ICS 43.040
CCS T 35

中华人民共和国国家标准

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

Road vehicles—Functional safety audit and assessment method—Part 3：Software 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　软件开发环境 …… 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　软件安全要求 …… 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　软件架构设计规范 …… 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　软件单元设计及实现 …… 5
8.1　目标 …… 5
8.2　审核及评估的输入 …… 5
8.3　审核及评估的要求 …… 5
9　软件单元验证 …… 6
9.1　目标 …… 6
9.2　审核及评估的输入 …… 6
9.3　审核及评估的要求 …… 6
10　软件集成和验证 …… 7
10.1　目标 …… 7
10.2　审核及评估的输入 …… 7
10.3　审核及评估的要求 …… 8
11　嵌入式软件测试 …… 8
11.1　目标 …… 8
11.2　审核及评估的输入 …… 8
11.3　审核及评估的要求 …… 9
12　软件标定和配置管理 …… 9
12.1　目标 …… 9
12.2　审核及评估的输入 …… 9
12.3　审核及评估的要求 …… 9

13 软件组件鉴定 …… 10
13.1 目标 …… 10
13.2 审核及评估的输入 …… 10
13.3 审核及评估的要求 …… 11
附录 A（资料性） 软件开发环境 …… 12
附录 B（资料性） 软件安全要求 …… 13
附录 C（资料性） 软件架构设计规范 …… 14
附录 D（资料性） 软件单元设计及实现 …… 17
附录 E（资料性） 软件单元验证 …… 18
附录 F（资料性） 软件集成和验证 …… 20
附录 G（资料性） 嵌入式软件测试 …… 22
附录 H（资料性） 软件标定和配置管理 …… 23
附录 I（资料性） 软件组件鉴定 …… 25

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3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、中国长安汽车集团有限公司、苏州博沃创新能源科技有限公司、东软睿驰汽车技术(上海)有限公司、上海集度汽车有限公司、上海机动车检测认证技术研究中心有限公司、中国第一汽车集团有限公司、知行汽车科技(苏州)有限公司、上海禾赛科技有限公司、上海拿森汽车电子有限公司、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：邵海贺、陈勇、郭晓东、付越、李波、李鸿鹏、闻继伟、胡国强、李小锋、王宇、王潇屹、尚世亮、宋炜瑾、赵鑫、范鹏、卢刚、花町、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。

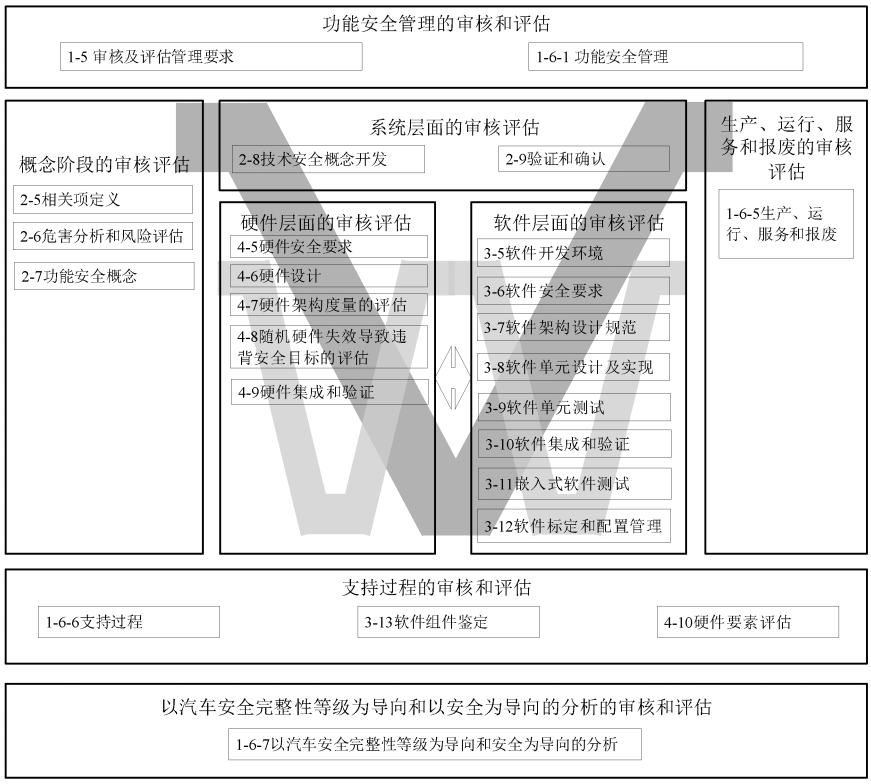

图1　功能安全审核及评估概览

道路车辆　功能安全审核及评估方法
第3部分:软件层面

1　范围

本文件规定了针对安全相关的电气/电子(E/E)系统在软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。

软件层面的功能安全审核及评估,主要涉及以下内容:

——软件开发环境;
——软件安全要求;
——软件架构设计规范;
——安全分析报告;
——相关失效分析报告;
——软件单元设计及实现;
——软件单元验证;
——软件集成和验证;
——嵌入式软件测试;
——软件标定和配置管理;
——软件组件鉴定。

通过审核及评估,基于证据判断软件层面的功能安全开发,符合:

——软件相关的技术安全需求规范是恰当和完整的;

——确保所开发软件能实现功能安全要求；
——确保所开发软件以及软件要素符合分配的软件安全要求。

5 软件开发环境

5.1 目标

本章的目标是对软件开发环境的相关工作成果进行审核及评估，以提供证据证明：
a） 与软件开发流程相符且一致；
b） 软件开发环境满足相关项功能安全开发的要求。

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：
——软件开发环境文档。

注：为了支持软件开发环境的审核及评估，可能需要提供如下支持材料：
——经鉴定合格的软件工具；
——用于建模、设计和编程语言的设计和编码指南；
——方法应用的指南；
——工具应用的指南。

