ICS 43.040
CCS T 35

中华人民共和国国家标准

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

Road vehicles—Functional safety audit and assessment method—Part 4：Hardware 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　硬件安全要求 …… 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　硬件设计 …… 3
6.1　目标 …… 3
6.2　审核及评估的输入 …… 3
6.3　审核及评估的要求 …… 4
7　硬件架构度量的评估 …… 6
7.1　目标 …… 6
7.2　审核及评估的输入 …… 6
7.3　审核及评估的要求 …… 6
8　随机硬件失效导致违背安全目标的评估 …… 7
8.1　目标 …… 7
8.2　审核及评估的输入 …… 7
8.3　审核及评估的要求 …… 7
9　硬件集成和验证 …… 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
10　硬件要素评估 …… 10
10.1　目标 …… 10
10.2　审核及评估的输入 …… 10
10.3　审核及评估的要求 …… 10
附录 A（资料性）　硬件安全要求 …… 13
附录 B（资料性）　硬件设计 …… 16
附录 C（资料性）　硬件架构度量的评估 …… 21

附录 D（资料性） 随机硬件失效导致违背安全目标的评估 …… 23
附录 E（资料性） 硬件集成和验证 …… 25
附录 F（资料性） 硬件要素评估 …… 28

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4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、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、南京芯驰半导体科技有限公司、英飞凌科技资源中心(上海)有限公司、中国第一汽车集团有限公司、中国长安汽车集团有限公司、东软睿驰汽车技术(上海)有限公司、上海机动车检测认证技术研究中心有限公司、上海禾赛科技有限公司、深圳市大疆卓见科技有限公司、舍弗勒(中国)有限公司、北京长安汽车工程技术研究有限责任公司、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：宋炜瑾、蔡香、魏斌、唐沙南、付越、尚世亮、李波、邵海贺、闻继伟、王潇屹、王宇、孙毓阳、赵鑫、刘辉、张晓亮、查小东、李兆麟。

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。

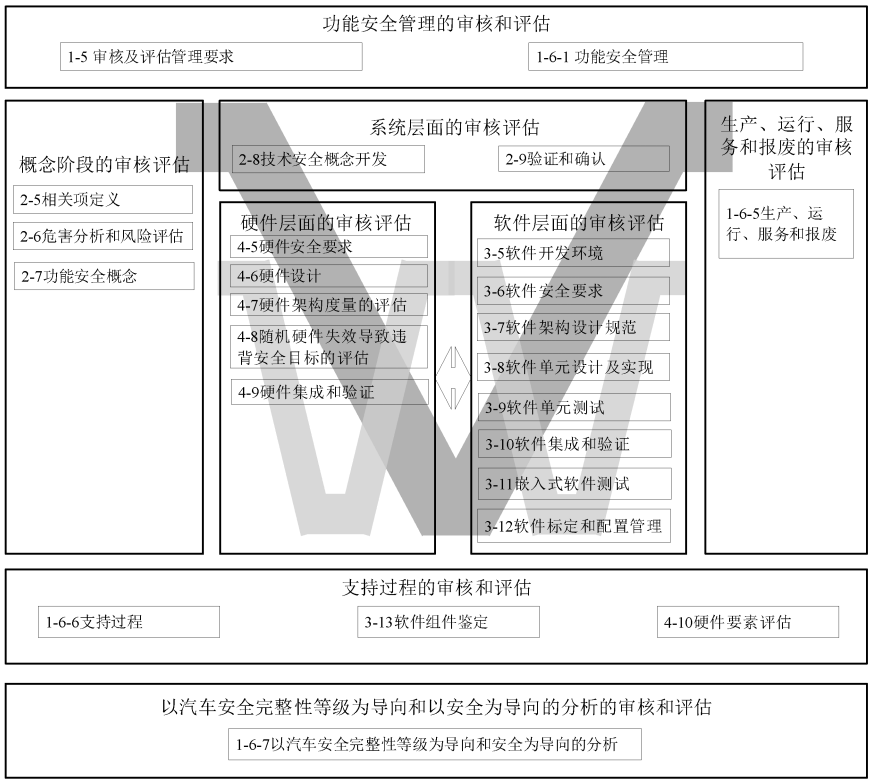

图1　功能安全审核及评估概览

道路车辆　功能安全审核及评估方法
第4部分:硬件层面

1　范围

本文件规定了针对安全相关的电气/电子(E/E)系统在硬件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

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。

硬件层面的功能安全审核及评估,主要涉及以下内容:

——硬件安全要求的定义;

——硬件设计;

——硬件架构度量的评估;

——随机硬件失效导致违背安全目标的评估;

——硬件集成和验证;

——硬件要素评估。

通过审核及评估,基于证据判断硬件层面的功能安全开发,符合:

——硬件安全要求是恰当和完整的;

——通过设计、验证保证硬件能实现硬件功能安全要求并满足软硬件接口规范;

——提供基于硬件架构度量的证据,来证明相关项硬件架构设计在安全相关的随机硬件失效探测和控制方面的适用性;

——确保所开发硬件符合硬件安全要求;

——确保硬件要素的功能表现足以满足分配的安全要求。

5 硬件安全要求

5.1 目标

本章的目标是对作为功能安全硬件安全要求的定义文档进行审核及评估，以检查其定义是否符合功能安全开发的需要，提供证据证明：

a) 定义了硬件安全要求，这些要求由技术安全概念和系统架构设计规范导出；

b) 细化了最初在 GB/T 34590.4—2022 中 6.4.7 定义的软硬件接口规范；

c) 验证了硬件安全要求及软硬件接口规范与技术安全概念及系统架构设计规范的一致性。

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：

——硬件安全需求规范（包括测试和认可准则）；

——软硬件接口规范（细化的）；

——硬件安全要求验证报告。

注：为支持审核及评估，可能需要提供的其他支持材料如下：

——技术安全概念；

——系统架构设计规范；

——软硬件接口规范；

——可参考的已有硬件架构设计；

——软件安全要求。

5.3 审核及评估的要求

对于硬件安全要求进行审核及评估，应涵盖表 1、表 2、表 3 的检查项。

表 1 硬件安全要求的审核及评估检查清单

序号	检查清单
1	是否定义了硬件安全要求和安全机制控制硬件内部失效（例如：对内核失效的检测、对存储失效的监控）？
2	是否定义了对外部失效容错的硬件安全要求和安全机制（例如：传感器开路或短路检测的支撑电路）？
3	是否为符合其他要素的安全要求定义了硬件安全要求和安全机制的相关属性？
4	是否定义了硬件安全要求和安全机制探测内外部失效和发送失效信息？
5	对于 ASIL（B）、C 和 D 等级，硬件安全要求是否设定了硬件架构度量目标值？
6	对于 ASIL（B）、C 和 D 等级，硬件安全要求是否设定了随机硬件失效概率度量目标值（如采用 EEC 方法，该问题不适用）？
7	硬件安全要求是否包含了非用以定义安全机制的硬件安全要求？
8	是否定义了相关项或要素的硬件设计验证准则，包括环境条件（温度、振动、EMI 等）、特定的运行环境（供电电压、任务剖面等）以及特定于组件的要求？
9	硬件安全要求所对应的安全机制的故障容错时间间隔或者最大故障处理时间间隔是否符合系统层级的定义？
10	硬件安全要求所对应的安全机制的多点故障探测时间间隔要求是否符合系统层级的定义？
11	硬件安全要求是否与技术安全要求之间保持了追溯性和一致性？硬件安全要求是否与技术安全概念、系统设计规范和硬件规范之间保持了一致性？
12	硬件安全要求是否按照 GB/T 34590.8—2022 第 6 章的要求进行定义和管理？

表 2　软硬件接口规范的审核及评估检查清单

序号	检查清单
1	是否细化了硬件设备的相关运行模式和相关配置参数(例如:对看门狗的配置)?
2	是否确保了要素间独立性或支持软件分区的硬件特征?
3	是否对硬件资源的共用和专用进行了明确定义?
4	是否对硬件设备的访问机制进行了明确定义?
5	由技术安全概念得出的时间约束是否在软硬件接口规范中进行了说明?
6	是否对硬件的诊断特性进行了明确定义?
7	是否对需要在软件中实现的对硬件的诊断特性进行了明确定义?
8	是否明确描述了硬件和软件之间的每一项安全相关的关联性?
9	是否对细化后的软硬件接口都定义了对应的验证准则?
10	是否细化后的软硬件接口(HSI)规范的充分性由软硬件开发人员进行了共同验证?

表 3　硬件安全要求验证报告的审核及评估检查清单

编号	检查清单
1	硬件安全要求的验证活动是否验证了与技术安全概念、系统设计规范以及硬件规范的一致性?
2	硬件安全要求的验证活动是否说明了技术安全要求分配给硬件要素的完整性?
3	硬件安全要求的验证活动是否验证了与相关软件安全要求的一致性?
4	硬件安全要求的验证活动是否验证了硬件安全要求的正确性与准确性?

