ICS 43.020
T40

中华人民共和国国家标准

GB/T XXXXX—XXXX

道路车辆 功能安全
第4部分：产品开发：系统层面

Road vehicles-Functional safety-Part 4: Product development at the system level

（ISO 26262-4：2011，MOD）

征求意见稿

（本稿完成日期：20150423）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　录

前言 II
引言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 2
4 要求 2
5 启动系统层面产品开发 2
6 技术安全要求的定义 5
7 系统设计 8
8 相关项集成和测试 13
9 安全确认 20
10 功能安全评估 22
11 生产发布 23
附　录　A （资料性附录） 24
附　录　B （资料性附录） 26

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：汽车安全完整性等级导向和安全导向分析；

——第10部分：指南。

本部分为GB/T XXXXX的第4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 26262-4：2011《Road vehicles — Functional safety — Part 4: Product development at the system level》。

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，不仅在驾驶员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（ASIL）；

c) 应用汽车安全完整性等级（ASIL）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 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/T XXXXX-2 的第 6 章。

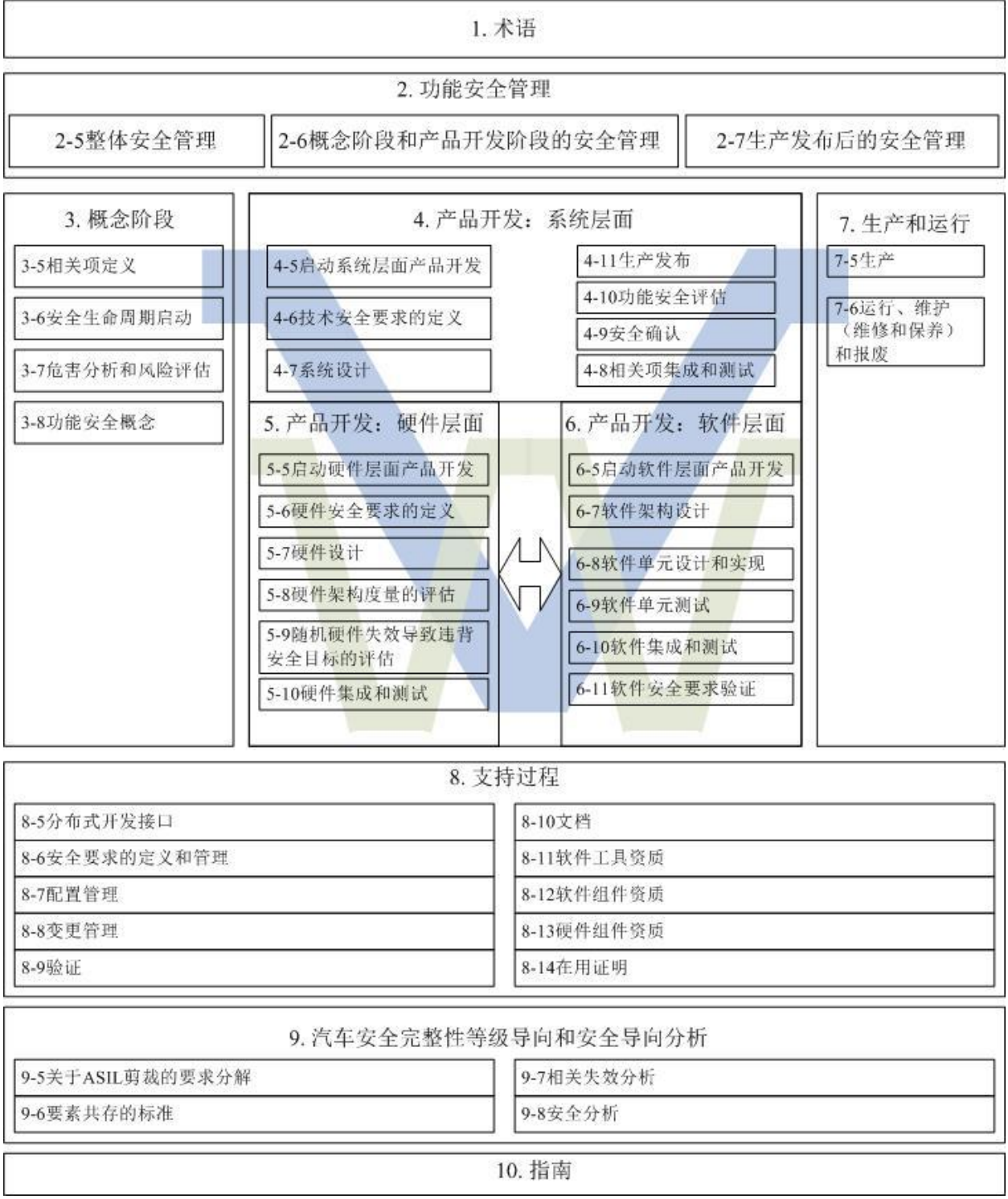


图 1 GB/T XXXXX 概览

道路车辆 功能安全

第4部分：产品开发：系统层面

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。

本部分规定了车辆在系统层面产品开发的要求，包括：

——启动系统层面产品开发的要求，

——技术安全要求的定义，

——技术安全概念，

——系统设计，

——相关项集成和测试，

——安全确认，

——功能安全评估，及

——产品发布。

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-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-8:201X，道路车辆 功能安全 第8部分：支持过程；

GB/T XXXXX-9:201X，道路车辆 功能安全 第9部分：汽车安全完整性等级导向和安全导向分析；

GB/T XXXXX-10:201X，道路车辆 功能安全 第10部分：指南。

3 术语和定义

GB/T XXXXX-1给出的术语和定义适用于本部分。

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，但在某些情况下，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，这并不意味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 启动系统层面产品开发

5.1 目的

启动产品开发系统层面的目的是确定并计划系统开发各子阶段过程中的功能安全活动，也包括在GB/T XXXXX-8中所描述的必要的支持过程。

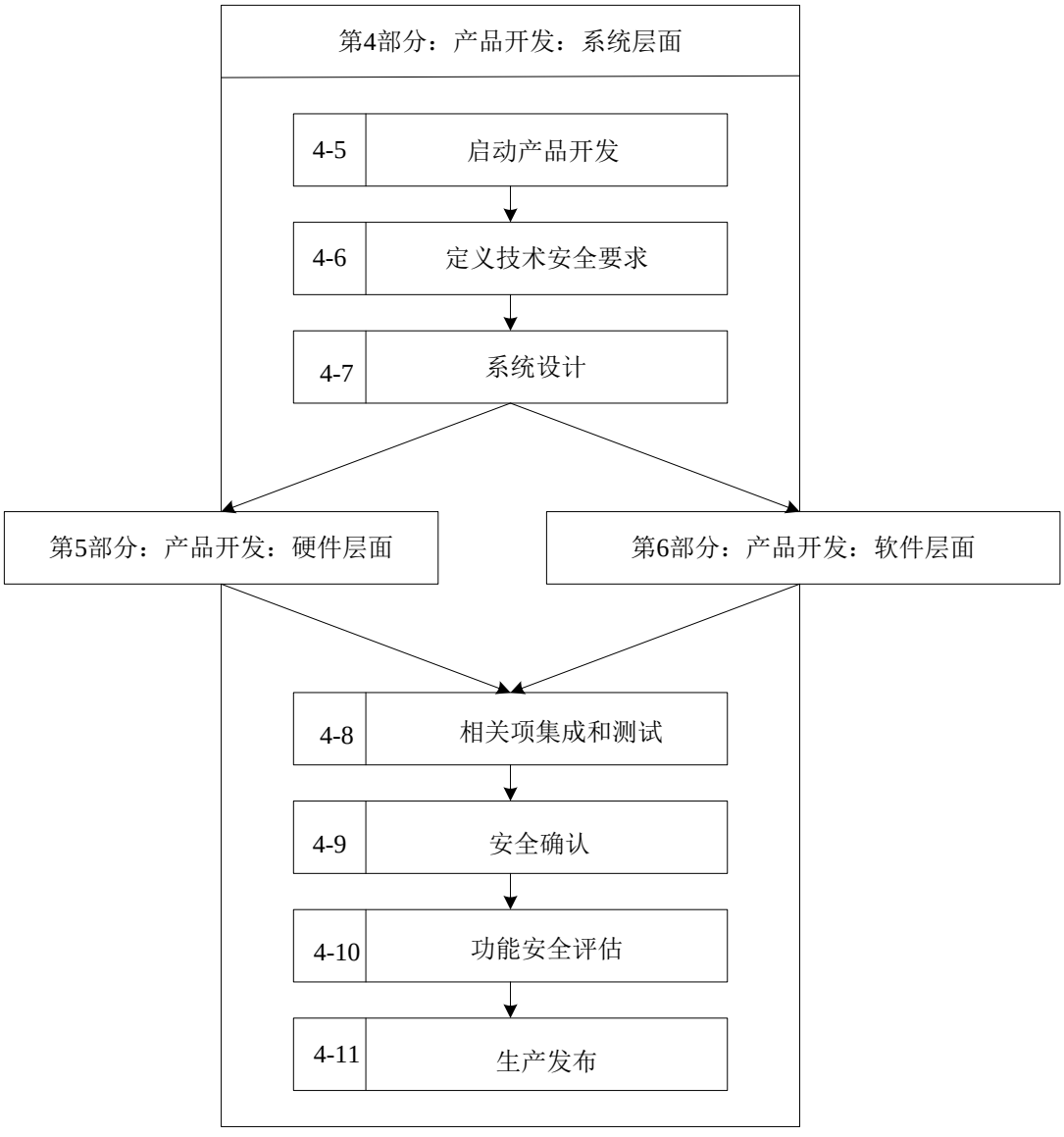
系统层面安全活动的计划包含在安全计划中。

5.2 总则

图2给出了在系统开发过程中的必要活动。在启动产品开发和定义技术安全要求后，进行系统设计。在系统设计过程中建立系统架构，将技术安全要求分配给硬件和软件，并且，如果适用，也可分配给其它技术。同时，细化技术安全要求，并添加来自系统架构的要求，包括软硬件接口的要求。根据架构的复杂性，可以逐步得出子系统的要求。完成相关开发后，集成硬件和软件要素并测试以形成一个相关项，然后，将该相关项集成在整车上。一旦在整车层面完成了系统集成，进行安全确认以提供与安全目标相关的功能安全证据。