5.3 审核及评估的要求

对于软件开发环境的审核及评估，应涵盖表 1 的检查项。

表 1 软件开发环境的审核及评估检查清单

序号	检查清单
1	在开发相关项时，使用的软件开发流程和软件开发环境是否适用并满足该相关项要求？ a） 适用于开发安全相关的嵌入式软件，包括方法、指南、语言和工具； b） 软件开发生命周期的各个阶段及相关阶段的工作成果的一致性； c） 与系统和硬件开发阶段在所需的交互和信息交换的一致性
2	在开发相关项时，所应用的设计语言、建模语言或编程语言是否满足以下准则？ a） 明确易理解的定义； b） 如果建模用于需求工程和管理，定义和管理安全要求的适用性； c） 支持模块化、抽象化和封装化的实现； d） 支持结构化构造的使用
3	建模和编码指南是否满足对应的 ASIL 等级所要求的通则，以涵盖适合于建模、设计或者编程语言的准则？ 注：具体要求参考 GB/T 34590.6—2022 中的表 1。

附录 A 提供了针对软件开发环境开展审核及评估的说明及示例。

6 软件安全要求

6.1 目标

本章的目标是对软件安全需求规范、细化的软硬件接口规范的相关工作成果进行审核及评估，以提供证据证明：
a） 定义或细化了由技术安全概念和系统架构设计规范导出的软件安全要求；
b） 定义了软件实现所需的安全相关功能和特性；

c) 细化了在 GB/T 34590.4—2022 第 6 章最初定义的软硬件接口要求；
d) 验证了软件安全要求和软硬件接口要求是否适用于软件开发，并验证了它们与技术安全概念和系统架构设计规范的一致性。

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：
——软件安全需求规范；
——软硬件接口规范（细化的）；
——软件安全需求规范的验证报告。

注：为支持软件安全需求规范、细化的软硬件接口规范的审核及评估，可能需要提供如下支持材料：
——技术安全需求规范；
——技术安全概念；
——系统架构设计规范；
——软硬件接口规范；
——软件开发环境文档。

6.3 审核及评估的要求

对于软件安全需求规范的审核及评估，应涵盖表 2 的检查项。

表 2 软件安全需求规范的审核及评估检查清单

序号	检查清单
1	软件安全要求的得出是否基于安全相关的软件功能和特性？如果嵌入式软件除了执行 GB/T 34590.6—2022 中 6.4.1 定义的安全要求的功能外，还执行了其他功能，是否按照所应用的质量管理体系的要求提供了这些功能及其特性的规范？
2	软件安全要求的得出是否继承于技术安全要求、技术安全概念和系统架构设计规范？软件安全要求的得出是否包含如下内容： a) 安全要求的定义和管理，按照 GB/T 34590.8—2022 第 6 章； b) 已定义的系统和硬件的配置； c) 软硬件接口规范； d) 硬件设计规范的相关要求； e) 时间约束； f) 外部接口； g) 对软件有影响的车辆、系统或者硬件的每个运行模式及运行模式之间的转换
3	若对软件安全要求进行了 ASIL 等级分解，其分解原则是否满足 GB/T 34590.9—2022 第 5 章的要求？
4	软硬件接口规范在软件开发阶段是否进行了细化？细化程度是否足以支持软件正确控制使用硬件？
5	软硬件接口规范是否描述了硬件和软件间每个与安全相关的依赖性？
6	是否建立了软件安全要求与技术安全要求、技术安全概念和系统架构设计规范之间的双向追溯性？
7	是否细化后的软硬件接口都定义了对应的验证准则？
8	是否为每个软件安全要求制定了验证准则？
9	是否基于 GB/T 34590.8—2022 第 6 章和第 9 章执行了软件安全要求、细化后的软硬件接口规范的验证？其验证结果是否能证明如下要求得到了满足？ a) 软件开发的适用性； b) 与技术安全要求的一致性和符合性； c) 与系统设计的符合性； d) 与软硬件接口的一致性

附录 B 提供了针对软件安全需求规范开展审核及评估的说明及示例。

7 软件架构设计规范

7.1 目标

本章的目标是对软件架构设计规范的相关工作成果进行审核及评估，以提供证据证明：

a) 开发了满足软件安全要求和其他软件要求的软件架构设计；
b) 验证了软件架构设计满足所分配的 ASIL 等级的软件安全要求；
c) 软件架构设计支持软件的实现与验证。

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：

——软件架构设计规范；
——安全分析报告；
——相关失效分析报告；
——软件架构设计的验证报告。

注：为支持软件架构设计规范的审核及评估，可能需要提供如下支持材料：

——软件安全需求规范；
——软硬件接口规范(细化的)。

7.3 审核及评估的要求

对于软件架构设计规范的审核及评估，应涵盖表 3 的检查项。

表 3 软件架构设计规范的审核及评估检查清单

序号	检查清单
1	是否按照 ASIL 等级要求定义软件架构的设计标记方法，且满足 GB/T 34590.6—2022 中表 2 的要求？
2	软件架构设计的描述是否满足如下特征？ a) 可理解性； b) 一致性； c) 简单性； d) 可验证性； e) 模块化； f) 抽象性； g) 封装性； h) 可维护性
3	软件架构设计的开发是否满足如下要求： a) 软件架构设计的可验证性； b) 可配置软件的适用性； c) 软件单元设计与实现的可行性； d) 软件集成测试中软件架构的可测试性； e) 软件架构设计的可维护性
4	是否定义软件架构设计的原则，且满足 GB/T 34590.6—2022 中表 3 的要求？
5	软件架构设计是否被开发到可识别软件单元的程度，且分配了相应的软件安全要求到软件单元？每个软件单元是否按照分配给它的最高 ASIL 等级进行的开发？
6	软件架构设计规范是否包含了静态设计和动态设计？
7	如果架构设计中复用了一个不满足功能安全开发的软件架构要素，是否对该软件架构要素进行了组件鉴定并满足 GB/T 34590.8—2022 第 12 章的要求？