附录 A 提供了针对硬件安全要求开展审核及评估的说明及示例。

6　硬件设计

6.1　目标

本章的目标是对硬件设计进行审核及评估,以检查其是否符合功能安全硬件设计的需要,提供证据证明:

a)　创建了一个硬件设计:支持以安全为导向的分析,考虑安全导向分析的结果,符合硬件安全要求、软硬件接口规范和系统架构设计规范,并满足所需的硬件设计特性;

b)　定义了在生产、运行、服务和报废期间的硬件功能安全要求并提供有关信息;

c)　验证了硬件设计能满足硬件安全要求和软硬件接口规范,假设的有效性(此假设用于开发集成在已开发硬件中的每个 SEooC),以及安全相关的特殊特性的适用性,以实现生产和服务期间的功能安全。

6.2　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:

——硬件设计规范(包括硬件架构设计和硬件详细设计);
——基于演绎法的硬件安全分析(例如:硬件 FTA);
——基于归纳法的硬件安全分析(例如:硬件 FMEA);
——相关失效分析(DFA)(如适用);
——硬件安全分析报告;
——硬件设计验证报告;
——与生产、运行、服务和报废相关的需求规范。

注:为支持审核及评估,可能需要提供的其他支持材料如下:
——硬件安全需求规范;
——细化的软硬件接口规范;
——系统架构设计规范。

6.3 审核及评估的要求

对于硬件设计的审核及评估,应涵盖表 4、表 5、表 6、表 7 的检查项。

表 4 硬件设计规范的审核及评估检查清单

序号	检查清单
1	所定义的硬件安全要求是否与硬件架构保持了追溯性和一致性,并保持到硬件组件的最底层? 注:对于不能划分为硬件子要素的硬件元器件,不分配硬件安全要求。例如,电容和电阻。
2	硬件安全要求是否都分配给了硬件要素及其子要素?每个硬件要素或子要素所定义的 ASIL 等级是否为分配给它的所有要求中最高的 ASIL 等级?如果一个硬件要素是由 ASIL 等级低于要素 ASIL 等级或没有指定 ASIL 等级的子要素组成,该要素是否满足 GB/T 34590.9—2022 第 6 章的共存准则?
3	硬件架构设计中如果对硬件安全要求应用 ASIL 等级分解,ASIL 等级的分解是否按照 GB/T 34590.9—2022 第 5 章的要求进行?
4	硬件架构设计是否按照对应的 ASIL 等级根据 GB/T 34590.5—2022 中的表 1 硬件架构设计原则进行设计,并使其具有模块化特性、适当的粒度水平和简单性?如未按照 ASIL 等级要求选取硬件设计原则,是否有合理的理由说明?
5	在硬件架构设计时,是否考虑安全相关硬件组件失效的非功能性原因(如温度、振动、水、灰尘、电磁干扰、噪声因素,或来自硬件架构的其他硬件组件或其所在环境的串扰)?
6	在进行硬件详细设计时,为避免常见的设计缺陷,是否运用相关的经验总结?
7	在硬件详细设计时,是否考虑安全相关硬件元器件失效的非功能性原因(如温度、振动、水、灰尘、电磁干扰、噪声因素、来自硬件组件的其他硬件元器件或其所在环境的串扰)?
8	硬件详细设计是否考虑硬件元器件或硬件组件的任务剖面和运行条件?是否保证硬件元器件或硬件组件在其规格范围内运行?
9	硬件详细设计是否考虑鲁棒性设计原则(如适用)?
10	硬件设计规范是否通过验证评审?

表 5　硬件安全分析的检查清单

序号	检查清单
1	是否定义了针对不同 ASIL 等级硬件产品要求的定性的安全分析方法？
2	对于 ASIL（B）、C 和 D 等级，是否用安全分析针对每个安全相关的硬件组件或元器件识别以下内容： a）　安全故障； b）　单点故障或残余故障； c）　多点故障（无论是可感知的、可探测的或潜伏的）
3	对于 ASIL（B）、C 和 D 等级，对于防止导致单点失效的故障或减少残余故障而实施的安全机制，是否具备证明安全机制具有实现和保持安全状态的能力（特别是在容错时间间隔和最大故障处理时间间隔内适当的失效减轻能力）的证据？由安全机制实现的残余故障的诊断覆盖率是否已评估？
4	对于 ASIL（B）、C 和 D 等级，防止潜伏故障而实施的安全机制，是否具备证据以证明安全机制在可接受的多点故障探测时间间隔内完成潜伏故障的失效探测和实现或保持安全状态及警示驾驶员的能力，以确定哪些故障保持潜伏，哪些故障可被探测到？由安全机制实现的潜伏故障的诊断覆盖率是否已评估？
5	是否进行相关失效分析以提供证据证明设计中的硬件要素与它们的独立性要求相符合？
6	如果硬件设计引入了新危害，且这个危害没有被现有的 HARA 报告覆盖，是否有变更管理流程对它们进行引入和评估？
7	硬件安全分析是否通过验证评审？
注：FTA、FMEA、DFA 按照 GB/T 43253.1—2023 的检查清单进行检查。	

表 6　硬件设计验证的审核及评估检查清单

序号	检查清单
1	是否按照对应的 ASIL 等级选取 GB/T 34590.5—2022 中表 3 要求的硬件设计验证方法，以验证硬件设计满足硬件安全要求，与软硬件接口规范兼容以及用来生产和服务过程中实现功能安全的安全相关特殊特性的适用性？如未按照 ASIL 等级要求选取方法，是否有合理的理由说明？
2	是否具有仿真或通过硬件原型的开发验证方法的验证计划、验证规范以及验证报告（如适用）？这些验证计划、验证规范和验证报告是否通过验证评审？
3	在硬件设计过程中，如果发现任何硬件安全要求的实施是不可行的，是否按照 GB/T 34590.8—2022 第 8 章中的变更管理流程提出变更请求？
4	是否根据硬件安全要求和硬件设计规范验证用于开发集成到硬件中的 SEooC 的假设的有效性？

表 7　与生产、运行、服务和报废相关的需求规范的审核及评估检查清单

序号	检查清单
1	是否有与生产、运行、服务和报废相关的安全相关的特殊特性？
2	是否定义这些安全相关的特殊特性： ——生产和运行的验证措施； ——这些措施的接受准则

表 7　与生产、运行、服务和报废相关的需求规范的审核及评估检查清单（续）

序号	检查清单
3	如果安全相关硬件要素的错误组装、拆卸和报废可能对实现或维护功能安全产生不利影响，是否将避免错误执行所需的信息告知负责生产、运行、服务和报废的人员？
4	安全相关硬件要素是否具有可追溯性？是否支持可进行有效的现场监测和可启用召回或更换管理？
5	如果错误的服务可能对实现或维护功能安全产生不利影响，是否将避免此类影响执行所需的信息定义至与生产、运行、服务和报废相关的需求规范中？是否告知负责生产、运行、服务和报废的人员？
6	硬件设计过程中产生的硬件要素的生产、运行、服务和报废要求，是否通过某种方式告知负责生产、运行、服务和报废的人员？
7	与生产、运行、服务和报废的需求规范是否通过验证评审？

附录 B 提供了针对硬件设计开展审核及评估的说明及示例。

7　硬件架构度量的评估

7.1　目标

本章的目标是通过评估硬件架构度量（包括单点故障度量 SPFM 和潜伏故障度量 LFM）是否达到目标值进而评估相关项架构或硬件元器件架构应对随机硬件失效的有效性。

7.2　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：

——相关项架构应对随机硬件失效的有效性的分析；

——相关项架构应对随机硬件失效的有效性评估的评审报告。

注 1：适用于等级为 ASIL（B）、C 和 D 的安全目标。评估产品如果为硬件元器件，则审核对象为针对硬件架构相关的工作成果。

注 2：为支持审核及评估，可能需要提供的其他支持材料如下：

——硬件安全需求规范；

——硬件设计规范；

——硬件安全分析报告；

——硬件相关失效分析报告；

——技术安全概念（如适用）；

——系统架构设计规范（如适用）。

7.3　审核及评估的要求

对于硬件架构度量的评估的审核及评估，应涵盖表 8 的检查项。

表 8　硬件架构度量的评估的审核及评估检查清单

序号	检查清单
1	对于 ASIL（B）、C 和 D 等级，是否为已制定的安全机制确定了诊断覆盖率？确定的诊断覆盖率是否合理？
2	对于 ASIL（B）、C 和 D 等级，硬件元器件预估失效率的确定是否采用了正确的方法？预估的失效率是否合理、正确？
3	对于 ASIL（B）、C 和 D 等级，当无法提供充足证据支持硬件元器件的失效率时，是否有相应的替代方案？替代方案是否合理？
4	对于 ASIL（B）、C 和 D 等级，是否为每一个安全目标都定义了 SPFM 的目标值？
5	对于 ASIL（B）、C 和 D 等级，是否为每一个安全目标都定义了 LFM 的目标值？
6	对于 ASIL（B）、C 和 D 等级，进行硬件架构度量评估时，是否将发生在安全相关硬件要素上的每个故障都进行了正确的分类？
7	对于 ASIL（B）、C 和 D 等级，是否每一个安全目标的 SPFM 的计算都采用了正确的计算公式？
8	对于 ASIL（B）、C 和 D 等级，是否每一个安全目标都满足了已定义的 SPFM 的目标值？
9	对于 ASIL（B）、C 和 D 等级，是否每一个安全目标的 LFM 的计算都采用了正确的计算公式？
10	对于 ASIL（B）、C 和 D 等级，是否每一个安全目标都满足了已定义的 LFM 的目标值？
11	对于 ASIL（B）、C 和 D 等级，每一个安全目标 SPFM 和 LFM 的结果是否都通过验证评审？

附录 C 提供了针对硬件架构度量的评估开展审核及评估的说明及示例。

8　随机硬件失效导致违背安全目标的评估

8.1　目标

本章的目标是通过评估随机硬件失效导致违背安全目标进而评估残余风险是否足够低。

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：

——由随机硬件失效导致违背安全目标的分析；

——硬件专用措施的定义，如果需要，包括专用措施有效性的依据；

——对随机硬件失效导致违背安全目标进行评估的评审报告。

注 1：适用于等级为 ASIL（B）、C 和 D 的安全目标。

注 2：为支持审核及评估，可能需要提供的其他支持材料如下：

——硬件安全需求规范；

——硬件设计规范；

——硬件安全分析报告；

——硬件相关失效分析报告；

——技术安全概念（如适用）；

——系统架构设计规范（如适用）。

8.3　审核及评估的要求

对于随机硬件失效导致违背安全目标的评估的审核及评估，应涵盖表 9 的检查项。

表 9　随机硬件失效导致违背安全目标评估的审核及评估检查清单

序号	检查清单
1	对于 ASIL (B)、C 和 D 等级，随机硬件失效导致违背安全目标评估中用到的硬件元器件预估失效率的确定是否采用了正确的方法？预估的失效率是否合理、正确？
2	对于 ASIL (B)、C 和 D 等级，随机硬件失效导致违背安全目标的评估是采用了随机硬件失效概率度量(PMHF)的评估方法，还是采用了对违背安全目标的每个原因的评估(EEC)的方法？
3	对于 ASIL C 和 D 等级，单一硬件元器件单点故障是否存在有效论据证明其发生概率足够低可被接受？
4	对于 ASIL C 和 D 等级，一个硬件元器件的残余故障诊断覆盖率低于 90%是否存在有效论据证明其发生概率足够低可被接受？
5	对于 ASIL (B)、C 和 D 等级，PMHF 评估的定量目标值是否表述为相关项的整个运行生命周期中每小时的平均概率？
6	对于 ASIL (B)、C 和 D 等级，是否为随机硬件失效在相关项层面导致违背每个安全目标的最大可能性定义了定量目标值？
7	对于 ASIL (B)、C 和 D 等级，PMHF 目标值的分配是否满足要求？
8	对于 ASIL (B)、C 和 D 等级，是否有证据证明 PMHF 的目标值已达到？
9	对于 ASIL (B)、C 和 D 等级，采用 EEC 评估时，对违背所考虑的安全目标的每个单点故障、残余故障和双点失效进行的单独评估是否在硬件层面执行？
10	对于 ASIL (B)、C 和 D 等级，采用 EEC 评估时，是否能按照要求提供证据证明违背安全目标的每个单点故障、残余故障和双点失效是可接受的？
11	对于 ASIL (B)、C 和 D 等级，采用 EEC 评估时，是否对硬件元器件失效率进行了失效率等级评级？
12	对于 ASIL (B)、C 和 D 等级，采用 EEC 评估时，是否可接受硬件元器件发生的单点故障？
13	对于 ASIL (B)、C 和 D 等级，采用 EEC 评估时，是否增加对应的安全机制并且可接受硬件元器件发生的残余故障？
14	对于 ASIL C 和 D 等级，采用 EEC 评估时，是否认为双点失效是可能的？
15	对于 ASIL C 和 D 等级，采用 EEC 评估时，是否增加或完善对应的安全机制并且可接受硬件元器件发生的可导致双点失效的双点故障？
16	对于 ASIL (B)、C 和 D 等级，对随机硬件失效导致违背安全目标评估的结果是否通过验证评审？