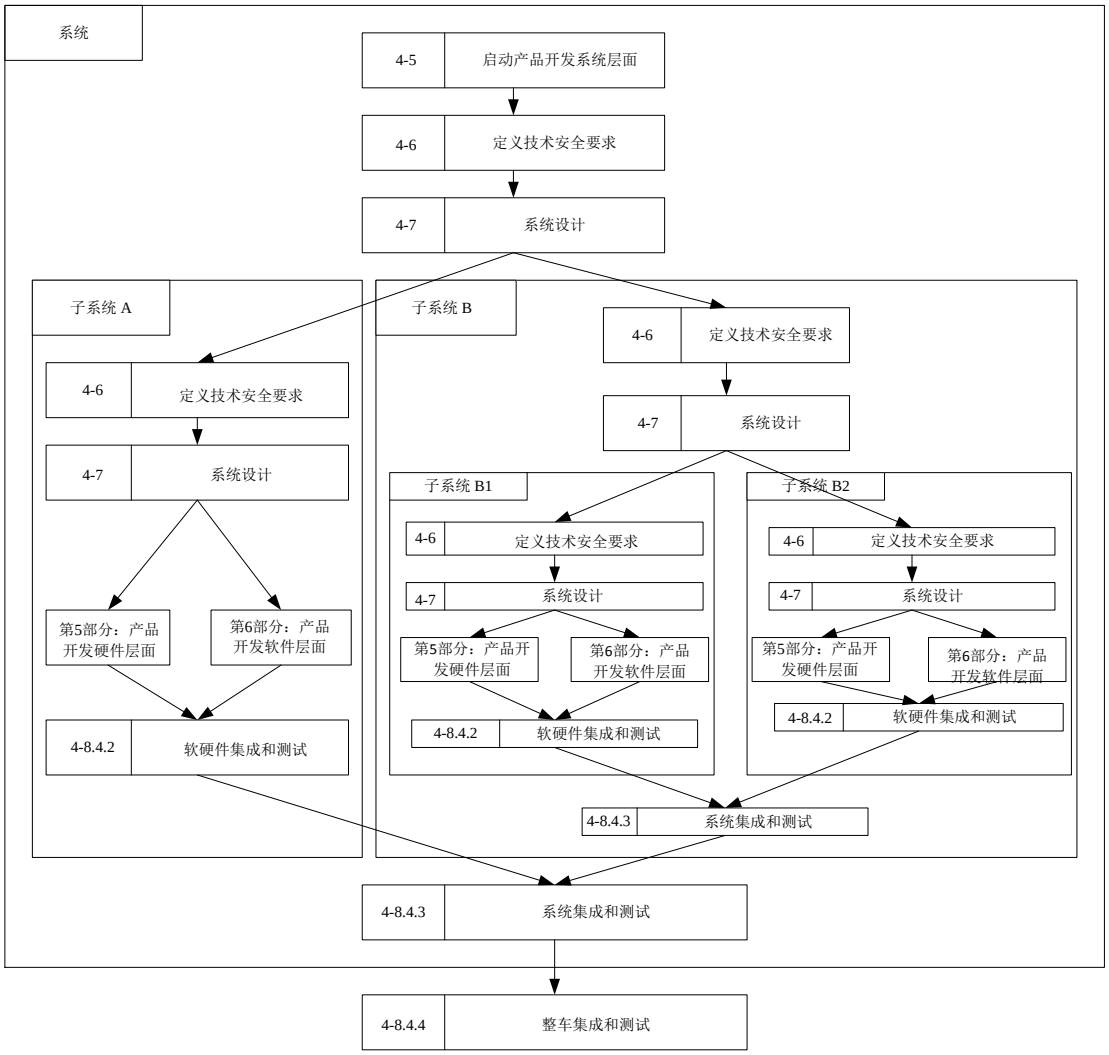
GB/T XXXXX-5和GB/T XXXXX-6描述了软硬件的开发要求。本部分适用于系统和子系统的开发。图3是具有多层集成的系统示例，阐明了如何应用本部分及GB/T XXXXX-5和GB/T XXXXX-6部分。

注1：表A.1提供了对产品开发系统层面特定子阶段的目的、前提条件和工作成果的概览。



注2：在图中，GB/T XXXXX 的各部分具体条款用以下列方式来表明：“m-n”，其中“m”代表“部分”的编号和“n”表示“章”的编号，例如，“4-5”表示 GB/T XXXXX 的第 4 部分的第 5 章。

图 2 安全相关的相关项开发参考阶段模型



注：在图中，GB/T XXXXX的各部分具体条款用以下列方式来表明：“m-n”，其中“m”代表“部分”的编号和“n”表示“章”的编号，例如，“4-5”表示GB/T XXXXX的第4部分的第5章。

图 3 产品开发系统层面示例

5.3 本章的输入

5.3.1 前提条件

应具备下列信息：

——项目计划（细化的），按照 GB/T XXXXX-2 中 6.5.2；

——安全计划，按照 GB/T XXXXX-3 中 6.5.2；

——功能安全评估计划，按照 GB/T XXXXX-2 中 6.5.4 及

——功能安全概念，按照 GB/T XXXXX-3 中 8.5.1。

5.3.2 支持信息

可考虑下列信息：

——初步的架构设想（来自外部）；及

——相关项定义（参见 GB/T XXXXX-3 中 5.5）。

5.4 要求和建议

5.4.1 应制定产品开发系统层面的安全活动计划，包括确定设计和集成过程中适当的方法和措施。

注：按照6.4.6（验证和确认）和7.4.8（系统设计验证）的要求，设计过程中对验证活动所做计划的结果是安全计划的组成部分，而按照8.4.2（硬件/软件），8.4.3（要素集成）和8.4.4（相关项集成）制定的相关项集成和测试计划在一个单独相关项集成和测试计划（按照8.4.1.3的要求）中进行了描述。

5.4.2 应制定确认活动的计划。

5.4.3 应制定产品开发系统层面的功能安全评估活动计划（参见 GB/T XXXXX-2）。

注：GB/T XXXXX-2中的附录E提供了一个功能安全评估安排的示例。

5.4.4 应按照 GB/T XXXXX-2 的要求并基于图 2 给出的参考阶段模型，进行产品开发系统层面的生命周期剪裁。

注：项目计划可用于提供产品开发系统层面各子阶段和软硬件开发阶段的关系。这包括每个层面的集成步骤。

5.5 工作成果

5.5.1 项目计划（细化的），由 5.4.4 的要求得出。

5.5.2 安全计划（细化的），由 5.4.1 至 5.4.4 的要求得出。

5.5.3 相关项集成和测试计划，由 5.4.1 的要求得出。

5.5.4 确认计划，由 5.4.2 的要求得出。

5.5.5 功能安全评估计划（细化的），由 5.4.3 的要求得出。

6 技术安全要求的定义

6.1 目的

该子阶段的第一个目的是制定技术安全要求。技术安全需求规范同时考虑功能概念和初步的架构设想（参见GB/T XXXXX-3），从而进一步细化功能安全概念。

第二个目的是通过分析来验证技术安全要求是否符合功能安全要求。

6.2 总则

在整个开发生命周期中，技术安全要求是实现功能安全概念必要的技术要求，目的是将相关项层面的功能安全要求细化到系统层面的技术安全要求。

注：避免潜伏故障的要求，可在第一轮系统设计子阶段之后引出。

6.3 本章的输入

6.3.1 前提条件

应具备下列信息：

——功能安全概念，按照 GB/T XXXXX-3,8.5.1；及

——确认计划，按照 5.5.4。

6.3.2 支持信息

可考虑下列信息：

——安全目标（参见 GB/T XXXXX-3，7.5.2）；

——功能概念(来自外部，参见 GB/T XXXXX-3, 5.4.1)；及

——初步的架构设想 (来源于外部，参见 GB/T XXXXX-3, 8.3.2)。

6.4 要求和建议

6.4.1 定义技术安全要求

6.4.1.1 技术安全要求应根据功能安全概念、相关项的初步架构设想和如下系统特性来定义：

a) 外部接口，如通讯和用户接口，如果适用；

b) 限制条件，例如环境条件或者功能限制；以及

c) 系统配置要求。

注：具有为选择性用途而重新配置系统的能力是重复使用已有系统的一种策略。

示例：标定数据(参见 GB/T XXXXX-6, 附录 C) 常用于定制不同车辆的发动机电子控制单元。

6.4.1.2 应确保 GB/T XXXXX-3, 8.3.2 中的初步架构设想和本子阶段中的初步架构设想的一致性。

6.4.1.3 除按照 6.4.1(技术安全要求的定义)定义技术安全要求的那些功能外，如果其它功能或要求也由系统或其要素实现，则应定义这些功能或要求，或者标明其参考规范。

