ICS 43.040
CCS T 35

中华人民共和国国家标准

GB/T 43253.2—2023

道路车辆　功能安全审核及评估方法　第2部分：概念阶段和系统层面

Road vehicles—Functional safety audit and assessment method—Part 2：Concept phase and system level

2023-11-27 发布　　2023-11-27 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　一般要求 …… 1
5　相关项定义 …… 2
5.1　目标 …… 2
5.2　审核及评估的输入 …… 2
5.3　审核及评估的要求 …… 2
6　危害分析和风险评估 …… 2
6.1　目标 …… 2
6.2　审核及评估的输入 …… 3
6.3　审核及评估的要求 …… 3
7　功能安全概念 …… 4
7.1　目标 …… 4
7.2　审核及评估的输入 …… 4
7.3　审核及评估的要求 …… 4
8　技术安全概念 …… 5
8.1　目标 …… 5
8.2　审核及评估的输入 …… 6
8.3　审核及评估的要求 …… 6
9　验证和确认 …… 8
9.1　目标 …… 8
9.2　审核及评估的输入 …… 8
9.3　审核及评估的要求 …… 9
附录A（资料性）　相关项定义 …… 13
附录B（资料性）　危害分析和风险评估 …… 16
附录C（资料性）　功能安全概念 …… 20
附录D（资料性）　技术安全概念 …… 24
附录E（资料性）　验证和确认 …… 31
参考文献 …… 40

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。

本文件是GB/T 43253《道路车辆　功能安全审核及评估方法》的第2部分。GB/T 43253已经发布了以下部分：

——第1部分：通用要求；

——第2部分：概念阶段和系统层面；

——第3部分：软件层面；

——第4部分：硬件层面。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会(SAC/TC 114)归口。

本文件起草单位：中国汽车技术研究中心有限公司、中国第一汽车集团有限公司、深圳市大疆卓见科技有限公司、广州汽车集团股份有限公司、上海机动车检测认证技术研究中心有限公司、东软睿驰汽车技术(上海)有限公司、中国长安汽车集团有限公司、知行汽车科技(苏州)有限公司、北京地平线机器人技术研发有限公司、蔚来汽车科技(安徽)有限公司、舍弗勒(中国)有限公司、爱信(苏州)汽车技术中心有限公司杭州分公司、重庆长安汽车软件科技有限公司、北京国家新能源汽车技术创新中心有限公司。

本文件主要起草人：尚世亮、刘辉、徐铱铱、孙毓阳、李波、林广义、付越、王宇、杨雪珠、王梓勋、王潇屹、闻继伟、邵海贺、宋炜瑾、蔡香、周宇、钟京华、储小勤、周宏伟、刘英。

引　言

GB/T 43253《道路车辆　功能安全审核及评估方法》以 GB/T 34590《道路车辆　功能安全》为基础，适用于道路车辆上安全相关的电气/电子(E/E)系统在安全生命周期内的审核及评估活动。

安全是道路车辆开发的关键问题之一，车辆上包含的电气、电子和软件相关功能的数量不断增加，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。

为了确认电气/电子(E/E)系统对于功能安全流程及功能安全要求的符合性，GB/T 43253：

a) 提供了组织层面开展功能安全审核及评估的通用流程、实施方法及要求；

b) 提供了安全相关的电气/电子(E/E)系统在概念阶段、系统层面、软件层面、硬件层面的功能安全审核及评估的过程、方法和要求；

c) 提供了功能安全审核及评估的检查清单和参考示例。

GB/T 43253 由 4 个部分构成。

——第 1 部分：通用要求。目的是规定功能安全审核及评估活动在不同阶段的通用要求。

——第 2 部分：概念阶段和系统层面。目的是规定功能安全审核及评估活动在概念阶段及系统层面的要求。

——第 3 部分：软件层面。目的是规定功能安全审核及评估活动在软件层面的要求。

——第 4 部分：硬件层面。目的是规定功能安全审核及评估活动在硬件层面的要求。

功能安全审核及评估活动伴随功能安全开发过程的迭代，图 1 为 GB/T 43253 的整体架构，基于 V 模型为产品开发的不同阶段、对象和范围，提供审核及评估参考过程模型。

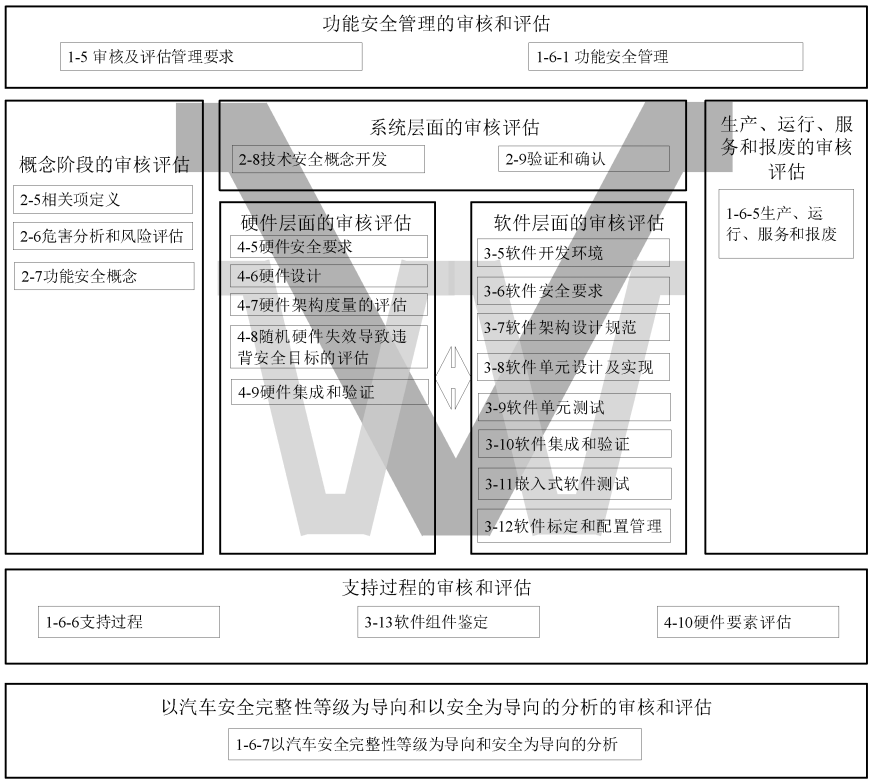

图 1　功能安全审核及评估概览

道路车辆　功能安全审核及评估方法
第2部分:概念阶段和系统层面

1　范围

本文件规定了针对安全相关的电气/电子(E/E)系统在概念阶段和系统层面的功能安全相关活动和工作成果,开展功能安全审核及评估的要求和方法,以检查和判断开发过程及工作成果对于功能安全的符合性。

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(E/E)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(E/E)系统,例如,为残疾驾驶者设计的车辆系统。

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 34590.1～34590.12—2022　道路车辆　功能安全

GB/T 43253.1—2023　道路车辆　功能安全审核及评估方法　第1部分:通用要求

GB/T 43253.3—2023　道路车辆　功能安全审核及评估方法　第3部分:软件层面

GB/T 43253.4—2023　道路车辆　功能安全审核及评估方法　第4部分:硬件层面

3　术语和定义

GB/T 34590.1—2022界定的术语和定义适用于本文件。

4　一般要求

GB/T 43253.1—2023中定义的审核及评估要求适用于本文件。

概念阶段和系统层面的功能安全审核及评估,主要涉及以下内容:

——接受评估的相关项定义;

——危害分析和风险评估;

——功能安全概念开发;

——技术安全概念开发;

——验证和确认。

通过审核及评估,基于证据判断功能安全概念及系统层面的功能安全开发,符合:

——功能安全目标、功能安全概念和技术安全概念是恰当和完整的;

——相关项设计实现了功能安全目标、功能安全概念和技术安全概念;

——功能安全开发过程、方法及使用的工具是恰当的。

5 相关项定义

5.1 目标

本章的目标是对作为功能安全开发对象的相关项的定义文档进行审核及评估，以检查其定义是否准确和充分，足以支持开展后续功能安全活动。

5.2 审核及评估的输入

为了开展本章规定的审核及评估过程，应具备以下输入及其可能存在的验证报告：

——相关项定义文档（含定义文档及相关设计文档的组合）。

注：在企业内部首次开展审核评估时，可能不存在对某些作为输入的工作成果的验证报告；对于后续审核评估活动，上述验证报告提供了审核评估的参考依据。

5.3 审核及评估的要求

对于相关项定义的审核及评估，应涵盖表1中的检查项。

表1 相关项定义的审核及评估检查清单

序号	检查清单
1	相关项需要满足的标准及法规要求有哪些？
2	相关项在整车层面的功能行为是什么？
3	是否定义了相关项的运行场景和运行模式？
4	是否定义了相关项的非功能性需求？
5	是否定义了相关项的约束？
6	是否分析了相关项行为不足的潜在后果？
7	是否定义了执行器的能力或假定了执行器的能力？
8	是否清晰地定义了相关项的边界、要素、接口及交互关系？
9	是否考虑了相关项的行为对整车影响的假设？
10	是否考虑了其他相关项和要素要求本相关项提供的功能？
11	是否考虑了本相关项要求其他系统和要素提供的功能？
12	是否考虑了功能在所涉及的系统和要素间的分配？
13	是否存在相关项定义的验证报告？

附录A提供了针对相关项定义开展审核及评估的说明及示例。

6 危害分析和风险评估

6.1 目标

本章的目标是对危害分析和风险评估过程及分析结果进行审核及评估，以检查：

a) 对电气/电子（E/E）系统相关的功能异常表现引起的危害事件进行了完整识别和正确归类；

b) 基于充分的理由，对识别出的危害事件进行了分级；

c) 针对分级后的危害事件，定义了充分的安全目标，以避免整车不合理的安全风险。

6.2 审核及评估的输入

为开展本章规定的审核及评估过程，应具备以下输入及其可能存在的验证报告：

——包含电气/电子(E/E)系统功能、运行场景、整车架构等内容的定义文档；

——危害分析和风险评估过程和结果报告；

——针对危害分析和风险评估中相关假设、依据和结果的验证确认计划和结论。

6.3 审核及评估的要求

对于危害分析和风险评估的审核及评估，应涵盖表 2 和表 3 中的检查项。

表 2 危害分析和风险评估过程和结果的审核及评估检查清单

序号	检查清单
1	危害分析是否涵盖了相关项的所有功能行为？是否与“相关项定义”阶段的功能行为保持了一致性及可追溯性？
2	在危害分析和风险评估过程中，对相关项内部安全机制是否未作为评估依据？
3	对于相关项的功能异常表现导致的危害事件发生时所处的运行场景及运行模式是否进行了描述？是否考虑了可合理预见的误用？
4	是否使用了系统性分析方法来确定危害？
5	是否在整车层面上，定义了由相关项的功能异常表现导致的危害？
6	危害分析过程中，是否识别出了因非电气/电子(E/E)系统功能异常表现导致的危害？若有，是否具备组织的特定流程对其进行了妥善处理？
7	是否对危害相关的危害事件进行了充分描述？
8	是否正确、全面地识别了危害事件的后果，是否包含合理的连锁反应后果？
9	运行场景列表的详细程度和分类是否合理？是否存在人为降低了暴露概率的情况？
10	针对所有已识别的因电气/电子(E/E)系统功能异常表现引起的危害事件，是否都按照以下参数进行了分类：严重度等级 S、运行场景的暴露概率等级 E、可控性等级 C？是否采取了保守分级的理念？
11	针对严重度等级 S 的评级是否合理？是否有明确的评级原则，并基于原则给予了充分的理由说明？是否考虑到危害事件中全部的涉险人员？涉险人员是否考虑了目标市场中有代表性的样本？
12	针对运行场景本身会导致伤害的情况(例如事故)，因电气/电子(E/E)系统功能异常表现导致的危害，其严重度分级是否基于有无功能异常表现导致的伤害差异？
13	是否存在 S0 评级的危害事件，若有，其评级理由是否充分？
14	针对暴露概率等级 E 的评级是否合理？是否有明确的评级原则，并基于原则给予了充分的理由说明？
15	在暴露概率评级时，是否排除了装备相关项的车型数量的影响？
16	是否存在场景评级为 E0 的危害事件，若有，其评级理由是否充分？
17	针对可控性等级 C 的评级是否合理？是否有明确的评级原则，并基于原则给予了充分的理由说明？对于可控性的评级是否存在必要的确认？
18	是否基于 S、E、C 分级，按照 GB/T 34590.1～34590.12—2022 正确地确定了每个危害事件的 ASIL 等级？
19	对于 S3 和 C3，而 ASIL 评级为 QM 的危害事件，其暴露概率的评级是否有充分的理由？
20	是否为每一个具有 ASIL 等级的危害事件都确定了其安全目标？
21	合并后的安全目标的 ASIL 等级是否为其对应危害事件的最高 ASIL 等级？
22	安全目标的属性和特性定义、安全目标的管理是否符合安全要求定义和管理的要求？