附录 D 提供了针对随机硬件失效导致违背安全目标的评估开展审核及评估的说明及示例。

9　硬件集成和验证

9.1　目标

本章的目标是对硬件集成和验证相关的活动和结果进行审核及评估，以检查硬件设计是否满足硬件功能安全要求和相应的 ASIL 等级。

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：

——硬件集成和验证计划；

——硬件集成和验证规范；

——硬件集成和验证报告。

注：为支持审核及评估，可能需要提供的其他支持材料如下：

——硬件安全需求规范；

——硬件设计文档；

——硬件安全分析报告。

9.3 审核及评估的要求

对于硬件集成和验证的审核及评估，应涵盖表10、表11、表12的检查项。

表10 硬件集成和验证计划的审核及评估检查清单

序号	检查清单
1	是否在硬件集成和验证计划中定义了验证对象的信息、验证目的和验证通过准则？
2	是否在硬件集成和验证计划中定义了符合产品硬件ASIL等级要求的活动与方法？
3	是否在硬件集成和验证计划中定义了符合产品硬件安全等级要求的测试策略？
4	是否在硬件集成和验证计划中定义了验证相关的依赖项？
5	是否在硬件集成和验证计划中定义了验证失败的应对措施？
6	是否对硬件集成和验证计划变更定义了相应的管理和追溯措施？
7	硬件集成和验证计划是否通过验证评审？

表11 硬件集成和验证规范的审核及评估检查清单

序号	检查清单
1	是否在硬件集成和验证规范中遵循了硬件集成和验证计划中定义的验证对象、验证目的和验证通过准则？
2	是否在硬件集成和验证规范中遵循了硬件集成和验证计划中定义的测试活动和方法？
3	是否在硬件集成和验证规范中遵循了硬件集成和验证计划中定义的测试策略？
4	是否在硬件集成和验证规范中遵循了硬件集成和验证计划中定义的验证依赖项？
5	是否在硬件集成和验证规范中，基于产品的ASIL等级，采用了适当的方法来推导出测试用例？
6	是否在硬件集成和验证规范中确认了硬件安全要求与测试用例间的追溯性？
7	是否在硬件集成和验证规范中确认了测试用例的完整性？
8	是否在硬件集成和验证规范中确认了测试用例的正确性？
9	是否在硬件集成和验证规范中，根据产品的ASIL等级，定义了硬件在环境和运行应力因素下的耐用性和鲁棒性测试？
10	是否对硬件集成和验证规范的变更定义了相应的管理和追溯措施？
11	硬件集成和验证规范是否通过验证评审？

表 12　硬件集成和验证报告的审核及评估检查清单

序号	检查清单
1	是否在硬件集成和验证报告中覆盖了所有的测试用例？
2	是否在硬件集成和验证报告中记录了完整的测试数据？
3	是否在硬件集成和验证报告中体现了测试用例完成状态？
4	是否在硬件集成和验证报告中体现了测试结果(每条测试用例)？
5	是否对硬件集成和验证报告中的测试偏离项提供解释说明或建议改进措施？
6	是否在硬件集成和验证报告中明确了测试结论(通过或者失败原因)？
7	硬件集成和验证报告是否通过验证评审？

附录 E 提供了针对硬件集成和验证开展审核及评估的说明及示例。

10　硬件要素评估

10.1　目标

本章的目标是对硬件要素评估计划、硬件要素测试计划以及硬件要素评估报告等相关工作成果进行审核及评估，以提供证据，证明硬件要素的功能表现足以满足分配的安全要求，从而保证由于硬件要素的系统性故障而违背安全目标或安全要求的风险是足够低的。

10.2　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：

——硬件要素评估计划；

——硬件要素测试计划(如适用)；

——硬件要素评估报告。

注：为支持审核及评估，可能需要提供的其他支持材料如下：

——硬件要素相关的安全要求；

——鉴定准则(分析和测试)，按照 GB/T 34590.5—2022 中的 6.4.6；

——制造商的硬件要素规范，如无法提供，则提供硬件要素定义的假设。

10.3　审核及评估的要求

对于硬件要素评估的审核及评估，应涵盖表 13、表 14、表 15 的检查项。

表 13　硬件要素评估计划的审核及评估检查清单

序号	检查清单
1	是否在硬件要素评估计划中定义了被评估硬件要素的范围的确认？
2	是否在硬件要素评估计划中定义了被评估硬件要素的相关的基本信息？
3	是否在硬件要素评估计划中定义了被评估硬件要素类别的识别？
4	是否在硬件要素评估计划中定义了被评估硬件要素的相关要求？

表 13　硬件要素评估计划的审核及评估检查清单（续）

序号	检查清单
5	是否在硬件要素评估计划中定义了被评估硬件要素失效模式和故障，及其随机故障的分布的识别？
6	是否在硬件要素评估计划中定义了被评估硬件要素的失效模式或故障安全相关性的分析与识别？
7	是否在硬件要素评估计划中定义了符合被评估硬件要素类别的评估策略？
8	是否在硬件要素评估计划中定义了符合被评估硬件要素类别的评估论证？
9	是否在硬件要素评估计划中定义了被评估硬件要素的依赖项？
10	是否在硬件要素评估计划中定义了被评估硬件要素的责任方？
11	是否在硬件要素评估计划中定义了硬件要素评估通过或不通过的准则？
12	是否对硬件要素评估计划变更定义了相应的管理和追溯措施？
13	硬件要素评估计划进行是否通过验证评审？

表 14　硬件要素测试计划的审核及评估检查清单

序号	检查清单
1	是否在硬件要素测试计划中定义了被测硬件要素的基本信息(如适用)？
2	是否在硬件要素测试计划中定义了符合集成了被测硬件要素的要素或系统的 ASIL 等级要求的硬件测试活动与方法(如适用)？
3	是否在硬件要素测试计划中定义了分配给被测硬件要素的安全要求(如适用)？
4	是否在硬件要素测试计划中定义了需要参考的测试规范和测试顺序(如适用)？
5	是否在硬件要素测试计划中体现了测试与安全要求之间的追溯性(如适用)？
6	是否在硬件要素测试计划中定义了组装和连接的需求(如适用)？
7	是否在硬件要素测试计划中定义了测试的依赖项(如适用)？
8	是否在硬件要素测试计划中定义了被测硬件要素数量(如适用)？
9	是否在硬件要素测试计划中定义了测试通过或不通过的准则(如适用)？
10	是否对硬件要素测试计划变更定义了相应的管理和追溯措施(如适用)？
11	硬件要素测试计划是否通过验证评审(如适用)？

表 15　硬件要素评估报告的审核及评估检查清单

序号	检查清单
1	是否在硬件要素评估报告中体现了被评估硬件要素的范围？
2	是否在硬件要素评估报告中体现了分配给被评估硬件要素的相关的基本信息？
3	是否在硬件要素评估报告中体现了分配给被评估硬件要素的安全要求？
4	是否在硬件要素评估报告中体现了被评估硬件要素的类别？
5	是否在硬件要素评估报告中体现了被评估硬件要素失效模式或故障，及其随机硬件故障的分布信息？
6	是否在硬件要素评估报告中体现了被评估硬件要素失效模式或故障的安全相关性？

表 15　硬件要素评估报告的审核及评估检查清单（续）

序号	检查清单
7	是否在硬件要素评估报告中体现了符合被评估硬件要素类别的评估策略？
8	是否在硬件要素评估报告中体现了符合被评估硬件要素类别的评估论证？
9	是否在硬件要素评估报告中体现了对被评估硬件要素相关的评估论证的评估？
10	是否对硬件要素评估报告中的偏离项提供了解释说明或建议改进措施？
11	是否在硬件要素评估报告中明确了评估结论(通过或失败)？
12	硬件要素评估报告是否通过验证评审？

