ICS 43.040
CCS T 35

中华人民共和国国家标准

GB/T 34590.4—XXXX
代替 GB/T 34590.4-2017

道路车辆 功能安全 第4部分：产品开发：系统层面

Road vehicles—Functional safety—Part4：Product development at the system level

(ISO 26262-4:2018,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。

本部分为GB/T 34590-XXXX的第4部分。

本部分按照GB/T 1.1-2020给出的规则起草。

本部分代替GB/T 34590.4-2017《道路车辆 功能安全 第4部分：产品开发：系统层面》，与GB/T 34590.4-2017相比，除结构调整和编辑性改动外，主要技术变化如下：

——修改了标准使用范围，由“量产乘用车”扩大到“除轻便摩托车外的量产道路车辆”；
——新增了对商用车辆的相关要求和示例、对摩托车的适应性要求等；
——修改了第 5 章的内容，由“启动系统层面产品开发”修改为“系统层面产品开发的概述”（见第 5 章）；
——修改了第 5 章的目的（见 5.1）；
——删除了第 5 章本章的输入、要求和建议、工作成果等内容（见 2017 版的 5.3、5.4、5.5）；
——整合了 2017 版第 6 章和第 7 章的内容，对技术安全概念阶段的开发目的做了细化（见 6.1，2017 版的 6.1、7.1）；
——修改了对技术安全要求的描述，更改为对技术安全概念的描述（见 6.2）；
——修改了“技术安全要求”的定义要求（见 6.4.4.1）；
——修改了安全机制的定义要求（见 6.4.2）；
——删除了 ASIL 分解对应的内容（见 2017 版的 6.4.3）；
——新增了系统架构设计中安全分析的目的（见 6.4.4.1）；
——删除了模块化系统设计的属性等相关内容及表表格（见 6.4.4.6，2017 版的 7.4.3.7）
——修改了关于生产、服务、运行和报废的相关概念（见 6.4.8.1）；
——删除了系统设计的验证相关内容及表格（见 2017 版的 7.4.8）；
——新增了系统阶段认证的相关内容及要求（见 6.4.9.2）；
——修改了集成和测试的子阶段和目标（见 7.1）；
——删除了集成和测试策略中的“安全机制的诊断或失效覆盖的有效性”的描述（见 7.4.1.1）；
——修改了系统层面和整车层面关于“安全机制的诊断或失效覆盖的有效性”的内容（见表 10，表 14）；

——修改了安全确认的目的（见 8.1）；

——新增了安全确认的环境（见 8.4.1）；

——修改了确认的计划的描述，变更为安全确认的规范（8.4.2）；

——删除了相关项层面实施随机硬件失效度量的确认（见 2017 版的 9.4.3.3）；

——删除了功能安全评估、生产发布两个章节（见 2017 版的第 10 章、第 11 章）

本部分使用重新起草法修改采用了ISO 26262-4：2018 《道路车辆 功能安全第4部分：产品开发：系统层面》。

本部分与ISO 26262-4：2018的技术性差异及其原因如下：

——关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第 2 章“规范性引用文件”中，具体调整如下：

- 用修改采用国际标准的GB/T 34590.2-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 26262-3：2018；
- 用修改采用国际标准的GB/T 34590.5-XXXX代替ISO 26262-5：2018；
- 用修改采用国际标准的GB/T 34590.6-XXXX代替ISO 26262-6：2018；
- 用修改采用国际标准的GB/T 34590.7-XXXX代替ISO 26262-7：2018；
- 用修改采用国际标准的GB/T 34590.8-XXXX代替ISO 26262-8：2018；
- 用修改采用国际标准的GB/T 34590.9-XXXX代替ISO 26262-9：2018；

——修改了 5.2 中关于进行安全确认以提供与安全目标和接受准则相关的功能安全证据的要求；

——7.3.1 中增加了关于安全准则的表述；

——8.1 的列项 a）中增加了关于安全准则的表述。

本标准做了下列编辑性修改：

——将国际标准中的“本国际标准”改为“本标准”；

——删除国际标准的前言；

——修改国际标准的引言及其表述。

本标准由中华人民共和国工业和信息化部提出。

本标准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：

本文件所代替文件的历次版本发布情况为：

——GB/T 34590.4,2017 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。

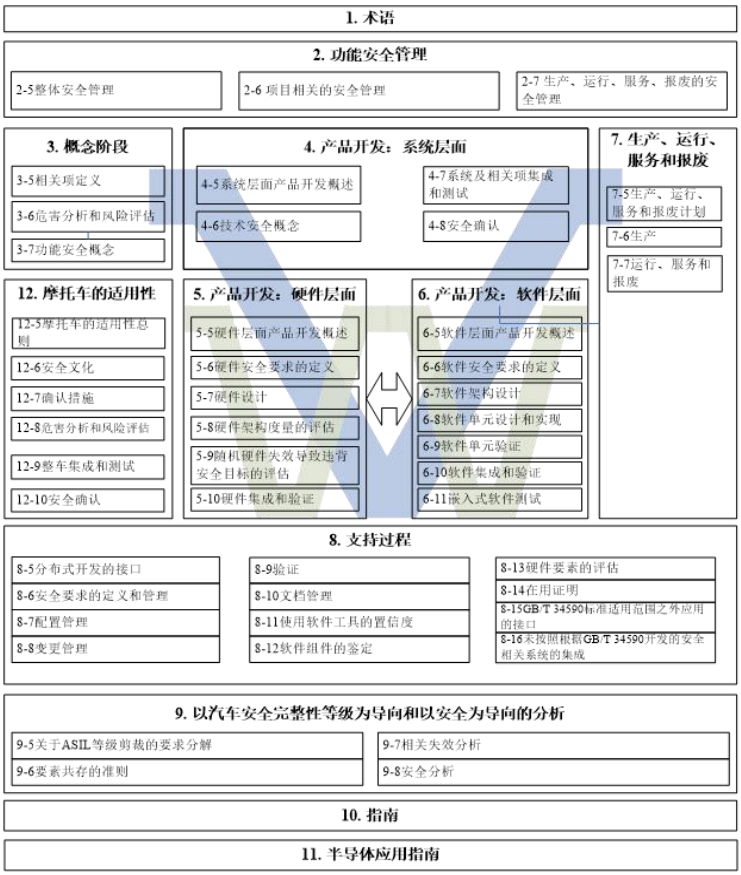


图1　GB/T 34590-XXXX 概览

道路车辆 功能安全 第4部分：产品开发：系统层面

1 范围

GB/T 34590的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总则；

——技术安全要求的定义；

——技术安全概念；

——系统架构设计；

——相关项集成和测试；

——安全确认；

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。

本文件不针对电气/电子系统的标称性能。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 34590.1-XXXX 道路车辆 功能安全 第1部分：术语(ISO 26262-1:2018,MOD)

GB/T 34590.2-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 34590.5-XXXX 道路车辆 功能安全 第5部分：产品开发：硬件层面(ISO 26262-5:2018,MOD)

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

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

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

GB/T 34590.9-XXXX 道路车辆 功能安全 第9部分：以汽车安全完整性等级为导向和以安全为导向的分析(ISO 26262-9:2018,MOD)

