或元器件定义的假设（来自外部）。

13.3.2 支持信息

可考虑下列信息：

— 测试准则，按照GB/T XXXXX-5第6章；

— 参见应用了硬件组件鉴定的安全生命周期阶段的支持信息。

13.4 要求和建议

13.4.1 总则

13.4.1.1 本章的应用准则是：

a) 被鉴定的组件或元器件应具有除复杂硬件组件和基础硬件元器件外的中等程度复杂性，及

b) 应假定被鉴定的组件或元器件的相关失效模式可通过测试、分析或通过两者来验证。

13.4.2 硬件组件或元器件的鉴定目标

13.4.2.1 以下目标应通过硬件组件或元器件的鉴定来达到：

a) 为满足安全概念，组件或元器件（应具备）足够的功能表现，

b) 通过使用适当的测试（例如过极限测试、加速测试...）或分析对失效模式和模型（它们分布的量化）进行识别，

c) 足够的鲁棒性，及

d) 组件或元器件使用限制的识别。

13.4.3 硬件组件或元器件的鉴定方法

13.4.3.1 硬件组件或元器件的鉴定应恰当的选择下述方法来执行：

a) 分析，及

b) 测试。

13.4.4 鉴定计划

13.4.4.1 应开发鉴定计划，并应描述：

a) 硬件组件或元器件的精确识别及版本，

b) 硬件组件或元器件预期使用环境的定义，

c) 鉴定策略和依据，

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) 实施该策略的责任方，及

f) 用于评估硬件组件或元器件通过或不通过鉴定的准则。

13.4.5 鉴定论证

13.4.5.1 应具备对硬件组件或元器件的性能符合其规范的全面论证。

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

13.4.5.2 对 13.4.5.1 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，或

b) 来自运行经验的数据，或

c) 现有测试结果。

13.4.5.3 应给出每一个假设（包括推断）的理由。

13.4.6 分析鉴定

13.4.6.1 分析应采用易于人员理解和检查的表达方式，这些人员具有相关工程学科和科学学科的资质。

注：可用的分析方法包括外推法、数学模型、损伤分析或类似方法。

13.4.6.2 分析应考虑硬件组件或元器件所暴露的全部环境条件、这些条件的限制及其它额外的运行压力（如预期的开关周期、充电和放电、长关闭时间）。

13.4.7 测试鉴定

13.4.7.1 应制定测试计划，且测试计划应包含下列信息：

a) 硬件组件或元器件的功能描述，

b) 将进行的测试的数量和顺序，

c) 组装和连接的要求，

d) 加速老化过程，考虑到硬件组件或元器件的运行条件，

e) 模拟的运行条件和环境条件，

f) 建立的通过/不通过标准，

g) 被测环境参数，

h) 对测试设备的要求，包括精度，及

i) 测试期间允许的维护和更换流程。

13.4.7.2 应使用标准化测试规范。

注：该规范可基于 ISO16750 系列标准或等效的企业标准。

13.4.7.3 应按照计划来进行测试，并应具备测试结果数据。

13.4.8 鉴定报告

13.4.8.1 鉴定报告应说明硬件组件或元器件是否通过关于运行范围的鉴定。

注：鉴定报告可由包括调查报告和解释记录在内的的一系列文件组成。

13.4.8.2 按照第 9 章，鉴定报告应被验证。

13.5 工作成果

13.5.1 鉴定计划，由 13.4.4 的要求得出。

13.5.2 硬件组件测试计划（如果适用），由 13.4.7.1 的要求得出。

13.5.3 鉴定报告，由 13.4.8.1 的要求得出。

14 在用证明

14.1 目的

本章提供了对在用证明的指导。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 XXXXX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：在用证明不是互换性：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、硬件或软件，可作为在用证明的候选项。

候选项也可针对系统的、硬件的或软件的工作成果，如技术安全概念、算法、模型、源代码、目标代码、软件组件、一组配置或标定数据。

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执行一个附加功能；或

c) 在GB/T XXXXX发布前已在现场使用的候选项；或

d) 在其它安全相关工业中使用的候选项；或

e) 作为被广泛使用的（且未必计划用于汽车应用的）商业货架产品（COTS）的候选项。

在用证明是通过适当的候选项相关文件、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。

一旦定义了候选项（参见14.4.3）期望的在用证明可信度（参见14.4.2），在准备在用证明时，需考虑两个重要准则：

— 在候选项服务期内的现场数据的相关性（参见14.4.5），及

—自候选项开始服务以来可能对候选项产生影响的变更（若有）（参见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经过认可措施。