表 3　针对危害分析和风险评估的验证和确认的审核及评估检查清单

序号	检查清单
1	在进行危害分析和风险评估过程中，是否使用到了或从中得出了假设？若存在假设，是否在安全确认阶段对这些假设进行了确认？
2	是否按照表 6 中关于验证的检查清单的要求对危害分析和风险评估包括安全目标进行了充分的验证，且具备相应的证据？

附录 B 提供了针对危害分析和风险评估开展审核及评估的说明及示例。

7　功能安全概念

7.1　目标

本章的目标是对功能安全概念开发过程及结果进行审核及评估，以检查：

a）　对电气/电子(E/E)系统与安全目标相关的功能行为、功能降级行为进行了完整的定义；

b）　针对电气/电子(E/E)系统安全相关故障，定义了恰当的策略或措施，以进行充分和及时的探测、约束和减轻；

c）　将识别出的策略和措施以及定义的功能安全要求，分配给系统架构设计或外部措施；

d）　针对上述过程开展了充分的验证，并定义了合理的安全确认准则。

7.2　审核及评估的输入

为开展本章规定的审核及评估过程，应具备以下输入及其可能存在的验证报告：

——包含电气/电子(E/E)系统功能、运行场景、整车架构等内容的定义文档；

——危害分析和风险评估过程和结果报告；

——系统架构设计文档；

——功能安全概念报告；

——功能安全验证和确认计划和报告。

7.3　审核及评估的要求

对于电气/电子系统功能安全概念文档内容的审核及评估，应涵盖表 4 中的检查项。

表 4　功能安全概念的审核及评估检查清单

序号	检查清单
1	功能安全要求的属性和特性、功能安全要求的管理是否符合安全要求定义和管理的要求？
2	功能安全要求是否由安全目标导出？在定义功能安全要求时，是否考虑了系统架构设计？
3	每个安全目标是否都可追溯到至少一项功能安全要求？
4	如果适用，在功能安全要求中是否定义了故障避免的策略？
5	如果适用，在功能安全要求中是否定义了故障探测的策略，以及对故障或其导致的功能异常表现的控制策略？
6	如果适用，在功能安全要求中是否定义了过渡到安全状态的策略，及如果适用，过渡出安全状态的策略？
7	如果适用，在功能安全要求中，是否定义了故障容错的策略？

表 4　功能安全概念的审核及评估检查清单（续）

序号	检查清单
8	如果适用，在功能安全要求中，是否定义了故障情况下的功能降级策略？是否定义了功能降级与驾驶员警告之间的交互策略？针对不同故障风险，驾驶员警告机制是否明确和有效？
9	如果适用，故障处理时间间隔的定义是否满足故障容错时间间隔的要求？
10	如果适用，对于不同功能的多个控制请求，是否定义了仲裁策略，以避免或减轻可能导致的危害风险？
11	是否进行了安全分析以得到完整有效的功能安全要求？
12	在定义每项功能安全要求时，如果适用，是否考虑了相关项的运行模式、故障容错时间间隔、安全状态、紧急运行时间间隔及功能冗余？
13	在功能安全要求中，是否定义了相应的一个或多个安全状态以避免安全目标的违背？
14	是否对相关项过渡到安全状态的时间间隔进行了分析？对于不能在可接受的时间间隔内过渡到安全状态的情况，是否定义了紧急运行？
15	在功能安全概念中，是否对避免违反安全目标的驾驶员或其他人员的必要行动进行了假设？若存在，是否在功能安全概念中对其进行了定义，并定义了可供驾驶员或其他人员使用的足够的方法和控制手段？
16	是否将功能安全要求分配给了系统架构设计中的要素？ASIL 等级等信息是否与安全目标保持一致？如果应用了 ASIL 等级分解，是否符合 GB/T 43253.1—2023 中 6.7 关于 ASIL 等级分级的检查清单的要求？
17	承接功能安全要求的架构要素的开发是否符合这些安全要求的初始最高 ASIL 等级？若使用了 ASIL 等级分解，则承接初始安全要求的不同架构要素间的独立性，是否根据 GB/T 43253.1—2023 中表 22 要素共存的检查清单的要求进行了证明？
18	针对包含多个电气/电子(E/E)系统的相关项，是否定义了各个电气/电子(E/E)系统以及系统之间接口的功能安全要求？
19	如果适用，是否在功能安全概念中为各个电气/电子(E/E)系统分配了随机硬件故障度量目标值？
20	若存在功能安全要求的 ASIL 等级分解，是否符合 GB/T 43253.1—2023 中 6.7 关于 ASIL 等级分解的检查清单的要求？
21	若功能安全概念的实现需要基于其他技术的要素，则针对这些其他技术要素，是否合理分配了功能安全要求及属性？是否定义了与其他技术要素的接口相关的功能安全要求？这些要求及属性的实现是否具备充分的措施保证，并进行了必要的验证和确认？
22	如果适用，在定义功能安全概念时，是否考虑了外部措施的功能安全要求？
23	是否依据功能安全要求和安全目标定义了相关项安全确认的接受准则？
24	是否按照本表检查清单的要求对功能安全概念进行了充分的验证，且具备相应的证据证明功能安全概念与安全目标的一致性和符合性，及功能安全概念减轻或避免危害的能力？

附录 C 提供了针对功能安全概念开展审核及评估的说明及示例。

8　技术安全概念

8.1　目标

本章的目标是对以技术安全概念和技术安全需求为核心的系统层面产品开发阶段的相关工作成果进行审核及评估，以检查其定义是否符合功能安全开发的需要。

8.2 审核及评估的输入

为开展本章规定的审核及评估过程，应具备以下输入及其可能存在的验证报告：

——危害分析和风险评估报告；

——功能安全概念；

——其他涉及安全的相关项，对此相关项的要求（如果适用）；

——技术安全需求规范；

——技术安全概念；

——系统架构规范；

——软硬件接口（HSI）规范；

——生产、运行、服务和报废需求规范；

——安全分析报告。

8.3 审核及评估的要求

对技术安全概念开发的相关工作成果的审核及评估应涵盖表5中的检查项。

注：由于技术安全概念开发设计工作成果较多，表5按照技术安全概念、架构设计方案、技术安全需求规范、软硬件接口规范和生产、运行、服务和报废的需求规范的顺序组织检查项。安全机制的设计检查纳入技术安全需求规范的检查项中。

表5 技术安全概念开发活动的审核及评估检查清单

序号	检查清单
1	如果存在其他涉及安全的相关项对本系统的安全要求，是否作为系统层面开发阶段技术安全概念的设计输入？
2	是否存在包含系统层面开发阶段的系统架构设计的系统架构规范？技术安全概念和该系统架构规范的系统架构设计描述是否基于相关项定义、功能安全概念和先前的系统架构设计？并保持一致？如果存在不一致，是否通过恰当的活动进行迭代？
3	系统层面开发阶段的系统架构设计是否能实现技术安全要求？
4	系统架构设计是否识别了安全相关要素及其内外部接口？是否具备恰当的措施确保其他要素不会对这些安全相关要素产生不利的安全影响？
5	如果在系统层面开发阶段的系统架构设计对安全要求进行ASIL等级分解，分解的实施是否符合GB/T 43253.1—2023中6.7关于ASIL等级分解的检查清单的要求？
6	是否根据对应的ASIL等级，按照GB/T 34590.4—2022中表1的要求进行技术安全概念阶段的系统架构设计的安全分析？
7	技术安全概念是否消除已识别出的引起失效的内部原因和外部原因，或在必要时减轻它们的影响？
8	技术安全概念是否复用值得信赖的系统设计原则？如果复用，是否对设计原则的适用性进行了分析并形成了文档？
9	系统层面开发阶段的系统架构设计是否具有以下特征？ a) 模块化； b) 适当的颗粒度水平； c) 简单化

表 5　技术安全概念开发活动的审核及评估检查清单（续）

序号	检查清单
10	在安全分析或系统架构设计过程中，是否识别到新的尚未被安全目标涵盖的危害？若有，是否更新到危害分析和风险评估（HARA）中？
11	技术安全要求中定义的安全机制是否充分，以探测故障并防止或减轻出现在系统输出端的、导致违反功能安全要求的失效？
12	对于使相关项实现或维持安全状态的每个安全机制的定义，是否完整？
13	对于 ASIL（A）、（B）、C 和 D 等级，如果适用，是否定义了充分的安全机制，以防止随机硬件故障的多点故障变为潜伏故障？
14	对于 ASIL（A）、（B）、C 和 D 等级，为了避免多点失效，用于探测多点故障的安全机制的诊断测试策略是否合理？
15	对于 ASIL（A）、（B）、C 和 D 等级，专门用于防止双点故障变成潜伏故障的安全机制的开发是否符合要求？
16	是否根据系统架构设计，定义了充分地探测、控制或减轻随机硬件失效的措施？
17	对于 ASIL（B）、C 和 D 等级，针对随机硬件失效导致违背安全目标的可能性是否定义了明确的目标值？是否按照 GB/T 34590.5—2022 第 9 章的要求，使用备选分析方法中的一个方法进行了评估？
18	对于 ASIL（B）、C 和 D 等级，如果适用，是否在要素层面定义了适当的失效率和诊断覆盖率的目标值要求？
19	对于 ASIL（B）、C 和 D 等级，针对分布式开发，推导出的失效率和诊断覆盖率的目标值是否通报给每个相关团队？
20	技术安全需求规范中安全机制的定义是否与安全分析的结果一致？
21	是否按照功能安全概念、系统架构设计来定义技术安全要求？
22	是否在技术安全要求中定义了系统对影响安全要求实现的激励的响应（包括各种相关运行模式下和定义的系统状态下，激励与失效的组合）？
23	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，是否定义了这些功能或要求，或者参考其规范？
24	技术安全要求和非安全要求是否存在矛盾？
25	技术安全要求是否全部分配给以系统、硬件或软件作为实施技术的系统架构设计要素？
26	技术安全要求的分配和分区决策是否符合系统架构设计？
27	每个系统架构设计要素的 ASIL 等级是否继承其实现的技术安全要求的最高的 ASIL 等级？
28	如果系统架构要素中存在分配了不同 ASIL 等级的子要素（或部分子要素为非安全相关），是否全部子要素都按照要素的最高 ASIL 等级进行了开发？对于按照各自不同 ASIL 等级开发的子要素，他们是否符合第 1 部分表 22 关于要素共存的检查清单的要求？
29	对于分配了技术安全要求的具备可编程功能的定制化硬件要素，是否定义和实施了适当的开发流程？
30	如果适用，技术安全要求是否包含因实施 ASIL 等级分解而产生的独立性要求？
31	技术安全要求的定义和管理是否符合安全要求的定义和管理的要求？
32	是否存在定义了硬件和软件交互的软硬件接口（HSI）规范作为工作成果？
33	软硬件接口（HSI）规范中考虑的软硬件接口要素是否完善？并保持与技术安全概念一致？

表 5　技术安全概念开发活动的审核及评估检查清单（续）

序号	检查清单
34	软硬件接口规范中考虑的软硬件接口要素特性是否完善？是否定义了相关运行模式和配置参数？是否定义了确保要素间独立性或支持软件分区的硬件特性？是否定义了硬件资源的共用和专用？是否定义了硬件设备的访问机制？是否由技术安全概念导出了时间约束？
35	是否在软硬件接口规范中定义硬件的相关诊断能力和软件对其的使用？
36	是否定义在系统架构设计过程中识别出的对生产、运行、服务和报废的技术安全要求？
37	是否定义需具备的诊断特性以提供对系统进行现场监控所需的数据？
38	是否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？
39	是否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？
40	是否按照 GB/T 34590.4—2022 中表 2 要求的验证方法，对技术安全概念、系统架构设计、软硬件接口（HSI）规范以及生产、运行、服务和报废的需求规范进行了验证？