3 术语、定义和缩略语

GB/T 34590.1-XXXX界定的术语、定义和缩略语适用于本文件。

4 要求

4.1 目的

本章规定了：

a) 如何符合 GB/T 34590-XXXX；
b) 如何解释 GB/T 34590-XXXX 中所使用的表格；及
c) 如何解释各章条基于不同的 ASIL 等级的适用性。

4.2 一般要求

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

a) 按照 GB/T 34590.2-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 34590.2-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 表的诠释

本文件中的表是规范性或资料性取决于上下文。在满足相关要求时，表中列出的不同方法有助于置信度水平。表中的每个方法是：

a) 一个连续的条目（在最左侧列以顺序号标明，如 1、2、3）；或
b) 一个选择的条目（在最左侧列以数字后加字母标明，如 2a、2b、2c）。

对于连续的条目，高度推荐和推荐的方法按照ASIL等级推荐予以使用。高度推荐或推荐的方法允许用未列入表中的其它方法替代,此种情况下，应给出满足相关要求的理由。如果可以给出不选择所有条目也能符合相应要求的理由，则不需要对缺省方法做进一步解释。

对于选择性的条目，应按照指定的ASIL等级对这些方法进行适当的组合，而与这些方法在表中是否列出无关。如果所列出的方法对于一个ASIL等级来说具有不同的推荐等级，宜采用具有较高推荐等级的方法。应给出选择组合方法或选择单一方法满足相应要求的理由。

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

对于每种方法，应用相关方法的推荐等级取决于ASIL等级，分类如下：

—— “++”表示对于指定的 ASIL 等级，高度推荐该方法；
—— “+” 表示对于指定的 ASIL 等级，推荐该方法；
—— “o” 表示对于指定的 ASIL 等级，不推荐也不反对该方法。

4.4 基于 ASIL 等级的要求和建议

若无其它说明，对于ASIL A、 B、 C和D等级，应满足每一章条的要求或建议。这些要求和建议参照安全目标的ASIL等级。如果在项目开发的早期对ASIL等级完成了分解，按照GB/T 34590-9第5章的要求，应遵循分解后的ASIL等级。

如果GB/T 34590-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 34590.12要求的摩托车的相关项或要素，GB/T 34590.12的要求替代本部分和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 系统层面产品开发的概述

5.1 目的

本章的目的是提供系统层面产品开发的概览。

5.2 总 则

图2给出了系统开发过程中的必要活动。技术安全概念在迭代过程中被开发出来，其包括技术安全要求和系统架构设计。系统架构建立后，将技术安全要求分配给系统的各要素，如果适用，也可分配给其他技术。此外，技术安全要求需要被细化，增加来自系统架构的包括软硬件接口（HSI）在内的要求。同时，基于架构的复杂程度，子系统的要求可通过迭代得到。

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集成，进行安全确认以提供与安全目标和接受准则相关的功能安全证据。

本部分适用于系统开发。GB/T 34590.5 和 GB/T 34590.6分别提出了针对硬件和软件开发的要求。图3 具有多层集成的系统示例，阐明了如何应用本部分及GB/T 34590.5和GB/T 34590.6。

注1：表A.1提供了对系统层面产品开发中特定子阶段的目标、前提条件和工作成果的概览。

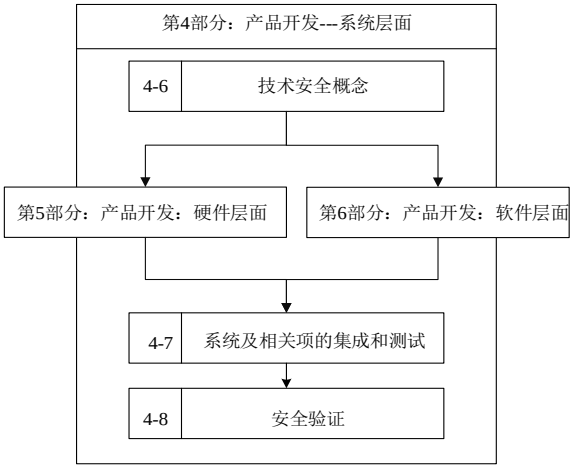


图2 安全相关的相关项开发的参考阶段模型

注2：在图2和图3中，GB/T 34590各部分的具体章用以下方式表示：“m-n”，其中“m”表示该部分的编号，“n”表示该章的编号，如“4-6”表示GB/T 34590.4-XXXX，第6章。

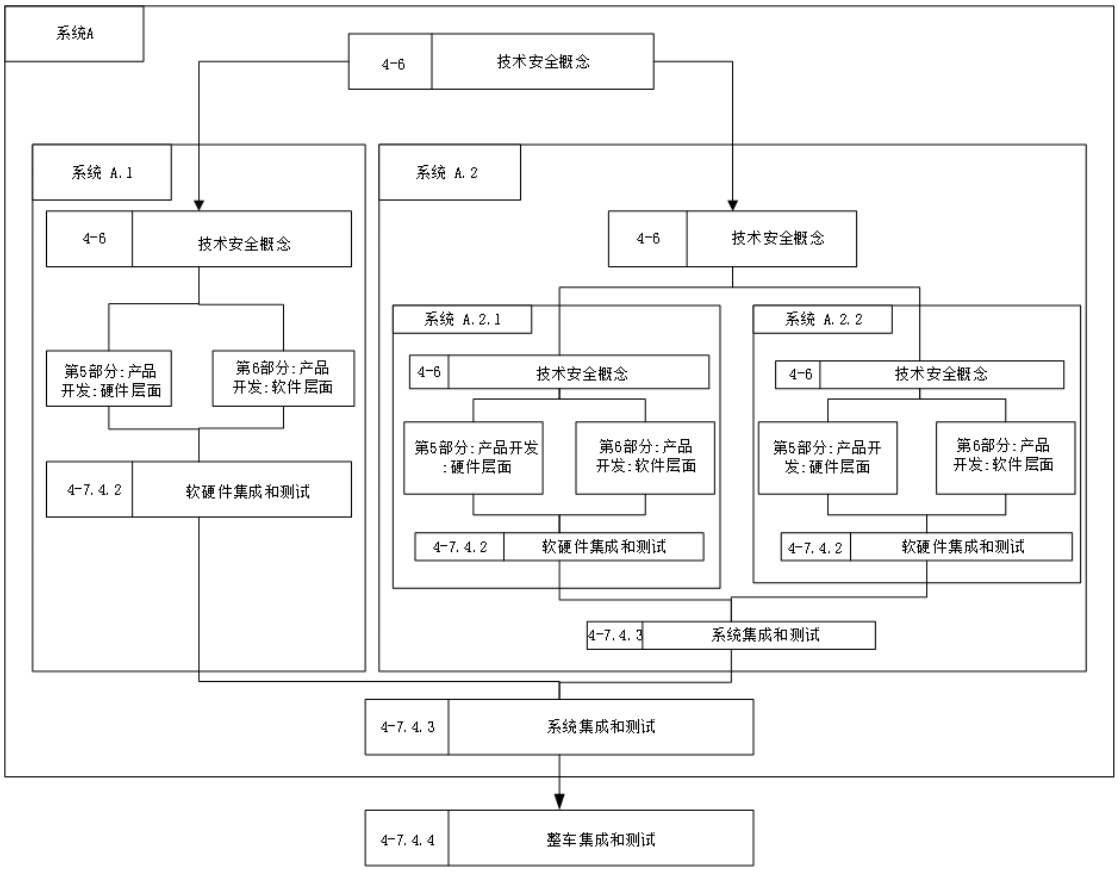


图3　系统层面产品开发示例

注3：关于系统层面产品开发的更多信息详见参考文献[1]和[2]。

6　技术安全概念

6.1　目的

本章目的为：

a)　为实现系统要素和接口的功能、相关性、约束和属性，制定所需的技术安全要求；
b)　为系统要素和接口中将要实施的安全机制，制定技术安全要求；
c)　制定在生产、运行、服务和报废过程中系统及其要素功能安全的相关要求；
d)　验证技术安全要求在系统层面是否符合功能安全要求并与功能安全要求一致；
e)　制定满足安全要求且不与非安全相关要求冲突的系统架构设计和技术安全概念；
f)　分析系统架构设计，以防止故障发生，并导出针对生产和服务必要的安全相关的特殊特性；及
g)　验证系统架构设计和技术安全概念是否满足相应 ASIL 等级的安全要求。