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

应考虑下列信息：

— 关于候选项之前的使用：

— 安全档案，按照GB/T XXXXX-2，6.5.3。

注：对于未按照 GB/T XXXXX 开发的候选项（例如商业货架产品（COTS）、基于 GB/T XXXXX 之外的其它安全标准（如 IEC61508 或 RTCA DO-178）所开发的候选项），可能不具备安全档案中的某些工作成果，那么，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

14.4.1.1 下述子章节针对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 至 14.4.5 时才应使用在用证明可信度。

14.4.2.2 应按照 GB/T XXXXX-2，6.4.3.5 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安全生命周期子阶段和被候选项在用证明覆盖的活动。

14.4.2.4 应按照 GB/T XXXXX-4 第 8 章，在适当层面执行在用证明的要素（相关项或要素中）的集成措施。

示例：某个电控单元的硬件有令人满意的服役记录，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 XXXXX-4 第 9 章执行对（嵌入了在用证明的要素的）相关项的安全验证。

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 XXXXX-2，6.4.7，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变更，都应符合 14.4.4，以保持相应的在用证明可信度。

注：本章用于任何类型的变更，包括那些由于安全相关事件而启动的变更。

14.4.3 候选项的最低限度信息

14.4.3.1 应具备对候选项及其之前使用的描述，包括：

a) 候选项的识别和追溯，及内部要素或组件（若有）目录，

b) 相应的配合要求、形式要求和功能要求，以描述（若适用）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) 候选项之前使用时的安全要求及相应的ASIL等级（若适用）。

14.4.4 候选项变更分析

14.4.4.1 在用证明的候选项

应按照14.4.4.2至14.4.4.3识别出对候选项及其环境的更改。

注 1：候选项的变更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，那么认为这些更改是对相关项的变更。

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变更

以未来应用为目的而引入的相关项及其环境的变更，应符合GB/T XXXXX-3，6.4.2。

14.4.4.3 为未来应用引入的要素变更

以不同相关项中的未来应用为目的而引入的要素及其环境的变更，应符合第8章。

14.4.4.4 独立于未来应用的候选项变更

在候选项服务期后引入的、独立于未来应用的候选项变更，应为在用证明的状态仍然有效提供证据。

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服务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 应具备候选项服务期的计算依据。

14.4.5.2.2 候选项的服务期应按照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，才能在候选项服务期的分析中考虑。

14.4.5.2.4 为了候选项达到在用证明状态，候选项服务期应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7，且具备单侧置信下限为70%（使用卡方分布）。

注 1：为了在用证明，可观察事故意味着报告给制造商、由候选项导致的潜在违背安全目标的失效。

表 7 可观察事故率的限制

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

注 2：在分析潜在的现场安全目标违背时，说明可观察事故的特征和事故率。

注 3：表 8 给出了所需的无可观察事故最短服务周期（须达到 70%置信度）的示例。

表 8 候选项最短服务期目标

ASIL	无可观察事故的最短服务期
D	1.2×10^{9}/h
C	1.2×10^{8}/h
B	1.2×10^{8}/h
A	1.2×10^{7}/h

注 4：如果在样本的采集数据中发现可观察事故，必要的最短服务期 t_service 可进行如下调整：

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

这里

CL 是置信度的绝对值（例如 0.7 对于 70%）；

t_{MTTF} 是平均失效间隔（1/失效率）；

f 是安全相关事故的数量；

$(X_{\alpha,\gamma})^2$ 是误差概率 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，候选项服务期应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9，且具备单侧置信下限为70%（使用卡方分布）。

表 9 可观察事故率的限制（临时期）

ASIL	可观察事故率
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故，应遵循以下方面：

— 停止对可观察事故率使用表9，而是为候选项使用表7；或反之

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

14.4.5.2.7 对具有非恒定失效率的候选项，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（诸如磨损、老化或关系到相关项生命周期的运行时间）的候选项。它们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，在候选项运行期间，获取并记录现场中任何由候选项引起的、具有潜在安全影响的可观察事故（参见GB/T XXXXX-7，6.4.2.1）。