附录 D 提供了针对技术安全概念开展审核及评估的说明及示例。

9　验证和确认

9.1　目标

本章的目标是对验证和确认的相关工作成果进行审核及评估，以检查：

a）　相关项要素的集成是否根据系统化的方法，完成软硬件集成和验证、系统集成和验证、整车集成和验证；

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的实施；

c）　是否有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；

d）　验证工作成果是否符合相应的要求；

e）　是否有证据证明集成到目标车辆的相关项实现了其安全目标；

f）　是否有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。

9.2　审核及评估的输入

为了开展本章规定的审核及评估过程，应具备以下输入及其可能存在的验证报告：

——功能安全概念；

——技术安全概念；

——架构设计规范；

——软硬件接口规范；

——集成和测试策略；

——集成和测试报告；

——验证计划；

——验证规范；

——验证报告；

——危害分析和风险评估报告；

——包含安全确认环境描述的安全确认规范；

——安全确认报告。

9.3 审核及评估的要求

对于验证和确认的审核及评估，应涵盖表 6 和表 7 中的检查项。

表 6 集成验证活动的审核及评估检查清单

序号	检查清单
1	系统架构设计是否按照表 5 的检查清单进行了审核评估，结果是否符合功能安全和技术安全要求？ 是否按计划开展了集成测试活动？验证以下方面： a) 功能安全要求及技术安全要求是否正确实施； b) 安全机制是否具有正确的功能性能、准确性和时序； c) 接口是否具有一致性和正确实施； d) 系统架构设计是否有足够的鲁棒性
2	定义集成和测试策略时是否考虑系统架构规范、功能安全概念和技术安全概念？ a) 是否有合适的能够提供功能安全证据的测试目标； b) 相关项的集成和测试是否有助于安全概念的验证
3	a) 相关项集成和测试策略的定义是否包括了软硬件集成和测试规范； b) 相关项集成和测试策略的定义是否包括系统和整车层面的集成测试规范。软硬件验证的未解决问题是否已处理； c) 相关项集成和测试策略是否考虑车辆系统（相关项内部和外部）与环境之间的接口； d) 若相关项集成了以独立于环境的要素（SEooC）方式进行开发的系统或要素，在相关项集成和测试策略中是否考虑了对 SEooC 开发过程中做过的假设进行验证？
4	系统或整车层面的验证是否提供证据证明用于量产实施层面的配置符合安全要求？
5	在整个集成子阶段，对于每条功能安全要求和技术安全要求的符合性，是否至少进行过一次验证？
6	是否恰当地定义集成测试的测试用例？集成测试的测试用例是否使用合适的方法导出？
7	是否按照 GB/T 43253.3—2023 和 GB/T 43253.4—2023 检查清单的要求进行软硬件的开发？是否完成软硬件的集成？是否对集成后的硬件和软件进行测试？
8	是否通过测试证明了集成后的软件和硬件符合软硬件接口规范的要求？
9	对于软硬件集成测试的目标，是否通过使用适当的测试方法得到了实现？
10	是否通过合适的测试方法（基于需求的测试、故障注入测试、背靠背测试等）来证明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？
11	对于 ASIL（A）、B、C 和 D 等级，是否通过合适的测试方法（背靠背测试、性能测试等）对安全机制在软硬件层面的功能性能、准确性和时序进行论证？
12	对于 ASIL（A）、B、C 和 D 等级，是否通过合适的测试方法（外部接口测试、内部接口测试、接口一致性检查等）来证明外部和内部接口在软硬件层面执行的一致性和正确性？
13	对于 ASIL（A）、（B）、C 和 D 等级，是否通过合适的测试方法（故障注入测试、错误猜测法测试等）对故障模型，硬件故障探测机制在软硬件层面上的有效性进行论证？
14	对于 ASIL（A）、（B）、（C）和 D 等级，是否通过合适的测试方法（资源使用测试、压力测试等）对要素在软硬件层面的鲁棒性水平进行论证？
15	系统的各个要素是否按照系统架构设计进行集成？系统的各个要素是否按照系统集成测试规范进行测试？

表 6　集成验证活动的审核及评估检查清单（续）

序号	检查清单
16	对于系统集成测试的目标，是否通过使用适当的测试方法得到了实现？
17	是否通过合适的测试方法（基于需求的测试、故障注入测试、背靠背测试等）来证明功能安全和技术安全要求在系统层面的正确执行？
18	对于 ASIL（A）、（B）、（C）和 D 等级，是否通过合适的测试方法（背靠背测试、故障注入测试、性能测试、错误猜测法测试、来自现场经验的测试等）对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、时序进行论证？
19	是否通过合适的测试方法（外部接口测试、内部接口测试、接口一致性检查、通信和交互测试等）来证明外部和内部接口在系统层面执行的一致性和正确性？
20	是否通过合适的测试方法（资源使用测试、压力测试、特定环境条件下的抗干扰性和鲁棒性测试等）对系统层面的鲁棒性水平进行论证？
21	是否将相关项集成到整车上？是否实施整车集成测试？
22	是否对相关项与车内通信网络以及车内供电网络的接口规范进行验证？
23	整车集成测试的测试目标是否使用适当的测试方法来实现？
24	是否通过合适的测试方法（基于需求的测试、故障注入测试、长期测试、实际使用条件下的用户测试等）对功能安全要求在整车层面的正确执行进行论证？
25	对于 ASIL（A）、（B）、C 和 D 等级，是否通过合适的测试方法（性能测试、长期测试、实际使用条件下的用户测试、故障注入测试、错误猜测法测试、来自现场经验的测试等）对安全机制在整车层面的正确功能性能、准确性和时序进行论证？
26	对于 ASIL（A）、（B）、C 和 D 等级，是否通过合适的测试方法（内部接口测试、外部接口测试、通信和交互测试等）对整车层面内部和外部接口实现的一致性和正确性进行论证？
27	对于 ASIL（A）、（B）、C 和 D 等级，是否通过合适的测试方法（资源使用测试、压力测试、特定环境条件下的抗干扰性和鲁棒性测试、长期测试等）对整车层面的鲁棒性水平进行论证？
28	是否针对安全生命周期的每个阶段及子阶段，制定了对应的验证计划？
29	制定的验证计划中，是否包括了需验证的工作成果内容？
30	制定的验证计划中，是否包括了验证的目的？
31	制定的验证计划中，是否包括了用于验证的方法？
32	制定的验证计划中，是否包括了验证通过和不通过的准则？
33	如果适用，制定的验证计划中，是否包括了验证环境、用于验证的设备、用于验证的资源？
34	制定的验证计划中，是否包括了当探测出异常时需采取的行动？
35	制定的验证计划中，是否包括了回归策略？
36	制定验证计划是否考虑到所适用验证方法的充分性？是否考虑到需验证的工作成果的复杂性？是否考虑到与验证目标材料相关的前期经验？是否考虑到所使用技术的成熟度，或使用这些技术的风险？
37	验证规范中是否对用于验证的方法进行细化？细化的内容是否包含了评审或分析的检查清单；或模拟场景；或测试用例、测试数据和测试目标？

表 6　集成验证活动的审核及评估检查清单（续）

序号	检查清单
38	对于测试，每条测试用例的定义是否包含以下内容： a）　唯一的识别； b）　需验证的相关工作成果的版本的参考； c）　前提条件和配置； d）　环境条件（如果适用）； e）　输入数据、数据时序及其值； f）　期望的表现，包括输出数据、输出值的可接受范围、时间表现和公差表现； g）　确定测试用例通过和不通过的准则？
39	对于测试，是否从所需的测试设备或测试环境、逻辑和时间的依赖性、资源这几个方面考虑来按使用的测试方法对测试用例进行分组？
40	对于测试，测试用例是否由与待验证的工作成果的完成人不同的人进行评审？
41	是否按照验证计划和验证规范，执行验证？
42	验证是否由与待验证的工作成果的完成人不同的人执行？
43	对验证结果的评估是否包含以下信息： a）　所验证工作成果的唯一识别； b）　验证计划和验证规范的参考； c）　如果适用，评估中用到的验证环境配置、验证工具及标定数据； d）　验证结果与期望结果的一致性水平； e）　验证通过或不通过的明确的陈述，如果验证不通过，陈述应包含不通过的理由和对所验证工作成果进行修改的建议； f）　每个验证步骤未执行的理由？
44	用于验证的测试设备是否提供有效的和可重复的结果，并应按照所采用的质量管理体系进行管控？

附录 E 中的 E.1 提供了针对集成验证活动开展审核及评估的说明及示例。

表 7　确认活动的审核及评估检查清单

序号	检查清单
1	是否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？
2	是否考虑基于车型和车辆配置的典型车辆来定义典型环境？
3	对于危害分析和风险评估中考虑的、影响相关项技术特性的运行变化，在安全目标的确认过程中是否进行了考量？
4	是否定义安全确认规范，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—2022 中的附录 C； 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。
5	整车安全确认是否使用了恰当的方法？若使用测试进行整车安全确认，是否对测试规范、测试的执行和测试结果的评估进行了规范性检查？

表 7　确认活动的审核及评估检查清单（续）

序号	检查清单
6	整车安全确认是否对可控性进行评估？整车安全确认是否对外部措施的有效性进行评估？整车安全确认是否对其他技术要素的有效性进行评估？整车安全确认是否对影响危害分析与风险评估中 ASIL 等级的假设进行评估？
7	整车层面的安全确认是否基于安全目标、功能安全要求和预期用途？ 每个安全目标的安全确认流程和测试用例，是否都包括详细的通过/未通过准则？整车层面的安全确认是否考虑其应用范围？
8	安全确认是否通过以下方法的适当组合予以实施？ ——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； ——安全分析方法； ——长期测试； ——基于实际使用条件的测试； ——抽检和盲测； ——基于专家经验的测试； ——评审
9	安全确认的结果是否进行评估？安全确认的结果是否能够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？

E.2 提供了针对确认活动开展审核及评估的说明及示例。

附 录 A
（资料性）
相关项定义

相关项定义的审核及评估的说明及示例见表 A.1。

表 A.1 相关项定义的审核及评估的说明及示例

序号	检查清单	说明及示例
1	相关项需要满足的标准及法规要求有哪些？	对相关项需要满足的法规、国家标准和国际标准进行描述，包含法规名称、标准号、标准名称、标准版本号、标准发布日期等
2	相关项在整车层面的功能行为是什么？	如果适用，则： a) 应从输入、处理、输出等方面对功能进行描述； b) 应描述相关项的内部限制；例如：××相关项×××功能工作的速度范围是 55 km/h～120 km/h； c) 应描述功能的使用场景
3	是否定义了相关项的运行场景和运行模式？	运行场景的定义考虑功能的正常使用及可合理预见的误用场景，还应与目标市场相关联。 定义运行模式，应包含如下内容。 a) 对于模式的定义。如模式名称、模式的描述、该模式下允许及禁用的功能的定义。 b) 定义模式之间的转换关系。包含当前模式、下一模式、模式跳转的条件及时间约束、模式跳转后要执行的动作及时间约束等。为了使运行模式定义清晰明了，可采用模式流转关系图来表达，示例见图 A.1
4	是否定义了相关项的非功能性需求？	如果适用，可定义安装要求、机械要求、电气性能要求、耐久及可靠性要求、质量要求等。 例如： a) 对于安装要求，可描述出安装位置、安装方法等； b) 对于机械要求，可描述出质量、体积、尺寸、振动噪声、操作行程、操作力等的要求； c) 对于电气要求，可描述电压范围、电流范围、电机型号、电机驱动方式、电机工作温度范围、电机额定转矩、电机额定转速等； d) 对于耐久及可靠性要求，可描述使用次数、行驶公里数、使用年限等要求； e) 对于质量要求，可参考 IATF 16949 进行定义
5	是否定义了相关项的约束？	如果适用，应描述相关项的功能依赖性、与其他相关项的依赖性、运行环境等。 例如： a) 功能依赖性：如车道线检测横向误差≤10 cm，如 LKA 系统不具备处理复杂交通状况或环境突变等特殊工况的能力，当 LKA 功能介入控制时，需要驾驶员对路面状况保持警惕； b) 其他相关项的依赖性：当 EPS 检测到驾驶员的手力矩＞3 N·m 时，退出对 LKA 的扭矩请求响应； c) 运行环境：如功能适用的道路类型、相关项对于天气、光照条件等的约束

表 A.1　相关项定义的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
6	是否分析了相关项行为不足的潜在后果？	如果适用，应列出已知的失效模式及潜在的危害后果，可采用 HAZOP 方法进行分析。 如果适用，应总结之前类似或相关的相关项的经验教训
7	是否定义了执行器的能力或假定了执行器的能力？	如果适用，应对执行器的能力或假定能力进行定量描述，例如：输出扭矩、所受的力、运行速度、亮度、音量等的值或其估算值
8	是否清晰地定义了相关项的边界、要素、接口及交互关系？	如果适用，可采用初始架构框图的形式展现，要求展现出相关项的各个要素及要素之间的连接交互关系。示例见图 A.2。 在描述相关项的要素时，如果适用，可描述要素的名称、数量、布置形式、核心参数指标、承担的功能等。 在描述相关项的接口及交互关系时，如果适用，可描述接口所传递的信号或数据、接口的形式、接口的收发关系、信号或数据的优先顺序等
9	是否考虑了相关项的行为对整车影响的假设？	根据相关项的边界及接口的定义，考虑本相关项的输出对整车的影响。例如：采用分析、仿真和测试手段
10	是否考虑了其他相关项和要素要求本相关项提供的功能？	例如，LKA 相关项要求 EPS 提供的功能，当 EPS 检测到驾驶员的手力矩＞3 N·m 时，EPS 提供超控响应功能，即要求 EPS 退出对 LKA 的扭矩请求响应
11	是否考虑了本相关项要求其他相关项和要素提供的功能？	例如，EPS 相关项要求制动电子控制系统相关项提供车速信号
12	是否考虑了功能在所涉及的系统和要素间的分配？	如果适用，可按照功能划分，分别绘制各个功能的初始架构框图，以表明功能在所涉及的系统和要素间的分配情况
13	是否存在相关项定义的验证报告？	针对相关项的定义文档及相关信息进行评审，以确保功能安全开发输入的准确性和充分性