示例：其它要求来源于欧洲经济委员会(ECE)法规，美国联邦机动车安全标准(FMVSS)或者企业平台策略。

6.4.1.4 技术安全要求应定义系统间或相关项要素间，及相关项和其它系统间的安全相关的关联性。

6.4.2 安全机制

6.4.2.1 技术安全要求应定义系统或要素对于影响实现安全目标的激励的响应。这包括失效和相关的激励组合，并与每个相关运行模式及规定的系统状态进行组合。

示例：如果自适应巡航(ACC)的电控单元从制动系统电控单元收到车辆稳定性控制功能不可用的通知，那么它会关闭 ACC 功能。

6.4.2.2 技术安全要求应定义必要的安全机制(参见 GB/T XXXXX-8,第 6 章) 包括：

a) 与系统自身故障相关的探测、指示和控制措施；

注1：包括系统或者要素的自身监控，用于探测随机硬件故障，以及，如果适用，探测系统性失效。

注2：包括对通讯通道（例如：数据接口，通讯总线，无线广播连接）失效模式的探测和控制的措施。

b) 涉及探测、指示和控制与本系统有相互影响的外部设备中所发生故障的措施；

示例：外部设备包括其它的电控单元、电源或者通讯设备。

c) 使系统实现或者维持在安全状态下的措施

注3：包括在安全机制冲突时的优先和仲裁逻辑。

d) 细化和执行报警和降级概念的措施；以及

e) 防止故障潜伏的措施[参见 6.4.4(潜伏故障的避免)]

注4：这些措施通常与上电过程（预驱检测），例如措施 a)到 d)，运行过程，下电过程（后驱检测），或者作为维护的一部分的测试相关。

6.4.2.3 对于每个使相关项实现或者维持安全状态的安全机制，应定义下列内容：

a) 向安全状态的过渡；

注1：包括执行器的控制要求。

b) 容错时间区间；

注2：整车测试和试验能够用于确定容错时间区间。

c) 如果不能立即进入安全状态时的紧急操作时间区间；以及

注3：整车测试和试验能够用于确定紧急操作时间区间

示例1：关闭系统可以是一种紧急操作。

d) 维持安全状态的措施。

示例2：一个依赖于电源的线控制动应用的安全机制，可以包括定义备用电源或储能设备(容量，启动和运行时间等)。

6.4.3 ASIL 分解

6.4.3.1 如果在定义技术安全要求的时候进行 ASIL 分解，应根据 GB/T XXXXX-9，第 5 章进行（与 ASIL 剪裁相关的要求分解）。

6.4.4 潜伏故障的避免

6.4.4.1 按照 4.3，此要求适用于 ASIL(A),(B),C 和 D：如果适用，应定义防止故障潜伏的安全机制。

注1：就随机故障而论，只有多点故障有可能包含潜伏故障。

示例：车载测试是用于检测潜伏故障的安全机制，它验证在不同运行模式（例如上电、下电、运行或一个额外的测试模式）下部件的状态。阀、继电器或灯在上电时做的功能测试就是这类车载测试的例子。

注2：识别是否需要防止故障潜伏的安全措施的评估标准来源于好的工程实践。GB/T xxxxx-5 第 8 章给出的潜伏故障度量，提供了评估的标准。

6.4.4.2 按照 4.3，此要求适用于 ASIL(A),(B),C 和 D：为了避免多点失效，应为每个按照 6.4.4(潜伏故障的避免)执行的安全机制定义多点失效探测时间区间。

6.4.4.3 按照 4.3，此要求适用于 ASIL(A),(B),C 和 D：为确定多点故障探测时间区间，宜考虑下列参数：

a) 硬件部件的可靠性，并考虑其在架构中的角色
b) 相关危害事件的暴露概率
c) 定义的量化目标值，表征由于硬件随机失效而违背各安全目标的最大可能性(参见要求 7.4.4.3)；及
d) 相关安全目标分配的 ASIL

注：下列措施的使用依赖于时间限制：

——系统或要素在运行过程中的周期性测试；

——要素在上下电时的车载测试；以及

——系统或要素在维护时的测试。

6.4.4.4 按照 4.3，此要求适用于 ASIL(A),(B),C 和 D：用于防止双点故障变成潜伏故障的安全机制的开发应符合：

a) ASIL B（对于分配为 ASIL D 技术安全要求）；
b) ASIL A（对于分配为 ASIL B 和 ASIL C 技术安全要求）；以及
c) 工程判断（对于分配为 ASIL A 的技术安全要求）。

6.4.5 生产、运行、维护和报废

6.4.5.1 应定义在 GB/T XXXXX-7 中所表述的生产、运行、维护、维修和报废期间的关于相关项或其要素的功能安全的技术安全要求。

注：在生产、运行、维护、维修和报废期间，有两个方面确保安全。第一个方面涉及到在6.4.5.1和7.4.7的要求(对生产、运行、维护和报废的要求)中所给出的开发阶段期间执行的那些活动，而第二个方面涉及到在GB/T XXXXX-7中描述的生产和运行阶段期间执行的那些活动。

6.4.6 验证和确认

6.4.6.1 技术安全要求应按照 GB/T XXXXX-8 第 9 章来验证，以提供证据证明它们：

a) 与功能安全概念的符合性和一致性；以及
b) 与初步架构设计设想的符合性。

6.4.6.2 应基于技术安全要求细化相关项的安全确认标准。

注：系统确认计划和系统确认规范是与技术安全要求并行开发的（参见第9章）。

6.5 工作成果

6.5.1 技术安全需求规范，由 6.4.1 到 6.4.5 的要求得出。

6.5.2 系统验证报告，由 6.4.6 的要求得出。

6.5.3 确认计划(细化的)，由 6.4.6.2 的要求得出。

7 系统设计

7.1 目的

该子阶段的第一个目的是开发系统设计和技术安全概念,以满足相关项的功能要求和技术安全需求规范。

该子阶段的第二个目的是验证系统设计和技术安全概念满足技术安全要求规范。

7.2 总则

系统设计和技术安全概念的开发是基于源自功能安全概念的技术安全需求规范。如果系统由子系统构成，这个子阶段可以迭代使用。

为了开发系统架构设计，需要实现功能安全要求、技术安全要求和非安全相关要求。因此在该子阶段,用同一个开发流程来处理安全相关和非安全相关要求。

7.3 本章的输入

7.3.1 前提条件

应具备下列信息:

——相关项集成与测试计划，按照 5.5.3；及

——技术安全需求规范，按照 6.5.1。

7.3.2 支持信息

可考虑下列信息:

——初步架构设想(来自外部，参见 GB/T XXXXX-3,8.3.2)；

——功能概念（来自外部)；和

——功能安全概念（参见 GB/T XXXXX-3,8.5.1)。

7.4 要求和建议

7.4.1 系统设计规范和技术安全概念

7.4.1.1 系统设计应基于功能概念、初步架构设想和技术安全要求。应保证在 GB/T xxxxx-3:20xx, 8.3.2 中的初步架构设想和这个子阶段中的初步架构设想的一致性.。

7.4.1.2 技术安全要求应分配给系统设计要素。

7.4.1.3 系统设计应实现技术安全要求。

7.4.1.4 与实现技术安全要求相关，在系统设计中应考虑：

a) 验证系统设计的能力；
b) 与实现功能安全相关的预期的软硬件设计的技术能力；以及
c) 系统集成中执行测试的能力。

7.4.2 系统架构约束条件

7.4.2.1 系统和子系统架构应满足它们各自 ASIL 等级的技术安全要求。

7.4.2.2 每个要素应继承来自它所执行的技术安全要求的最高 ASIL 等级。

7.4.2.3 如果一个要素由指定为不同 ASIL 等级的子要素组成，或由非安全相关子要素和安全相关子要素组成，则它们中的每一个应按照最高的 ASIL 等级来处理，除非它们满足按照 GB/T xxxxx-9:20xx 第 6 章所定义的共存标准。

7.4.2.4 应定义安全相关要素的内部和外部接口，以避免其它要素对于安全相关要素有不利于安全的影响。

7.4.2.5 如果在系统设计期间对安全要求应用了 ASIL 等级分解，应按照 GB/T xxxxx-9:20xx 中第 5 章进行。

7.4.3 避免系统性失效的措施

7.4.3.1 对系统设计进行安全分析以识别系统性失效的原因和系统性故障的影响,应按照表 1 和 GB/T XXXXX-9 第 8 章进行。

表 1-系统设计分析

方法		功能安全完整性等级			
		A	B	C	D
1	演绎分析 [a]	o	+	++	++
2	归纳分析 [b]	++	++	++	++
[a] 演绎分析方法包括故障树分析 (FTA), 可靠性框图, 鱼骨图。 [b] 归纳分析方法包括失效模式与影响分析（FMEA），事件树分析 (ETA)，马尔科夫（Markov）模型。					