6.2　总则

技术安全概念是技术安全要求及其对应的系统架构设计的集合，提供了系统架构设计适合于满足GB/T 34590.3（包括考虑非安全要求）中所述活动产生的安全要求和设计约束的依据。

技术安全要求规定了功能安全要求在其各自层级上的技术实现；要同时考虑相关项定义和系统架构设计，并述及潜伏失效的探测、故障避免、安全完整性以及运行和服务方面的问题。

系统构架设计是由技术系统实现的所选系统层面解决方案。系统构架设计旨在同时满足所分配的技术安全要求和非安全要求。

系统开发可以迭代执行。

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 34590.3-XXXX,7.5.1;

——系统架构设计（来自外部，见 GB/T 34590.3-XXXX,7.3.1）；及

——其他涉及安全的相关项对此相关项的要求（如果适用）。

示例：泊车辅助系统对制动系统的要求。

注：在分布式开发中，一个技术安全概念可基于由子系统实现的另一个技术安全概念。

6.3.2 支持信息

可考虑下列信息：

——危害分析和风险评估报告（见 GB/T 34590.3-XXXX，6.5.1）；及

——相关项定义(见 GB/T 34590.3-XXXX,5.5.1)。

6.4 要求和建议

6.4.1 技术安全要求的定义

6.4.1.1 技术安全要求应按照功能安全概念、相关项的系统架构设计来定义，考虑如下：

a) 相关项、系统及其要素安全相关的关联性及约束条件；

b) 系统的外部接口，如果适用；及

c) 系统可配置性。

注1：设计约束可能来自于：环境条件、安装空间、实施本身（例如可用性能、热容量、热扩散）以及其他功能或非功能性要求（例如安全性、所用技术的物理限制）。

注2：系统的可配置性由系统要素中的变量、配置数据或标定数据来确定，通常作为将现有系统复用于不同应用的策略的一部分。

6.4.1.2 技术安全要求应定义影响安全要求实现的系统应激响应。 这包括相关激励和失效与每种相关运行模式和定义的系统状态的组合。

示例：如果收到的 ACC 指令信息未通过错误检测代码检查,则制动系统电控单元(ECU)将禁用自适应巡航控制(ACC)制动。

6.4.1.3 除技术安全要求已定义的那些功能外，如果其他功能或要求也由该系统或其要素实现，则应定义这些功能或要求，或者参考其规范。

示例：其他要求可能来自联合国欧洲经济委员会（UN/ECE）法规、美国汽车安全技术法规（FMVSS）、公司平台战略、功能概念或其他概念，例如信息安全概念。

6.4.1.4 技术安全要求和非安全要求不应矛盾。

6.4.2 安全机制

6.4.2.1 技术安全要求应定义安全机制，用于探测故障并防止或减轻出现在系统输出端的违反功能安全要求（见 GB/T 34590.3-XXXX,第 7 章）的失效，包括：

a) 与系统自身故障的探测、指示和控制相关的安全机制；

注1：包括用于探测随机硬件故障及探测系统性故障（如果适用）的系统自身监控。

注2：包括对通讯通道失效（例如：数据接口、通讯总线、无线射频链接）的探测和控制的安全机制。

注3：可以在系统架构适当的层级定义安全机制。

b) 涉及探测、指示和控制与本系统有相互影响的其他外部要素中所发生故障的安全机制；

示例：外部设备包括其他的电控单元、电源或者通讯设备。

c) 使系统实现或者维持在相关项的安全状态的安全机制；

注4：包括来自安全机制的多个控制请求的仲裁。

d) 定义和执行报警和降级策略的安全机制；及

e) 防止故障变为潜伏故障的安全机制。

注5：如同a)到d)，这些安全机制通常与上电过程（运行前检查）、运行中、下电过程（运行后检查）及维护过程中发生的自检相关。

6.4.2.2 对于每个使相关项实现安全状态或维持安全状态的安全机制，应定义下列内容：

a) 状态间的转换；

注1：包括控制执行器的要求。

b) 与从适当的架构层级分配得到的时间要求相关的故障处理时间间隔；及

注2：该子要求的目的是在针对每个安全目标定义的故障处理时间间隔的范围内，实现时间一致。

c) 不能在 FTTI 内进入相关项安全状态时的紧急运行容错时间间隔（见 GB/T 34590.1-XXXX，3.45）。

注3：整车测试和试验能够用于确定紧急运行容错时间间隔。

示例1：安全状态之前的降级运行持续时间。

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)。

6.4.2.3 本要求适用于 ASIL(A)、(B)、C 和 D 等级：如果适用，应定义安全机制，以防止故障变为潜伏故障。

注1：仅随机硬件故障的多点故障有可能成为潜伏故障。

示例：自检可作为检测多点故障的安全机制。用于验证组件在不同运行模式（例如上电、下电、运行或额外的自检模式）下的状态。阀、继电器或灯在常规上电时进行的功能检测就是自检的例子。

注2：识别是否需要防止故障成为潜伏故障的安全机制的评估标准来源于良好的工程实践。GB/T 34590.5-XXXX第8章给出的潜伏故障度量提供了评估标准。

6.4.2.4 此要求适用于 ASIL(A)、(B)、C 和 D 等级：为了避免多点失效，应为每个探测多点故障的安全机制定义诊断测试策略，包括：

a) 硬件组件的可靠性要求，并考虑其在架构中的角色及其对多点失效的贡献；

b) 定义的量化目标值，表征由于随机硬件失效而违背各安全目标的最大可能性(见 GB/T 34590.5-XXXX,第 9 章)；

c) 已分配的 ASIL 等级，从相关安全目标、功能安全要求或更高层面的技术安全要求中导出；及

d) 多点故障探测时间间隔。

注1：诊断测试策略可以是时间驱动（例如使用诊断测试时间间隔）或者事件驱动（例如启动测试）。

注2：二阶多点失效包含以多点故障检测时间间隔分隔的两个故障。

注3：下列措施的使用取决于时间约束：

——系统或要素在运行过程中的周期性测试；

——要素在上下电时的自检；及

——系统或要素在维护时的测试。

6.4.2.5 本要求适用于 ASIL(A)、(B)、C 和 D 等级。仅为了防止双点故障变成潜伏故障而实施的安全机制的开发应至少符合：

a) ASIL B 等级（对于分配为 ASIL D 等级的技术安全要求）；
b) ASIL A 等级（对于分配为 ASIL B 等级和 ASIL C 等级的技术安全要求）；及
c) QM 等级（对于分配为 ASIL A 等级的技术安全要求）。