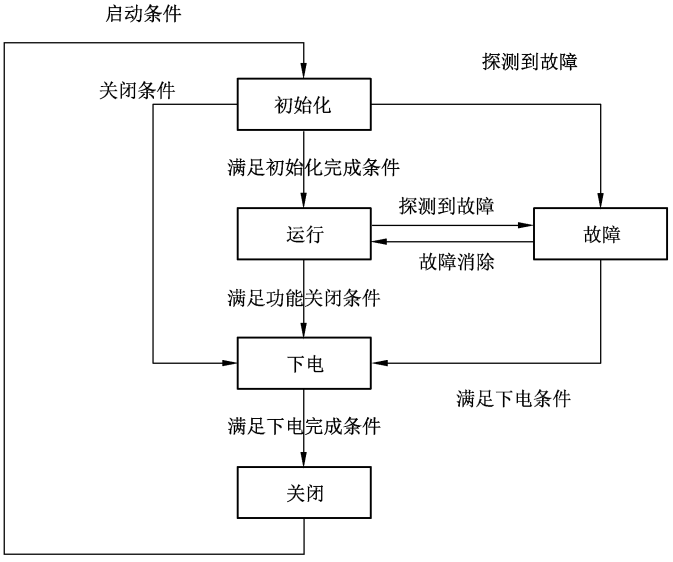

图 A.1　模式流转关系图示例

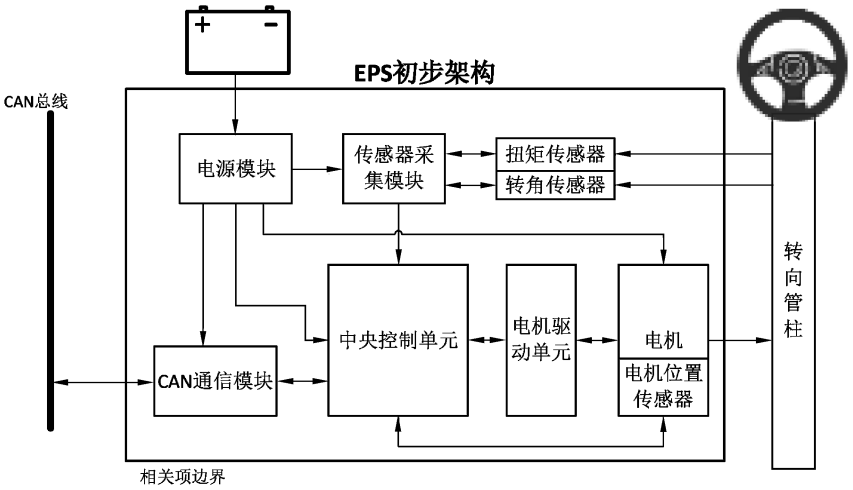

图 A.2　相关项架构框图示例

附 录 B
（资料性）
危害分析和风险评估

危害分析和风险评估的审核及评估的说明及示例见表 B.1、表 B.2。

表 B.1 危害分析和风险评估的审核及评估的说明及示例

序号	检查清单	说明及示例
1	危害分析是否涵盖了相关项的所有功能行为？是否与“相关项定义”阶段的功能行为保持了一致性及可追溯性？	—
2	在危害分析和风险评估过程中，对相关项内部安全机制是否未作为评估依据？	即在危害分析和风险评估过程中，不宜考虑将要实施或已经在先前相关项中实施的安全机制
3	对于相关项的功能异常表现导致的危害事件发生时所处的运行场景及运行模式是否进行了描述？是否考虑了可合理预见的误用？	a) 在进行运行场景描述时，如果适用，参考 GB/Z 42285—2022，可从车速、地点（高速公路、城市公路、乡村公路、交叉路口、停车场等）、道路条件（道路附着系数、道路坡度、道路宽度等）、驾驶操纵（启动、直行、倒车、转弯、变道等）、车辆状态（加速、减速、驻车、拖车、远程车辆启动等）、天气（雨天、雾天、侧风等）、周围交通（施工区域、交通拥堵、事故场景等）、车内外交通参与者（行人经过等）等方面进行描述。 b) 对于可合理预见的误用，可从驾驶员潜在的错误识别、决定和操作入手，给出分析
4	是否使用了系统性分析方法来确定危害？	a) FMEA 方法和 HAZOP 适用于支持相关项层面的危害识别。这些可通过头脑风暴、检查表、质量历史记录和现场研究来支持。 b) 在进行 HAZOP 分析时，如果适用，可参考 GB/Z 42285—2022，从如下几个方面对相关项功能进行分析，以确定危害： ——功能丧失（在有需求时，不提供功能）； ——在有需求时，提供错误的功能（多于预期、少于预期、方向相反）； ——非预期的功能（在无需求时，提供功能）； ——输出卡滞在固定值上（功能不能按照需求更新）
5	是否在整车层面上，定义了由相关项的功能异常表现导致的危害？	可从车辆行为或人员可感受到的表现出发，描述整车层面的影响，例如，非预期的减速，而非非预期的制动压力
6	危害分析过程中，是否识别出了因非电气/电子（E/E）系统功能异常表现导致的危害？若有，是否具备组织的特定流程对其进行了妥善处理？	a) 由相关项非失效情况下的行为导致的危害，不属于本文件的范围。 b) 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（E/E）系统的功能异常表现而引起的。 c) 若识别出上述范围外的危害，应进行记录，并明确组织处理流程、责任人、处理结果等

表 B.1　危害分析和风险评估的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
7	是否对危害相关的危害事件进行了充分描述？	a）　危害事件应由运行场景和危害的相关组合确定。 b）　危害事件的定义应足够，以支持我们在后续的风险评估中得到完整的、最危险的结果
8	是否正确、全面地识别了危害事件的后果，是否包含合理的连锁反应后果？	如果相关项层面的功能异常表现导致该相关项丧失多个功能，则场景分析和危害识别要考虑其综合影响。 **示例 1**：制动电子控制系统的功能丧失可能导致驾驶辅助功能同步无效。 **示例 2**：整车供电系统的失效可能导致同时丧失一系列功能，包括发动机扭矩、助力转向及前向照明
9	运行场景列表的详细程度和分类是否合理？是否存在人为降低了暴露概率的情况？	对一个危害来说，一个非常详细的关于车辆状况、道路条件和环境条件的运行场景列表，会使得用于危害事件分类的场景的颗粒度更为精细。这可更容易地评估可控性和严重度。然而，大量的不同运行场景可能导致相应地降低各自的暴露等级，从而导致不恰当地降低 ASIL 等级。这可通过合并类似的场景来避免
10	针对所有已识别的因电气/电子（E/E）系统功能异常表现引起的危险事件，是否都按照以下参数进行了分类：严重度等级 S、运行场景的暴露概率等级 E、可控性等级 C？是否采取了保守分级的理念？	如果难以对一个给定的危害进行严重度（S）、暴露概率（E）或可控性（C）的分级，需要采取保守分级的方法，即，一旦分级存在合理的怀疑，就采用较高的 S、E 或 C 等级
11	针对严重度等级 S 的评级是否合理？是否有明确的评级原则，并基于原则给予了充分的理由说明？是否考虑到危害事件中全部的涉险人员？涉险人员是否考虑了目标市场中有代表性的样本？	a）　应制定明确的严重度 S 评级标准。评级原则和理由例如 GB/T 34590.3—2022 中表 B.1，及 GB/Z 42285—2022 中表 B.1 基于碰撞速度的 S 分级原则。 b）　针对每一个危害事件，应依据评分标准，给出确定的理由来说明 S0、S1、S2 或 S3 确定的合理性。 c）　除引起危害事件的车辆的驾驶员或乘客，还需考虑其他潜在的处于风险中的人员，如骑自行车的人员、行人或其他车辆上的人员。 d）　对于涉险人员的代表性样本，例如上海老龄化比例约 35%。 e）　如果出现了 S0 严重度等级，则应提供足够的证据，证明后果明显仅限于物体损坏并不涉及对人员的伤害，此时无需分配 ASIL 等级
12	针对运行场景本身会导致伤害的情况（例如事故），因电子/电气（E/E）系统功能异常表现导致的危害，其严重度分级是否基于有无功能异常表现导致的伤害差异？	**示例**：被考虑的相关项包含用于减少碰撞所致伤害的安全气囊功能。如果事故发生时安全气囊未能正常打开，那么由碰撞导致的伤害可被确定。如果相同事故中安全气囊正常打开可将伤害降低到一个较低的严重度等级，那么，在严重度评级时只需考虑两者的差异。
13	是否存在 S0 评级的危害事件，若有，其评级理由是否充分？	相关项的功能异常表现的后果仅限于物损，不涉及人员伤害

表 B.1　危害分析和风险评估的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
14	针对暴露概率等级 E 的评级是否合理？是否有明确的评级原则，并基于原则给予了充分的理由说明？	a）　应制定明确的暴露概率 E 评分标准，包括基于场景的持续时间和基于场景发生的频率两种。可参考 GB/T 34590.3—2022 中表 B.2～表 B.5 或目标市场运行场景的统计数据等，给出评级标准与 GB/T 34590.1～34590.12—2022 暴露概率等级 E0、E1、E2、E3 或 E4 的对应关系。 b）　针对每一个危害事件，应依据评级标准，给出确定的理由来说明 E0、E1、E2、E3 或 E4 确定的合理性
15	在暴露概率评级时，是否排除了装备相关项的车型数量的影响？	暴露概率的评估是基于假设每个车辆都配备有该相关项进行的。这意味着“因为该相关项未装备在每台车辆上（只有一些车辆装备该相关项），所以暴露概率会降低”的观点是不成立的
16	是否存在场景评级为 E0 的危害事件，若有，其评级理由是否充分？	如果出现了 E0 暴露概率等级，则应提供足够的证据，证明该场景是不寻常或令人难以置信的，此时无需分配 ASIL 等级。 例如： a）　极其不寻常的或不可能同时发生的情况，例如车辆涉及在高速公路上降落的飞机的事故。 b）　自然灾害，如地震、飓风、森林大火
17	针对可控性等级 C 的评级是否合理？是否有明确的评级原则，并基于原则给予了充分的理由说明？对于可控性的评级是否存在必要的确认？	a）　应制定明确的可控性等级 C 的评级标准。可参考 GB/T 34590.3—2022 中表 B.6。 b）　针对每一个危害事件，应依据评分标准，给出确定的理由来说明 C0、C1、C2 或 C3 确定的合理性。 c）　如果出现了 C0 可控性等级，则应提供足够的证据，证明危害不影响车辆的安全运行，或者可通过常规的驾驶员行为来避免事故，此时无需分配 ASIL 等级。例如：一些驾驶员辅助系统不可用的危害。 d）　对于可控性的预估，应在验证和确认阶段对可控性分级的合理性进行检查
18	是否基于 S、E、C 分级，按照 GB/T 34590—2022 正确地确定了每个危害事件的 ASIL 等级？	见 GB/T 34590.3—2022 中的表 4
19	对于 S3 和 C3，而 ASIL 评级为 QM 的危害事件，其暴露概率的评级是否有充分的理由？	如果几种不太可能的场景组合导致暴露概率低于 E1，即使危害事件达到 S3 和 C3 仍然可认定为 QM **示例 1**：对于高压系统错误供电的功能异常，组合运行场景是： ——导致安全气囊点爆的碰撞； ——车辆的一部分处于水中； ——高压系统部分暴露，没有造成内部短路。 **示例 2**：对于燃油泵错误供应汽油的功能异常，组合运行场景是： ——导致安全气囊点爆的碰撞； ——泵后面的油箱系统保持功能齐全； ——泵的燃油管路破裂，以致汽油会滴在热部件上； ——泵的能源供应功能齐全。

表 B.1　危害分析和风险评估的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
20	是否为每一个具有 ASIL 等级的危害事件都确定了其安全目标？	对于具有 ASIL 等级的危害，均应定义安全目标，且对于同类安全目标可合并 **示例**：对于 EPS 非预期输出转向扭矩和转向扭矩过大导致的危害，可将安全目标合并描述为：避免因 EPS 转向扭矩异常导致车辆非预期的侧向运动。
21	合并后的安全目标的 ASIL 等级是否为其对应危害事件的最高 ASIL 等级？	根据安全目标与危害事件的追溯关系，确认安全目标继承了相关危害事件的最高 ASIL 等级
22	安全目标的属性和特性定义、安全目标的管理是否符合安全要求定义和管理的要求？	a）　安全目标的属性：安全目标应具备唯一识别并保持不变、状态、ASIL 等级。 b）　安全目标的特性：安全目标应是明确的、可理解的、不可分割的、内部一致的、可行和可实现的、可验证的、必要的、实施自由的、完整合规的。 c）　安全目标的管理：可追溯、可维护、合理地验证