注1：这些分析的目的是帮助设计。因此在该阶段，定性分析可能是足够的。如果有必要,可以采用定量分析。

注2：在足以识别或排除系统性失效的原因和影响的细节层面上进行分析。

7.4.3.2 应消除已识别出的引起系统性失效的内部原因，或减轻它们的影响。

7.4.3.3 应消除已识别出的引起系统性失效的外部原因，或减轻它们的影响。

7.4.3.4 为减少系统性失效，宜应用值得信赖的汽车系统设计原则. 这些原则可能包括：

a) 值得信赖的技术安全概念的再利用；
b) 值得信赖的要素设计的再利用，包括硬件和软件组件；

c) 值得信赖的探测和控制失效的机制的再利用，及

d) 值得信赖的或标准化接口的再利用。

7.4.3.5 为了确保值得信赖的设计原则或要素在新相关项中的适用性，应分析其应用结果，以及应在再利用之前检查其基本设想。

注：影响分析包括确定的诊断、环境限制、时序限制的能力和可行性，确定资源的兼容性，以及系统设计的鲁棒性。

7.4.3.6 本要求适用于 ASIL D：宜对不再利用值得信赖的设计原则的决定阐明理由。

7.4.3.7 按照 4.3，本要求适用于 ASIL(A), (B), C 和 D：为了避免高度复杂性导致的失效，架构设计应通过使用表 2 中的原则来展示所有下述属性：

a) 模块性；

b) 适当的粒度水平；及

c) 简单。

表 2-模块化系统设计的属性

属性		功能安全完整性等级			
		A	B	C	D
1	分层的设计	+	+	++	++
2	精确定义的接口	+	+	+	+
3	避免硬件组件和软件组件不必要的复杂性	+	+	+	+
4	避免接口的不必要的复杂性	+	+	+	+
5	维护期间的可维护性	+	+	+	+
6	开发和运行期间的可测性	+	+	++	++

7.4.4 **运行过程中随机硬件失效的控制措施**

7.4.4.1 **应按照 7.4.1（系统设计规范和技术安全概念）中的系统设计，定义探测和控制，或者减轻随机硬件失效的措施。**

示例1：这些措施可以是硬件的诊断特性和通过软件对其的使用来探测随机硬件失效。

示例2：在随机硬件失效发生时，直接导引至安全状态的硬件设计，甚至不需要探测即可控制失效。

7.4.4.2 本要求适用于 ASILs (B), C 和 D，根据 4.3：应为相关项层面的最终评估（参见 9.4.3.3）定义单点故障和潜伏故障度量（参见 GB/T XXXXX-5，第 8 章）的目标值。

7.4.4.3 根据 4.3，本要求适用于 ASILs (B), C 和 D：应选择可替代流程中的一个，用于评估随机硬件失效导致的对安全目标的违背 (参见 GB/TXXXXX-5，第 9 章) ，并应定义目标值以用于相关项层面的最终评估(参见 9.4.3.3)。

7.4.4.4 根据 4.3，本要求适用于 ASILs (B), C 和 D：适当的失效率和诊断覆盖率的目标值应在要素层面进行定义，以符合：

a) GB/TXXXXX-5，第 8 章中的度量的目标值；及

b) GB/TXXXXX-5，第 9 章中的流程。

7.4.4.5 根据 4.3，本要求适用于 ASILs (B), C 和 D：对于分布式开发(参见 GB/TXXXXX-8，第 5 章)，推导出的目标值应通报给每个相关团队。

注：GB/TXXXXX-5，第 8 章和第 9 章中描述的构架限制，不直接适用于货架商品类的部件和组件。这是因为供应商

通常无法预测终端相关项中如何使用他们的产品以及潜在的安全影响。在这种情况下，零部件供应商会提供基本的数据，例如失效率、失效模式、每种失效模式的失效率分布、内置的诊断，等等，以便于允许在整体硬件架构层面上预估架构约束。

7.4.5 分配到硬件和软件

7.4.5.1 技术安全要求应直接或通过进一步的细化后，分别或同时分配到硬件和软件。

7.4.5.2 如果技术安全要求分配到具备可编程功能的定制硬件要素(比如专用集成芯片（ASICs），可编程门阵列（FPGA）或是其它形式的数字化硬件)，宜结合 GB XXXXX-5 和 GB XXXXX-6 的要求来定义和实施适当的开发流程。

注：如果满足应用GBXXXXX-8第13章的判断标准，可按照该章的认证措施提供上述硬件要素中的某些要素满足分配的安全要求的证据。

7.4.5.3 系统设计应遵从分配和分区决策。

注：为了实现独立性和避免失效传播，系统设计可采用功能分区和组件分区。

7.4.6 硬件-软件接口规范(HSI)

7.4.6.1 HSI 规范应定义硬件和软件的交互，并保持与技术安全概念一致。HSI 规范应包括组件中由软件控制的硬件装置以及支持软件运行的硬件资源。

示例：HSI 中详细描述的方面和特性见附录 B。

7.4.6.2 HSI 规范应包含下列特性：

a) 硬件装置的相关运行模式和相关配置参数；

示例1：硬件装置的运行模式，例如：默认模式、初始化模式、测试模式或者高级模式。

示例2：配置参数，例如：增益控制，带通频率或时钟分频。

b) 确保要素间独立性和支持软件分区的硬件特征；

c) 硬件资源的共用和专用；

示例3：内存映射、寄存器分配、计时器、中断、I/O 端口。

d) 硬件装置的访问机制；及

示例4：串、并、从、主/从。

e) 为技术安全概念涉及到的每一个服务定义的时序限制。

7.4.6.3 硬件的相关诊断能力和软件对其的使用应在 HSI 规范中定义：

a) 应定义硬件的诊断特性；及

示例：过流、短路或过温的探测.

b) 应定义需要在软件中实现的对硬件的诊断特性。

7.4.6.4 HSI 应在系统设计过程中定义，并在硬件开发 (见 GBXXXXX-5 第 7 章) 和软件开发(见 GBXXXXX-6 第 7 章)过程中细化。

7.4.7 生产、运行、维护和报废的要求

7.4.7.1 在考虑了安全分析的结果和所实施的安全机制的情况下，应定义需具备的诊断特性，以提供运行中对相关项或其要素进行现场监控所需的数据。

7.4.7.2 为了保持功能安全，应定义诊断特性以便需要维护时车间人员能够识别故障。

7.4.7.3 应定义在系统设计中识别出的对生产、运行、维护和报废的要求(见 GB/T XXXXX-7)，包括：

a) 装配指导的要求；
b) 安全相关的特殊特性；
c) 专用于确保正确识别系统或要素的要求；

示例1：要素标识。

d) 生产的验证方法和措施；
e) 维护要求，包括诊断数据和维护记录；及
f) 报废要求。

示例2：报废指南。

7.4.8 系统设计的验证

7.4.8.1 应使用表 3 列出的方法验证系统设计对于技术安全概念的符合性和完备性。

表 3 -系统设计验证

方法		功能安全完整性等级			
		A	B	C	D
1a	系统设计检查 [a]	+	++	++	++
1b	系统设计走查 [a]	++	+	o	o
2a	仿真 [b]	+	+	++	++
2b	系统原型和车辆测试 [b]	+	+	++	++
3	系统设计分析 [c]	参见表 1			
[a] 方法 1a 和 1b 用于检查技术安全要求得到完整和正确的实施。 [b] 方法 2a 和 2b 可作为故障注入技术有效地使用。 [c] 对于如何实施安全分析，参见 GB/T XXXXX-9 第 8 章。					

注：根据GB/T XXXXX-2,5.4.2，报告系统设计中识别的关于技术安全概念的异常和不完备。

7.4.8.2 应按照 GB/T XXXXX-3 危害分析和风险评估及 GB/T XXXXX-8 第 8 章变更管理流程，引入和评估系统设计中新识别出且未包含在安全目标中的危害。

注：新识别出且未在安全目标中体现的危害，通常是非功能性的危害。非功能性的危害不在GB/T XXXXX考虑的范围内，但在危害分析和风险评估中可以标注为“因不在GB/T XXXXX规定范围内，不为其指定ASIL等级”。然而，也可以指定ASIL等级作为参考。

7.5 工作成果

7.5.1 技术安全概念，由 7.4.1 和 7.4.5 的要求得出。

7.5.2 系统设计规范，由 7.4.1 到 7.4.5 的要求得出。

7.5.3 硬件-软件接口(HSI)规范，由 7.4.6 的要求得出。

7.5.4 生产、运行、维护和报废要求的定义，由 7.4.7 的要求得出。

7.5.5 系统验证报告（细化的），由 7.4.8 的要求得出。

7.5.6 安全分析报告，由 7.4.3 的要求得出。

8 相关项集成和测试

8.1 目的

相关项集成和测试阶段包含三个阶段和两个主要目标：第一个阶段是相关项所包含的每一个要素的软硬件集成；第二个阶段是构成一个完整系统的一个相关项的所有要素的集成；第三个阶段是相关项与车辆上其它系统的集成以及与整车的集成。

相关项集成过程的第一个目标是测试每一条安全要求是否满足规范以及ASIL级别要求。

相关项集成过程的第二个目标是验证涵盖安全要求的“系统设计”【参见第7章（系统设计）】在整个相关项上得到正确实施。

8.2 总则

相关项要素的集成按照系统化的方法进行，从软件-硬件集成开始，经过系统集成，最后完成整车集成。在每个集成阶段要进行特定的集成测试，以证明所集成的要素之间交互的正确性。