注：如果安全要求运用了ASIL等级分解，那么本章的要求亦适用于分解后的要求。

示例：某内存存储采用奇偶校验作为安全机制，其安全要求被评为 ASIL B 等级。针对用于测试该奇偶校验机制在探测和指示内存故障的能力的自检测试，其要求可被评为 ASIL A 等级。

6.4.3 系统架构设计规范和技术安全概念

6.4.3.1 技术安全概念和该子阶段的系统架构设计应基于相关项定义，功能安全概念和先前的系统架构设计。

6.4.3.2 应检查 GB/T 34590.3-XXXX,7.3.1 中的系统架构设计和本子阶段中的系统架构设计的一致性。如果发现差异，则可能有必要对 GB/T 34590.3-XXXX 描述的活动进行迭代。

6.4.3.3 系统架构设计应实现技术安全要求。

6.4.3.4 关于技术安全要求的实现，系统架构设计应考虑：

a) 验证系统架构设计的能力；
b) 与实现功能安全相关的预期软硬件要素的技术能力；及
c) 在系统集成过程中执行测试的能力；

6.4.3.5 应定义安全相关要素的内部和外部接口，其他要素不应对安全相关要素产生不利的安全相关影响。

6.4.3.6 如果在系统架构设计期间对安全要求进行 ASIL 等级分解，应按照 GB/T 34590.9-XXXX，第 5 章进行。

6.4.4 安全分析及避免系统性失效

6.4.4.1 应按照表 1 和 GB/T 34590.9-XXXX 第 8 章进行系统架构设计的安全分析，其目的在于：

——为系统设计的适合性提供证据，以证明其适合提供与 ASIL 等级相适应的特定安全功能和特性；
——识别失效原因和故障影响；
——识别或确认安全相关系统要素和接口；及
——支持设计规范，并基于已识别的故障原因和失效影响验证安全机制的有效性。

表1 系统架构设计分析

方法		ASIL 等级			
		A	B	C	D
1	演绎分析	o	+	++	++
2	归纳分析	++	++	++	++

注1：安全相关特性包括独立性及免于干扰的要求。

注2：这些分析的目的是辅助设计。因此在该阶段，定性分析是足够的。如果有必要,可采用定量分析。

注3：在足以识别随机硬件失效和系统性失效的原因和影响的细节层面上进行分析。

注4：演绎和归纳的方法结合使用的目的是提供互补的分析方法，见GB/T 34590.9-XXXX, 8.2。

6.4.4.2 为符合安全目标或要求，应消除已识别出的引起失效的内部原因，或在必要时减轻它们的影响。

6.4.4.3 为符合安全目标或要求，应消除已识别出的引起失效的外部原因，或在必要时减轻它们的影响。

6.4.4.4 为了减少系统性失效的可能性，宜在适用处应用值得信赖的系统设计原则。这些原则可能包括：

a) 值得信赖的技术安全概念的复用；
b) 值得信赖的要素设计的复用，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复用；
d) 值得信赖的或标准化接口的复用。

6.4.4.5 应对值得信赖的设计原则的适用性进行分析并形成文档，以确保其和最终产品应用的一致性和适用性。

6.4.4.6 为了避免系统性故障，系统架构设计应具有以下特征：

a) 模块化；
b) 适当的颗粒度水平；及
c) 简单。

注：可以通过使用诸如分层的设计，精确的接口定义，避免组件和接口不必要的复杂性，可维护性和可验证性之类的设计原则实现上述特征。

6.4.4.7 在安全分析或系统架构设计过程中新识别的尚未被安全目标涵盖的危害，应更新到按照 GB/T 34590.3 定义的危害分析和风险评估（HARA）中。

注：安全目标尚未涵盖的危害可能是非功能性危害。非功能性危害不在GB/T 34590的范围内，但可在危害分析和风险评估中增加注释；例如，通过增加“此危害中未指定ASIL等级，因为它不在GB/T 34590的范围内”的注释进行说明。

6.4.5 运行过程中随机硬件失效的控制措施

6.4.5.1 应按照 6.4.3 中的系统架构设计，定义探测、控制或减轻随机硬件失效的措施。

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

示例2：随机硬件失效发生时，不需要探测即可进入安全状态的硬件设计（即，失效-安全的硬件设计）。

注：6.4.4.1中归纳和演绎分析的量化估计有助于确定是否需要采取进一步的安全措施。可按照GB/T 34590.5-XXXX进行硬件分析，并做出决定。

6.4.5.2 本要求适用于等级为ASIL(B)、C和D的安全目标。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 (见GB/T 34590.5-XXXX，第9章)，并应定义目标值以用于相关项层面的最终评估。

6.4.5.3 本要求适用于等级为ASIL(B)、C和D的安全目标。适当的失效率和诊断覆盖率的目标值宜在要素层面进行定义，以符合：

a) GB/T 34590.5-XXXX,第8章中度量的目标值；及
b) GB/T 34590.5-XXXX,第9章中的流程。

6.4.5.4 本要求适用于 ASIL(B)、C和D等级。对于分布式开发（见GB/T 34590.8-XXXX,第5章），推导出的目标值应通报给每个相关团队。

注1：GB/T34590.5-XXXX，第8章和第9章中描述的架构约束，不一定适用于商业现成产品的元器件和组件。这是因为供应商通常不能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，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，以便允许在整体硬件架构层面上预估架构约束。

6.4.6 分配到硬件和软件

6.4.6.1 技术安全要求应分配给以系统、硬件或软件作为实施技术的系统架构设计要素。

注：如果将技术安全要求分配给作为实施技术的系统中，则再次按照GB/T 34590.4进一步开发这些要求，直到能将他们分配给硬件和软件为止。

6.4.6.2 分配和分区决策应符合系统架构设计。

注：为了实现独立性和避免失效传播，系统架构设计可以采用功能分区和组件分区。

6.4.6.3 每个系统架构设计要素都应继承其实现的技术安全要求的最高的ASIL等级。

6.4.6.4 如果系统架构设计要素由指定为不同ASIL等级的子要素组成,或由安全相关和非安全相关的子要素组成,那么每个子要素都应按照最高ASIL等级进行处理,除非满足共存标准(按照GB/T 34590.9-XXXX，第6章）。

6.4.6.5 如果技术安全要求分配到具备可编程功能的定制化硬件要素(比如:专用集成芯片(ASICs)、可编程门阵列（FPGA）或是其他形式的数字化硬件），宜结合GB/T 34590.5和GB/T 34590.6的要求来定义和实施适当的开发流程。

注1：如果满足GB/T 34590.8-XXXX第13章的应用准则，则可以按照该章的评估方法提供证据证明上述硬件要素中的一些要素满足所分配的安全要求。

注2：GB/T 34590.11-XXXX 提供了相应指导。

6.4.7 软硬件接口(HSI)规范

6.4.7.1 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元器件以及支持软件运行的硬件资源。

注：软硬件接口（HSI）中详细描述的方面和特性见附录B。

6.4.7.2 软硬件接口（HSI）规范应包含下列特性：

a) 硬件设备的相关运行模式和相关配置参数；

示例1：硬件设备的运行模式，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) 确保要素间独立性或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) 硬件设备的访问机制；及