表 B.2　针对危害分析和风险评估的验证和确认的审核及评估的说明及示例

序号	检查清单	说明及示例
1	在进行危害分析和风险评估过程中，是否使用到了或从中得出了假设？若存在假设，是否在安全确认阶段对这些假设进行了确认？	a）　如果适用，在 HARA 中考虑的假设包括：驾驶员或处于风险中的人员的假定行为以及外部措施的相关假设。 b）　参考 GB/T 34590.4—2022 中 8.4.3.2，影响危害分析与风险评估中 ASIL 等级的假设应在最终车辆上进行检查。 c）　**示例**：假设一个机械组件能够防止或减轻由电气/电子（E/E）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应在整车层面进行确认
2	是否按照表 6 中关于验证的检查清单的要求对危害分析和风险评估包括安全目标进行了充分的验证，且具备相应的证据？	应提供证据，以证明： ——场景和危害组合的代表性、适用性说明； ——对相关项功能异常的识别充分涵盖了相关项功能定义； ——是否考虑了其他相关项 HARA 结果中与本相关项有关的内容； ——危害事件分析采用了系统化方法，分析具有完备性； ——对于分配了 ASIL 等级的危害事件，其安全目标的定义能充分避免危害事件的发生。安全目标与所分配的 ASIL 等级以及相应的危害事件保持一致

附 录 C
（资料性）
功能安全概念

功能安全概念的审核及评估的说明及示例见表 C.1。

表 C.1 功能安全概念的审核及评估的说明及示例

序号	检查清单	说明及示例
1	功能安全要求的属性和特性、功能安全要求的管理是否符合安全要求定义和管理的要求？	a) 功能安全要求应具有如下属性：功能安全要求应具备唯一识别并保持不变、状态、ASIL 等级。 b) 功能安全要求应具有如下特性：明确的、可理解的、不可分割的、内部一致的、可行和可实现的、可验证的、必要的、实施自由的、完整的、合规的。 c) 功能安全要求的管理：可追溯、可维护、合理地验证
2	功能安全要求是否由安全目标导出？在定义功能安全要求时，是否考虑了系统架构设计？	a) 如果适用，应为每一条 FSR 指定其对应的 SG，确保 FSR 与 SG 之间的双向可追溯性； b) 如果适用，考虑系统架构设计中各要素与安全目标之间的对应关系，通过对相关系统要素进行安全分析，得出功能安全要求
3	每个安全目标是否都可追溯到至少一项功能安全要求？	a) 每一条安全目标都具备承接的 FSR； b) 同一个功能安全要求可由几个不同的安全目标导出
4	如果适用，在功能安全要求中是否定义了故障避免的策略？	为避免随机硬件故障，可参考 FMEA、行业最佳实践等的故障避免措施，例如：为避免短路采用 ECU 电路板热熔胶工艺、为避免进水短路或腐蚀采用密封圈/密封胶工艺
5	如果适用，在功能安全要求中是否定义了故障探测的策略，以及对故障或其导致的功能异常表现的控制策略？	如果适用，应依据安全分析系统性地得出违背安全目标的相关故障，并针对这些故障定义探测和控制策略。例如：根据 EPS 的 FMEA 分析，电源管理芯片应探测电源的过压、欠压、漂移、尖峰故障，当出现上述故障后，为避免可能导致非预期侧向运动的转向助力，系统应关闭部分或全部助力
6	如果适用，在功能安全要求中是否定义了过渡到安全状态的策略，及如果适用，过渡出安全状态的策略？	定义了系统状态机、各个状态间的过渡过程和跳转条件，在此过程中考虑跳转条件和状态的组合符合安全目标 **示例**：对于 EPS 系统，当总线车速信号发生信号丢失故障后，系统进入默认助力的安全状态，同时发出驾驶员警示；当总线车速信号恢复后，助力柔和恢复至正常状态，同时取消驾驶员警示。
7	如果适用，在功能安全要求中，是否定义了故障容错的策略？	**示例**：当 EPS 失去助力可能导致违背安全要求时（失去助力后转向力沉重或主动转向功能非预期关闭），增加了冗余助力设计。
8	如果适用，在功能安全要求中，是否定义了故障情况下的功能降级策略？是否定义了功能降级与驾驶员警告之间的交互策略？针对不同故障风险，驾驶员警告机制是否明确和有效？	a) 针对“故障情况下的功能降级策略”，例如：当 EPS 的 ECU 电路板温度超过 110 ℃后，EPS 将从正常助力状态，平缓过渡到过温条件发生后的降低助力状态。 b) 针对“将风险暴露时间缩短到可接受时间所需的驾驶员警告”，例如：序号 6 中，安全状态的警示为“转向备份系统故障，10 个点火循环后将关闭助力，请尽快维修”。 c) 针对“增加驾驶员可控性所需的驾驶员警告”，例如：发生过温故障降低助力时，驾驶员警告信息为“转向助力降低，请控制方向”

表 C.1　功能安全概念的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
9	如果适用，故障处理时间间隔的定义是否满足故障容错时间间隔的要求？	a）针对不同类型的故障，应根据故障容错时间间隔定义故障处理时间间隔，以确保故障探测和处理的及时性，避免危害风险。例如：针对 EPS 非预期转向的探测和助力关断时间，避免错误的助力可能使车辆产生非预期的侧向运动。 b）相关时间间隔的制定可基于测试、仿真或分析，并最终得到确认
10	如果适用，对于不同功能的多个控制请求，是否定义了仲裁策略，以避免或减轻可能导致的危害风险？	a）不同功能的控制请求可能来自内部功能（如 EPS 主动回正、摩擦补偿功能）或外部功能（如车道保持 LKA 功能）； b）仲裁策略可能是功能优先级顺序（如 LKA 功能优先级高于主动回正功能）或功能约束限制（如为 EPS 主动回正和摩擦补偿功能设置力矩上限）等
11	是否进行了安全分析以得到完整有效的功能安全要求？	a）为了制定一套完整有效的功能安全要求，可使用例如 FMEA、FTA、STPA、HAZOP 等分析方法； b）针对安全分析中识别出的故障和风险，都针对性制定了功能安全要求，并进行有效性的验证确认
12	在定义每项功能安全要求时，如果适用，是否考虑了相关项的运行模式、故障容错时间间隔、安全状态、紧急运行时间间隔及功能冗余？	见表 A.1 中序号 3 运行模式，表 C.1 中序号 9 故障容错时间间隔、序号 6 安全状态、序号 8 紧急运行时间间隔及功能冗余的说明及示例
13	在功能安全要求中，是否定义了相应的一个或多个安全状态以避免安全目标的违背？	**示例**：根据不同的故障，EPS 的安全状态可为关闭助力、降低助力、维持助力到当前点火循环结束、维持助力到一定的点火循环结束、关闭部分辅助功能、关闭主动转向功能等。
14	是否对相关项过渡到安全状态的时间间隔进行了分析？对于不能在可接受的时间间隔内过渡到安全状态的情况，是否定义了紧急运行？	**示例**：针对部分 EPS 故障，其安全状态可能是“车辆静止后警告驾驶员并关闭助力”，但在行车过程中，不能马上进入到该安全状态，为此，可采取的紧急运行是“提供有限的助力并警告驾驶员，直到车辆停止”，再进入安全状态。
15	在功能安全概念中，是否对避免违反安全目标的驾驶员或其他人员的必要行动进行了假设？若存在，是否在功能安全概念中对其进行了定义，并定义了可供驾驶员或其他人员使用的足够的方法和控制手段？	在功能安全概念中，针对 EPS 非预期转向行为，可能假设和定义了驾驶员会施加必要的纠正力矩。为此，可能对 EPS 转向力矩进行约束，同时在发生故障时，通过警示信息提醒驾驶员及时采取纠正操作
16	是否将功能安全要求分配给了系统架构设计中的要素？ASIL 等级等信息是否与安全目标保持一致？如果应用了 ASIL 等级分解，是否符合 GB/T 43253.1—2023 中 6.7 关于 ASIL 等级分级的检查清单的要求？	a）对于每项功能安全要求，应将其分配给系统架构设计中一个或多个要素，确保功能安全要求与系统要素之间的双向可追溯性。 b）功能安全要求的 ASIL 等级及信息（运行模式、FTTI、安全状态、紧急运行时间间隔、功能冗余等）应从安全目标中继承得到。 c）如果应用了 ASIL 等级分解，应符合 GB/T 34590.9—2022 中第 5 章的要求

表 C.1　功能安全概念的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
17	系统架构中，承接了不同 ASIL 等级安全要求的架构要素之间，是否根据 GB/T 43253.1—2023 中表 22 要素共存的检查清单免于干扰的要求，若不符合，这些要素是否按照相关要求的最高 ASIL 等级进行了开发？	根据功能安全要求与架构要素的双向追溯关系，识别每个架构要素所需满足的最高 ASIL 等级。对于系统架构中，承接了不同 ASIL 等级安全要求的要素，应明确相关要素之间是否存在可能导致违背安全要求的级联失效，是否符合免于干扰的要求 **示例**：某 EPS 内扭矩传感器分配了 ASIL D 等级要求（来自 EPS 内部），而内置的转角传感器分配了 ASIL B 等级要求（来自车辆稳定性控制功能要求），若不能证明该转角传感器与扭矩传感器之间免于干扰（无级联失效），则转角传感器也应按照 ASIL D 等级要求开发
18	针对包含多个电气/电子（E/E）系统的相关项，是否定义了各个电气/电子（E/E）系统以及系统之间接口的功能安全要求？	a）　功能安全概念文档中，包含相关项架构，在该架构中能清楚识别组成相关项的全部电气/电子（E/E）系统及其内外部接口。 **示例**：LKA 包括摄像头系统和 EPS 系统。 b）　针对这些系统和接口定义功能安全要求，并将接口的要求也分配到相关系统中，避免实施遗漏 **示例**：针对 LKA 功能，摄像头系统与 EPS 系统间的功能交互，对摄像头系统和 EPS 系统同时提出通信保护和监控要求。
19	如果适用，是否在功能安全概念中为各个电气/电子系统分配了随机硬件故障度量目标值？	a）　可根据组成相关项的各个电气/电子（E/E）系统对危害行为和安全目标的贡献，采用系统性分析手段，如 FTA，对各个系统进行随机硬件故障度量目标值的分配。 b）　分配的目标一方面是确保最终目标值的达成，同时也有利于在开发早期合理平衡开发难度。例如：对于成熟可靠的系统分配较高目标，而对于全新开发的复杂系统分配较低目标
20	若存在功能安全要求的 ASIL 等级分解，是否符合 GB/T 43253.1—2023 中 6.7 关于 ASIL 等级分解的检查清单的要求？	ASIL 等级分解符合 GB/T 34590.9—2022 第 5 章的要求，见 ASIL 等级分解检查清单要求
21	若功能安全概念的实现需要基于其他技术的要素，则针对这些其他技术要素，是否合理分配了功能安全要求及属性？是否定义了与其他技术要素的接口相关的功能安全要求？这些要求及属性的实现是否具备充分的措施保证，并进行了必要的验证和确认？	若适用： a）　相关安全要求应包含针对其他技术要素的功能安全要求，其实现具备可追溯性； b）　相关安全要求应包含相关项与其他技术要素的接口要求； c）　对上述要求的实现，是否具备特定的措施保证； d）　确认计划中应包含上述安全要求的确认； e）　对于分配给其他技术要素的功能安全要求无需分配 ASIL 等级，但对于承接了同一功能安全要求的相关项内部要素，可按照 GB/T 34590.9—2022 第 5 章，使用 ASIL 等级分解，在此情况下，应在 GB/T 34590—2022 的基础上，定义实施和验证规则 **示例**：对于 EPS，通过关断助力而进入安全状态的功能安全概念，需要依靠车辆机械转向系统保证，为此需要对机械转向系统的转向助力比值提出要求，以确保人员具备足够的可控性，并应对整车实现效果进行验证和确认。