按照GB/T XXXXX-5和GB/T XXXXX-6充分完成硬件和软件开发后，按照第8章（相关项集成和测试）的系统集成可以启动。

8.3 本章的输入

8.3.1 前提条件

应具备下列信息：

——安全目标，按照 GB/T XXXXX-3，7.5.2；

——功能安全概念，按照 GB/T XXXXX-3，8.5.1；

——相关项集成与测试计划，按照 5.5.3；

——技术安全概念，按照 7.5.1；

——系统设计规范，按照 7.5.2；及

——硬件软件接口规范（HSI），按照 7.5.6。

8.3.2 支持信息

可考虑下列信息：

——整车架构（来自外部）；

——其它车辆系统的技术安全概念（来自外部）；及

——安全分析报告（参见 7.5.6）。

8.4 要求和建议

8.4.1 集成和测试的计划与定义

8.4.1.1 为证明系统设计符合功能和技术安全要求，应按照 GB/T XXXXX-8 第 9 章执行集成测试活动。

注：下列测试目标参见表4到表18：

a) 功能安全要求和技术安全要求的正确实施；

b) 安全机制的正确的功能表现、准确性和时序；

c) 接口实现的一致性与正确性；

d) 安全机制的诊断或失效覆盖的有效性；及

e) 鲁棒性水平。

8.4.1.2 应基于系统设计规范、功能安全概念、技术安全概念、相关项集成与测试计划，定义集成和测试策略，提供测试目标被充分覆盖的证据。该策略应覆盖电子电气要素以及在安全概念中考虑的其它技术要素。

注：通常集成层面包括软硬件、系统及整车层面。

8.4.1.3 为使系统集成子阶段能够进行，应执行：

a) 应细化集成与测试计划以用于软硬件集成与测试；
b) 应细化相关项集成与测试计划以包含系统及整车层面的集成测试规范。应确保来自于软硬件验证的未解决问题得到描述。
c) 系统及整车层面的相关项集成与测试计划应考虑车辆子系统（与该相关项相关的内部与外部）与环境之间的接口。

注1：当制定整车层面相关项集成与测试计划时，可考虑车辆在典型和极端车辆状况和环境条件下的正确行为，但应组成一个充分的子集（参见表 4）。

注2：在软硬件集成层面和相关项层面上进行的集成与测试计划，要考虑软硬件间的接口及其交互。

8.4.1.4 如果系统使用了配置或标定数据，在系统或整车层面的验证应为在应用层面的每个配置或用于量产的每个配置提供满足安全要求的证据。

注：如果在系统或整车层面每个配置的完整验证是不可行的，则可选择一个合理的子集。

8.4.1.5 测试设备应服从质量监控体系的控制。

8.4.1.6 在整个集成子阶段，每个功能和技术安全要求应至少进行一次验证（如果可以通过测试来验证的话）。

注1：一个常规的做法是在更高一级的集成层面上对已定义的安全要求进行验证。

注2：集成测试期间识别出的安全异常要按照 GB/T XXXXX-2，5.4.2.的要求进行报告。

8.4.1.7 为了恰当的定义集成测试的测试案例，应考虑集成的层面，使用表 4 中所列的恰当的方法组合导出测试用例。

表 4 导出集成测试案例的方法

方法		功能安全完整性等级			
		A	B	C	D
1a	需求分析	++	++	++	++
1b	外部和内部接口分析	+	++	++	++
1c	软硬件集成等价类的生成和分析	+	+	++	++
1d	边界值分析	+	+	++	++
1e	基于知识或经验的错误猜测法	+	+	++	++
1f	功能的相关性分析	+	+	++	++
1g	相关失效的共有限制条件、次序及来源分析	+	+	++	++
1h	环境条件和操作用例分析	+	++	++	++
1i	现场经验分析	+	++	++	++

8.4.2 **硬件-软件集成和测试**

8.4.2.1 硬件-软件集成

8.4.2.1.1 应对按照 GB/T XXXXX-5 开发的硬件和按照 GB/T XXXXX-6 开发的软件进行集成，作为表 4 至 8 中测试活动的对象。

8.4.2.1.2 按照 4.3，该要求适用于 ASIL C 和 D：应以适当的覆盖率测试硬件-软件接口（HSI）要求，同时考虑 ASIL 等级或应给出没有关于 HSI 遗留问题的理由。

注：首选使用用于生产的硬件和软件。如必要，特定测试技术可以使用修改的硬件或者软件。

8.4.2.2 硬件-软件测试中的测试目标和测试方法

8.4.2.2.1 为了发现系统设计中的系统故障，在软硬件集成过程中，由 8.4.2.2.2 至 8.4.2.2.6 得出的测试目标，应使用对应表中给出的充分的测试方法来实现。

注：基于系统已实施的功能、功能复杂性或分布特性，如有足够的理由，将测试方法转移到其它集成的子阶段可能是合理的。

8.4.2.2.2 技术安全要求在硬件-软件层面的正确的执行，应通过使用表 5 中给出的可行的测试方法进行论证。

表 5 - 技术安全要求在硬件-软件层面的正确执行

方法		功能安全完整性等级			
		A	B	C	D
1a	基于需求的测试[a]	++	++	++	++
1b	故障注入测试[b]	+	++	++	++
1c	背靠背测试[c]	+	+	++	++

[a] 基于需求的测试是指针对功能性和非功能性要求的测试。

[b] 故障注入测试使用特殊的方法向运行中的测试对象注入故障。这可以通过特殊的测试接口在软件中完成，或通过特殊准备的硬件完成。该方法经常用于提高安全要求的测试覆盖率，因为在正常运行中安全机制不会被调用。

[c] 背靠背测试对比测试对象和仿真模型对相同激励的反应，以发现模型和其实现的表现差异。

注：5和表10 的条目1b的工作量的差异，是由系统层的故障注入测试的工作量引起的。

8.4.2.2.3 按照 4.3，该要求适用于 ASIL (A)、B、C 和 D：安全机制在硬件-软件层的正确功能性能、准确性和时序应使用表 6 中给出的可行的测试方法进行论证。

表 6 -安全机制在硬件-软件层的正确功能性能、准确性和时序

方法		功能安全完整性等级			
		A	B	C	D
1a	背靠背测试[a]	+	+	++	++
1b	性能测试[b]	+	++	++	++

[a] 背靠背测试对比测试对象和仿真模型对相同激励的反应，以发现模型和其实施的行为差异。

[b] 性能测试可验证在整个测试对象环境中的性能（如任务调度、时序、功率输出），也可验证目标控制软件与硬件同时运行的能力。

8.4.2.2.4 按照 4.3，该要求适用于 ASIL (A)、B、C 和 D：外部和内部接口在硬件-软件层执行的一致性和正确性应使用表 7 中给出的可行的测试方法进行论证。

表 7 -外部和内部接口在硬件-软件层执行的一致性和正确性

方法	功能安全完整性等级			
	A	B	C	D

1a	外部接口测试 [a]	+	++	++	++
1b	内部接口测试 [a]	+	++	++	++
1c	接口一致性检查 [a]	+	++	++	++
[a] 测试对象的接口测试包括模拟和数字输入输出的测试、边界测试和等价类测试，用来完整的测试被测对象的特定接口、兼容性、时序及其它特定等级。ECU 内部接口的测试，可以用静态测试检测软件和硬件兼容性，也可用动态测试检测串行外设接口（SPI）或集成电路（IC）通信或 ECU 其它要素间任意接口。					

8.4.2.2.5 按照 4.3，该要求适用于 ASIL (A)、（B）、C 和 D：针对故障模型，硬件失效探测机制在硬件-软件层面的诊断覆盖率的有效性，应使用表 8 中给出的可行的测试方法进行论证。

注：参考的故障模型，见GB/T XXXXX-5，附录D。

表 8 -安全机制在硬件-软件层面的诊断覆盖率的有效性

方法		功能安全完整性等级			
		A	B	C	D
1a	故障注入测试 [a]	+	+	++	++
1b	错误猜测法测试 [b]	+	++	++	++
[a] 故障注入测试使用特殊的方法向运行中的测试对象注入故障。这可以通过特殊的测试接口在软件中完成，或通过特殊准备的硬件完成。该方法经常用于提高安全要求的测试覆盖率，因为在正常运行中安全机制不会被调用。 [b] 错误猜测法测试使用专家知识和经验教训中收集的数据来预测被测对象的错误。然后设计一组包括适当的测试设备的测试以检查这些错误。如果测试者有相似测试对象的经验时，错误猜测法是一种有效的方法。					

8.4.2.2.6 按照 4.3，该要求适用于 ASIL (A)、(B)、(C)和 D：要素在硬件-软件层的鲁棒性水平，应使用表 9 中给出的可行的测试方法进行论证。

表 9 - 在硬件-软件层的鲁棒性水平

方法		功能安全完整性等级			
		A	B	C	D
1a	资源使用测试 [a]	+	+	+	++
1b	压力测试 [b]	+	+	+	++
[a] 资源使用测试可静态的完成（如：通过检查编码量或分析关于中断使用的编码，目的是验证最恶劣案例的情况不会耗尽资源），或通过运行监控来动态的完成。 [b] 压力测试验证测试对象在高运行负荷或高环境要求下的正确运行。因此，测试可以通过施加高负荷、或异常的接口负荷、或一些值（总线负载、电击等）完成，也可以是极限的温度、湿度或机械冲击测试。					

8.4.3 系统集成和测试

8.4.3.1 系统集成

8.4.3.1.1 组成系统的各个要素应按照系统设计进行集成，并按照系统集成测试和 GB/T XXXXX-5 和 GB/T XXXXX-6 中规定的系统集成测试进行测试。

注：测试目的是提供证据证明各个系统要素正确交互，符合技术和功能安全要求，并为没有可能导致违背安全目标的非预期行为提供足够的置信度水平。

8.4.3.2 系统测试中的测试目标和测试方法

8.4.3.2.1 为了发现系统集成过程中的系统性故障，按照 8.4.3.2.2 至 8.4.3.2.6 得出的测试目标，应通过应用对应表中给出的充分的测试方法来进行表述。