表 3　软件架构设计规范的审核及评估检查清单（续）

序号	检查清单
8	如果架构设计要素被分配了不同的 ASIL 等级，该软件架构要素是否符合 GB/T 34590.9—2022 第 6 章定义的共存准则或按照了最高 ASIL 等级要求进行了开发？
9	软件架构设计如进行了软件分区，是否实现了软件组件间免于干扰且确保满足如下要求？ a）　共享资源的使用方式应确保软件分区免于干扰； b）　专用的硬件特性或等效方法可支持软件分区（该要求适用于 ASIL D）； c）　实现软件分区的软件要素是根据分配给分区软件任何要求的最高 ASIL 等级开发的； d）　软件分区有效性的证据会在软件集成和验证期间生成（按照 GB/T 34590.6—2022 第 10 章的要求）
10	是否对软件架构进行了安全分析？安全分析的结果是否满足如下要求： a）　提供软件的适用性证据证明具备了相应的 ASIL 等级要求所需的特定的安全相关的功能和特性； b）　识别或确认软件的安全相关部分； c）　支持安全措施的定义并验证其有效性
11	如果软件安全要求的实现依赖于软件组件间免于干扰或足够的独立性，检查是否按照 GB/T 34590.9—2022 第 7 章进行了相关失效及其影响分析？
12	基于软件架构的安全分析结果，错误检测和错误处理的安全机制是否嵌入到软件架构设计中？
13	是否对嵌入式软件所需资源进行了上限预估，包括： a）　执行时间； b）　存储空间； c）　通信资源
14	是否基于 GB/T 34590.8—2022 第 9 章执行了软件架构设计的验证？软件架构设计的验证方法是否按照 GB/T 34590.6—2022 中表 4 的要求进行，为下列目标提供证据？ a）　软件架构设计应满足对应 ASIL 等级的软件安全要求； b）　软件架构设计的评审或审核能够为满足对应 ASIL 等级的软件安全要求提供证据； c）　与目标环境的兼容性； d）　与设计指南保持一致

附录 C 提供了针对软件架构设计规范开展审核及评估的说明及示例。

8　软件单元设计及实现

8.1　目标

本章的目标是对软件单元设计和软件实现的相关工作成果进行审核及评估，以提供证据证明：

a）　软件单元设计和实现满足了所分配的所有软件安全要求；
b）　软件源代码实现了软件详细设计规范；
c）　软件单元设计实现了软硬件接口规范；
d）　软件单元设计有充分的资源支持功能和特性，避免非预期的功能和特征；
e）　软件单元设计实现了安全分析中得出的安全措施。

8.2　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：

——软件单元设计规范；
——软件单元实现。

8.3　审核及评估的要求

对于软件单元设计及实现的审核及评估，应涵盖表 4 的检查项。

表 4　软件单元设计及实现的审核及评估检查清单

序号	检查清单
1	软件单元设计是否与软件安全要求和软件架构设计保持了一致性和追溯性？
2	软件单元设计是否符合软硬件接口规范(如果适用)？
3	软件单元设计的标记方法是否使用了 GB/T 34590.6—2022 中表 5 要求的对应 ASIL 等级推荐的标记方法？
4	软件单元的定义是否将功能表现和内部设计描述到必要的细节程度以支持其实现？
5	软件单元设计和实现的设计是否满足了以下原则： a)　基于软件架构设计，软件单元内的子程序和函数执行的正确次序； b)　软件单元间接口的一致性； c)　软件单元内和软件单元间的数据流及控制流的正确性； d)　简单性； e)　可读性和可理解性； f)　鲁棒性； g)　软件修改的适宜性； h)　可测性
6	软件单元设计是否符合 GB/T 34590.6—2022 中表 6 要求的对应 ASIL 等级推荐的设计原则？

附录 D 提供了针对软件单元设计及实现开展审核及评估的说明及示例。

9　软件单元验证

9.1　目标

本章的目标是对软件单元验证规范、单元验证报告的相关工作成果进行审核及评估，以提供证据证明：

a)　软件单元设计满足分配的软件要求且适合于实施；

b)　由软件单元模块、函数层面的相关失效分析和安全分析得出的已定义的安全措施得到适当实施；

c)　软件单元、函数符合软件单元设计与根据所需的 ASIL 等级分配的软件安全要求；

d)　单元不包含与功能安全相关的非预期功能和特性。

9.2　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：

——软硬件接口规范；

——软件单元验证计划；

——软件验证规范；

——安全计划；

——嵌入式软件；

——软件单元设计规范；

——软件单元实现；

——软件单元验证报告。

注：为支持软件单元验证规范的审核及评估，可能需要提供如下支持材料：

——工具应用指南。

9.3　审核及评估的要求

对于软件单元验证的审核及评估，应涵盖表 5 的检查项。

表 5　软件单元验证的审核及评估检查清单

序号	检查清单
1	是否基于 GB/T 34590.6—2022 第 9 章要求，定义了软件单元验证的方法和策略？
2	是否按照 GB/T 34590.6—2022 中表 7 的要求确定了单元验证方法的合理组合？选择的单元验证方法组合是否与单元设计与实现中的 ASIL 定义保持一致？选择的软件单元验证方法是否与标准推荐 ASIL 保持一致？未使用及不适用的方法是否提供了合理理由？
3	是否按照 GB/T 34590.6—2022 中表 8 的要求得到单元测试用例？选择的单元测试用例开发方法是否与软件单元设计与实现(软件详细设计)中的 ASIL 定义保持一致？
4	是否按照 GB/T 34590.6—2022 中表 9 的要求确定了软件单元验证的结构覆盖率？软件单元验证的结构覆盖率是否与单元设计与实现中的 ASIL 定义保持一致？软件单元验证结构覆盖率是否与标准推荐 ASIL 保持一致？测试结果是否能够提供证据说明单元验证活动满足已定义的软件单元设计及实现(软件详细设计)层级的结构覆盖度？
5	是否按要求对软件单元验证过程中所有的缺陷进行了管理，并跟踪至关闭？
6	是否对通过软件单元验证的软件范围进行了分析，其是否包含定义的功能和性能？对于未定义的功能，是否评估了风险或执行了解决措施？
7	是否对软件单元验证环境进行了分析？如果软件单元环境与目标环境不一致，是否给出了对应措施？
8	是否按照 GB/T 34590.8—2022 第 9 章要求，对已制定的单元验证计划进行了验证？验证中发现的问题是否均已关闭？未关闭的问题是否明确了对应措施，并符合测试结束准则？