表 C.1　功能安全概念的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
22	若功能安全概念的实现需要基于外部措施，则针对这些外部措施，是否定义并对其传递了功能安全要求？并确认了其实现？	a）　相关安全要求应包含相关项与外部措施的接口； b）　若外部措施是由电气/电子(E/E)系统实现，则对其要求的定义应符合 GB/T 34590.1～34590.12—2022； c）　确认计划中应包含外部措施实现安全要求的确认 **示例**：对于同时具备 EPS 和 ARS 系统的车辆，EPS 自动转向功能安全概念的实现，可依赖于通过 ARS 系统实施备份的主动转向功能。为此，可导出针对 ARS 系统的接口需求，如 ARS 应监控 EPS 功能状态，若探测到故障，应激活主动转向功能。
23	是否依据功能安全要求和安全目标定义了相关项安全确认的接受准则？	a）　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： ——可控性； ——外部措施的有效性； ——其他技术要素的有效性； ——影响危害分析与风险评估中 ASIL 等级的假设只能在最终车辆上进行检查。 b）　安全确认不仅在 V 流程的安全确认活动（V 流程的右侧顶端）中执行，也在开发阶段中执行（而不仅在开发结束时执行） **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应在整车层面进行确认，例如针对机械转向可控性的确认。
24	是否按照本表检查清单的要求对功能安全概念进行了充分的验证，且具备相应的证据证明功能安全概念与安全目标的一致性和符合性，及功能安全概念减轻或避免危害的能力？	a）　通过验证，确保功能安全概念与安全目标的一致性和符合性； b）　通过验证，证明功能安全概念在减轻或避免危害上的能力 **示例**：减轻或避免危害的能力，可通过测试、试运行或专家判断来评估，可结合原型、研究报告、专项测试或仿真。

附 录 D
（资料性）
技术安全概念

技术安全概念开发的审核及评估的说明及示例见表 D.1。

表 D.1 技术安全概念开发的审核及评估的说明及示例

序号	检查清单	说明及示例
1	如果存在其他涉及安全的相关项对本系统的安全要求，是否作为系统层面开发阶段技术安全概念的设计输入？	例如，LKA 相关项对 EPS 相关项提出了功能安全要求，当 EPS 检测到驾驶员的手力矩＞3 N·m 时，EPS 提供超控响应功能，即要求 EPS 退出对 LKA 的扭矩请求响应。这个要求也应纳入 EPS 的系统层面开发输入
2	是否存在包含系统层面开发阶段的系统架构设计的系统架构规范？技术安全概念和该系统架构规范的系统架构设计描述是否基于相关项定义、功能安全概念和先前的系统架构设计？并保持一致？如果存在不一致，是否通过恰当的活动进行迭代？	应对比和检查技术安全概念/系统层面开发阶段的架构设计/安全架构方案与相关项定义/功能安全概念阶段使用的架构设计的一致性。 例如：输入输出的接口定义、架构要素的描述、工作模式、系统状态定义等。 对于不一致的地方，是否对功能安全概念阶段的活动进行了迭代更新？
3	系统层面开发阶段的系统架构设计是否能实现技术安全要求？	应具备证据说明系统架构设计实现了技术安全要求，证据包括： ——系统架构设计与技术安全要求的对应关系； ——用于实现技术安全要求的软硬件具备充分的技术能力； ——对于系统架构设计实现的技术安全要求可被验证，且在系统集成过程中进行了测试
4	系统架构设计是否识别了安全相关要素及其内外部接口？是否具备恰当的措施确保其他要素不会对这些安全相关要素产生不利的安全影响？	恰当的措施应确保： ——对系统架构中所有安全相关要素进行识别； ——对安全相关要素，定义其内部和外部接口； ——考虑其他要素对安全相关要素的影响，避免影响安全 **示例**：可通过 FMEA、相关失效分析、接口测试等实现上述过程。
5	如果在系统层面开发阶段的系统架构设计对安全要求进行 ASIL 等级分解，分解的实施是否符合 GB/T 43253.1—2023 中 6.7 关于 ASIL 等级分解的检查清单的要求？	如果适用，应按照 GB/T 43253.1—2023 中 ASIL 等级分解的审核评估检查清单执行
6	是否根据对应的 ASIL 等级，按照 GB/T 34590.4—2022 中表 1 的要求进行技术安全概念阶段的系统架构设计的安全分析？	应提供证据证明安全分析开展符合 ASIL 等级的要求，安全分析的实施符合 GB/T 43253.1—2023 中关于 ASIL 等级分解的检查清单的要求，安全分析的评审记录、开口项信息和版本信息，其相关状态信息都应在技术安全概念的工作成果中存在相应记录

表 D.1　技术安全概念开发的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
7	技术安全概念是否消除已识别出的引起失效的内部原因和外部原因，或在必要时减轻它们的影响？	应提供证据证明对于在安全分析中发现的，引起失效的内部原因和外部原因都有合适安全机制或缓解措施
8	技术安全概念是否复用值得信赖的系统设计原则？如果复用，是否对设计原则的适用性进行了分析并形成了文档？	值得信赖的系统设计原则可能包括： ——值得信赖的技术安全概念的复用； ——值得信赖的要素设计的复用，包括硬件和软件组件； ——值得信赖的探测和控制失效的机制的复用； ——值得信赖的或标准化接口的复用。如果复用，需要提供设计原则的适用性或差异分析报告，以确保最终产品应用的一致性和适用性
9	系统层面开发阶段的系统架构设计是否具有以下特征： a）　模块化； b）　适当的颗粒度水平； c）　简单化	架构设计的模块化，适当的颗粒度水平和简单原则可有效的避免系统失效；可通过分层设计、精确的接口定义、避免组件和接口的不必要的复杂性、可维护性和可验证性之类的设计原则实现
10	在安全分析或系统架构设计过程中，是否识别到新的尚未被安全目标涵盖的危害？若有，是否更新到危害分析和风险评估（HARA）中？	如果适用，提供更新的相关证据
11	技术安全要求中定义的安全机制是否充分，以探测故障并防止或减轻出现在系统输出端的、导致违反功能安全要求的失效？	a）　如果适用，在定义安全机制时，应包含： ——与系统自身故障相关的安全机制； ——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； ——使系统实现或者维持在相关项的安全状态的安全机制； ——定义和执行报警和降级策略的安全机制； ——防止故障处于潜伏状态的安全机制。 b）　如果适用，在定义每一个安全机制时，宜考虑如下方面： ——故障的探测，可定义探测何种故障，采用何种方法进行故障探测； ——故障的指示，描述当出现何种现象时，认为故障发生，包含对时间、周期等的描述； ——故障的控制，当确认故障发生后，系统应如何响应以避免违背安全目标； ——故障的恢复条件，定义在什么条件下，可认为故障恢复； ——安全机制的有效性评估

表 D.1　技术安全概念开发的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
12	对于使相关项实现或维持安全状态的每个安全机制的定义，是否完整？	定义应包括： a）　相关项可能所处的状态与安全状态间的转换的定义，包括转换过程中对执行器的如何控制的要求； **示例**：对于一个激光 LiDAR 传感器，用于监测发射功率异常的安全机制明确定义当监测到激光发射功率超出安全标准时，激光 LiDAR 从正常工作状态切换到错误工作状态，而错误工作状态也明确定义了会关闭激光发射。 b）　故障处理时间间隔的定义，该定义宜考虑架构层面的时间约束要求，以确保满足相关安全目标的 FTTI； c）　若不能在 FTTI 允许的时间内进入相关项的安全状态，则应定义紧急运行容错时间间隔。该定义可基于整车测试或试验 **示例 1**：进入安全状态之前的降级运行持续时间。 **示例 2**：线控制动的供电安全机制，定义了备用电源或储能设备，及其电能容量、启动所需的时间、运行能持续的时间等。
13	对于 ASIL（A）、（B）、C 和 D 等级，如果适用，是否定义了充分的安全机制，以防止随机硬件故障的多点故障变为潜伏故障？	**示例**：系统各个状态下的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。
14	对于 ASIL（A）、（B）、C 和 D 等级，为了避免多点失效，用于探测多点故障的安全机制的诊断测试策略是否合理？	用于探测多点故障的安全机制的针对测试策略宜考虑： a）　诊断测试策略与被探测硬件组件的可靠性要求、该硬件组件在架构中的角色、其对多点失效的贡献是否匹配？ b）　是否符合 GB/T 34590—2022 第 9 章随机硬件失效度量目标值的要求？ c）　与分配的 ASIL 等级（来自安全目标或上一级的安全要求）是否匹配？ d）　是否小于多点故障探测时间间隔？ **示例 1**：诊断测试策略可为时间驱动（例如使用诊断测试时间间隔）或者事件驱动（例如启动测试）。 **示例 2**：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；系统或要素在维护时的测试。
15	对于 ASIL（A）、（B）、C 和 D 等级，专门用于防止双点故障变成潜伏故障的安全机制的开发是否符合要求？	对于分配为 ASIL D 等级的技术安全要求，为了防止双点故障变成潜伏故障而实施的安全机制至少为 ASIL B 等级。 对于分配为 ASIL B 等级和 ASIL C 等级的技术安全要求，为了防止双点故障变成潜伏故障而实施的安全机制至少为 ASIL A 等级。 对于分配为 ASIL A 等级的技术安全要求了防止双点故障变成潜伏故障而实施的安全机制至为 QM 等级 **示例**：某内存存储采用奇偶校验作为安全机制，该机制要求为 ASIL B 等级。为了防止双点故障变成潜伏故障，开发了专门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，对于该自检测试的开发应至少满足 ASIL A 的要求。

表 D.1　技术安全概念开发的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
16	是否根据系统架构设计，定义了充分地探测、控制或减轻随机硬件失效的措施？	基于定量分析（例如 FMEDA、FTA 等），确定已定义的措施是否充分 **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）。
17	对于 ASIL（B）、C 和 D 等级，针对随机硬件失效导致违背安全目标的可能性是否定义了明确的目标值？是否按照 GB/T 34590.5—2022 第 9 章的要求，使用备选分析方法中的一个方法进行了评估？	目标值的定义应根据安全目标的 ASIL 等级，在 GB/T 34590.5—2022 中表 6 随机硬件失效目标值中选取。还宜考虑其他相关项对本相关项的随机失效目标要求。 例如：ADAS 相关项对 EPS 相关项的转向失效目标值要求，可能与 EPS 自身安全目标要求不同。 潜在分析方法包括：随机硬件失效概率度量（PMHF）的评估和通过对违背安全目标的每个原因的评估（EEC）
18	对于 ASIL（B）、C 和 D 等级，如果适用，是否在要素层面定义了适当的失效率和诊断覆盖率的目标值要求？	为了满足硬件架构度量的要求，并且为了支持对随机硬件失效导致违背安全目标的评估，推荐在要素层面定义失效率和诊断覆盖率目标
19	对于 ASIL（B）、C 和 D 等级，针对分布式开发，推导出的失效率和诊断覆盖率的目标值是否通报给每个相关团队？	导出的失效率和诊断覆盖率目标值，应在分布式开发团队间进行书面传递。可由负责架构安全开发的团队将导出的目标值传递给要素开发团队，作为其设计输入；也可由要素开发团队，反馈要素的失效模式、失效率、诊断覆盖率等信息，由架构层面进行集成和评估。 例如，对于商业现成产品的元器件和组件，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，以便允许在整体硬件架构层面上预估架构约束
20	技术安全需求规范中安全机制的定义是否与安全分析的结果一致？	—
21	是否按照功能安全概念、系统架构设计来定义技术安全要求？	技术安全要求应与功能安全概念、相关项的系统架构设计保持一致性，不存在冲突。 在定义技术安全要求时，是否考虑了如下方面： 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； c）　系统可配置性。 设计约束可能来自环境条件、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）。 如果适用，系统的外部接口可考虑：接口的形式（CAN、LIN、PWM 等）、接口的方向（输入、输出）、传递的内容、传递的周期或其他时间要求等。 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