注：基于系统已实施的功能、功能复杂性或分布特性，如有足够的理由，将测试方法转移到其它集成的子阶段可能是合理的。

8.4.3.2.2 功能和技术要求在系统层面的正确执行，应通过使用表 10 中给出的可行的测试方法进行论证。

表 10 – 功能安全和技术安全要求在系统层面的正确执行

方法		功能安全完整性等级			
		A	B	C	D
1a	基于需求的测试 [a]	++	++	++	++
1b	故障注入测试 [b]	+	+	++	++
1c	背靠背测试 [c]	o	+	+	++

[a] 基于需求的测试是指针对功能性和非功能性要求的测试。

[b] 故障注入测试使用特殊的方法向系统注入故障。这可以通过特殊的测试接口、或特殊准备的要素、或通讯设备在系统内完成。该方法经常用于提高安全要求的测试覆盖率，因为在正常运行中安全机制不会被调用。

[c] 背靠背测试对比测试对象和仿真模型对相同激励的反应，以发现模型和其实施的行为差异。

8.4.3.2.3 按照 4.3，该要求适用于 ASIL (A)、B、C 和 D：安全机制在系统层的正确功能性能行为、准确性和时序应使用表 11 中给出的可行的测试方法进行论证。

表 11 -安全机制在系统层的正确功能性能行为、准确性和时序

方法		功能安全完整性等级			
		A	B	C	D
1a	背靠背测试 [a]	o	+	+	++
1b	性能测试 [b]	o	+	+	++

[a] 背靠背测试对比测试对象和仿真模型对相同激励的反应，以发现模型和其实施的行为差异。

[b] 性能测试可验证相关系统安全机制的性能（如执行器速度或强度、整个系统的响应时间）。

8.4.3.2.4 外部和内部接口在系统层面执行的一致性和正确性，应使用表 12 中给出的可行的测试方法进行论证。

表 12 - 外部和内部接口在系统层面执行的一致性和正确性

方法		功能安全完整性等级			
		A	B	C	D
1a	外部接口测试 [a]	+	++	++	++
1b	内部接口测试 [a]	+	++	++	++
1c	接口一致性检查 [a]	o	++	++	++
1d	交互/通讯测试 [b]	++	++	++	++

[a] 系统的接口测试包括模拟和数字输入输出的测试、边界测试和等价类测试，用来完整的测试系统的特定接口、兼容性、时序及其它特定参数。系统内部接口的测试，可以用静态测试（如接插件的匹配），也可用总线通信或系统其它要素间任意接口相关的动态测试。

[b] 通讯和交互测试包括系统要素间、及被测系统和车辆其它运行系统间，针对功能性和非功能性要求的通讯测试。

8.4.3.2.5 按照 4.3，该要求适用于 ASIL (A)、(B)、C 和 D：安全机制在系统层面的失效覆盖率的有效性，应使用表 13 中给出的可行的测试方法进行论证。

表 13 – 安全机制在系统层面的失效覆盖率的有效性

方法	功能安全完整性等级

		A	B	C	D
1a	故障注入测试[a]	++	++	++	++
1b	错误猜测法测试[b]	+	+	++	++
1c	来自现场经验的测试	o	+	++	++

[a] 故障注入测试使用特殊的方法向系统注入故障。这可以通过特殊的测试接口、或特殊准备的要素、或通讯设备在系统内完成。该方法经常用于提高安全要求的测试覆盖率，因为在正常运行中安全机制不会被调用。

[b] 错误猜测法测试使用专家知识、经验教训中收集的数据和现场经验预测系统中的错误。然后设计一组包括适当的测试设备的测试以检查这些错误。如果测试者有相似系统的经验时，错误猜测法是一种有效的方法。

8.4.3.2.6 系统层面的鲁棒性水平应使用表 14 中给出的可行的测试方法进行论证。

表 14 – 系统层面的鲁棒性水平

方法		功能安全完整性等级			
		A	B	C	D
1a	资源使用测试[a]	o	+	++	++
1b	压力测试[b]	o	+	++	++
1c	特定环境条件下的抗干扰性和鲁棒性测试[c]	++	++	++	++

[a] 系统层面的资源使用测试通常在动态环境中进行（如：试验室车辆模型（lab car）或原型车）。测试的问题包括功耗和总线负荷。

[b] 压力测试验证在高运行负荷或高环境要求下系统的正确运行。因此，测试可以通过在系统上施加高负荷、或极限的用户输入、或来自于其它系统的极限要求完成，也可以是极限的温度、湿度或机械冲击测试。

[c] 在特定环境条件下的抗干扰性和鲁棒性测试，是一种特殊的压力测试，包括电磁兼容性（EMC）和静电放电（ESD）测试（如：参见[2], [3]）。

8.4.4 整车集成和测试

8.4.4.1 整车集成

8.4.4.1.1 应将相关项集成到整车上，并完成整车集成测试。

8.4.4.1.2 应对相关项与车内通讯网络以及车内供电网络的接口规范进行验证。

8.4.4.2 整车测试期间的测试目标和测试方法

8.4.4.2.1 为了探测整车集成期间的系统故障，由 8.4.4.2.2 至 8.4.4.2.6 得出的测试目标，应使用相应表格中所给出的充分的测试方法来表述。

注：基于相关项已实施的功能、功能复杂性或分布特性，如有足够的理由，将测试方法转移到其它集成的子阶段可能是合理的。

8.4.4.2.2 功能安全要求在整车层面的正确的执行，应通过使用表 15 中给出的可行的测试方法进行论证。

表 15 –功能安全要求在整车层面上的正确执行

方法		功能安全完整性等级			
		A	B	C	D
1a	基于需求的测试[a]	++	++	++	++
1b	故障注入测试[b]	++	++	++	++
1c	长期测试[c]	++	++	++	++
1d	现实生活条件下的用户测试[c]	++	++	++	++

[a] 基于需求的测试是指针对功能性和非功能性要求的测试。

[b] 故障注入测试使用特殊的方法向相关项注入故障。这可以通过特殊测试接口，或者特别准备的要素或通讯设备，在相关

项内部完成。该方法经常用于提高安全要求的测试覆盖率，因为在正常运行中安全机制不会被调用。

[c]长期测试和现实生活条件下的用户测试，类似于来自现场经验的测试，但使用更大的样本量，将普通用户当作测试者，并不局限于之前规定的测试场景，而是在日常生活现实条件下执行。为确保测试人员的安全，如果有必要，这类测试会有限制，例如带有额外的安全措施或者非使能的执行器。

8.4.4.2.3 按照 4.3，该要求适用于 ASIL (A)、(B)、C 和 D：安全机制在整车层面的正确功能性能、准确性和时序应使用表 16 中给出的可行的测试方法进行论证。

表 16-安全机制在整车层面的正确功能性能,准确性和时序

方法		功能安全完整性等级			
		A	B	C	D
1a	性能测试[a]	+	+	++	++
1b	长期测试[b]	+	+	++	++
1c	现实生活条件下的用户测试[b]	+	+	++	++

[a] 性能测试可以验证有关相关项的安全机制的性能(例如:故障出现时的容错时间区间和车辆的可控性)。

[b]长期测试和现实生活条件下的用户测试，类似于来自现场经验的测试，但使用更大的样本量，将普通用户当作测试者，并不局限于之前规定的测试场景，而是在日常生活现实条件下执行。为确保测试人员的安全，如果有必要，这类测试会有限制，例如带有额外的安全措施或者非使能（停用、禁用）的执行器。

8.4.4.2.4 按照 4.3，该要求适用于 ASIL (A)、(B)、C 和 D：整车层面外部接口实现的一致性和正确性应使用表 17 中给出的可行的测试方法进行论证。

表 17-整车层面内外部接口实现的一致性和正确性

方法		功能安全完整性等级			
		A	B	C	D
1a	外部接口的测试[a]	o	+	++	++
1b	交互和通讯的测试[b]	o	+	++	++

[a] 整车层面的接口测试，是对整车系统接口的兼容性测试。这些测试可以通过验证值域，额定值或者几何尺寸静态的完成，也可以在整车运行过程中动态的完成。

[b] 通讯和交互测试包括车辆系统在运行期间内的针对功能和非功能要求的通讯测试。

8.4.4.2.5 按照 4.3，该要求适用于 ASIL(A), (B), C 和 D：安全机制在整车层面的失效覆盖率的有效性应使用表 18 中给出的可行的测试方法进行论证。

表 18-安全机制在整车层面的失效覆盖率的有效性

方法		功能安全完整性等级			
		A	B	C	D
1a	故障注入测试[a]	o	+	++	++
1b	错误猜测法测试[b]	o	+	++	++
1c	来自现场经验的测试[c]	o	+	++	++

[a] 故障注入测试使用特殊的方法向车辆注入故障。这可以通过特殊测试接口，或者特别准备的硬件或通讯设备，在车辆内部完成。该方法经常用于提高安全要求的测试覆盖率，因为在正常运行中安全机制不会被调用。

[b] 错误猜测法测试使用专家知识和经验教训中收集的数据来预测整车错误。然后设计一组包括适当的测试设备的测试以检查这些错误。如果测试者有相似车辆的应用经验时，错误猜测法是一种有效的方法。

[C] 来自现场经验的测试采用从现场收集到的经验和数据。错误的车辆行为或者新发现的运行工况可以得到分析，并针对这些新发现设计一组测试检查车辆。

8.4.4.2.6 按照 4.3，该要求适用于 ASIL(A)，(B)，C 和 D：整车层面的鲁棒性水平应使用表 19 中给出的可行的测试方法进行论证。

表 19-整车层面的鲁棒性水平

方法		功能安全完整性等级			
		A	B	C	D
1a	资源使用测试[a]	o	+	++	++
1b	压力测试[b]	o	+	++	++
1c	特定环境条件下的抗干扰性和鲁棒性测试[c]	o	+	++	++
1d	长期测试[d]	o	+	++	++