附录 E 提供了针对软件单元验证开展审核及评估的说明及示例。

10　软件集成和验证

10.1　目标

本章的目标是对软件验证规范、嵌入式软件和软件验证报告的相关工作成果进行审核及评估，以提供证据证明：

——定义集成步骤并集成软件要素，直至嵌入式软件完全集成；

——由软件架构层面的安全分析得出的已定义的安全措施得到适当实施；

——集成的软件单元和集成的软件组件符合软件架构设计的要求；

——集成软件不包含与功能安全相关的非预期功能和特性。

10.2　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：

——软件验证规范(细化的)；

——嵌入式软件；

——软件验证报告(细化的)。

注：为支持软件验证规范、嵌入式软件和软件验证报告的审核及评估，可能需要提供如下支持材料：

——软硬件接口规范(细化的)；

——软件架构设计规范；

——安全分析报告；

——相关失效分析报告；

——软件单元实现；

——配置数据；

——标定数据；

——软件开发环境文档；

——软件验证规范；
——经鉴定合格的软件组件。

10.3 审核及评估的要求

对于软件集成和验证的审核及评估，应涵盖表 6 的检查项。

表 6 软件集成和验证的审核及评估检查清单

序号	检查清单
1	是否基于 GB/T 34590.6—2022 第 10 章的要求，定义了软件集成及验证的方法和策略？
2	是否按照 GB/T 34590.6—2022 第 10 章的要求，通过表 10 软件集成验证方法确定了软件集成验证方法的合理组合？
3	针对已选择的软件集成及验证方法，是否有相关内容说明相应的软件集成及验证活动执行符合要求？
4	是否按照 GB/T 34590.6—2022 中表 11 软件集成测试用例的得出方法，要求开发了软件集成测试用例？
5	是否按照 GB/T 34590.6—2022 第 10 章的要求确定了测试用例在软件架构层级的需求覆盖率和结构覆盖率(包括函数覆盖率和调用覆盖率)？结构覆盖率是否满足 GB/T 34590.6—2022 中表 12 的要求[适用性：本要求适用于 ASIL(A)、(B)、C 和 D 等级]？
6	是否建立了软件集成测试用例和软件架构及软件安全要求的追溯关系？是否对软件集成及验证的软件范围进行了验证，其是否包含全部定义的功能和性能？对于未定义的功能，是否评估了风险或执行了解决措施？
7	是否对软件集成测试及验证环境进行了分析？如果软件集成测试及验证环境与目标环境不一致，是否进行分析并给出了对应措施？
8	软件集成及验证是否实施完成？集成及验证中发现的问题是否已关闭？未关闭的问题是否明确了对应措施，并符合测试结束准则？

附录 F 提供了针对软件集成和验证开展审核及评估的说明及示例。

11 嵌入式软件测试

11.1 目标

本章的目标是对软件验证规范和软件验证报告的相关工作成果进行审核及评估，以提供证据证明嵌入式软件：

a) 在目标环境执行时满足安全相关要求；
b) 不包含与功能安全相关的非预期功能和特性。

11.2 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：
——软件验证规范(细化的)；
——软件验证报告(细化的)。

注：为支持软件验证规范和软件验证报告的审核及评估，可能需要提供如下支持材料：
——软件架构设计规范；
——软件安全需求规范；
——嵌入式软件；
——标定数据；
——软件开发环境文档；
——技术安全概念；
——系统架构设计规范；
——集成和测试策略；

——集成和测试报告。

11.3 审核及评估的要求

对于嵌入式软件测试的审核及评估，应涵盖表 7 的检查项。

表 7 嵌入式软件测试的审核及评估检查清单

序号	检查清单
1	是否基于 GB/T 34590.6—2022 第 11 章的要求，制定了嵌入式软件测试策略？
2	是否按照 GB/T 34590.6—2022 中表 13 用于执行软件测试的测试环境要求，确定了嵌入式软件测试的测试环境？
3	是否按照 GB/T 34590.6—2022 中表 14 嵌入式软件的测试方法要求，确定了嵌入式软件测试方法的合理组合？
4	针对已选择的嵌入式软件测试方法，是否有相关内容说明相应的嵌入式软件测试活动执行符合要求？
5	是否按照 GB/T 34590.6—2022 中表 15 嵌入式软件测试用例的得出方法要求，开发了嵌入式软件测试用例？
6	嵌入式软件测试是否实施完成？测试中发现的问题是否均已关闭？未关闭的问题是否明确了对应措施，并符合测试结束准则？
7	是否建立了软件安全要求与嵌入式软件测试用例间的追溯关系？是否对嵌入式软件测试的测试结果及覆盖率进行了评估？

附录 G 提供了针对嵌入式软件测试开展审核及评估的说明及示例。

12 软件标定和配置管理

12.1 目标

本章的目标是对软件配置，包括配置数据规范、标定数据规范、配置数据、标定数据、验证规范、验证报告、软件架构设计规范和软件开发环境的相关工作成果进行审核及评估，以提供证据证明：