14.5 工作成果

14.5.1 安全计划（细化的），由 14.4.2.1 至 14.4.2.7 的要求得出。

14.5.2 用于在用证明的候选项描述，由 14.4.3 的要求得出。

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

附录 A

（资料性附录）

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	本章目的是描述相关项和要素进行分布式开发的流程及相关责任的分配。	参见计划和开展了分布式开发的安全生命周期相关阶段的适用前提条件。	5.5.1 供应商选择报告 5.5.2 开发接口协议（DIA） 5.5.3 供应商项目计划 5.5.4 供应商安全计划 5.5.5 功能安全评估报告 5.5.6 供应协定
6. 安全要求的定义和管理	第一个目的是确保正确的定义安全要求及其属性和特性。 第二个目的是确保在整个安全生命周期内一致的管理安全要求。	参见定义和管理安全要求的安全生命周期相关阶段的适用前提条件。	无。
7. 配置管理	第一个目的是确保工作成果及其产生的原理和一般条件，在任何时间以可控的方式可被唯一识别和重生成。 第二个目的是确保较早版本和当前版本的关系及区别可被追溯。	安全计划，按照GB/T XXXXX-2，6.5.1。 在配置管理计划和管理的安全生命周期的相关阶段中适用的前提条件。	7.5.1 配置管理计划
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工作成果的变更。	配置管理计划，按照7.5.1。 安全计划，按照GB/T XXXXX-2，6.5.2。	8.5.1 变更管理计划 8.5.2 变更需求 8.5.3 影响分析和变更需求计划

			8.5.4 变更报告
9. 验证	验证的目的是确保工作成果符合对其的要求。	参见计划和执行验证的安全生命周期的相关阶段中适用的前提条件。	9.5.1 验证计划 9.5.2 验证规范 9.5.3 验证报告
10. 文档	主要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。	安全计划，按照 GB/T XXXXX-2，6.5.1。	10.5.1 文档管理计划 10.5.2 文档指南要求
11. 使用软件工具的置信度	本章的第一个目的是，在适用时提供制定软件工具置信度水平要求的准则。 本章的第二个目的是，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剪裁 GB/T XXXXX 要求的活动或任务（即，对那些 GB/T XXXXX 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 XXXXX-4，5.5.2； 使用了软件工具的各安全生命周期阶段的适用前提条件。	11.5.1 软件工具准则评估报告 11.5.2 软件工具鉴定报告
12. 软件组件的鉴定	软件组件鉴定的目的是在按照 GB/T XXXXX开发相关项中，为重复使用这些软件组件的适合性提供证据。	对软件组件的要求。	12.5.1 软件组件文档。 12.5.2 软件组件鉴定报告。 12.5.3 软件计划（细化的）。
13. 硬件组件的鉴定	硬件组件鉴定的第一个目的是为中等复杂性的硬件组件及元器件作为按照 GB/T XXXXX 开发的相关项、系统或要素的一部分来使用的合适性（考虑安全概念所关注的功能表现和运行限	相关安全要求 鉴定准则（分析和测试），按照 GB/T XXXXX-5 第 6 章；及生产商的硬件组件或元器件定义，如果没有，或硬件组件或元器件定义的	13.5.1 鉴定计划 13.5.2 硬件组件测试计划 13.5.3 鉴定报告

	制）提供证据。 硬件组件鉴定的第二个目的是提供其失效模式、失效模式分布及其与相关项安全概念相关的诊断能力的有关信息。	假设（来自外部）。	
14. 在用证明	本章提供了对在用证明的指导。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 XXXXX 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（来自外部）。	14.5.1 安全计划（细化的） 14.5.2 用于在用证明的候选项描述 14.5.3 在用证明分析报告

附录 B

（资料性附录）

开发接口协议(DIA)示例

B.1 目的

本附录依照第5章的要求（特别是5.4.3.1 c)到g)的要求），提供了开发接口协议（DIA）的一个说明性示例，并提供了符合GB/T XXXXX-2，5.4.5和5.5.1中要求和建议的组织特定调整（如果有），还可应用符合GB/T XXXXX-2，6.4.5的项目特定剪裁。

B.2 总则

许多因素会影响客户-供应商交互的类型和数量；本示例是一个被简化的、基于在表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，增加了某些组织特定内容，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，增加了某些组织特定内容，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 XXXXX 章节在括号内表示。

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：它还不是一个商业货架产品（COTS）。它所涉及的新技术没有足够的、经过检验的供应商。

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) 使用模型化的开发流程。

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，并得到独立的评估，被评定为最高完整性等级。

1) 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。

2）其它资源（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。

3）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。

4）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无歧义的定义。

5）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) 还有其它高质量执行的客户-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–供应商数据交互

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 XXXXX-2，5.4.2）； — 能力的证据（GB/T XXXXX-2，5.4.3）； — 质量管理的证据（GB/T XXXXX-2，5.4.4）； — GB/T XXXXX 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 XXXXX-2 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	5.4.2 评定供应商（通过预审的）[a] 5.4.2	客户组织特定的对 GB/T XXXXX-2，5.4.5 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 XXXXX-3，5.5）和安全目标（GB/T XXXXX-3，7.5.2）	—
A.7	—	—	报价， 符合性声明； 之前递交信息的更新 [a]
A.8		建议的 DIA（项目特有）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 XXXXX-2，5.5.2）； 组织特有的规章和流程（GB/T XXXXX-2，5.5.1），包括工具、库； 初步计划，例如：安全计划（GB/T XXXXX-2，6.5.1）
A.10		迭代评估和询问，例如关于技能的差距 [a]	迭代修改，解决客户的质疑 [a]
A.11		DIA 的接受	DIA 的接受