[a] 相关项层面的资源使用测试通常在动态环境中进行（如：试验室车辆模型（lab car）或原型车）。测试的问题包括相关项内部资源、功率消耗或者其它整车系统的有限资源。

[b] 压力测试验证在高运行负荷或高环境要求下整车的正确运行。因此，测试可以通过在整车上施加高负荷、或极限的用户输入、或来自于其它系统的极限要求完成，也可以是极限的温度、湿度或机械冲击测试。

[c] 在特定环境条件下的抗干扰性和鲁棒性测试，是一种特殊的压力测试，包括电磁兼容性（EMC）和静电放电（ESD）测试（如：参见[2]，[3]）

[d] 长期测试和现实生活条件下的用户测试，类似于来自现场经验的测试，但使用更大的样本量，将普通用户当作测试者，并不局限于之前规定的测试场景，而是在日常生活现实条件下执行。

8.5 工作成果

8.5.1 相关项集成和测试计划（细化的），由 8.4.1 的要求得出。

8.5.2 集成测试规范，由 8.4.1 的要求得出。

8.5.3 集成测试报告，由 8.4.2，8.4.3 和 8.4.4 的要求得出。

9 安全确认

9.1 目的

第一个目的是提供符合安全目标和功能安全概念适合相关项的功能安全的证据。

第二个目的是提供在整车层面的安全目标正确、完整且得到完全实现的证据。

9.2 总则

前述验证活动（如：设计验证、安全分析、硬件集成和测试、软件集成和测试、相关项的集成和测试）的目的是提供每项特定活动的结果符合规定要求的证据。

对典型车辆上所集成的相关项的确认，目的是为预期使用的恰当性提供证据并确认安全措施对一类或一组车辆的充分性。安全确认基于检查和测试，确保安全目标足够且得到实现。

9.3 本章的输入

9.3.1 前提条件

应具备下列信息：

——危害分析和风险评估，按照 GB/T XXXXX-3，7.5.1；

——安全目标，按照 GB/T XXXXX-3，7.5.2；及

——功能安全概念，按照 GB/T XXXXX-3，8.5.1。

9.3.2 支持信息

可考虑下列信息：

——项目计划（细化的）（参见 5.5.1）；

——技术安全概念（参见 7.5.1）；

——功能概念（来自外部）；及

——相关项的集成和测试计划（细化的）（参见 8.5.1）；

——安全分析报告（参见 7.5.6）。

9.4 要求和建议

9.4.1 确认环境

9.4.1.1 应确认典型车辆上所集成的相关项的安全目标。

注：如适用，集成的相关项包括：系统、软件、硬件、其它技术要素和外部措施。

9.4.2 确认的计划

9.4.2.1 应细化确认计划，包括：

a) 待确认的相关项配置，包括其标定数据，按照 GB/T XXXXX-6，附录 C；

注：如果对于每个相关项配置的完整确认是不可行的，那么可选择合理的子集。

b) 确认流程、测试案例、驾驶操作和接受准则的定义；及

c) 设备和要求的环境条件。

9.4.3 确认的执行

9.4.3.1 如果测试用于确认，那么可应用与验证测试（参见 GB/T XXXXX-8，9.4.2 和 9.4.3）相同的要求。

9.4.3.2 应在整车层面确认相关项的安全目标，通过评估：

a) 可控性；

注：使用运行场景确认可控性，包括预期用途和可预见的误用。

b) 用于控制随机失效和系统失效的安全措施的有效性；

c) 外部措施的有效性；及

d) 其它技术要素的有效性。

9.4.3.3 此要求适用于安全目标的 ASILs (B), C 和 D：应在相关项层面实施随机硬件失效度量的确认，为了：

a) 在 GB/T XXXXX-5，第 9 章中确定的由于随机硬件失效违背安全目标的评估，与 7.4.4.3 定义的目标值相比较；及

b) 按照 GB/T XXXXX-5，第 8 章的评估准则对硬件架构度量进行评估，与 7.4.4.2 定义的目标值相比较。

注：在GB/T XXXXX-5，9.4.2和9.4.3中定义了相关项要素的定量评估。假如相关项中涉及其它技术，则定性评估整个相关项。

9.4.3.4 基于安全目标，在整车层面确认功能安全要求和预期用途应**按计划**执行，**使用**：

基于安全目标、功能安全要求和预期用途，整车层面的确认应按计划执行，使用：

a) 包括详细的通过/未通过准则的每个安全目标的确认流程和测试案例；及

b) 应用范围。可包括例如配置、环境条件、驾驶场景和操作用例等。

注：可创建操作用例，以助于将安全确认集中在整车层面上。

9.4.3.5 应使用以下方法的适当组合：

a) 已定义了测试流程、测试案例和通过/未通过准则的可重复性测试。

示例1：功能和安全要求的正向测试、黑盒测试、仿真，边界条件下的测试、故障注入、耐久测试、压力测试、高加速寿命测试、外部影响模拟。

b) 分析；

示例2：FMEA、FTA、ETA、仿真。

c) 长期测试，例如车辆驾驶日程安排和受控测试车队。

d) 现实生活条件下的用户测试、抽测或盲测、专家小组；及

e) 评审。

9.4.4 评估

9.4.4.1 应对确认结果进行评估。

9.5 工作成果

9.5.1 确认计划（细化的），由 9.4.2 的要求得出。

9.5.2 确认报告，由 9.4.3 和 9.4.4 的要求得出。

10 功能安全评估

10.1 目的

本章中所列要求的目的是评估相关项所实现的功能安全。

10.2 总则

负责功能安全的组织（如：整车厂或供应商，如果后者负责功能安全）启动功能安全评估。

10.3 本章的输入

10.3.1 前提条件

应具备下列信息：

——安全档案，按照 GB/T XXXXX-2, 6.5.3；

——安全计划（细化的），按照 5.5.2，GB/T XXXXX-5, 5.5.2 和 GB/T XXXXX-6；

——认可措施报告，按照 GB/T XXXXX-2, 6.5.5；

——审核报告（如有），按照 GB/T XXXXX-2, 6.5.4；及

——功能安全评估计划（细化的），按照 5.5.5。

10.3.2 支持信息

无。

10.4 要求和建议

10.4.1 该要求适用于安全目标 ASILs(B), C 和 D：对于 GB/T XXXXX-2 图 2 中的安全生命周期各步骤，应识别功能安全评估的具体议题。