a) 软件配置满足不同应用的软件行为变化的可控性；

b) 配置数据和标定数据满足所需的 ASIL 等级要求；

c) 专用嵌入式软件及其标定数据的成熟度满足生产发布。

12.2 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：

——配置数据规范；

——标定数据规范；

——配置数据；

——标定数据；

——验证规范(细化的)；

——验证报告(细化的)；

——软件架构设计规范(细化的)；

——软件开发环境文档(细化的)。

注：为了开展软件标定和配置的审核及评估，可能需要提供如下支持材料：

——软件配置的相关阶段中的适用的支持信息。

12.3 审核及评估的要求

对于软件标定和配置管理的审核及评估，应涵盖表 8 的检查项。

表 8　软件标定和配置管理的审核及评估检查清单

序号	检查清单
1	是否对配置数据进行了定义？ a)　配置数据的有效值； b)　配置数据的目的和用法； c)　范围、比例、单位； d)　配置数据不同要素之间的相互依赖
2	配置数据及其规范是否能够提供证据证明以下内容？ a)　配置数据符合软件架构设计规范； b)　配置数据符合软件单元设计规范； c)　配置数据使用的值在其规定的范围内； d)　配置数据与其他配置数据的兼容性
3	是否规定了配置数据的 ASIL 等级应等于应用于该数据的可配置软件的最高 ASIL 等级？
4	是否按照 GB/T 34590.8—2022 第 9 章定义了对相关项开发中要使用的配置数据集对可配置软件的验证？
5	是否按照以下组合执行了可配置软件的验证？ a)　可配置软件的验证； b)　配置数据的验证； c)　已配置软件的验证
6	是否定义了与软件组件关联的标定数据以确保配置后软件的正确运行和预期性能？ a)　标定数据的有效值； b)　标定数据的目的和用法； c)　范围、比例和单位，以及它们对运行状态的依赖(如果适用)； d)　不同标定数据之间已知的相互依赖； e)　配置数据和标定数据之间的已知的相互依赖
7	是否规定了标定数据的 ASIL 等级应等于其可能违反的软件安全要求的最高 ASIL 等级？
8	是否按照 GB/T 34590.8—2022 第 9 章定义并正确完成标定数据验证？ a)　定义的标定数据合适并符合软件安全要求； b)　定义的标定数据符合软件架构设计规范； c)　定义的标定数据符合软件单元设计规范； d)　定义的标定数据与其他定义的标定数据是一致且兼容的
9	是否按照 GB/T 34590.8—2022 第 9 章定义并正确完成生产发布的标定数据的验证？ a)　发布的标定数据符合其规范； b)　嵌入式软件的已标定的、应用特定的变体提供了定义的安全相关功能和特性
10	是否定义并应用了数据非预期变化的探测机制？ **注**：具体要求参考 GB/T 34590.6—2022 中的表 C.1。
11	是否定义并应用了标定数据应遵循的流程、生成标定数据的工具和验证标定数据的流程？
12	软件开发环境文档中是否针对软件配置的更新细化内容？

附录 H 提供了针对软件标定和配置管理开展审核及评估的说明及示例。

13　软件组件鉴定

13.1　目标

本章的目标是对软件组件鉴定定义、软件组件鉴定报告、软件组件鉴定的验证报告的相关工作成果进行审核及评估，以提供证据，证明在符合 GB/T 34590.1～34590.12—2022 开发的相关项中对软件组件的重复使用是合适的。

13.2　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：

——软件组件；
——软件组件的文档；
——软件组件鉴定报告；
——软件组件鉴定的验证报告。

注：为支持软件组件的文档、软件组件鉴定报告和软件组件鉴定的验证报告的审核及评估，可能需要提供如下支持材料：
——安全计划；
——组织专门的功能安全规章和流程；
——对软件组件的要求；
——软件组件的设计规范；
——先前对软件组件采用的验证措施的结果。

13.3 审核及评估的要求

对于软件组件鉴定的审核及评估，应涵盖表 9 的检查项。

表 9 软件组件鉴定的审核及评估检查清单

序号	检查清单
1	安全计划中是否由于软件组件鉴定而按照 GB/T 34590.2—2022 中 6.4.5.1 对某一安全活动进行了剪裁？若有，剪裁是否满足 GB/T 34590.8—2022 第 12 章的要求？
2	软件组件的软件开发过程是否基于适当的国家或国际标准？
3	软件组件的文档是否按 GB/T 34590.8—2022 中 12.4.2.1 软件组件鉴定定义的要求得出？
4	软件组件鉴定的定义是否包括了软件组件的唯一识别？
5	软件组件鉴定的定义是否包含当软件组件错误执行时，可能违背的所有安全要求的最高 ASIL 等级？
6	软件组件鉴定的定义是否包括了为鉴定软件组件所应执行的活动？
7	软件组件鉴定的定义是否包含以下要求？ ——软件组件的要求； ——软件组件预期用途的要求； ——配置描述； ——所需接口、供给接口、共享资源描述（如果适用）； ——软件组件集成的描述； ——异常运行条件下的功能反应； ——对已知异常及相应应急措施的描述
8	是否提供了软件组件的鉴定报告，以证明组件的开发过程符合标准的证据，并记录了论证结果？
9	软件组件鉴定报告是否提供了软件组件的验证结果，以证明符合以下要求，并记录了论证结果？ ——分配给软件组件的要求的测试覆盖率应满足 GB/T 34590.6—2022 第 9 章； ——满足测试用例完整性要求（ASIL D 适用），结构覆盖率应按照 GB/T 34590.6—2022 第 9 章来测量； ——既覆盖正常运行条件，也覆盖失效情况下的表现； ——没有导致违背安全要求的已知错误； ——验证结果仅对软件组件未经改变的实现有效
10	对软件组件的鉴定记录中是否包含下述信息： a) 软件组件的唯一识别； b) 软件组件的唯一配置； c) 执行鉴定的人员或组织； d) 用于鉴定的环境； e) 用于鉴定软件组件的验证措施的结果； f) 分配给软件组件的安全要求的最高 ASIL 等级
11	是否按照 GB/T 34590.8—2022 第 9 章的要求验证了软件组件的鉴定结果，以证明是否对软件组件资质评估结果进行验证？