附录 F 提供了针对硬件要素评估开展审核及评估的说明及示例。

附 录 A
（资料性）
硬件安全要求

硬件安全要求的审核及评估的说明及示例见表 A.1。

表 A.1 硬件安全要求的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否定义了硬件安全要求和安全机制控制硬件内部失效（例如：对内核失效的检测、对存储失效的监控）？	可检查是否根据硬件内部失效分析（DFMEA 等）的结果定义了相关要求 **示例 1**：根据 DFMEA 的分析结果，如果内核失效，可能造成程序跑飞，需要检查是否有定义看门狗的定时和探测能力的要求。 **示例 2**：根据 DFMEA 的分析结果，如果存储区域失效，会造成数据丢失，需要检查是否有存储区域的校验要求。
2	是否定义了对外部失效容错的硬件安全要求和安全机制（例如：传感器开路或短路检测的支撑电路）？	可检查是否根据外部接口失效分析（DFMEA 等）的结果定义了相关要求 **示例**：EPS 的输入开路时，有硬件安全要求支持对开路故障的检测。
3	是否为符合其他要素的安全要求定义了硬件安全要求和安全机制的相关属性？	可检查是否有硬件安全要求满足根据来自其他系统的安全要求定义 **示例**：有支持转角、转矩传感器和电机供电状态读取的硬件安全要求。
4	是否定义了硬件安全要求和安全机制探测内外部失效和发送失效信息？	可检查是否有对应发送失效信息的硬件安全要求 **示例**：设计点亮报警灯或发送 CAN 信号的硬件电路的硬件安全要求。
5	对于 ASIL（B）、C 和 D 等级，硬件安全要求是否设定了硬件架构度量目标值？	可检查定义的硬件度量设定目标值是否符合单点故障度量和潜伏故障度量指标的要求（GB/T 34590.5—2022 中表 4 和表 5）。 如涉及 ASIL 分解，则可检查硬件度量设定目标值是否按照分解前的 ASIL 等级设置
6	对于 ASIL（B）、C 和 D 等级，硬件安全要求是否设定了随机硬件失效概率度量目标值（如采用 EEC 方法，该问题不适用）？	可检查定义的硬件随机失效设定目标值是否满足随机硬件失效目标值（PMHF）或者对违背安全目标的每个原因的评估（EEC）方法的定义。 a） 随机硬件失效目标值（PMHF 见 GB/T 34590.5—2022 中的表 6）。 b） 违背安全目标的每个原因的评估（EEC）： ——针对单点故障的硬件元器件失效率等级目标（见 GB/T 34590.5—2022 中的表 7 和表 8）； ——针对双点故障的硬件元器件失效率等级和覆盖率的目标（见 GB/T 34590.5—2022 中的表 9）。 如果采用对违背安全目标的每个原因的评估（EEC）方法，则可检查是否需要定义专用措施。专用措施可能包括： ——设计特征，如硬件元器件过设计（例如电气或热应力等级）或者物理隔离（例如印刷电路板上的触点间隔）； ——专门的来料抽样测试，以降低此失效模式发生的风险； ——老化测试； ——作为控制计划一部分的专用控制设备； ——安全相关的特殊特性的分配

表 A.1　硬件安全要求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	硬件安全要求是否包含了非用以定义安全机制的硬件安全要求？	可检查是否有相关定义，例如：线束屏蔽 EMC 干扰的硬件安全要求、接插件插拔防呆的硬件安全要求
8	是否定义了相关项或要素的硬件设计验证准则，包括环境条件（温度、振动、EMI 等）、特定的运行环境（供电电压、任务剖面等）以及特定于组件的要求？	可检查是否有针对每条硬件安全要求都定义了硬件设计验证准则（设计评审或测试验证都可作为验证准则）。 **示例：** ——硬件安全要求：×××的电源接口应提供 3.3 V 的电压给×××传感器； ——验证准则：设计评审。
9	硬件安全要求所对应的安全机制的故障容错时间间隔或者最大故障处理时间间隔是否符合系统层级的定义？	如果为单点故障，可检查是否与所关联的技术安全要求的故障容错时间间隔或者最大故障处理时间间隔要求保持一致
10	硬件安全要求所对应的安全机制的多点故障探测时间间隔要求是否符合系统层级的定义？	如果为多点故障，对于 ASIL 等级为 ASIL C 和 ASIL D 的安全目标来说： a) 如果对应的安全概念没有描述明确的量值，可检查是否参照安全概念的定义； b) 如果对应的安全概念没有描述明确的量值，可检查多点故障探测时间间隔是否等于或小于该相关项从上电到下电的周期。 如通过对随机硬件失效的发生概率的定量分析来确定，可检查是否符合 MTTF 的合理性
11	硬件安全要求是否与技术安全要求之间保持了追溯性和一致性？硬件安全要求是否与技术安全概念、系统设计规范和硬件规范之间保持了一致性？	可检查是否有验证报告可表现有对追溯性和一致性的检查，是否可提供工具统计的硬件安全要求与技术安全要求的覆盖度报告或类似证据，并对实际交付物进行抽查，例如：硬件安全要求和技术安全要求的要求是否都有唯一的标识号，标识号之间是否可互相追溯，上下级要求之间描述是否一致
12	硬件安全要求是否按照 GB/T 34590.8—2022 第 6 章的要求进行定义和管理？	可检查硬件安全要求是否按照 GB/T 34590.8—2022 中表 1 定义安全要求的方法进行定义；是否具备明确的安全要求的属性和特性；是否按照安全要求的管理要求进行管理；是否运用 GB/T 34590.8—2022 中表 2 所列方法的恰当组合进行安全要求的验证

软硬件接口规范的审核及评估的说明及示例见表 A.2。

表 A.2　软硬件接口规范的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否细化了硬件设备的相关运行模式和相关配置参数（例如：对看门狗的配置）？	可检查运行模式是否有定义，例如：上电、下电、初始化、故障模式等，以及检查对应参数是否有配置，例如：看门狗的时间窗口设置
2	是否确保了要素间独立性或支持软件分区的硬件特征？	可结合 DFA 分析的结果检查是否对系统层面的软硬件接口规划进行了细化，例如：对多核 MCU 的核内资源分配
3	是否对硬件资源的共用和专用进行了明确定义？	可检查例如：是否对内存映射、寄存器分配、计时器、中断、I/O 端口等进行了细化

表 A.2　软硬件接口规范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	是否对硬件设备的访问机制进行了明确定义？	可检查例如：是否对硬件设备间的主从、串并关系进行了细化
5	由技术安全概念得出的时间约束是否在软硬件接口规范中进行了说明？	可检查软件和硬件的响应时间之和是否满足技术安全概念得出的时间约束
6	是否对硬件的诊断特性进行了明确定义？	可检查例如：是否定义了硬件的过流过压过温阈值，并在对应的硬件安全要求中进行了描述
7	是否对需要在软件中实现的对硬件的诊断特性进行了明确定义？	可检查例如：软硬件接口规范中所定义的硬件过流、过压、过温的阈值，是否在关联的软件安全要求里定义了相应的诊断要求
8	是否明确描述了硬件和软件之间的每一项安全相关的关联性？	可根据例如：硬件 FMEA 和软件 FMEA 的分析结果检查是否都进行了明确描述
9	是否细化后的软硬件接口都定义了对应的验证准则？	可检查每一条接口对应的要求定义是否有关联验证准则（设计评审或测试验证都可作为验证准则），如需软件实现的诊断特性，则检查软件安全要求是否有关联验证准则。验证可为评审或测试
10	是否细化后的软硬件接口（HSI）规范的充分性由软硬件开发人员进行了共同验证？	可检查设计评审及测试验证的参与人员是否包含软件和硬件开发人员

硬件安全要求验证报告的审核及评估的说明及示例见表 A.3。

表 A.3　硬件安全要求验证报告的审核及评估的说明及示例

序号	检查清单	说明及示例
1	硬件安全要求的验证活动是否验证了与技术安全概念、系统设计规范以及硬件规范的一致性？	可检查是否有记录体现硬件安全要求与技术安全概念、系统设计规范以及硬件规范的一致性的证据
2	硬件安全要求的验证活动是否说明了技术安全要求分配给硬件要素的完整性？	可检查是否有记录体现技术安全要求分配给硬件要素的完整性的证据
3	硬件安全要求的验证活动是否验证了与相关软件安全要求的一致性？	可检查是否有记录体现硬件安全要求与相关软件安全要求的一致性的证据
4	硬件安全要求的验证活动是否验证了硬件安全要求的正确性与准确性？	可检查是否有记录体现硬件安全要求的正确性和准确性的证据，例如：检查硬件安全要求的评审记录和测试记录，确认其结果与硬件安全要求的验证准则一致

附 录 B
（资料性）
硬 件 设 计

硬件设计的审核及评估的说明及示例见表 B.1。

表 B.1 硬件设计的审核及评估的说明及示例

序号	检查清单	说明及示例
1	所定义的硬件安全要求是否与硬件架构保持了追溯性和一致性，并保持到硬件组件的最底层？ **注**：对于不能划分为硬件子要素的硬件元器件，不分配硬件安全要求。例如，电容和电阻。	可检查是否有验证报告表示所定义的硬件安全要求与硬件架构（甚至到硬件组件的最底层）保持了追溯性和一致性，是否有工具统计的硬件架构与硬件安全要求的覆盖度报告或类似证据。对实际交付物进行抽查，例如：硬件安全要求是否有独立的 ID，硬件架构描述是否有独立的 ID，ID 之间是否可相互追溯，相互之间的描述是否一致 **注**：硬件安全要求的可追溯性不要求深入到硬件详细设计。对于不能划分为硬件子元素的硬件元器件，不分配硬件安全要求。例如，试图建立每个电容和电阻等硬件的可追溯性既没有意义，也没有益处。
2	硬件安全要求是否都分配给了硬件要素及其子要素？每个硬件要素或子要素所定义的 ASIL 等级是否为分配给它的所有要求中最高的 ASIL 等级？如果一个硬件要素是由 ASIL 等级低于要素 ASIL 等级或没有指定 ASIL 等级的子要素组成，该要素是否满足 GB/T 34590.9—2022 第 6 章的共存准则？	可检查是否有验证报告表示硬件要求都分配给了硬件要素及其子要素，且每个硬件要素或子要素所定义的 ASIL 等级为分配给它的所有要求中最高的 ASIL 等级，并对交付物进行抽查。 如果一个硬件要素是由 ASIL 等级低于要素 ASIL 等级或没有指定 ASIL 等级的子要素组成，需要检查 DFA 中基于硬件架构对于 ASIL 等级低于要素 ASIL 等级或没有指定 ASIL 等级的子要素分析的完整性和正确性，证明其不存在干扰 **示例 1**： 硬件要素 1 含有两个子要素，分别为硬件子要素 1.1 和硬件子要素 1.2，如果一个 ASIL B 要求被分配给硬件要素 1，那么硬件子要素 1.1 和硬件子要素 1.2 都要继承 ASIL B。 硬件子要素 1.2 仅在满足以下条件时在较低的 ASIL 等级下开发： a) 硬件要素 1 的至少一个子要素能够满足硬件要素 1 在 ASIL B 下的要求（例如：硬件子要素 1.1）； b) 硬件子要素 1.2 不能违反硬件要素 1 的安全要求； c) 满足共存的准则：从硬件子要素 1.2 到硬件子要素 1.1 没有级联失效（免于干扰）。 **示例 2**： 如果将 ASIL D 的要求分配给一个 ECU，其可在独立并且冗余的硬件要素 1 和硬件要素 2 之间进行分解。分解需要满足以下要求： ——使用 GB/T 34590.9—2022 第 5 章的 ASIL 等级的分解方案，如 ASIL D → ASIL B (D) + ASIL B (D)； ——硬件要素 1 本身满足 ASIL B (D) 的 ECU 的安全要求； ——硬件要素 2 本身满足 ASIL B (D) 的 ECU 的安全要求。
3	硬件架构设计中如果对硬件安全要求应用 ASIL 等级分解，ASIL 等级的分解是否按照 GB/T 34590.9—2022 第 5 章的要求进行？	可检查硬件架构设计中硬件安全要求 ASIL 等级的分解的方案，分解方案满足 GB/T 34590.9—2022 第 5 章的要求 **示例**：分配给电源 ASIL D 要求可分解为两路不同源的电源输入，并且两路的电源都使用监控输出的电压或电流的安全机制，那么这两路电源的 ASIL 等级可都为 ASIL B(D)。