表 D.1　技术安全概念开发的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
22	是否在技术安全要求中定义了系统对影响安全要求实现的激励的响应（包括各种相关运行模式下和定义的系统状态下，激励与失效的组合）？	a）　相关设计规范或安全文档中，具备系统运行模式和系统状态的定义清单； b）　基于安全分析、已有经验等，给出不同激励与失效的组合 **示例**：如果收到的 ACC 指令信息，未通过错误检测代码，如 CRC 校验的检查，则制动电子控制系统将禁用自适应巡航控制（ACC）制动。
23	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，是否定义了这些功能或要求，或者参考其规范？	除技术安全要求中已涉及的功能或要求外，对于相关项需要实现或符合的其他功能或要求，应进行定义或给出参考索引。 此举有助于考虑技术安全要求的完整性，及安全要求与非安全要求的交互，避免矛盾
24	技术安全要求和非安全要求是否存在矛盾？	对于技术安全要求和非安全要求可能存在的矛盾，进行了统筹分析和评审，具备分析和评审结论
25	技术安全要求是否全部分配给以系统、硬件或软件作为实施技术的系统架构设计要素？	对于每项技术安全要求，应将其分配给系统架构设计中软件或硬件要素。 如果某项技术安全要求被分配给作为实施技术的系统中，则再次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； 要确保技术安全要求与软件和硬件要素之间的双向可追溯性
26	技术安全要求的分配和分区决策是否符合系统架构设计？	为了实现独立性和避免失效传播，系统架构设计可能采用功能分区和组件分区，技术安全要求的分配和分区应与系统架构设计采用功能分区和组件分区保持一致
27	每个系统架构设计要素的 ASIL 等级是否继承其实现的技术安全要求的最高的 ASIL 等级？	如果有多项技术安全要求分配到同一个系统架构设计中软件或硬件要素，则这个软件或硬件要素按照 ASIL 等级最高的技术安全要求的 ASIL 等级开发
28	如果系统架构要素中存在分配了不同 ASIL 等级的子要素（或部分子要素为非安全相关），是否全部子要素都按照要素的最高 ASIL 等级进行了开发？对于按照各自不同 ASIL 等级开发的子要素，他们是否符合第 1 部分表 22 关于要素共存的检查清单的要求？	对于架构要素的子要素，应按照要素的最高 ASIL 等级开发，或者开展相关失效分析，在证明子要素之间满足共存原则后，这些子要素可按照各自分配的 ASIL 等级开发
29	对于分配了技术安全要求的具备可编程功能的定制化硬件要素，是否定义和实施了适当的开发流程？	适用的硬件要素例如：专用集成芯片（ASIC）、可编程门阵列（FPGA）或其他形式的数字化硬件。 对于这些硬件要素，其开发流程应符合 GB/T 34590.5—2022、GB/T 34590.6—2022、GB/T 34590.8—2022 第 13 章和 GB/T 34590.11—2022 的要求，具体可见对应部分的审核评估清单要求

表 D.1　技术安全概念开发的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
30	如果适用，技术安全要求是否包含因实施 ASIL 等级分解而产生的独立性要求？	如果适用，对于每个存在 ASIL 等级分解的设计，是否有存在对应的独立性要求？或能提供实施分解后技术安全要求的要素之间符合独立性的证据？
31	技术安全要求的定义和管理是否符合安全要求的定义和管理的要求？	系统阶段开发每项技术安全要求应按照 GB/T 34590.8—2022 第 6 章进行定义和管理，包括： ——定义方法（如自然语言、非形式或形式标记法）的要求； ——技术安全要求属性的要求（明确标识、标识的唯一不变性、状态、ASIL 等级）； ——技术安全要求特性的要求（明确的、可理解的、不可分割的、内部一致的、可行和可实现的、可验证的、实施自由的、完整的）； ——技术安全要求管理特性的要求（分层结构、按照适当分组原则建立的组织结构，完整性、外部一致性、分层结构中任意一层的信息不重复、可维护性）； ——技术安全要求的可追溯要求（与上层的功能安全要求之间、与下层的硬件安全要求和软件安全要求的之间）； ——技术安全要求验证方法的要求； ——配置管理的要求（维护整个安全生命周期的一致性）
32	是否存在定义了硬件和软件交互的软硬件接口（HSI）规范作为工作成果？	在系统架构设计过程中对软硬件接口（HSI）进行定义，在硬件开发（见 GB/T 34590.5—2022 第 6 章）和软件开发（见 GB/T 34590.6—2022 第 6 章）过程中对软硬件接口（HSI）进行细化
33	软硬件接口（HSI）规范中考虑的软硬件接口要素是否完善？并保持与技术安全概念一致？	软硬件接口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，为了定义软硬件接口（HSI），可考虑但不限于下述软硬件接口（HSI）要素： ——存储器[易失性存储器（例如，RAM），非易失性存储器（例如，NvRAM）]； ——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）]； ——转换器[模/数转换器、数/模转换器、脉冲宽度调制（PWM）]； ——多路转换器； ——电气输入/输出； ——看门狗

表 D.1　技术安全概念开发的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
34	软硬件接口规范中考虑的软硬件接口要素特性是否完善？是否定义了相关运行模式和配置参数？是否定义了确保要素间独立性或支持软件分区的硬件特性？是否定义了硬件资源的共用和专用？是否定义了硬件设备的访问机制？是否由技术安全概念导出了的时间约束？	软硬件接口规范是否包含下列特性： 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； **示例 4**：串、并、从、主/从。 e) 由技术安全概念得出的时间约束
35	是否在软硬件接口规范中定义硬件的相关诊断能力和软件对其的使用？	硬件的诊断特性示例，如过流、短路或过温的探测。 软件中实现的对硬件的诊断特性，如通过 AD 转换检测电流、电压、温度等，并在出现异常时的操作
36	是否定义在系统架构设计过程中识别出的对生产、运行、服务和报废的技术安全要求？	对生产、运行、服务和报废的技术安全要求包括： 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； 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。
37	是否定义需具备的诊断特性以提供对系统进行现场监控所需的数据？	**示例**：ECU 中的功能安全相关的错误日志功能。
38	是否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？	**示例**：ADAS 系统控制器的功能安全相关的故障或事件记录，诊断和报警功能。
39	是否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？	提供按照安全要求的定义和管理的要求，对技术安全要求的定义和管理进行验证的证据。 提供按照表 4 检查清单的要求对技术安全要求进行验证的证据
40	是否按照 GB/T 34590.4—2022 中表 2 要求的验证方法，对技术安全概念，系统架构设计，软硬件接口(HSI)规范以及生产、运行、服务和报废的需求规范进行了验证？	验证的目的是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； c)　先前开发步骤中系统架构设计的有效性和符合性

附 录 E
（资料性）
验证和确认

集成验证活动的审核及评估的说明及示例见表 E.1。

表 E.1 集成验证活动的审核及评估的说明及示例

序号	检查清单	说明及示例
1	系统架构设计是否按照表 5 的检查清单进行了审核评估，结果是否符合功能安全和技术安全要求？ 是否按计划开展了集成测试活动？验证以下方面： a) 功能安全及技术安全要求是否正确实施； b) 安全机制是否具有正确的功能性能、准确性和时序； c) 接口是否具有一致性和正确实施； d) 系统架构设计是否有足够的鲁棒性	列项 a)、b)导出集成测试案例的方法至少包括基于需求分析的方法。基于需求分析的测试结果可证明功能安全及技术安全需求正确实施，安全机制符合安全设计。 **示例 1**：例如对于 EPS，通过关断助力而进入安全状态的功能安全需求，为此需要对转向系统进行集成测试，以确保关断助力的安全设计正确实施。 列项 c)导出集成测试案例的方法至少包括基于外部和内部接口分析的方法。基于接口的测试结果可证明内部接口和外部接口是一致的 **示例 2**：针对 LKA 功能，通过感知系统对 EPS 转向系统间的交互，对感知系统和 EPS 系统提出接口一致性的要求。 列项 d)参考 GB/T 34590.4—2022 中表 3 导出集成测试案例的方法，来证明系统架构设计具有足够的鲁棒性，如使用边界值分析的方法导出集成测试用例。 **示例 3**：测试用例中考虑例如 EPS 转向系统的转向角不应大于××值，或超过××值的范围等边界值分析方法。
2	定义集成和测试策略时是否考虑系统架构规范、功能安全概念和技术安全概念？ a) 是否有合适的能够提供功能安全证据的测试目标； b) 相关项的集成和测试是否有助于安全概念的验证	集成和测试策略中应具备包括可证明符合安全设计的测试目标，同时要考虑对功能安全概念和技术安全概念的验证提供有利证据。需要注意的是，如果安全概念中考虑了其他技术手段来确保安全设计，也需要对该技术手段进行集成测试验证 **示例**：假设 EPS 系统通过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，那么需要对 EPS 系统中的这个机械组件进行集成测试验证，验证该机械组件的有效性。
3	a) 相关项集成和测试策略的定义是否包括了软硬件集成和测试规范； b) 相关项集成和测试策略的定义是否包括系统和整车层面的集成测试规范。软硬件验证的未解决问题是否已处理； c) 相关项集成和测试策略是否考虑车辆系统（相关项内部和外部）与环境之间的接口； d) 若相关项集成了以独立于环境的要素（SEooC）方式进行开发的系统或要素，在相关项集成和测试策略中是否考虑了对 SEooC 开发过程中做过的假设进行验证？	列项 b)软硬件验证阶段基于已实施的功能、功能复杂性或系统的分布特性，如有足够的理由，未完成验证的可在系统或整车层面进行验证，来解决软硬件阶段验证出现的不足和问题。 列项 c)相关项集成测试在软硬件集成层面考虑软硬件之间的接口及其交互；在相关项层面应验证整车系统与环境之间的接口及其交互。 列项 d) 如果安全概念是独立于环境的安全要素（SEooC）进行开发，需要对安全概念中的假设进行集成测试验证 **示例**：假设 EPS 系统通过 SEooC 的方案进行平台化开发，那么在具体某一个项目过程中，需要对平台化开发方案中的假设进行验证。

表 E.1　集成验证活动的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
4	系统或整车层面的验证是否提供证据证明用于量产实施层面的配置符合安全要求？	例如：某车型项目具有多个配置，在系统和整车层面针对不同配置进行安全验证，证明全部配置符合功能安全要求。若能证明合理性，可使用配置的子集进行验证
5	在整个集成子阶段，对于每条功能安全要求和技术安全要求的符合性，是否至少进行过一次验证？	如果适用以下情况： a) 为了验证每个功能安全和技术安全要求得到满足，普遍的做法是在系统层面或整车层面对已定义的安全要求进行验证； b) 安全概念是独立于环境的安全要素（SEooC）进行开发，需要对安全概念中的假设进行集成测试验证； c) 集成测试期间识别出的安全异常要按照 GB/T 34590.2—2022 中 5.4.3 的要求进行报告
6	是否恰当地定义集成测试的测试用例？集成测试的测试用例是否使用合适的方法导出？	不同层级的集成测试，应使用 GB/T 34590.4—2022 中表 3 导出集成测试案例的方法中所列的恰当的方法组合导出测试用例。如需求分析、外部和内部接口分析、边界值分析、错误猜测等方法 **示例**：可基于先前已测试的项目经验进行错误猜测，导出测试案例。
7	是否按照 GB/T 43253.3—2023 和 GB/T 43253.4—2023 检查清单的要求进行软硬件的开发？是否完成软硬件的集成？是否对集成后的硬件和软件进行测试？	软硬件集成测试的对象应首选用于生产的硬件和软件，对于特定的测试技术，必要时可适用修改过的硬件或软件进行测试
8	是否通过测试证明了集成后的软件和硬件符合软硬件接口规范的要求？	—
9	对于软硬件集成测试的目标，是否通过使用适当的测试方法得到了实现？	软硬件集成测试的测试目标和使用的测试方法可帮助在系统架构设计中对系统性故障的探测。 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
10	是否通过合适的测试方法（基于需求的测试、故障注入测试、背靠背测试等）来证明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？	软硬件集成测试，应使用 GB/T 34590.4—2022 中表 4 技术安全要求在软硬件层面的正确执行中所列的恰当的方法进行测试。如基于需求的测试、故障注入测试、背靠背测试等方法 **示例**：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。
11	对于 ASIL（A）、B、C 和 D 等级，是否通过合适的测试方法（背靠背测试、性能测试等）对安全机制在软硬件层面的功能性能、准确性和时序进行论证？	软硬件集成测试，针对安全机制在软硬件层面的功能性能、准确性和时序进行论证应使用 GB/T 34590.4—2022 中表 5 所列的恰当的方法进行测试。如背靠背测试、性能测试 **示例 1**：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表现差异。 **示例 2**：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。

表 E.1　集成验证活动的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
12	对于 ASIL（A）、B、C 和 D 等级，是否通过合适的测试方法（外部接口测试、内部接口测试、接口一致性检查等）来证明外部和内部接口在软硬件层面执行的一致性和正确性？	软硬件集成测试，针对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 GB/T 34590.4—2022 中表 6 给出的测试方法来提供证据。如外部接口测试、内部接口测试、接口一致性检查 **示例**：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。
13	对于 ASIL（A）、（B）、C 和 D 等级，是否通过合适的测试方法（故障注入测试、错误猜测法测试等）对故障模型，硬件故障探测机制在软硬件层面上的有效性进行论证？	软硬件集成测试，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 GB/T 34590.4—2022 中表 7 列出的测试方法进行论证。如故障注入测试、错误猜测法测试 **示例 1**：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。 **示例 2**：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。
14	对于 ASIL（A）、（B）、（C）和 D 等级，是否通过合适的测试方法（资源使用测试、压力测试等）对要素在软硬件层面的鲁棒性水平进行论证？	软硬件集成测试，要素在软硬件层面的鲁棒性水平，应按照 GB/T 34590.4—2022 中表 8 给出的测试方法进行论证。如资源使用测试、压力测试 **示例 1**：资源使用测试可静态地完成（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地完成。 **示例 2**：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，也可为极限的温度、湿度或机械冲击测试。
15	系统的各个要素是否按照系统架构设计进行集成？系统的各个要素是否按照系统集成测试规范进行测试？	系统集成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
16	对于系统集成测试的目标，是否通过使用适当的测试方法得到了实现？	系统集成测试的测试目标和使用的测试方法可帮助在系统架构设计中对系统性故障的探测。 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