		（5.5.2） 选择报告（5.5.1）	（5.5.2）
A.12		概念（GB/T XXXXX-3；GB/T XXXXX-4）和计划阶段（GB/T XXXXX-4 第 5 章）的合同，包括开发工作的声明	接受。
[a] 活动或数据为组织所特有的，GB/T XXXXX 未作要求。			

表 B. 2 在项目启动和系统概念阶段客户–供应商的数据交换

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 XXXXX-3，第 5 至 8 章）	系统层面的计划 相关项定义（GB/T XXXXX-3，5.5）及其生命周期（图 1、GB/T XXXXX-2，5.2.2；GB/T XXXXX-2，图 2 和 GB/T XXXXX-2，6.4.5） 功能安全概念（GB/T XXXXX-3，第 8 章）	—
B.2	—	—	项目计划（5.5.3） 安全计划（5.5.4） H&R 分析（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 XXXXX-5，附录 B 和 GB/T XXXXX-5，9.4.3.1]。 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，以符合所需的工作成果。[5.4.3 c) e), g),，5.4.5]
B.3	—	接受	—
B.4	对已用于类似项目（5.4.4.5）的组件、工具、库的在用证明经验的考量，以及可能的候选项的在用证明数据和分析（GB/T XXXXX-8，第 14 章）	初步的安全计划（GB/T XXXXX-2，第 5 章），包括系统安全档案结构	—

B.5	—	—	提供的在用证明的要素（第 14 章），及项目合适性的独立评估（5.4.5 和 GB/T XXXXX-2 表 1）
B.6	—	接受	—
B.7	系统开发生命周期[5.4.3 b)]	技术安全概念（GB/T XXXXX-4，7.5.1）、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 XXXXX，7.5.3）	迭代评估、澄清疑问及冲突反馈，完整性、一致性等；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 XXXXX-4，7.5.2，GB/T XXXXX-4，7.5.5）、硬件规范（GB/T XXXXX-5，7.5.1）	关于组件 C 与其环境边界的反馈
B.9	—	—	接受

表 B3 在硬件开发生命周期中客户与供应商的数据交换

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（5.5.4 和 GB/T XXXXX-5，5.5.1），项目计划（5.5.3 和 GB/T XXXXX-5，5.5.2），相关项集成和测试计划（参见 GB/T XXXXX-4，5.5.3），DIA 的计划（5.4.3）等。 计划符合性的独立评审（5.4.4.8 和 5.4.5）
C.3		接受。授权开始需求定义。	—
C.4	要求 (5.4.5 和 GB/T XXXXX-5)	—	得出和细化硬件规范；D&I 限制（GB/T XXXXX-5，7.5.1）。 验证计划的延伸 [a] 软硬件接口的变更请求，如果有（GB/T XXXXX-5，10.5） 独立的安全审核（5.4.4.8） 独立的确认（5.4.5 和 5.5.5）

C.5	—	接受。授权开始设计。	—
C.6	设计 (5.4.5 和 GB/T XXXXX-5)	—	设计规范（GB/T XXXXX-5，7.5.1）；实施限制，包括架构的限制（GB/T XXXXX-5 第 8 章）。 H&R 分析的扩展或修改（GB/T XXXXX 第 7 章），如果有。 相关项集成和测试计划的扩展（GB/T XXXXX-5，10.5）。 软硬件接口的变更请求，如果有（GB/T XXXXX-5，10.5）。 独立的安全审核（5.4.4.8，5.4.5）
C.7	5.4.4 and 5.4.5 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、修改及其它响应。 独立的评估（5.4.5 和 5.5.5）。
C.8	5.4.4 and 5.4.5 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 5.5.5）。
C.9	—	接受	—
C.10	—	—	原型件 集成验证（GB/T XXXXX-5，10.5） 独立的评估（5.4.5）。
C.11	—	集成的评估（GB/T XXXXX-4 第 8 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 5.5.5）。
C.13	—	接受	—
C.14	—	—	批量生产的样品 独立的评估（5.4.5 和 5.5.5）。
C.15	—	集成的评价（GB/T XXXXX-4 第 8 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 5.5.5）
C.17	—	授权开始生产阶段	—
C.18	—	—	量产后的报告（5.4.6、5.5.6 和 GB/T XXXXX-2, 7.5）
[a] 活动或数据为组织所特有的，GB/T XXXXX 未作要求。			