示例4：串、并、从、主/从。

e) 由技术安全概念得出的时间约束。

6.4.7.3 硬件的相关诊断能力和软件对其的使用应在软硬件接口（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。

6.4.7.4 应在系统架构设计过程中对软硬件接口（HSI）进行定义。

注：在硬件开发(见GB/T 34590.5-XXXX第6章)和软件开发(见GB/T 34590.6-XXXX第6章)过程中对软硬件接口(HSI)进行细化。

6.4.8 生产、运行、服务和报废

6.4.8.1 应定义在系统架构设计过程中识别出的 GB/T 34590.7-XXXX 中对生产、运行、服务和报废的要求。这些包括：

a) 在生产、服务或报废期间达到、保持或修复相关项及其要素的安全相关功能和特性所需的措施；
b) 安全相关的特殊特性；
c) 确保正确识别系统或要素的要求；
d) 生产的验证措施；
e) 包含诊断数据及服务记录的服务要求；及
f) 报废措施。

示例：组装或拆卸指南、服务记录、关于系统要素允许维修的指南、报废指南、要素标签。

注：确保生产、运行、服务和报废期间的功能安全主要包含两方面。第一个方面涉及那些在开发阶段中确保充分的系统架构设计和对合适的安全相关的特殊特性的定义而开展的活动，这些活动在要求6.4.8.1中给出，第二方面涉及确保在生产和运行阶段实现或维持功能安全的活动（例如：基于特定的与安全相关的特殊特性），这些活动在GB/T 34590.7-XXXX中进行了阐述。

6.4.8.2 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，以提供按照 GB/T 34590.2-XXXX,第 7 章对相关项或其要素进行现场监控所需的数据。

6.4.8.3 为了修复或保持功能安全，应定义诊断特性以便服务时能够识别故障并对维护或修复的有效性进行检查。

6.4.9 验证

6.4.9.1 应按照 GB/T 34590.8-XXXX，第 6 章和第 9 章对技术安全要求进行验证，以提供其在给定系统边界条件下的正确性、完整性和一致性的证据。

6.4.9.2 应使用表 2 所列的验证方法对系统架构设计，软硬件接口（HSI）规范以及生产、运行、服务和报废的要求规范以及技术安全概念进行验证，以提供证据表明实现以下目标：

a) 它们适合并足以达到按照相关 ASIL 等级所要求的功能安全水平；
b) 系统架构设计与技术安全概念的一致性；及
c) 先前开发步骤中系统架构设计的有效性和符合性。

注：识别出的安全异常和不完备性将按照GB/T 34590.2-XXXX,5.4.3进行报告。

表2 验证

方法		ASIL等级			
		A	B	C	D
1a	检查[a]	+	++	++	++
1b	走查[a]	++	+	o	o
2a	仿真[b]	+	+	++	++
2b	系统原型和车辆测试[b]	+	+	++	++
3	系统架构设计分析[c]	见表1			

[a] 方法 1a 和 1b 用于检查要求是否得到完整和正确的实施。

[b] 2a 和 2b 可以作为故障注入测试的有利方法，以支持系统架构设计关于故障方面的完整性和正确性的论证。

[c] 对于如何实施安全分析，见 GB/T 34590.9-XXXX 第 8 章。

6.5 工作成果

6.5.1 技术安全需求规范，由 6.4.1 和 6.4.2 的要求得出。

6.5.2 技术安全概念，由 6.4.3～6.4.6 的要求得出。

6.5.3 系统架构设计规范，由 6.4.3～6.4.6 的要求得出。

6.5.4 软硬件接口(HSI)规范，由 6.4.7 的要求得出。

6.5.5 生产、运行、服务和报废需求规范，由 6.4.8 的要求得出。

6.5.6 针对系统架构设计、软硬件接口（HSI）规范、生产、运行、服务和报废需求规范及技术安全概念的验证报告，由 6.4.9 的要求得出。

6.5.7 安全分析报告，由 6.4.4 的要求得出。

7 系统及相关项的集成和测试

7.1 目的

集成和测试阶段包括三个子阶段和三个目标，如下所述。第一个子阶段是各要素硬件和软件的集成；第二个子阶段是组成一个系统的要素的集成，以形成一个完整的相关项；第三个子阶段是相关项与车辆内其他系统的集成。本章的目的是：

a) 定义集成步骤并集成系统要素，直到系统完全集成；
b) 验证由系统架构层级安全分析定义的安全措施是否得到正确实施；及
c) 提供证据表明所集成的系统要素满足按照系统架构设计的安全要求。

7.2 总则

相关项要素的集成按照系统化的方法进行，从软硬件集成和验证开始，经过系统集成和验证，到整车集成和验证。在每个集成阶段要进行特定的集成测试，以提供证据证明所集成的要素之间正确地交互。

在按照GB/T 34590.5和GB/T 34590.6对硬件和软件进行充分开发后，可按照本章启动系统集成。

7.3 本章的输入

7.3.1 前提条件

应具备下列信息：

——危害分析和风险评估报告中得出的安全目标和接受准则，按照 GB/T 34590.3-XXXX,6.5.1；
——功能安全概念，按照 GB/T 34590.3-XXXX，8,7.5.1；
——技术安全概念，按照 6.5.2；
——架构设计规范，按照 6.5.3；及
——软硬件接口（HSI）规范，按照 6.5.4、GB/T 34590.5-XXXX,6.5.2 和 GB/T 34590.6-XXXX,6.5.2。

7.3.2 支持信息

可考虑下列信息：

——整车架构(来自外部)；
——整车其他系统的技术安全概念(来自外部)；及
——安全分析报告(见 6.5.7)。

7.4 要求和建议

7.4.1 集成和测试策略规范

7.4.1.1 为了提供证据证明系统架构设计符合功能安全和技术安全要求，应按照 GB/T34590.8-XXXX，第 9 章进行集成测试活动，以检查：

a) 功能安全及技术安全要求的正确实施；
b) 安全机制正确的功能性能、准确性和时序；
c) 接口的一致性和正确实施；及
d) 足够的鲁棒性。

7.4.1.2 应考虑系统架构设计规范、功能安全概念和技术安全概念，定义集成和测试策略，其应该述及：

a) 适合提供功能安全证据的测试目标；及
b) 相关项及该相关项中有助于安全概念的要素的集成和测试；

注：这包括有助于安全概念的其他技术要素。

7.4.1.3 为使相关项集成子阶段能够进行，应根据集成和测试策略执行以下内容：

a) 应为软硬件集成和测试定义相关项集成和测试策略；
b) 相关项集成和测试策略的定义应包括系统和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处理；
c) 相关项集成和测试策略应考虑车辆系统（相关项内部和外部）与环境之间的接口；及
d) 相关项集成和测试策略应考虑被集成的系统或要素是否是作为独立于环境的安全要素（SEooC）进行开发，以及开发期间所做的假设是否需要验证。

注：在软硬件集成层面和相关项层面进行集成与验证的规范，要考虑软硬件之间的接口及其交互。

7.4.1.4 如果系统是可配置的（如通过要素的变量或标定数据），在系统或整车层面的验证应提供证据证明用于量产实施层面的配置符合安全要求

注：测试一个合适的配置子集可能是足够的。

7.4.1.5 在整个集成子阶段，对每个功能安全和技术安全要求是否得到了满足，应至少进行一次验证（如果适用，通过测试来验证）。

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：当一个SEooC集成到一个安全相关系统中，其开发中使用的假设的有效性需要进行验证。