表 B.1　硬件设计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	硬件架构设计是否按照对应的 ASIL 等级根据 GB/T 34590.5—2022 中的表 1 硬件架构设计原则进行设计，并使其具有模块化特性、适当的粒度水平和简单性？如未按照 ASIL 等级要求选取硬件设计原则，是否有合理的理由说明？	可根据 GB/T 34590.5—2022 中表 1 按照对应 ASIL 等级的要求检查硬件架构框图是否具有对应的设计原则。如未按照 ASIL 等级要求选取硬件设计原则，确认是否有合理的理由说明。 确认硬件架构中的硬件要素的设计是否无需修改就可重复使用。例如：温度探测电路模块、微控制器中的 ECC 模块。 确认硬件架构是否在必要的详细程度上体现必要的信息，来显示安全机制的有效性。 确认硬件架构是否避免不必要的接口复杂性并且避免不必要的硬件组件复杂性
5	在硬件架构设计时，是否考虑安全相关硬件组件失效的非功能性原因（如温度、振动、水、灰尘、电磁干扰、噪声因素，或来自硬件架构的其他硬件组件或其所在环境的串扰）？	可检查是否定义了安全相关硬件组件失效的非功能性原因 **示例**：功能性需求为×××的温度工作范围为（－40 ℃，125 ℃）。
6	在进行硬件详细设计时，为避免常见的设计缺陷，是否运用相关的经验总结？	可检查例如 FMEA 中的相关经验总结，之前项目的经验总结等是否被运用到实际的硬件详细设计中。可抽查相关设计 FMEA 中的预防措施是否被运用，以及之前项目经验总结相关的措施是否被运用
7	在硬件详细设计时，是否考虑安全相关硬件元器件失效的非功能性原因（如温度、振动、水、灰尘、电磁干扰、噪声因素、来自硬件组件的其他硬件元器件或其所在环境的串扰）？	可检查是否定义了安全相关硬件元器件失效的非功能性原因 **示例**：硬件元器件非功能性需求为 Sensor 1 的温度工作范围为（－40 ℃，125 ℃）。
8	硬件详细设计是否考虑硬件元器件或硬件组件的任务剖面和运行条件？是否保证硬件元器件或硬件组件在其规格范围内运行？	可检查定义的硬件元器件或硬件组件的运行条件是否在硬件元器件或硬件组件的任务剖面和运行条件范围内 **示例**：选择硬件元器件时，预期适用温度范围为（－40 ℃，125 ℃），则选择的硬件元器件的工作温度需要覆盖此范围。
9	硬件详细设计是否考虑鲁棒性设计原则（如适用）？	可检查硬件详细设计是否遵循其鲁棒性设计原则 **注**：关于硬件组件设计，可遵循企业内部的关于硬件组件应对环境和运行应力因素鲁棒性方面的规范。
10	硬件设计规范是否通过验证评审？	可检查对应的硬件设计规范验证评审报告是否存在，并且验证评审报告中的检查项要求都满足

硬件安全分析的审核及评估的说明及示例见表 B.2。

表 B.2　硬件安全分析的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否定义了针对不同 ASIL 等级硬件产品要求的定性的安全分析方法？	可检查对不同 ASIL 等级硬件产品要求的定性的安全分析方法？如演绎硬件安全分析(例如 FTA)、归纳安全分析(例如 FMEA)、相关失效分析(例如 DFA)等
2	对于 ASIL (B)、C 和 D 等级，是否用安全分析针对每个安全相关的硬件组件或元器件识别以下内容： a) 安全故障； b) 单点故障或残余故障； c) 多点故障(无论是可感知的、可探测的或潜伏的)	可检查 FMEA、FMEDA 或 FTA 中失效是否为安全相关，并且对安全相关失效故障进行分类。 硬件要素的短路故障，若其不会导致违反安全目标，则其为安全故障，若其导致直接违反安全目标且没有安全机制存在，则其为单点故障，若有安全机制覆盖，那么安全机制未覆盖到的部分为残余故障，若该硬件要素的短路故障需要与另一的失效故障一起发生才会导致违反安全目标，则其为多点故障
3	对于 ASIL (B)、C 和 D 等级，对于防止导致单点失效的故障或减少残余故障而实施的安全机制，是否具备证明安全机制具有实现和保持安全状态的能力(特别是在容错时间间隔和最大故障处理时间间隔内适当的失效减轻能力)的证据？由安全机制实现的残余故障的诊断覆盖率是否已评估？	可检查对于防止导致单点失效的故障或减少残余故障的而实施的安全机制对于侦测到故障到安全机制作动的时间是否能满足 FTTI 进行评估或测试的证据。 安全机制的诊断覆盖率的评估方法，如： a) 参考标准：GB/T 34590.5—2022 附录 D 和 GB/T 34590.11—2022 第 5 章； b) 深入分析：故障注入测试、数学分析、仿真等； c) 专家判断
4	对于 ASIL (B)、C 和 D 等级，防止潜伏故障而实施的安全机制，是否具备证据以证明安全机制在可接受的多点故障探测时间间隔内完成潜伏故障的失效探测和实现或保持安全状态及警示驾驶员的能力，以确定哪些故障保持潜伏，哪些故障可被探测到？由安全机制实现的潜伏故障的诊断覆盖率是否已评估？	可检查对于防止潜伏故障而实施的安全机制对于侦测到多点故障发生到安全机制作动的时间是否能满足多点故障探测时间间隔进行评估或测试的证据。 安全机制的诊断覆盖率的评估方法，如： a) 参考标准：GB/T 34590.5—2022 附录 D 和 GB/T 34590.11—2022 第 5 章； b) 深入分析：故障注入测试、数学分析、仿真等； c) 专家判断
5	是否进行相关失效分析以提供证据证明设计中的硬件要素与它们的独立性要求相符合？	可检查对于硬件要素的 DFA 的必要性和充分性。 可检查不同的耦合因素(如共享资源，共享信息输入，环境抗干扰能力不足；通信；非预期接口，共享资源，同类组件等)对于两个或多个硬件要素之间的相关失效影响，这些要素之间不存在级联失效和共因失效
6	如果硬件设计引入了新危害，且这个危害没有被现有的 HARA 报告覆盖，是否有变更管理流程对它们进行引入和评估？	可检查 FMEA 中该新危害是否被记录，是否有相应的变更申请，变更影响分析和变更需求计划以及变更报告
7	硬件安全分析是否通过验证评审？	可检查对应的硬件安全分析的验证评审报告是否存在，并且验证评审报告中的检查项要求都满足

硬件设计验证的审核及评估的说明及示例见表 B.3。

表 B.3　硬件设计验证的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否按照对应的 ASIL 等级选取 GB/T 34590.5—2022 中表 3 要求的硬件设计验证方法，以验证硬件设计满足硬件安全要求，与软硬件接口规范兼容以及用来生产和服务过程中实现功能安全的安全相关特殊特性的适用性？如未按照 ASIL 等级要求选取方法，是否有合理的理由说明？	可按照 ASIL 等级检查 GB/T 34590.5—2022 中表 3 的验证方法是否被使用，可检查硬件设计走查会议记录、硬件设计检查报告、安全分析报告、仿真报告以及通过硬件原型的开发记录和报告等，说明硬件设计满足硬件安全的要求、硬件设计与软硬件接口规范兼容且能证明硬件设计用来在生产和服务过程中实现功能安全的安全相关特殊特性的适用性。 如未按照 ASIL 等级要求选取方法，确认是否有合理的理由并且能够满足硬件设计验证目的
2	是否具有仿真或通过硬件原型的开发验证方法的验证计划、验证规范以及验证报告，如适用？这些验证计划、验证规范和验证报告是否通过验证评审？	可检查仿真或通过硬件原型的开发验证是否按照 GB/T 34590.8—2022 第 9 章要求来进行，具有对应的验证计划、验证规范以及验证报告。 检查验证计划，验证规范以及验证报告对应的验证评审报告是否存在，并且验证评审报告中的检查项要求都满足
3	在硬件设计过程中，如果发现任何硬件安全要求的实施是不可行的，是否按照 GB/T 34590.8—2022 第 8 章中的变更管理流程提出变更请求？	可检查是否有相应的变更申请，变更影响分析和变更需求计划以及变更报告
4	是否根据硬件安全要求和硬件设计规范验证用于开发集成到硬件中的 SEooC 的假设的有效性？	可检查是否有验证报告可表现集成到硬件中的 SEooC 的假设被硬件安全要求和硬件设计规范覆盖，并且证明其是有效的

与生产、运行、服务和报废相关的需求规范的审核及评估的说明及示例见表 B.4。

表 B.4　与生产、运行、服务和报废相关的需求规范的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否有与生产、运行、服务和报废相关的安全相关的特殊特性？	可检查是否有与生产、运行、服务和报废相关的安全相关要求，这些安全相关的要求需要定义特殊特性。可检查产品特殊特性清单 **示例**：当报废带有安全气囊的汽车或转向盘总成（内含安全气囊组件）时，应引爆安全气囊，以防安全气囊误爆引起的事故。
2	是否定义这些安全相关的特殊特性： ——生产和运行的验证措施； ——这些措施的接受准则	可检查与生产、运行、服务和报废相关的特殊特性清单以及硬件安全需求中定义的这些特殊特性的生产和运行的验证措施和这些措施的接受准则 **示例**：对一种依赖于新的传感器技术的硬件设计的安全分析（如摄像头或雷达传感器），能揭示出这些传感器与特殊安装流程的关系。则在生产阶段对这些组件的必要的额外验证措施需要被定义在硬件需求中。