表 E.1　集成验证活动的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
17	是否通过合适的测试方法（基于需求的测试、故障注入测试、背靠背测试等）来证明功能安全和技术安全要求在系统层面的正确执行？	系统集成测试，功能安全和技术安全要求在系统层面的正确执行，应使用 GB/T 34590.4—2022 中表 9 列出的测试方法来提供证据。如基于需求的测试、故障注入测试、背靠背测试 **示例 1**：基于需求的测试是指针对功能性和非功能性要求的测试。 **示例 2**：故障注入测试使用特殊的方法向系统注入故障。这可通过特殊的测试接口、或特殊准备的要素、或通信设备在系统内完成。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。GB/T 34590.4—2022 中表 8 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。 **示例 3**：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。
18	对于 ASIL（A）、（B）、（C）和 D 等级，是否通过合适的测试方法（背靠背测试、故障注入测试、性能测试、错误猜测法测试、来自现场经验的测试等）对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、时序进行论证？	系统集成测试，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 GB/T 34590.4—2022 中表 10 给出的测试方法进行论证。如背靠背测试、故障注入测试、性能测试、错误猜测法测试、来自现场经验的测试 **示例 1**：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。 **示例 2**：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—2022 中 4.8 的详细描述。 **示例 3**：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）。 **示例 4**：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。 **示例 5**：来自现场经验的测试采用从现场收集到的经验和数据。
19	是否通过合适的测试方法（外部接口测试、内部接口测试、接口一致性检查、通信和交互测试等）来证明外部和内部接口在系统层面执行的一致性和正确性？	系统集成测试，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 GB/T 34590.4—2022 中表 11 列出的测试方法来提供证据。如外部接口测试、内部接口测试、接口一致性检查、通信和交互测试 **示例 1**：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。 **示例 2**：通信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信测试。

表 E.1　集成验证活动的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
20	是否通过合适的测试方法（资源使用测试、压力测试、特定环境条件下的抗干扰性和鲁棒性测试等）对系统层面的鲁棒性水平进行论证？	系统集成测试，系统层面的鲁棒性水平，应使用 GB/T 34590.4—2022 中表 12 给出的测试方法进行论证。如资源使用测试、压力测试、特定环境条件下的抗干扰性和鲁棒性测试 **示例 1**：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。 **示例 2**：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，测试可通过在系统上施加高负荷，或极限的用户输入，或来自其他系统的极限要求完成，也可为极限的温度、湿度或机械冲击测试。 **示例 3**：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。
21	是否将相关项集成到整车上？是否实施整车集成测试？	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 GB/T 34590.4—2022 中的表 3）
22	是否对相关项与车内通信网络以及车内供电网络的接口规范进行验证？	—
23	整车集成测试的测试目标是否使用适当的测试方法来实现？	整车集成测试的测试目标和使用的测试方法可帮助在整车集成过程中对系统性故障的探测。 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
24	是否通过合适的测试方法（基于需求的测试、故障注入测试、长期测试、实际使用条件下的用户测试等）对功能安全要求在整车层面的正确执行进行论证？	整车集成测试，功能安全要求在整车层面的正确执行，应使用 GB/T 34590.4—2022 中表 13 给出的测试方法进行论证。如基于需求的测试、故障注入测试、长期测试、实际使用条件下的用户测试 **示例 1**：基于需求的测试是指针对功能性和非功能性要求的测试。 **示例 2**：故障注入测试使用特殊的方法向相关项注入故障。这可通过特殊测试接口，或者特别准备的要素或通信设备，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。 **示例 3**：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。

表 E.1　集成验证活动的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
25	对于 ASIL（A）、（B）、C 和 D 等级，是否通过合适的测试方法（性能测试、长期测试、实际使用条件下的用户测试、故障注入测试、错误猜测法测试、来自现场经验的测试等）对安全机制在整车层面的正确功能性能、准确性和时序进行论证？	整车集成测试，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 GB/T 34590.4—2022 中表 14 列出的测试方法进行论证。如性能测试、长期测试、实际使用条件下的用户测试、故障注入测试、错误猜测法测试、来自现场经验的测试 **示例 1**：性能测试可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）。 **示例 2**：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。 **示例 3**：故障注入测试使用特殊的方法向相关项注入故障。这可通过特殊测试接口，或者特别准备的要素或通信设备，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。 **示例 4**：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。 **示例 5**：来自现场经验的测试采用从现场收集到的经验和数据。
26	对于 ASIL（A）、（B）、C 和 D 等级，是否通过合适的测试方法（内部接口测试、外部接口测试、通信和交互测试等）对整车层面内部和外部接口实现的一致性和正确性进行论证？	整车集成测试，整车层面内部和外部接口实现的一致性和正确性，应使用 GB/T 34590.4—2022 中表 15 给出的测试方法进行论证。如内部接口测试、外部接口测试、通信和交互测试 **示例 1**：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。 **示例 2**：整车层面的接口测试，是对整车系统接口的兼容性测试。这些测试可通过验证值域、额定值或几何尺寸静态地完成，也可在整车运行过程中动态地完成。 **示例 3**：通信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信测试。
27	对于 ASIL（A）、（B）、C 和 D 等级，是否通过合适的测试方法（资源使用测试、压力测试、特定环境条件下的抗干扰性和鲁棒性测试、长期测试等）对整车层面的鲁棒性水平进行论证？	整车集成测试，整车层面的鲁棒性水平，应使用 GB/T 34590.4—2022 中表 16 列出的测试方法进行论证。如资源使用测试、压力测试、特定环境条件下的抗干扰性和鲁棒性测试、长期测试 **示例 1**：整车层面的资源使用测试通常在动态环境下进行（例如，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。 **示例 2**：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，测试可通过在整车上施加高负荷，或极限的用户输入，或来自其他系统的极限要求下完成，也可为极限的温度、湿度或机械冲击测试。

表 E.1　集成验证活动的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
27	对于 ASIL（A）、(B)、C 和 D 等级，是否通过合适的测试方法(资源使用测试、压力测试、特定环境条件下的抗干扰性和鲁棒性测试、长期测试等)对整车层面的鲁棒性水平进行论证？	**示例 3**：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。 **示例 4**：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。
28	是否针对安全生命周期的每个阶段及子阶段，制定了对应的验证计划？	安全生命周期的每个阶段及子阶段的验证，需要在验证计划中体现
29	制定的验证计划中，是否包括了需验证的工作成果内容？	验证计划中，应写明需要验证的工作成果内容，如技术安全概念
30	制定的验证计划中，是否包括了验证的目的？	验证计划中，应包括验证的目的。以验证技术安全概念为例，验证的目的可为根据工作产品审查技术安全要求和规范，确保其完整性、正确性和一致性
31	制定的验证计划中，是否包括了用于验证的方法？	验证计划中，应包括用于验证的方法，如评审、仿真、分析、测试等
32	制定的验证计划中，是否包括了验证通过和不通过的准则？	以验证技术安全需求为例，通过准则可使需求覆盖率达到100%，需求具备可追溯性。完成评审清单，且评审清单中记录的问题已关闭
33	如果适用，制定的验证计划中，是否包括了验证环境、用于验证的设备、用于验证的资源？	**注**：验证环境可为测试环境或模拟环境。 **示例**：用于验证的设备，包括测试工具或者测量设备。
34	制定的验证计划中，是否包括了当探测出异常时需采取的行动？	验证计划中，需要说明探测出异常后，要采取的行动。
35	制定的验证计划中，是否包括了回归策略？	**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。验证可被全部或部分重复，并可包含其他能影响验证结果的相关项或要素。
36	制定验证计划是否考虑到所适用验证方法的充分性？是否考虑到需验证的工作成果的复杂性？是否考虑到与验证目标材料相关的前期经验？是否考虑到所使用技术的成熟度，或使用这些技术的风险？	**注**：与验证目标材料相关的前期经验，包括维修历史及在用证明达到的程度。
37	验证规范是否对用于验证的方法进行细化？细化的内容是否包含了评审或分析的检查清单；或模拟场景；或测试用例、测试数据和测试目标？	—

表 E.1　集成验证活动的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
38	对于测试，每条测试用例的定义是否包含以下内容： a）　唯一的识别； b）　需验证的相关工作成果的版本的参考； c）　前提条件和配置； d）　如果适用，环境条件； e）　输入数据、数据时序及其值； f）　期望的表现，包括输出数据、输出值的可接受范围、时间表现和公差表现； g）　确定测试用例通过和不通过的准则？	针对 c），**注 1**：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）。 针对 d），**注 2**：境条件与周围物理属性（例如，温度）有关，测试在该环境进行或模拟部分测试。 针对 f），**注 3**：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 4**：为避免重复定义和存储不同测试用例用到的前提条件、配置及环境条件，有必要使用明确的参考。
39	对于测试，是否从所需的测试设备或测试环境、逻辑和时间的依赖性、资源这几个方面考虑来按使用的测试方法对测试用例进行分组？	**示例**：将测试用例分成回归测试用例和完整测试用例。
40	对于测试，测试用例是否由与待验证的工作成果的完成人不同的人进行评审？	—
41	是否按照验证计划和验证规范，执行验证？	—
42	验证是否由与待验证的工作成果的完成人不同的人执行？	—
43	对验证结果的评估是否包含以下信息： a）　所验证工作成果的唯一识别； b）　验证计划和验证规范的参考； c）　如果适用，评估中用到的验证环境配置、验证工具及标定数据； d）　验证结果与期望结果的一致性水平； e）　验证通过或不通过的明确的陈述，如果验证不通过，陈述应包含不通过的理由和对所验证工作成果进行修改的建议； f）　每个验证步骤未执行的理由？	**注**：按照验证的完成和结束准则（验证通过和不通过的准则），以及预期的验证结果，对验证进行评估。
44	用于验证的测试设备是否提供有效的和可重复的结果，并应按照所采用的质量管理体系进行管控？	—

表 E.2　确认活动的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否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？	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
2	是否考虑基于车型和车辆配置的典型车辆来定义典型环境？	宜将危害分析和风险评估报告（见 GB/T 34590.3—2022 中的 6.5.1）作为选择典型车辆的其中一个输入
3	对于危害分析和风险评估中考虑的、影响相关项技术特性的运行变化，在安全目标的确认过程中是否进行了考量？	整车安全确认可从以下两个维度来考虑。 a) 在危害分析和风险评估阶段，需要定义出可验证的安全目标、可控度的确认方案等。在整车安全确认阶段，安全确认方案可来源于危害分析和风险评估报告，以此来确保设计方案不会导致安全目标的违背。 b) 确保运行过程变化也不会导致安全目标的违背
4	是否定义安全确认规范，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—2022 附录 C； 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	基于相关项的安全确认，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
5	整车安全确认是否使用了恰当的方法？若使用测试进行整车安全确认，是否对测试规范、测试的执行和测试结果的评估进行了规范性检查？	整车安全确认使用的方法需要有充分的论据。 如果整车安全确认使用了测试的方法，需要按照（GB/T 34590.8—2022 中的 9.4.2 和 9.4.3）相同的要求
6	整车安全确认是否对可控性进行评估？整车安全确认是否对外部措施的有效性进行评估？整车安全确认是否对其他技术要素的有效性进行评估？整车安全确认是否对影响危害分析与风险评估中 ASIL 等级的假设进行评估？	对可控性的评估是需要基于使用运行场景，包括预期用途及可预见的误用。 安全确认的一个接受准则是对 GB/T 34590.3—2022 中 7.4.2.5 定义的安全状态有充分的可控性。 外部措施有效性的安全确认示例： 假设一个机械组件能够防止或减轻由电气/电子（E/E）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
7	整车层面的安全确认是否基于安全目标、功能安全要求和预期用途？ 每个安全目标的安全确认流程和测试用例，是否都包括详细的通过/未通过准则？整车层面的安全确认是否考虑其应用范围？	可创建操作用例，以助于将安全确认集中在整车层面上
8	安全确认是否通过以下方法的适当组合予以实施？ ——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； ——安全分析方法； ——长期测试； ——基于实际使用条件的测试； ——抽检和盲测； ——基于专家经验的测试； ——评审	导出测试用例的方法示例：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。 安全确认的安全分析方法示例：FMEA、FTA、ETA、仿真
9	安全确认的结果是否进行评估？安全确认的结果是否能够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？	整车安全确认需根据通过/未通过准则来评估测试结果，进而通过数据和整车实际表现来判断是否违背了安全目标。 如 EPS“避免非预期转向”的安全目标，可通过车辆是否偏离车道作为安全目标实现的证据之一

参 考 文 献

[1] GB/Z 42285—2022 道路车辆 电子电气系统 ASIL 等级确定方法指南