注3：集成测试期间识别出的安全异常要按照GB/T34590.2-XXXX,5.4.3的要求进行报告。

7.4.1.6 为了恰当的定义集成测试的测试用例，应考虑集成的层面，使用表 3 中所列的恰当的方法组合导出测试用例。

表3 导出集成测试案例的方法

方法		ASIL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，见GB/T 34590.9-34590，第7章	+	+	++	++
1h	环境条件和操作用例分析	+	++	++	++
1i	现场经验分析	+	++	++	++

7.4.2 软硬件集成和测试

7.4.2.1 软硬件集成

7.4.2.1.1 应对按照 GB/T 34590.5 开发的硬件和按照 GB/T 34590.6 开发的软件进行集成，并作为表 4 至表 8 中测试活动的对象。

7.4.2.1.2 应对集成后的硬件和软件进行测试，以符合软硬件接口（HSI）规范的要求。

注：首选用于生产的硬件和软件。对于特定的测试技术，必要时可以使用修改过的硬件或软件。

7.4.2.2 软硬件测试中的测试目标和测试方法

7.4.2.2.1 按照 7.4.2.2.2～7.4.2.2.6 要求得出的测试目标，应使用对应表中给出的适当的测试方法来实现。

注1：这些目标和方法可以帮助在系统架构设计中对系统性故障的探测

注2：基于已实施的功能、功能复杂性或系统的分布特性，如有足够的理由，在其他集成子阶段执行测试也是可行的。

7.4.2.2.2 技术安全要求的安全相关功能和行为在软硬件层面的正确执行，应使用表 4 中列出的测试方法来提供证据。

表4 技术安全要求在软硬件层面的正确执行

方法		ASIL 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：表4和表9中的方法1b的工作量差异，是由系统层面的故障注入测试所需要的工作量引起的。

7.4.2.2.3 本要求适用于 ASIL (A)、B、C 和 D 等级。安全机制在软硬件层面的正确功能性能、准确性和时序，应使用表 5 中给出的测试方法进行论证。

表5 安全机制在软硬件层面的正确功能性能、准确性和时序

方法		ASIL 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] 性能测试能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），也能验证目标控制软件与硬件同时运行的能力。

7.4.2.2.4 本要求适用于 ASIL (A)、B、C 和 D 等级。外部和内部接口在软硬件层面执行的一致性和正确性，应使用表 6 中给出的测试方法来提供证据。

表6 外部和内部接口在软硬件层面执行的一致性和正确性

方法		ASIL 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，用来测试兼容性、时序及其他特定等级。ECU 内部接口的测试，能用静态测试检测软件和硬件兼容性，也能用动态测试检测串行外设接口（SPI）或集成电路（IC）通信或 ECU 其他要素间的其他任意接口。

7.4.2.2.5 本要求适用于 ASIL (A)、（B）、C 和 D 等级。对于故障模型，硬件故障探测机制在软硬件层面上的有效性，应使用表 7 中列出的测试方法进行论证。

注：参考的故障模型，见GB/T 34590.5-XXXX，附录D。

表7 安全机制在软硬件层面的有效性

方法		ASIL 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。该方法通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。

7.4.2.2.6 本要求适用于 ASIL（A）、（B）、（C）和 D 等级。要素在软硬件层面的鲁棒性水平，应使用表 8 中给出的测试方法进行论证。

表8 在软硬件层面的鲁棒性水平

方法		ASIL 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（例如，通过检查编码量或分析有关中断使用的代码,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能否正确运行。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。

7.4.3 系统集成和测试

7.4.3.1 系统集成

7.4.3.1.1 系统的各个要素应按照系统架构设计进行集成,并按照系统集成测试规范进行测试。

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。

7.4.3.2 系统测试中的测试目标和测试方法

7.4.3.2.1 按照 7.4.3.2.2～7.4.3.2.5 得出的测试目标,应使用对应表中给出的适当的测试方法来实现。

注1：这些将支持在系统集成和测试过程中对系统性故障的探测。

注2：基于系统已实施的功能、功能复杂性或系统的分布特性,如给出足够的理由,在其他集成的子阶段执行测试也是可行的。

7.4.3.2.2 功能安全和技术安全要求在系统层面的正确执行，应使用表 9 中列出的测试方法来提供证据。

表9 功能安全和技术安全要求在系统层面的正确执行

方法		ASIL 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，以发现模型和其实现的表现差异。

7.4.3.2.3 本要求适用于 ASIL(A)、(B)、(C)和 D 等级。安全机制在系统层面的正确功能性能、准确性、系统层面失效模式的覆盖率、时序，应使用表 10 中给出的测试方法进行论证。

表10 安全机制在系统层面的正确功能性能、准确性和时序

方法		ASIL 等级			
		A	B	C	D
1a	背靠背测试 [a]	o	+	+	++
1b	故障注入测试 [b]	+	+	++	++
1c	性能测试 [c]	o	+	+	++
1d	错误猜测法测试 [d]	+	+	++	++
1e	来自现场经验的测试 [e]	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，以发现模型和其实现的表现差异。

[b] 为证明安全机制失效模式覆盖度在系统层面的有效性，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。这种方法适用于一组有限故障的模型，即可在系统层面实际注入的简单故障模型（如再现组件引脚的卡滞）。对于半导体层面的故障模型（如软错误或晶体管卡滞），故障注入方法的应用将在 GB/T 34590.11-XXXX.4.8 中详细描述。

[c] 性能测试可验证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）。

[d] 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系统错误。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。如果测试者有相似性系统的应用经验时，错误猜测法是一种有效的方法。

[e] 来自现场经验的测试采用从现场收集到的经验和数据。

7.4.3.2.4 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 11 中列出的测试方法来提供证据。

表11 外部和内部接口在系统层面执行的一致性和正确性

方法		ASIL 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]	+	+	++	++
1d	通讯和交互测试[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，用来完整地测试系统的特定接口、兼容性、时序及其他特定参数。对于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他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他运行系统间，针对功能性和非功能性要求的通讯测试。

7.4.3.2.5 系统层面的鲁棒性水平，应使用表 12 中给出的测试方法进行论证。

表12 系统层面的鲁棒性水平

方法		ASIL 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能否正确运行。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，或来自于其他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：见参考文献[4],[5],[6],[7]）。

7.4.4 整车集成和测试

7.4.4.1 整车集成

7.4.4.1.1 应将相关项集成到整车上，并实施整车集成测试。

注：当制定整车层面集成与验证计划时，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（见表3）。

7.4.4.1.2 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。

7.4.4.2 整车测试期间的测试目标和测试方法

7.4.4.2.1 由 7.4.4.2.2～7.4.4.2.5 的要求得出的测试目标，应使用对应表格中所列出的适当的测试方法来实现。

注1：这些将支持在整车集成过程中对系统性故障的探测。

注2：基于系统已实施的功能、功能复杂性或分布特性，如有给出足够的理由，在其他集成的子阶段进行测试是可行的。

7.4.4.2.2 功能安全要求在整车层面的正确的执行，应使用表 13 中给出的测试方法进行论证。

表13 功能安全要求在整车层面上的正确执行

方法		ASIL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	实际使用条件下的用户测试[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，因为在正常运行期间不会触发安全机制。