表 B.4　与生产、运行、服务和报废相关的需求规范的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
3	如果安全相关硬件要素的错误组装、拆卸和报废可能对实现或维护功能安全产生不利影响，是否将避免错误执行所需的信息告知负责生产、运行、服务和报废的人员？	可检查为避免安全相关硬件要素的错误组装、拆卸和报废可能对实现或维护功能安全产生不利影响执行所需的信息。负责生产、运行、服务和报废的人员是否参与了与生产、运行、服务和报废相关的需求规范的评审并认可
4	安全相关硬件要素是否具有可追溯性？是否支持可进行有效的现场监测和可启用召回或更换管理？	可检查安全相关硬件要素是否有适当的标签或其他的硬件要素识别方法，来表示它们是与安全相关的
5	如果错误的服务可能对实现或维护功能安全产生不利影响，是否将避免此类影响执行所需的信息定义至与生产、运行、服务和报废相关的需求规范中？是否告知负责生产、运行、服务和报废的人员？	可检查与生产、运行、服务和报废相关的需求规范中是否定义了避免错误的服务可能对实现或维护功能安全产生不利影响执行所需的信息。负责生产、运行、服务和报废的人员是否参与了与生产、运行、服务和报废相关的需求规范的评审并认可
6	硬件设计过程中产生的硬件要素的生产、运行、服务和报废要求，是否通过某种方式告知负责生产、运行、服务和报废的人员？	可检查负责生产、运行、服务和报废的人员是否参与了与生产、运行、服务和报废相关的需求规范的评审并认可
7	与生产、运行、服务和报废的需求规范是否通过验证评审？	可检查与生产、运行、服务和报废的需求规范的验证报告，说明与生产、运行、服务和报废的需求规范通过验证评审

附 录 C
（资料性）
硬件架构度量的评估

硬件架构度量的评估的审核及评估的说明及示例见表 C.1。

表 C.1 硬件架构度量的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	对于 ASIL（B）、C 和 D 等级，是否为已制定的安全机制确定了诊断覆盖率？确定的诊断覆盖率是否合理？	可检查所制定的安全机制是否考虑了残余故障和相关的潜伏故障，及声明的诊断覆盖率有合适的理由支持。 残余故障及潜伏故障可参考 GB/T 34590.5—2022 附录 B。 诊断覆盖率可参考 GB/T 34590.10—2022 参与失效率评估条款和 GB/T 34590.11—2022 附录 A 中的示例
2	对于 ASIL（B）、C 和 D 等级，硬件元器件预估失效率的确定是否采用了正确的方法？预估的失效率是否合理、正确？	可检查预估失效率的确定方法是否为以下三种情况之一： a） 使用业界公认的数据库，例如 SN 29500、IEC 61709 等； b） 使用现场反馈的数据； c） 采用专家判断，例如 SAE J1211、JEDEC-JEDS89 等。 还可检查确定过的预估失效率的合理性，比如： ——对于采用业界公认的数据库的方法时，使用实际的任务剖面，以便得到合理的基础失效率； ——对于使用现场反馈的数据的方法，有 70%以上的置信度
3	对于 ASIL（B）、C 和 D 等级，当无法提供充足证据支持硬件元器件的失效率时，是否有相应的替代方案？替代方案是否合理？	可检查替代方案的合理性。 例如，增加的安全机制是否带来更高的诊断覆盖率
4	对于 ASIL（B）、C 和 D 等级，是否为每一个安全目标都定义了 SPFM 的目标值？	可检查已定义 SPFM 目标值的合理性。 如采用本表中序号 2 中的方法 a）来确定 SPFM 目标值，提供足够的证据证明参考设计的可信赖性和相似性。 如采用本表中序号 2 中的方法 b）来确定 SPFM 目标值，确保是否与安全目标的 ASIL 等级相一致。 SPFM 目标值可体现在相关工作产出物中，例如安全计划、FMEDA 等
5	对于 ASIL（B）、C 和 D 等级，是否为每一个安全目标都定义了 LFM 的目标值？	可检查已定义 SPFM 目标值的合理性。 如采用本表中序号 2 中的方法 a）来确定 LFM 目标值，提供足够的证据证明参考设计的可信赖性和相似性。 如采用本表中序号 2 中的方法 b）来确定 LFM 目标值，确保是否与安全目标的 ASIL 等级相一致。 LFM 目标值可体现在相关工作产出物中，例如安全计划、FMEDA 等
6	对于 ASIL（B）、C 和 D 等级，进行硬件架构度量评估时，是否将发生在安全相关硬件要素上的每个故障都进行了正确的分类？	故障归类为： a） 单点故障； b） 残余故障； c） 多点故障； d） 安全故障。 故障的分类方法可参照 GB/T 34590.10—2022 中的 8.1

表 C.1　硬件架构度量的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	对于 ASIL（B）、C 和 D 等级，是否每一个安全目标的 SPFM 的计算都采用了正确的计算公式？	SPFM 的计算采用 GB/T 34590.5—2022 中 C.7 的公式
8	对于 ASIL（B）、C 和 D 等级，是否每一个安全目标都满足了已定义的 SPFM 的目标值？	可检查： ——如果相关项包含失效率等级有显著差异的不同种类的硬件要素，每一类硬件要素的度量目标是否都具有合理的 SPFM 值； ——如适用，可考虑瞬态故障相关的 SPFM； ——是否结合多个安全目标确定 SPFM，并且采用最高 ASIL 等级的安全目标的度量目标。 如果未满足 SPFM 目标值，按照 GB/T 34590.5—2022 中的 4.2 对给出的如何实现安全目标的论据进行评估
9	对于 ASIL（B）、C 和 D 等级，是否每一个安全目标的 LFM 的计算都采用了正确的计算公式？	LFM 的计算采用 GB/T 34590.5—2022 中 C.8 的公式
10	对于 ASIL（B）、C 和 D 等级，是否每一个安全目标都满足了已定义的 LFM 的目标值？	可检查： ——如果相关项包含失效率等级有显著差异的不同种类的硬件要素，每一类硬件要素的度量目标是否都具有合理的 LFM 值； ——如适用，可考虑瞬态故障相关的 LFM； ——是否结合多个安全目标确定 LFM，并且采用最高 ASIL 等级的安全目标的度量目标。 如果未满足 LFM 目标值，按照 GB/T 34590.5—2022 中的 4.2 对给出的如何实现安全目标的论据进行评估
11	对于 ASIL（B）、C 和 D 等级，每一个安全目标 SPFM 和 LFM 的结果是否通过验证评审？	可检查是否采用了 GB/T 34590.8—2022 第 9 章的要求对 SPFM 和 LFM 结果进行了验证评审，及验证评审相关的证据。 评审报告及相应的计算过程通常体现在 FMEDA 中

附 录 D
（资料性）
随机硬件失效导致违背安全目标的评估

随机硬件失效导致违背安全目标的评估的审核及评估说明见表 D.1。

表 D.1 随机硬件失效导致违背安全目标的评估的审核及评估说明

序号	检查清单	示例及说明
1	对于 ASIL（B）、C 和 D 等级，随机硬件失效导致违背安全目标评估中用到的硬件元器件预估失效率的确定是否采用了正确的方法？预估的失效率是否合理、正确？	可检查预估失效率的确定方法是否为以下三种情况之一： a） 使用业界公认的数据库，例如 SN 29500、IEC 61709 等； b） 使用现场反馈的数据； c） 采用专家判断，例如 SAE J1211、JEDEC-JEDS89 等。 还可检查确定过的预估失效率的合理性，例如： ——对于采用业界公认的数据库的方法时，使用实际的任务剖面，以便得到合理的基础失效率； ——对于使用现场反馈的数据的方法，有 70％以上的置信度
2	对于 ASIL（B）、C 和 D 等级，随机硬件失效导致违背安全目标的评估是采用了随机硬件失效概率度量（PMHF）的评估方法，还是采用了对违背安全目标的每个原因的评估（EEC）的方法？	可检查是采用了 PMHF 的评估方式还是 EEC 的评估方式。 如采用 PMHF，则采用本表中序号 3～序号 8 的检查清单。 如采用 EEC，则采用本表中序号 9～序号 15 的检查清单。 另外，无论采用哪种评估方式，本表中序号 1 和序号 16 检查清单均适用
3	对于 ASIL C 和 D 等级，单一硬件元器件单点故障是否存在有效论据证明其发生概率足够低可被接受？	此检查清单针对 ASIL C 和 D 的安全目标，可检查可接受单点故障足够低的论据的有效性。 如采用专用措施，可能的方法包括硬件过设计、物理隔离、老化测试等
4	对于 ASIL C 和 D 等级，一个硬件元器件的残余故障诊断覆盖率低于 90％是否存在有效论据证明其发生概率足够低可被接受？	此检查清单针对 ASIL C 和 D 的安全目标，可检查可接受残余故障诊断覆盖率足够低论据的有效性
5	对于 ASIL（B）、C 和 D 等级，PMHF 评估的定量目标值是否表述为相关项的整个运行生命周期中每小时的平均概率？	可检查 PMHF 评估过程中所使用的单位为相关项的整个运行生命周期中每小时的平均概率，而不是失效率的单位
6	对于 ASIL（B）、C 和 D 等级，是否为随机硬件失效在相关项层面导致违背每个安全目标的最大可能性定义了定量目标值？	如参考目标值来自于本表中序号 1 中的方法 a），确保是否与安全目标的 ASIL 等级相一致。 如参考目标值来自于本表中序号 1 中的方法 b）或方法 c），提供证据证明设计的可信赖性和相似性。 目标参考值应体现在相关工作产出物中，例如安全计划、FMEDA 等