附录 I 提供了针对软件组件鉴定开展审核及评估的说明及示例。

附 录 A
（资料性）
软件开发环境

软件开发环境的审核及评估的说明及示例见表 A.1。

表 A.1 软件开发环境的审核及评估的说明及示例

序号	检查清单	说明及示例
1	在开发相关项时，使用的软件开发过程和软件开发环境是否适用并满足该相关项要求？ a) 适用于开发安全相关的嵌入式软件，包括方法、指南、语言和工具； b) 软件阶段及相关阶段的工作成果的一致性； c) 与系统和硬件开发阶段在所需的交互和信息交换的一致性	a) 开发软件代码时参考的编码指南，如 MISRA C； b) 软件开发时用到的编程语言，如模型、C 语言； c) 在软件开发过程中用到的软件工具，如编译工具、建模工具等； d) 需要体现软件阶段各子阶段的对应的流程及工作成果描述； e) 描述相关项软件开发的阶段、任务和活动的排序，包括迭代步骤，和硬件/系统层面产品开发保持一致
2	在开发相关项时，所应用的设计语言、建模语言或编程语言是否满足以下准则？ a) 明确易理解的定义； b) 如果建模用于需求工程和管理，定义和管理安全要求的适用性； c) 支持模块化、抽象化和封装化的实现； d) 支持结构化构造的使用	a) 所选择语言的语法和语义定义明确，或对开发环境配置的限制。 b) 选择语言需要考虑相应准则，如某软件模型语言支持模块化、抽象化和封装化；汇编语言能用于那些不适合使用高级编程语言的软件部分，如与硬件接口的底层软件、中断处理程序、或对时间敏感的算法
3	建模和编码指南是否满足对应的 ASIL 等级所要求的通则，以涵盖适合于建模、设计或者编程语言的准则？ **注**：具体要求参考 GB/T 34590.6—2022 中的表 1。	检查建模、设计或者编程语言的指南，按照不同 ASIL 等级需要考虑如下准则： a) 强制低复杂度； b) 语言子集的使用； **示例 1**：规定函数的行数限制、圈复杂度限制等。 c) 强制强类型； **示例 2**：避免容易导致错误的语言结构，如递归调用等。 d) 防御性实施技术的使用； **示例 3**：除法运算前检查除数不为 0 等。 e) 使用值得信赖的设计原则； **示例 4**：避免使用全局变量等。 f) 使用无歧义的图形表示； g) 风格指南的使用； h) 命名惯例的使用； i) 并发方面 **示例 5**：规定同时进行的任务数限制等。

附 录 B
（资料性）
软件安全要求

软件安全要求的审核及评估的说明及示例见表 B.1。

表 B.1 软件安全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	软件安全要求的得出是否基于安全相关的软件功能和特性？如果嵌入式软件除了执行 GB/T 34590.6—2022 中 6.4.1 定义的安全要求的功能外，还执行了其他功能，是否按照所应用的质量管理体系的要求提供了这些功能及其特性的规范？	应对软件功能和特殊特性进行失效分析，软件安全要求应基于软件安全功能进行定义 **示例 1**：软件安全功能可为与安全相关硬件要素故障探测、指示和减轻相关的功能（检测 EPS 电机驱动电路故障并进行安全响应）。 **示例 2**：安全的特殊特性包括对错误输入的鲁棒性、不同功能之间的独立性或免于干扰、或软件的容错能力。
2	软件安全要求的得出是否继承于技术安全要求、技术安全概念和系统架构设计规范？软件安全要求的得出是否包含如下内容： a) 安全要求的定义和管理，按照 GB/T 34590.8—2022 第 6 章； b) 已定义的系统和硬件的配置； c) 软硬件接口规范； d) 硬件设计规范的相关要求； e) 时间约束； f) 外部接口； g) 对软件有影响的车辆、系统或者硬件的每个运行模式及运行模式之间的转换	a) 检查软件安全要求和技术安全要求、技术安全概念和系统架构设计规范之间的追溯性和一致性； b) 检查软件安全要求的属性应包括：每条要求都有唯一标识、ASIL 等级及状态； c) 检查不同 ASIL 等级的软件安全要求的描述方法是否符合 GB/T 34590.8—2022 中表 1 的要求（ASIL C/D 应选择半形式记法）： **示例 1**：配置参数，可考虑增益控制、带通频率和时钟分频。 **示例 2**：时间约束，软件功能执行或响应时间应满足技术安全要求定义的 FTTI。 **示例 3**：运行模式可包括初始化、正常运行、降级、休眠和用于测试的其他高级模式。 **示例 4**：外部接口，如通信接口、用于测试的缺陷口。
3	若对软件安全要求进行了 ASIL 等级分解，其分解原则是否满足 GB/T 34590.9—2022 第 5 章的要求？	检查 ASIL 等级分解的正确性应符合 GB/T 34590.9—2022 第 5 章的要求 **示例**：见 GB/T 34590.9—2022 附录 B。
4	软硬件接口规范是否进行了细化，细化程度是否足以支持软件正确控制使用硬件？	检查软硬件接口规范的细化程度，应描述支持软件正确控制使用硬件
5	软硬件接口规范是否描述了硬件和软件间每个与安全相关的依赖性？	检查细化后的软硬件接口规范中对硬件和软件间每个与安全相关的依赖性的描述
6	是否建立了软件安全要求与技术安全要求、技术安全概念和系统架构设计规范之间的双向追溯性？	检查软件安全要求和与技术安全要求、技术安全概念和系统架构设计规范之间的双向追溯性
7	是否细化后的软硬件接口都定义了对应的验证准则？	检查细化后的每条软硬件接口规范的验证准则，验证的方式可为检查、仿真分析、测试等。 细化后的软硬件接口的验证由负责系统开发、硬件开发和软件开发的人员共同完成
8	是否为每个软件安全要求制定了验证准则？	检查每条软件安全要求的验证准则，验证的方式可为检查、仿真分析、测试等
9	是否基于 GB/T 34590.8—2022 第 6 章和第 9 章执行了软件安全要求、细化后的软硬件接口规范的验证？其验证结果是否能证明如下要求得到了满足？ a) 软件开发的适用性； b) 与技术安全要求的一致性和符合性； c) 与系统设计的符合性； d) 与软硬件接口的一致性	检查软件安全要求的验证方法，不同安全等级等级的要求验证方法应按照 GB/T 34590.8—2022 中的表 2 进行选择，并给理由。软件安全要求的验证应满足 GB/T 34590.8—2022 第 6 章和第 9 章的要求 **示例 1**：半形式化验证可通过 FMEA/DFA 的形式分析安全机制的完整性。 **示例 2**：检查可通过会议、软件安全要求检查单等检查软件安全要求。