[c] 长期测试和实际使用条件下的用户测试，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停用执行器。

7.4.4.2.3 本要求适用于 ASIL(A),(B),C 和 D 等级。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 14 中列出的测试方法进行论证。

表14 安全机制在整车层面的正确功能性能、准确性和时序

方法		ASIL 等级			
		A	B	C	D
1a	性能测试[a]	+	+	++	++
1b	长期测试[b]	+	+	++	++
1c	实际使用条件下的用户测试[b]	+	+	++	++
1d	故障注入测试[c]	o	+	++	++

1e	错误猜测法测试[d]	o	+	++	++
1f	来自现场经验的测试[e]	o	+	++	++

[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，整车层面故障容错时间间隔和车辆的可控性）

[b] 长期测试和实际使用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，而是在实际使用条件下执行。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停用执行器。

[c] 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，因为在正常运行期间不会触发安全机制。

[d] 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系统错误。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应用经验时，错误猜测法是一种有效的方法。

[e] 来自现场经验的测试采用从现场收集到得经验和数据。

7.4.4.2.4 本要求适用于 ASIL（A）、（B）、C 和 D 等级。整车层面内部和外部接口实现的一致性和正确性，应使用表 15 中给出的测试方法进行论证。

注：内部接口是相关项之间或系统之间的接口，外部接口是相关项和整车环境的接口。

表15 整车层面内外部接口实现的正确性

方法		ASIL 等级			
		A	B	C	D
1a	内部接口测试[a]	+	+	++	++
1b	外部接口测试[a]	+	+	++	++
1c	通讯和交互测试[b]	+	+	++	++

[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针对功能性和非功能性要求的通讯测试。

7.4.4.2.5 本要求适用于 ASIL（A）、（B）、C 和 D 等级。整车层面的鲁棒性水平，应使用表 16 中列出的测试方法进行论证。

表16 整车层面的鲁棒性水平

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

[a] 整车层面的资源使用测试通常在动态环境下进行（如：电子控制单元网络环境，原型车或整车）。测试的问题包括相关项内部资源，功率消耗或其他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能否正确运行。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，或来自于其他系统的极限要求下完成，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（EMD）测试。（如：见参考文献[4],[5],[6],[7]）。

[d] 长期测试和实际使用条件下的用户测试，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，而是在实际使用条件下执行。

7.5 工作成果

7.5.1 集成和测试策略，由 7.4.1 的要求得出。

7.5.2 集成和测试报告，由 7.4.2，7.4.3，7.4.4 的要求得出。

8 安全确认

8.1 目的

本章的目的是：

a) 提供证据，证明集成到目标车辆的相关项实现了其安全目标，并满足安全接受准则。

b) 提供证据，证明功能安全概念和技术安全概念对于实现相关项的功能安全是合适的。

8.2 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安全确认，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，为安全目标的实现提供了保证。

8.3 本章的输入

8.3.1 前提条件

应具备下列信息：

——危害分析和风险评估报告，按照 GB/T 34590.3-XXXX，6.5.1；

——功能安全概念，按照 GB/T 34590.3-XXXX，7.5.1。

8.3.2 支持信息

可考虑下列信息：

——技术安全概念（见 6.5.2）；

——相关项定义（见 GB/T 34590.3-XXXX，5.5.1）；及

——安全分析报告（见 6.5.7）。

8.4 要求和建议

8.4.1 安全确认的环境

8.4.1.1 应对整车层面的典型环境下所集成的相关项的安全目标进行确认。

注1：如果适用，集成的相关项包括：系统、软件、硬件、其他技术要素和外部措施。

注2：这对于T&B特别重要，因为它们安全确认的对象可能是不同类型的基础车辆。

8.4.1.2 为了定义典型环境，应考虑基于车型和车辆配置的典型车辆。

注：危害分析和风险评估报告相关（见GB/T 34590.3-XXXX,6.5.1）可能是选择典型车辆的一个相关输入。

8.4.1.3 安全目标的确认应考虑运行过程变化对技术特性的影响，该因素已经在危害分析和风险评估中进行考虑。

8.4.2 安全确认的规范

8.4.2.1 应定义安全确认规范，包括：

a) 待安全确认的相关项配置，包括其标定数据，按照 GB/T 34590.6-XXXX，附录 C；

注：如果对于每个相关项配置的完整安全确认是不可行的，那么可选择合理的子集。

b) 安全确认流程、测试案例、驾驶操作和接受准则的定义；

c) 设备和要求的环境条件。

8.4.3 安全确认的执行

8.4.3.1 如果使用测试进行安全确认,那么可应用与验证测试(见 GB/T 34590.8-XXXX,9.4.2 和 9.4.3）相同的要求。

8.4.3.2 当相关项集成到整车时，应通过评估如下方面对相关项的功能安全实现进行确认，包括：

a) 可控性；

注1：使用运行场景确认可控性，包括预期用途及可预见的误用。

注2：安全确认的一个接受准则是对GB/T 34590.3-XXXX, 7.4.2.5中定义的安全状态有充分的可控性。

b) 外部措施的有效性；

c) 其他技术要素的有效性；及

d) 影响危害分析与风险评估（见 GB/T 34590.3-XXXX, 6.4.4.4）中 ASIL 等级的假设只能在最终车辆上进行检查。

示例：假设一个机械组件能够防止或减轻由电气电子系统的功能失效造成的潜在危害，那么这个机械组件防止或减轻危害的有效性只能在整车层面进行确认。

8.4.3.3 应基于安全目标、功能安全要求和预期用途，按计划执行整车层面的安全确认，使用：

a) 针对每个安全目标的安全确认流程和测试用例，包括详细的通过/未通过准则；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。

8.4.3.4 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) 实际使用条件下的操作用例、抽测或盲测、专家小组；及