表 D.1　随机硬件失效导致违背安全目标的评估的审核及评估说明（续）

序号	检查清单	示例及说明
7	对于 ASIL（B）、C 和 D 等级，PMHF 目标值的分配是否满足要求？	可检查构成相关项的每个系统的目标值之和是否超过了原有相关项目标值一个数量级。 例如，如果一个等级为 ASIL D 的安全目标分配给由多个系统（最多 10 个）组成的相关项，其中每个系统都有可能违背该安全目标，则能将目标值 10^{-8} h 分配给组成该相关项的每个系统
8	对于 ASIL（B）、C 和 D 等级，是否有证据证明 PMHF 的目标值已达到？	PMHF 值不具有绝对意义，但有助于比较新设计与现有设计。 如果未满足 PMHF 目标值，按照 GB/T 34590.5—2022 中 4.2 对给出的如何实现安全目标的论据进行评估
9	对于 ASIL（B）、C 和 D 等级，采用 EEC 评估时，对违背所考虑的安全目标的每个单点故障、残余故障和双点失效进行的单独评估是否在硬件层面执行？	可检查评估应用的层级是否为硬件
10	对于 ASIL（B）、C 和 D 等级，采用 EEC 评估时，是否能按照要求提供证据证明违背安全目标的每个单点故障、残余故障和双点失效是可接受的？	如果不能按照要求提供证据证明每个单点故障、残余故障和双点故障是可接受的，可按照 GB/T 34590.5—2022 中 4.2 对给出的如何实现安全目标的论据进行评估
11	对于 ASIL（B）、C 和 D 等级，采用 EEC 评估时，是否对硬件元器件失效率进行了失效率等级评级？	可检查失效率的等级评级是否满足 GB/T 34590.5—2022 中 9.4.3.3 的要求。 如果失效率等级评级可除以不等于 100 的数字，需要提供理由，并确保考虑了单点故障、残余故障。 可检查是否失效率等级分配是基于不考虑安全机制有效性的硬件元器件失效率
12	对于 ASIL（B）、C 和 D 等级，采用 EEC 评估时，是否可接受硬件元器件发生的单点故障？	可检查是否满足 GB/T 34590.5—2022 中的表 7。 专用措施可能包括硬件过设计、物理隔离、老化测试等
13	对于 ASIL（B）、C 和 D 等级，采用 EEC 评估时，是否增加对应的安全机制并且可接受硬件元器件发生的残余故障？	可检查接受条件是否满足 GB/T 34590.5—2022 中 9.4.3.6 和 9.4.3.7 的要求。 所考虑的失效率是硬件元器件失效率，不考虑安全机制的有效性
14	对于 ASIL C 和 D 等级，采用 EEC 评估时，是否认为双点失效是可能的？	此项适用于 ASIL C 和 D 的安全目标。 如果认为一个双点失效是不可能的，则可认为是与安全目标相符合
15	对于 ASIL C 和 D 等级，采用 EEC 评估时，是否增加或完善对应的安全机制并且可接受硬件元器件发生的可导致双点失效的双点故障？	此项适用于 ASIL C 和 D 的安全目标。 所考虑的失效率是硬件元器件失效率，不考虑安全机制的有效性
16	对于 ASIL（B）、C 和 D 等级，对随机硬件失效导致违背安全目标评估的结果是否通过验证评审？	可检查是否采用了 GB/T 34590.8—2022 第 9 章的要求对 PMHF 或 EEC 结果进行了验证评审，及验证评审相关的证据。 PMHF 的评审一般通过 FMEDA 体现

附 录 E
（资料性）
硬件集成和验证

硬件集成和验证计划的审核及评估的说明及示例见表 E.1。

表 E.1 硬件集成和验证计划的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否在硬件集成和验证计划中定义了验证对象的信息、验证目的和验证通过准则？	可检查是否在计划中根据项目开发进度和测试需求明确了验证对象信息，例如样品级别和产品零件号，与产品生命周期内不同阶段的验证目的和验证通过准则
2	是否在硬件集成和验证计划中定义了符合产品硬件 ASIL 等级要求的活动与方法？	可检查硬件集成和验证计划中： a） 是否明确了符合产品 ASIL 等级的硬件集成和验证活动，包括产品设计和生产阶段； b） 是否制定了符合产品 ASIL 等级的硬件集成和验证方法
3	是否在硬件集成和验证计划中定义了符合产品硬件安全等级要求的测试策略？	可检查是否在计划中制定了符合产品实际开发情况和 ASIL 等级的硬件集成和验证策略，例如完整的硬件集成和验证测试或回归硬件集成和验证测试
4	是否在硬件集成和验证计划中定义了验证相关的依赖项？	可检查是否在计划中定义了硬件集成和测试所需环境、设备、工具等资源
5	是否在硬件集成和验证计划定义了验证失败的应对措施？	可检查是否在计划中明确了测试偏离或失败可接受的条件，建议的改进措施等
6	是否对硬件集成和验证计划的变更定义了相应的管理和追溯措施？	见 GB/T 43253.1—2023 中的变更管理的要求
7	硬件集成和验证计划是否通过验证评审？	可检查是否有交付物进行相关定义，验证评审可采用走查或审查的方式

硬件集成和验证规范的审核及评估的说明及示例见表 E.2。

表 E.2 硬件集成和验证规范的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否在硬件集成和验证规范中遵循了硬件集成和验证计划中定义的验证对象、验证目的和验证通过准则？	可检查硬件集成和验证规范中定义的验证对象、验证目的和验证通过准则是否与计划中一致
2	是否在硬件集成和验证规范中遵循了硬件集成和验证计划中定义的测试活动和方法？	可检查硬件集成和验证规范中定义的测试活动与方法是否与计划中一致

表 E.2　硬件集成和验证规范的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
3	是否在硬件集成和验证规范中遵循了硬件集成和验证计划中定义的测试策略？	可检查硬件集成和验证规范中定义的测试策略是否与计划中一致
4	是否在硬件集成和验证规范中遵循了硬件集成和验证计划中定义的验证依赖项？	可检查是否在硬件和验证规范中定义的依赖项是否与计划定义一致
5	是否在硬件集成和验证规范中，基于产品的 ASIL 等级，采用了适当的方法来推导出测试用例？	可检查是否在硬件集成和验证规范中是否按照 GB/T 34590.5—2022 中的表 10 导出硬件集成测试案例的方法进行了测试用例的创建
6	是否在硬件集成和验证规范中确认了硬件安全要求与测试用例间的追溯性？	可检查是否在硬件集成和验证规范中确保了硬件功能安全要求与测试用例之间的对应关系，通常可通过需求管理工具分析
7	是否在硬件集成和验证规范中确认了硬件安全要求与测试用例间的完整性？	可检查是否在硬件集成和验证规范中按照 GB/T 34590.8—2022 中的 9.4.2.2、9.4.2.3 定义了测试范例
8	是否在硬件集成和验证规范中确认了硬件安全要求与测试用例间的正确性？	可检查是否在硬件集成和验证规范中是否按照 GB/T 34590.5—2022 中的表 11 进行了测试用例的类型定义（不同类型测试对应的需求类型应匹配）
9	是否在硬件集成和验证规范中，根据产品的 ASIL 等级，定义了硬件在环境和运行应力因素下的耐用性和鲁棒性测试？	可检查是否在硬件集成和验证规范中是否按照 GB/T 34590.5—2022 中的表 12 定义了耐用性和鲁棒性测试，并链接了相关测试材料
10	是否对硬件集成和验证规范的变更定义了相应的管理和追溯措施？	见 GB/T 43253.1—2023 中的变更管理的要求
11	硬件集成和验证规范是否通过验证评审？	硬件集成和验证规范的验证评审可采用走查或审查的方式

硬件集成和验证报告的审核及评估的说明及示例见表 E.3。

表 E.3　硬件集成和验证报告的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否在硬件集成和验证报告中体现了集成和验证计划与规范的执行？	可检查硬件集成和验证报告中测试的执行是否符合计划所定义的阶段与责任方，测试的策略、方法、步骤、依赖项等是否与所参考的硬件集成和验证规范保持一致
2	是否在硬件集成和验证报告中记录了测试数据或现象？	可检查硬件集成和验证报告中是否提供每个测试用例所对应的数据记录或现象

表 E.3　硬件集成和验证报告的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
3	是否在硬件集成和验证报告中体现了测试完成状态？	可检查硬件集成和验证报告中是否明确了每一个测试用例的完成状态
4	是否在硬件集成和验证报告中体现了测试结果？	可检查硬件集成和验证报告中是否明确了每一条测试用例的测试结果（通过或失败）
5	是否对硬件集成和验证报告中的测试偏离项提供解释说明或建议改进措施？	可检查硬件集成和验证报告中是否对与测试用例预期结果偏离的相关项提供了解释说明或建议改进措施
6	是否在硬件集成和验证报告中明确了测试结论？	可检查硬件集成和验证报告中，是否根据 GB/T 34580.8—2022 中9.4.3.3的要求对测试结果进行了评估并给出了相应的结论（整个测试通过或不通过）
7	硬件集成和验证报告是否通过验证评审？	硬件集成和验证报告的验证评审可采用走查或审查的方式

附 录 F
（资料性）
硬件要素评估

硬件要素评估计划的审核及评估的说明及示例见表 F.1。

表 F.1 硬件要素评估计划的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否在硬件要素评估计划中定义了被评估硬件要素的范围的确认？	可检查硬件要素评估计划中，是否定义了被评估硬件要素范围的确认，即符合评估条件的被评估要素应满足以下条件，即： ——最初不是按照 GB/T 34590.1～34590.12—2022 开发或设计的； ——集成到符合 GB/T 34590.1～34590.12—2022 的相关项或要素中，被认为是与安全相关的 **注**：符合评估条件的硬件要素可为特定于应用的要素或者标准要素，这些要素通常被开发用于多个行业，包括汽车应用和非汽车应用。
2	是否在硬件要素评估计划中定义了被评估硬件要素相关的基本信息？	可检查硬件要素评估计划中，是否定义了被评估硬件要素的唯一识别号及版本号，以及预期使用的环境等信息
3	是否在硬件要素评估计划中定义了被评估硬件要素类别的识别？	可检查在硬件要素评估计划中，是否按照 GB/T 34590.8—2022 中的 13.4.1.1 定义了被评估硬件要素类别的识别，并将提供相应的参考材料作为识别依据
4	是否在硬件要素评估计划中定义了被评估硬件要素的相关要求？	可检查在硬件要素评估计划中，是否定义了由硬件安全要求分配和安全概念产生的硬件要素安全要求（包括其工作范围和条件）
5	是否在硬件要素评估计划中定义了被评估硬件要素失效模式和故障，及其随机故障的分布的识别？	可检查在硬件要素评估计划中，是否定义了被评估硬件要素失效模式或故障，及其随机故障的分布的识别，并提供识别所用到的可靠性标准信息，例如 IEC 61709
6	是否在硬件要素评估计划中定义了被评估硬件要素的失效模式或故障安全相关性的分析与识别？	可检查在硬件要素评估计划中，是否按照 GB/T 34590.5—2022 中的 7.4.3、第 8 章和第 9 章定义了被评估硬件要素的失效模式以及故障安全相关性的分析与识别，并提供相应的证据证明其分析与识别满足相应的要求
7	是否在硬件要素评估计划中定义了符合被评估硬件要素类别的评估策略？	可检查硬件要素评估计划中，是否按照 GB/T 34590.8—2022 中的 13.4.2（适合Ⅰ类硬件要素）、13.4.3（适合Ⅱ类硬件要素）和 13.4.4（适合Ⅲ类硬件要素）定义了符合要素类别的评估策略，如： ——对于Ⅰ类要素的评估，由于功能简单，无需对其本身进行评估，对于集成了Ⅰ类硬件要素后的硬件开发应按照 GB/T 34590.5—2022 第 10 章进行充分的测试； ——对于Ⅱ类要素的评估，可通过测试与分析相结合的方式来完成； ——对于Ⅲ类要素的评估，除了Ⅱ类要素所必需的评估活动以外，还需提供额外的措施来论证由于其系统性故障导致安全目标或要求违背的风险足够低