附 录 C
（资料性）
软件架构设计规范

软件架构设计规范的审核及评估的说明及示例见表 C.1。

表 C.1 软件架构设计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	是否按照 ASIL 等级要求定义软件架构的设计标记方法，且满足 GB/T 34590.6—2022 中表 2 的要求？	软件架构设计的标记法根据不同的 ASIL 等级进行选择，需满足 GB/T 34590.6—2022 中表 2 的要求，对于 ASIL A/ASIL B 的应使用非形式记法和自然语言结合的描述方式，对于 ASIL C/ASIL D 的，应使用半形式记法和自然语言结合的描述方法 **示例 1**：半形式记法可使用 UML、SysML、软件建模语言。 **示例 2**：非形式记法：图片、图表。
2	所选择软件架构设计标记方法是否支持软件架构设计的描述满足如下特征： a） 可理解性； b） 一致性； c） 简单性； d） 可验证性； e） 模块化； f） 抽象性； g） 封装性； h） 可维护性	检查软件架构设计规范的描述应可理解、简单可维护、可验证、模块化设计、一致性、抽象性及封装性
3	软件架构设计的开发是否满足如下要求： a） 软件架构设计的可验证性； b） 可配置软件的适用性； c） 软件单元设计与实现的可行性； d） 软件集成测试中软件架构的可测试性； e） 软件架构设计的可维护性	检查软件架构设计应和软件安全要求之间建立双向追溯性，且软件架构设计是可实现及可验证的
4	是否定义软件架构设计的原则，且满足 GB/T 34590.6—2022 中表 3 的要求？	a） 检查定义的软件架构设计原则，满足 GB/T 34590.6—2022 中表 3 针对不同安全等级的要求； b） 若未满足 GB/T 34590.6—2022 中表 3 要求的软件架构设计的原则，应给出合理的理由 **示例 1**：限制组件的规模和复杂度：可限制函数的规模。 **示例 2**：限制接口规模：可限制函数参数变量的个数，可限制返回出口的数量。 **示例 3**：软件组件的适当空间隔离：MPU 分区。
5	软件架构设计是否被开发到可识别软件单元的程度，且分配了相应的软件安全要求到软件单元？每个软件单元是否按照分配给它的最高 ASIL 等级进行的开发？	检查软件安全要求和软件单元之间的双向追溯性； 检查软件单元的安全等级应继承所分配给其软件安全要求中的最高安全等级
6	软件架构设计规范是否包含了静态设计和动态设计？	检查软件架构的静态设计和动态设计内容 **示例 1**：静态设计可包括： a） 分层次的软件结构； b） 数据类型和它们的特征参数； c） 软件组件的外部接口； d） 嵌入式软件的外部接口； e） 全局变量； f） 约束。 **示例 2**：动态设计可包括： a） 事件和行为的功能链； b） 数据处理的逻辑顺序； c） 控制流和并发流程； d） 通过接口和全局变量传递的数据流； e） 时间的限制； f） 运行状态及其跳转

表 C.1 软件架构设计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
7	如果架构设计中复用了一个不满足功能安全开发的软件架构要素，是否对该软件架构要素进行了组件鉴定并满足 GB/T 34590.8—2022 第 12 章的要求？	复用不满足安全等级要求开发的软件架构要素时应进行软件组件鉴定且满足 GB/T 34590.8—2022 第 12 章的要求
8	如果嵌入式软件不得不实现不同 ASIL 等级的软件组件，或实现安全相关或非安全相关的软件组件，软件组件是否符合 GB/T 34590.9—2022 第 6 章定义的共存准则或按照了最高 ASIL 等级要求进行了开发？	检查不同安全等级的软件组件之间的共存原则 **示例**：不同安全等级的软件组件共存条件可为： a) 分解的组件之间没有功能依赖性； b) 安全相关的元素不受干扰。
9	软件架构设计如进行了软件分区，是否实现了软件组件间免于干扰且确保满足如下要求？ a) 共享资源的使用方式应确保软件分区免于干扰； b) 专用的硬件特性或等效方法可支持软件分区（该要求适用于 ASLL D）； c) 实现软件分区的软件要素是根据分配给分区软件任何要求的最高 ASIL 等级开发的； d) 软件分区有效性的证据会在软件集成和验证期间生成（按照 GB/T 34590.6—2022 第 10 章的要求）	检查软件分区设计的原则，应保证软件组件之间免于干扰 **示例 1**：一个软件分区不能改变其他软件分区的代码或数据。 **示例 2**：存储器保护单元等硬件特性。 **示例 3**：软件分区应按照分区内组件的最高 ASIL 等级进行开发。 **示例 4**：软件集成测试应提供软件分区有效性的证据。 **示例 5**：见 GB/T 34590.6—2022 附录 D。
10	是否对软件架构进行了安全分析？安全分析的结果是否满足如下要求： a) 提供软件的适用性证据证明具备了相应的 ASIL 等级要求所需的特定的安全相关的功能和特性； b) 识别或确认软件的安全相关部分； c) 支持安全措施的定义并验证其有效性	检查软件架构的安全分析报告，并检查安全分析结果满足该检查点所列的要求 **示例**：见 GB/T 34590.6—2022 附录 E。
11	如果软件安全要求的实现依赖于软件组件间免于干扰或足够的独立性，检查是否按照 GB/T 34590.9—2022 第 7 章进行了相关失效及其影响分析？	如果软件安全要求的实现依赖于软件组件间免于干扰或足够的独立性，应检查相关性安全分析，且分析结果应满足该检查点所列的要求 **示例**：见 GB/T 34590.6—2022 附录 E。
12	基于软件架构的安全分析结果，错误检测和错误处理的安全机制是否嵌入到软件架构设计中？	检查安全分析的结果应在软件架构设计中进行体现，软件架构设计中应包含错误探测和错误处理的安全机制 **示例 1**：用于错误探测的安全机制可能包括： a) 输入输出数据的范围检查； b) 合理性检查； c) 数据错误探测； d) 外部要素监控程序执行； e) 程序执行的时间监控； f) 设计中的异构冗余； g) 在软件或硬件中实施的访问冲突控制机制，与授权访问或拒绝访问安全相关共享资源有关。 **示例 2**：用于错误处理的安全机制可能包括： a) 为了达到或维持安全状态的功能； b) 静态恢复机制； c) 通过划分功能的优先级进行平稳降级，从而最小化潜在失效对功能安全的影响； d) 设计中的同构冗余，主要侧重于控制运行相似软件的硬件中瞬态故障或随机硬件故障的影响； e) 设计中的异构冗余，意味着在每个并行路径中使用不同的软件，主要侧重于预防或控制软件中的系统性故障； f) 数据纠错码； g) 在软件或硬件中实施的访问许可管理，与授权访问或拒绝访问安全相关共享资源有关。