10.4.2 该要求适用于安全目标 ASILs(B), C 和 D：应根据 GB/T XXXXX-2，6.4.9(功能安全评估)开展功能安全评估。

10.5 工作成果

10.5.1 功能安全评估报告，由 10.4.1 和 10.4.2 的要求得出。

11 生产发布

11.1 目的

11.1.1 本章的目的是定义相关项开发完成后生产发布的准则。生产发布确认了相关项在整车层面满足功能安全要求。

11.2 总则

11.2.1 生产发布确认相关项已做好量产和运行的准备。

11.2.2 满足量产前提条件的证据由以下提供：

——完成硬件、软件、系统、相关项及整车层面开发过程中的验证和确认；及
——成功通过整体功能安全评估。

11.2.3 发布的文件是零部件、系统或整车生产的基础，并由负责发布的人员签字。

11.3 本章的输入

11.3.1 前提条件

应具备下列信息：

——功能安全评估报告，按照 10.5.1；及
——安全档案，按照 GB/T XXXXX-2, 6.5.3。

11.3.2 支持信息

无。

11.4 要求和建议

11.4.1 生产发布

11.4.1.1 如果适用（视 ASIL 等级而定），只有具备 11.3.1 所列的工作成果才能批准相关项的生产发布，为功能安全提供信心。

11.4.2 生产发布文件

11.4.2.1 功能安全生产发布文件应包含下面的信息：

a) 负责发布人员的名字和签名；
b) 所发布相关项的版本；
c) 所发布相关项的配置；
d) 参考的相关文件信息；及
e) 发布日期。

注：功能安全文件可以是相关项生产发布文件的一部分或是一个独立的文件。

11.4.2.2 生产发布时，应具备软件和硬件的基线，并应依据 GB/T XXXXX-8, 第 10 章进行文档记录。

11.4.2.3 应根据 GB/T XXXXX-2, 5.4.2 和 GB/T XXXXX-8，第 8 章处理识别出的安全异常。

11.5 工作成果

11.5.1 生产发布报告，由 11.4.1 和 11.4.2 的要求得出。

附 录 A
（资料性附录）

产品开发系统层面的概览和文档流

表A.1提供了产品开发系统层面特定子阶段的目的、前提条件和工作成果的概览。

表 A.1 — 产品开发系统层面概览

条目	目的	前提条件	工作成果
5 启动产品开发的系统层面	启动系统层面产品开发的目的是确定并计划系统各子阶段开发过程中的功能安全活动，也包括在GB/T XXXXX-8中所描述的必要的支持过程。 系统层面安全活动的计划包含在安全计划中。	项目计划(细化的)，(参见 GB/T XXXXX-2 中 6.5.)； 安全计划（参见按照 GB/T XXXXX-2 中 6.5.1）； 功能安全概念(参加按照 GB/T XXXXX-3中8.5.1)	5.5.1项目计划（细化的） 5.5.2安全计划 （细化的） 5.5.3相关项集成和测试计划 5.5.4验证计划 5.5.5 功能安全评估计划（细化的）
6技术安全要求的定义	该子阶段的第一个目的是制定技术安全要求 技术安全需求规范同时考虑功能概念和初步的架构设想（参见 GB/T XXXXX-3)，从而进一步细化功能安全概念。 第二个目的是通过分析来验证技术安全要求符合功能安全要求。	功能安全概念（参见 GB/T XXXXX-3，8.5.1） 确认计划（参见 5.5.4）	6.5.1 技术安全需求规范 6.5.2 系统验证报告 6.5.3 确认计划（细化的）
7系统设计	该子阶段的第一个目的是开发系统设计和技术安全概念，以满足相关项的功能要求和技术安全需求规范。 该子阶段的第二个目的是验证系统设计和技术安全概念满足技术安全要求规范	相关项集成和测试计划（参见5.5.3） 技术安全需求规范(参见 6.5.1）	7.5.1技术安全概念 7.5.2 系统设计规范 7.5.3硬件-软件接口规范(HSI) 7.5.4 生产、运行、维护和报废要求的定义 7.5.5 系统验证报告(细化的） 7.5.6 安全分析报告，由 7.4.3 的要求得出
8相关项集成和测试	集成和测试阶段包括三个阶段和两个主要目标描述如下： 第一个阶段是相关项所包含的每一个要素的软硬件集成 第二个阶段是构成一个完整系统的一个相关项的所有要素的集成	安全目标（参见 GB/T XXXXX-3, 7.5.2） 功能安全概念（参见 GB/T XXXXX-3, 8.5.1） 相关项集成和测试计划（参见 5.5.3） 技术安全概念（参见	8.5.1 相关项集成和测试计划（细化的） 8.5.2 集成测试规范 8.5.3 集成测试报告

	第三个阶段是相关项与车辆上其它系统的集成以及与整车的集成 集成过程的第一个目标是测试每一条安全要求是否满足规范以及 ASIL 级别要求。 第二个目标是验证涵盖安全要求的“系统设计”【参见第 7 章（系统设计）】在整个相关项上得到正确实施。	7.5.1） 系统设计规范（参见 7.5.2） 硬件-软件接口规范 (HSI) (参见 7.5.3)	
9安全确认	第一个目标是提供符合安全目标和功能安全概念适合相关项的功能安全的证据 第二个目标是提供证据表明在车辆层面上完全实现安全目标是正确的。 第二个目标是提供在整车层面的安全目标正确、完整且得到完全实现的证据	危害分析和风险评估(参见 GB/T XXXXX-3, 7.5.1) 安全目标（参见 GB/T XXXXX-3, 7.5.2） 功能安全概念（参见 GB/T XXXXX-3, 8.5.1） 验证计划（细化的）（参见 6.5.3）	9.5.1 确认计划（细化的），由 9.4.2 的要求得出。 9.5.2 确认报告，由 9.4.3 和 9.4.4 的要求得出。
10功能安全评估	本章中所列要求的目的是评估相关项所实现的功能安全。	安全档案（参见 GB/T XXXXX-2, 6.5.3） 安全计划（细化的）（见 5.5.2, GB/T XXXXX-5, 5.5.2 和 GB/T XXXXX-6, 5.5.2） 认可评审报告（参见 GB/T XXXXX-2, 6.5.5） 审核报告（如有）（参见 GB/T XXXXX-2, 6.5.5） 功能安全评估计划（细化的）（见 5.5.5）	10.5.1 功能安全评估报告，由 10.4.1 至 10.4.2 要求得出。
11生产发布	本章的目的是定义相关项开发完成后生产发布的准则 生产发布确认了相关项在整车层面满足功能安全要求	功能安全评估报告（参见 10.5.1） 安全档案（参见 GB/T XXXXX-2, 6.5.3）	11.5.1 生产发布报告，由 11.4.1 和 11.4.2 的要求得出。

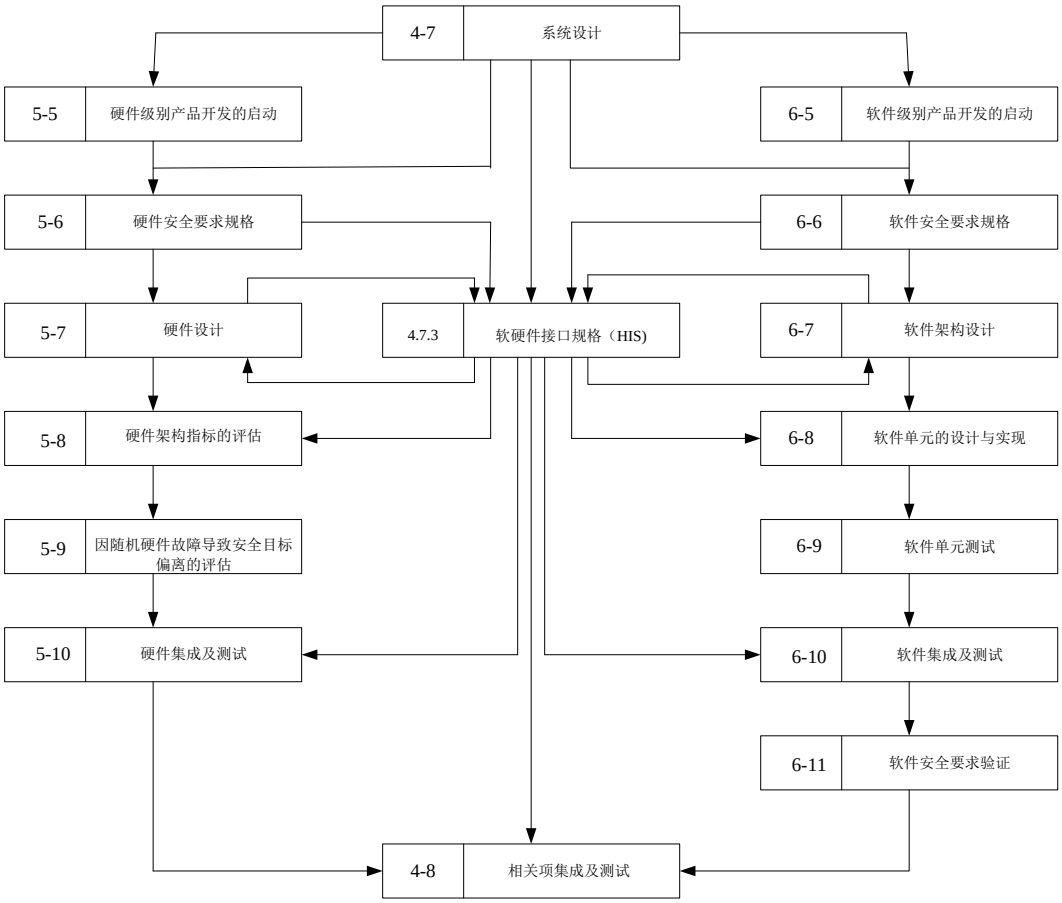
附 录 B
（资料性附录）

软硬件接口内容示例

B.1 本附录提供了有关软硬件接口更进一步的解释。

软硬件接口在GB/T XXXXX本部分“系统设计”子阶段中有详细定义。随着开发在硬件开发(GB/T XXXXX-5)和软件开发(GB/T XXXXX-6)子阶段的继续，软硬件接口规范要得到细化。

首先,图B.1的概述提供了产品在系统层面、软硬件层面的开发和软硬件接口作用之间的关系。软硬件接口起到了连接不同开发阶段的作用。软硬件接口用于在软硬件开发均相关的问题上达成共识。



注：在该图中，GB/T XXXXX的各个部分的具体章节以下列方式表示： “m-n”，其中“m”表示部分号，“n”表示章节号，例如“3-6”表示GB/T XXXXX-3的第6章。

图 B.1 -软硬件接口交互概述

其次，为了更容易定义软硬件接口，要提供一份典型软硬件接口要素的列表，以及一份应用于软硬件接口要素的执行特性的非穷尽列表。

B.2 在定义软硬件接口的时候可考虑以下软硬件接口要素：

a) 存储器
   1) 易失性存储器（如：RAM）；
   2) 非易失性存储器（如：NvRAM）；
b) 总线接口[如：控制器局域网络(CAN)，局域互联网(LIN),内部高速串行链路(HSSL)]；
c) 转换器：
   1) 模/数转换器；
   2) 数/模转换器；
   3) 脉冲宽度调制（PWM）；
d) 多路转换器；
e) 电气输入/输出；
f) 看门狗：
   1) 内部；
   2) 外部。

B.3 在定义软硬件接口时可考虑以下软硬件接口特性：

a) 中断；
b) 时序一致性；
c) 数据完整性；
d) 初始化：
   1) 存储器及寄存器；
   2) 引导管理；
e) 信息传输：
   1) 发送信息；
   2) 接收信息；
f) 网络模式；
   1) 睡眠；
   2) 唤醒；
g) 存储器管理
   1) 读；
   2) 写；
   3) 诊断；
   4) 地址空间；
   5) 数据类型；
h) 实时计数器：
   1) 启动计数器；
   2) 停止计数器；
   3) 冻结计数器；
   4) 加载计数器

表 B.1 提供的示例有助于把软硬件接口特性分配给软硬件接口要素。

表 B.1 内部信号的输入示例

描述	硬件标识符	软件标识符	通道 1	通道 2	多路转换器通道 1	多路转换器通道 2	数据类型硬件接口	地址通道 1	地址通道 2	单位	接口类型	注解	值域	精度（值域%）
输入														
输入 1	IN_1	IN_1	X		4		U16	0x8000		v	模拟-内部	模拟输入 1	0 to 5	0.50 %