e) 评审。

8.4.4 评估

应对安全确认的结果进行评估，以提供证据证明已实施的安全目标实现了相关项的功能安全。

8.5 工作成果

8.5.1 包含安全确认环境描述的安全确认规范，由 8.4.1 和 8.4.2 的要求得出。

8.5.2 安全确认报告，由 8.4.3 和 8.4.4 的要求得出。

附 录 A
（资料性）
系统层面产品开发的概览和工作流

表 A.1 提供了有关系统层面产品开发特定子阶段的目的、前提条件和工作成果概览。

表A.1 系统层面产品开发概览和工作流

章	目的	前提条件	工作成果
5 系统层面产品开发的概述	本章的目的是在系统层面提供产品开发的概览	—	—
6 技术安全概念	a)为实现系统要素和接口的功能、相关性、约束和属性，制定所需的技术安全要求； b)为系统要素和接口中将要实施的安全机制，制定技术安全要求； c) 制定在生产、运行、服务和报废过程中系统及其要素功能安全的相关要求； d)验证技术安全要求在系统层面是否符合功能安全要求并与功能安全要求一致； e)制定满足安全要求且不与非安全相关要求冲突的系统架构设计和技术安全概念； f)分析系统架构设计，以防止故障，并导出针对生产和服务必要的安全相关的特殊特性；及 g) 验证系统架构设计和技术安全概念是否满足相应 ASIL 等级的安全要求。	功能安全概念，见 GB/T 34590.3-XXXX,7.5.1； 系统架构设计（来自外部，见 GB/T 34590.3-XXXX,7.3.1）；及 其他涉及功能安全的相关项对此相关项的要求（如果适用）。	6.5.1 技术安全需求规范，由 6.4.1 和 6.4.2 的要求得出。 6.5.2 技术安全概念，由 6.4.3~6.4.6 的要求得出。 6.5.3 系统架构设计规范，由 6.4.3~6.4.6 的要求得出。 6.5.4 软硬件接口(HSI)规范，由 6.4.7 的要求得出。 6.5.5 生产、运行、服务和报废的需求规范，由 6.4.8 的要求得出。 6.5.6 针对系统架构设计、软硬件接口规范、针对生产、运行、服务和报废要求规范及技术安全概念的验证报告，由 6.4.9 的要求得出。 6.5.7 安全分析报告，由 6.4.4 的要求得出。
7 系统及相关项的集成和测试	本章的目的是： a）定义集成步骤并集成系统要素，直到系统完全集成； b）验证由系统架构层级安全分	危害分析和风险评估报告得出的安全目标（见 GB/T 34590.3-XXXX，6.5.1） 功能安全概念(见 GB/T 34590.3-	7.5.1 集成和测试策略，由 7.4.1 的要求得出。 7.5.2 集成和测试报告，由 7.4.2、7.4.3 和 7.4.4 的

	析定义的安全措施是否得到正确实施；及； c）提供证据表明所集成的系统要素满足按照系统架构设计的安全要求。	XXXX，7.5.1)； 技术安全概念（见 6.5.2） 系统架构设计规范（见 6.5.3） 软硬件接口（HSI）规范（见 6.5.4)	要求得出。
8 安全确认	本章的目的是： a)提供证据，证明集成到目标车辆的相关项实现了其安全目标。 b)提供证据，证明功能安全概念和技术安全概念实现相关项的功能安全是合适的。	危害分析和风险评估报告（见 GB/T 34590.3-XXXX，6.5.1）. 由危害分析和风险评估报告得出的安全目标（见 GB/T 34590.3-XXXX,6.5.1） 功能安全概念（见 GB/T 34590.3-XXXX，7.5.1。	8.5.1 包含安全确认环境描述的安全确认规范，由 8.4.1 和 8.4.2 的要求得出。 8.5.2 安全确认报告，由 8.4.3 和 8.4.4 的要求得出

附 录 B
（资料性）
软硬件接口（HSI）内容示例

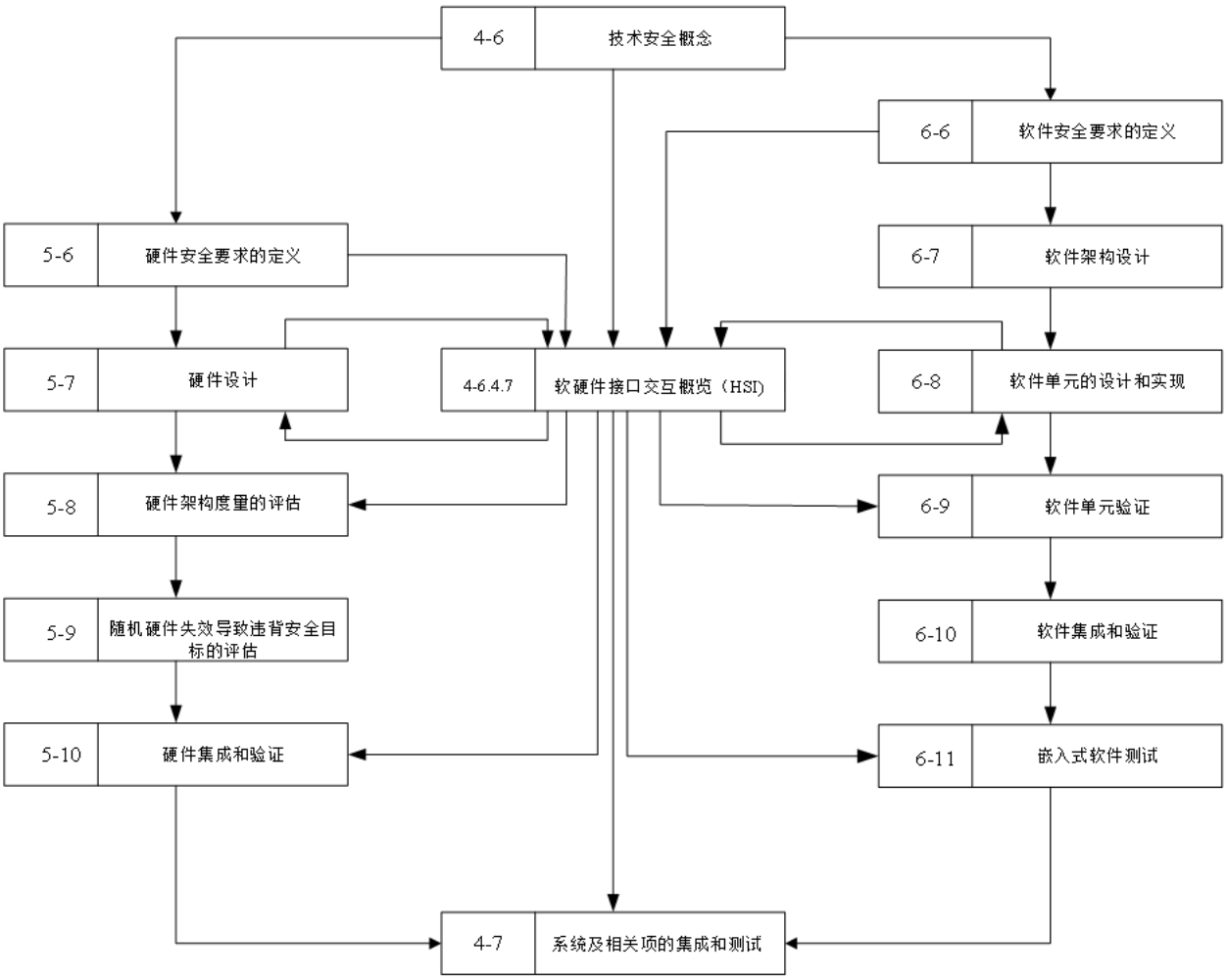
B.1 总则

本附录提供软硬件接口的进一步说明。

软硬件接口规范在子阶段“技术安全概念”中启动。随着开发在硬件和软件开发的继续，软硬件接口（HSI）规范得到细化。

图B.1概述了软硬件接口（HSI）的作用及其在系统、硬件和软件层面的产品开发之间的关系。软硬件接口（HSI）用于约定硬件和软件开发之间的技术依赖性。

注：在该图中，GB/T 34590的各个部分的具体章以下列方式表示：“m-n”，其中“m”表示部分号，“n”表示章号，例如“3-6”表示GB/T 34590.3-XXXX的第6章。



图B.1 软硬件接口（HSI）交互概述

B.2 软硬件接口（HSI）要素

为了定义软硬件接口（HSI），可以考虑下述软硬件接口（HSI）要素：

a) 存储器：

1) 易失性存储器 （例如：RAM）；

2) 非易失性存储器（例如：NvRAM）；

b) 总线接口[例如：控制器局域网（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 软硬件接口特性

为了定义软硬件接口（HSI），可以考虑下述软硬件接口（HSI）要素：
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（HSI）特性分配给软硬件接口（HSI）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（值域的百分比）
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%

参 考 文 献

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

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

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

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

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

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

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

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