表 F.1　硬件要素评估计划的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
8	是否在硬件要素评估计划中定义了符合被评估硬件要素类别的评估论证？	对于Ⅰ类要素，按照 GB/T 34590.8—2022 中的 13.4.2，无需单独的评估论证，集成了Ⅰ类要素的硬件开发应按照 GB/T 34590—2022 进行。 对于Ⅱ类要素和Ⅲ类要素，如果适用，则应检查在硬件要素评估计划中，是否按照 GB/T 34590.8—2022 中的 13.4.3.3 和 13.4.4.2，定义了符合硬件要素类别的论证，例如基于合理的分析方法和假设，运行经验的数据及现有的测试结果等信息的组合。 对于需要提供额外措施来进行评估的Ⅲ类要素，如果适用，则应检查在硬件要素评估计划中，是否按照 GB/T 34590.8—2022 中的 13.4.4.3，定义了合适的额外措施的实施，来论证其由于系统性故障而违背安全目标或安全要求的风险足够低 **注**：相关的额外措施可包括但不限于： ——安全相关功能的验证性； ——现场经验/“值得信赖的组件”； ——由具备安全相关失效模式检测能力的、独立的多样化要素进行监控； ——符合不同安全标准但具有同等完整性等级的开发
9	是否在硬件要素评估计划中定义了被评估硬件要素的依赖项？	可检查在硬件要素评估计划中，是否定义了评估相关的工具和设备等
10	是否在硬件要素评估计划中定义了被评估硬件要素的责任方？	可检查在硬件要素评估计划中，是否定义了不同评估方式和依据相应的责任方
11	是否在硬件要素评估计划中定义了硬件要素评估通过或不通过的准则？	可检查在硬件要素评估计划中，是否为各被评估硬件要素定义了相应的通过/不通过准则
12	是否对硬件要素评估计划变更定义了相应的管理和追溯措施？	见 GB/T 43253.1—2023 中的变更管理的要求
13	硬件要素评估计划进行是否通过验证评审？	硬件要素评估计划的验证评审可采用走查或审查的方式

硬件要素测试计划的审核及评估的说明及示例见表 F.2。

表 F.2　硬件要素测试计划的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否在硬件要素测试计划中定义了被测硬件要素的基本信息，如适用？	可检查硬件要素测试计划中，是否定义了被测硬件要素的标识及基本功能，运行模式等信息，并应与评估计划中定义一致
2	是否在硬件要素测试计划中定义了符合集成了被测硬件要素的要素或系统的 ASIL 等级要求的硬件测试活动与方法，如适用？	可检查在硬件要素测试计划中是否按照 GB/T 34590.5—2022 中的表 11、表 12，定义了符合集成了被测硬件要素的要素或系统的 ASIL 等级要求的硬件测试活动与方法，包括被测硬件要素的功能性能测试、故障注入测试、电气测试以及对外部压力的鲁棒性测试

表 F.2　硬件要素测试计划的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
3	是否在硬件要素测试计划中定义了分配给被测硬件要素的安全要求，如适用？	可检查硬件要素测试计划中是否定义了被测硬件要素相关的安全要求（包括其工作范围和条件），并应与评估计划中定义一致
4	是否在硬件要素测试计划中定义了需要参考的测试规范和测试顺序，如适用？	可检查在硬件要素测试计划中是否定义了硬件要素测试涉及的测试规范和不同测试的时间顺序
5	是否在硬件要素测试计划中确认了测试与安全要求之间的追溯性，如适用？	可检查是否在硬件测试计划中确认了被测硬件要素相关的测试相关项与安全要求之间的对应关系
6	是否在硬件要素测试计划中定义了组装和连接的需求，如适用？	可检查硬件要素测试计划中是否定义了测试所需的各设备组装和连接需求，或是引用了同等的材料
7	是否在硬件要素测试计划中定义了测试的依赖项，如适用？	可检查硬件要素测试计划中是否定义了测试需要考虑的运行条件、环境参数、测试的工具和设备精度要求
8	是否在硬件要素测试计划中定义了被测硬件要素的数量，如适用？	可检查硬件要素测试计划中是否定义了测试需要考虑的被测要素数量
9	是否在硬件要素测试计划中定义了测试通过或不通过的准则，如适用？	可检查在硬件要素测试计划中是否为各被测硬件要素定义了相应的通过/不通过准则
10	是否对硬件要素测试计划变更定义了相应的管理和追溯措施，如适用？	见 GB/T 43253.1—2023 中的变更管理的要求
11	硬件要素测试计划是否通过验证评审，如适用？	硬件要素测试计划的验证评审可采用走查或审查的方式

硬件要素评估报告的审核及评估的说明及示例见表 F.3。

表 F.3　硬件要素评估报告的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否在硬件要素评估报告中体现了被评估硬件要素的范围？	可检查在硬件要素评估报告中，是否体现了被评估硬件要素的范围，并与评估计划定义的一致
2	是否在硬件要素评估报告中体现了被评估硬件要素相关的基本信息？	可检查硬件要素评估计划中，是否定义了被评估硬件要素的唯一识别和版本，以及预期使用的环境等信息，并与评估计划定一致
3	是否在硬件要素评估报告中体现了被评估硬件要素的类别？	可检查在硬件要素评估报告中，是否体现了被评估硬件要素的类别，并按照 GB/T 34590.8—2022 中的 13.4.1.1 要求引用了相应的材料作为类别识别的依据
4	是否在硬件要素评估报告中体现了分配给被评估硬件要素的安全要求？	可检查在硬件要素评估报告中是否体现了被评估硬件要素相关的安全要求（包括其工作范围和条件），并与评估计划定义一致

表 F.3　硬件要素评估报告的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
5	是否在硬件要素评估报告中体现了被评估硬件要素失效模式或故障，及其随机硬件故障的分布信息？	可检查硬件要素评估报告中是否体现了各被评估要素，基于选定的可靠性标准，相对于其运行条件的失效模式或故障，及其随机硬件故障的分布信息
6	是否在硬件要素评估报告中体现了被评估硬件要素失效模式或故障的安全相关性？	可检查在硬件要素评估报告中，是否按照 GB/T 34590.5—2022 中的 7.4.3、第 8 章、第 9 章，对各评估硬件要素失效模式或故障进行了安全相关性的识别，并能提供相应的安全分析与识别证据
7	是否在硬件要素评估报告中体现了符合被评估硬件要素类别的评估策略？	可检查在硬件要素评估报告中，各被评估硬件要素选取的评估策略是否满足 GB/T 34590.8—2022 中的 13.4.2（适合Ⅰ类要素）、13.4.3（适合Ⅱ类要素）和 13.4.4（适合Ⅲ类要素）的相关要求
8	是否在硬件要素评估报告中体现了符合被评估硬件要素类别的评估论证？	可检查在硬件要素评估报告中，各被评估硬件要素的选取的评估论证方式是否满足 GB/T 34590.8—2022 中的 13.4.2（适合Ⅰ类要素）、13.4.3.3 和 13.4.3.3（适合需要提供额外论证措施的Ⅲ类要素）的相关要求
9	是否在硬件要素评估报告中体现了对被评估硬件要素相关的评估论证的评估？	基于被评估硬件要素分析评估论证的评估，可检查在硬件要素评估报告中： ——是否按照 GB/T 34590.8—2022 中的 13.4.4.1，对分析评估的全面性和可验证性进行了评估； ——是否按照 GB/T 34590.8—2022 中的 13.4.4.2，对分析评估所涉及的硬件要素暴露的环境条件完整性进行了评估。 基于被评估硬件要素测试评估论证的评估，如果适用，则应检查在硬件要素评估报告中： ——是否按照 GB/T 34590.8—2022 中的 13.4.3.5.1～13.4.3.5.3，对测试评估的执行是否与计划一致性进行了评估； ——是否按照 GB/T 34590.8—2022 中的 13.4.3.5.3，对测试评估所涉及的测试数据的完备性进行了评估； ——是否按照 GB/T 34590.5—2022 第 10 章或 GB/T 34590.4—2022 第 7 章的要求对集成到符合 GB/T 35490—2022 的要素的被测硬件要素测试进行了评估。 基于被评估硬件要素需要额外措施论证的评估，可检查在硬件要素评估报告中： ——是否按照 GB/T 34590.5—2022 中的 13.4.4.3 的要求对措施实施的合理性和完备性进行了评估
10	是否对硬件要素评估报告中的偏离项提供了解释说明或建议改进措施？	可检查在硬件要素评估报告中是否对安全要求偏离项做出了解释说明或建议改进措施，例如提供了外部安全机制来控制偏离项引发的影响
11	是否在硬件要素评估报告中明确了评估结论（通过或失败）？	可检查硬件要素评估报告中，是否对各硬件要素提供了相应的评估结论
12	硬件要素评估报告是否通过验证评审？	硬件要素评估报告的验证评审可采用走查或审查的方式