表 C.1　软件架构设计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
13	是否对嵌入式软件所需资源进行了上限预估，包括： a）　执行时间； b）　存储空间； c）　通信资源	检查软件的所需资源上限预估策略 **示例 1**：评估存储堆和栈的 RAM 及存储程序和非易失性数据的 ROM 资源占用上限。 **示例 2**：评估程序运行的最长时间。 **示例 3**：评估通信的负载率。
14	是否基于 GB/T 34590.8—2022 第 9 章执行了软件架构设计的验证？软件架构设计的验证方法是否按照 GB/T 34590.6—2022 中表 4 的要求进行，为下列目标提供证据： a）　软件架构设计应满足对应 ASIL 等级的软件安全要求； b）　软件架构设计的评审或审核能够为满足对应 ASIL 等级的软件安全要求提供证据； c）　与目标环境的兼容性； d）　与设计指南保持一致	a）　检查软件架构设计的验证应满足 GB/T 34590.8—2022 第 9 章的要求； b）　检查软件架构设计的验证方法应满足 GB/T 34590.6—2022 中表 4 对不同的 ASIL 等级的要求； c）　检查软件架构设计的验证结果满足本审核点所列出的要求

附 录 D
（资料性）
软件单元设计及实现

软件单元设计及实现的审核及评估的说明及示例见表 D.1。

表 D.1 软件单元设计及实现的审核及评估的说明及示例

序号	检查清单	说明及示例
1	软件单元设计是否与软件安全要求和软件架构设计保持了一致性和追溯性？	软件需求的 ID 被相关的软件单元承接，软件单元设计是具体的软件架构模块的分解和细化。相关追溯关系可通过需求管理工具、架构设计工具和软件模型进行了链接，也可建立手工追溯表格等形式进行
2	软件单元设计是否符合软硬件接口规范（如果适用）	如适用，应检查软件单元设计和细化后的软硬件接口规范的符合性
3	软件单元设计的标记方法是否使用了 GB/T 34590.6—2022 中表 5 要求的对应 ASIL 等级推荐的标记方法？	软件单元设计使用了软件建模等工具开展，并且有规范的设计原则和命名规则等确保了软件单元设计满足半形式的标记方法
4	软件单元的定义是否将功能表现和内部设计描述到必要的细节程度以支持其实现？	软件单元设计使用了软件建模等工具开展，以支持后续 C-code 的实现
5	软件单元设计和实现的设计是否满足了以下原则： a） 基于软件架构设计，软件单元内的子程序和函数执行的正确次序； b） 软件单元间接口的一致性； c） 软件单元内和软件单元间的数据流及控制流的正确性； d） 简单性； e） 可读性和可理解性； f） 鲁棒性。 g） 软件修改的适宜性； h） 可测性	软件单元设计基于软件架构设计，检查软件单元设计满足如下原则： a） 软件单元内的子程序和函数执行次序正确； b） 软件单元间接口满足一致性要求； c） 软件单元内和软件单元间的数据流及控制流的正确性； d） 简单性、可读性和可理解性、鲁棒性、可测性 **示例 1**：GB/T 34590.6—2022 中 8.4.5 的相关单元设计的原则定义在软件开发相关指南文件中，本项目对应的软件单元存放在数据库中，满足了软件开发相关指南中定义的单元设计的原则。 **示例 2**：函数体对应（一入口，一出口）。符合 MISRA C 编程规范，可借助静态测试检查编程原则。
6	软件单元设计是否符合 GB/T 34590.6—2022 中表 6 要求的对应 ASIL 等级推荐的设计原则？	GB/T 34590.6—2022 中 8.4.5 的相关单元设计的要求和方法定义在软件开发相关指南文件中，本项目对应的软件单元存放在数据库中，满足软件开发相关指南中定义的单元设计的要求和方法，以满足后续 C-code 的实现： a） 子程序和函数采用一个入口和一个出口； b） 无动态对象或动态变量，例如，符合 MISRA C 编程规范即可； c） 变量初始化；例如，符合 MISRA C 编程规范即可，通过测试工具进行检测变量是否初始化； d） 不能重复使用变量名称等

附 录 E
（资料性）
软件单元验证

软件单元验证的审核及评估的说明及示例见表 E.1。

表 E.1 软件单元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	是否基于 GB/T 34590.6—2022 第 9 章要求，定义了软件单元验证的方法和策略？	a) 检查软件测试对象，软件单元划分，确认软件单元设计满足分配的软件要求，软件单元验证验证了软件详细设计。 b) 检查软件测试计划评审记录，是否使用审查的评审方法，评审问题是否形成闭环？ c) 检查软件单元验证层级的追溯的实现工具、追溯矩阵、覆盖率等相关资料。 d) 检查软件测试用例是否基于知识与经验的故障猜测建立，是否使用了功能安全要求的开发方法？是否通过评审，评审问题形成闭环？ e) 检查软件代码是否符合 MISRA 及企业自己的编码规范检？ f) 检查静态分析方法、工具、步骤，圈复杂度要求是否满足？ g) 检查动态测试方法、工具、步骤是否满足要求？ h) 检查软件单元验证缺陷管理流程。 i) 检查软件单元验证结束后退出准则要求
2	是否按照 GB/T 34590.6—2022 中表 7 的要求确定了单元验证方法的合理组合？选择的单元验证方法组合是否与单元设计与实现中的 ASIL 定义保持一致？选择的软件单元验证方法是否与标准推荐 ASIL 保持一致？未使用及不适用的方法是否提供了合理理由？	检查单元验证的确认评审检查单及记录，并确认软件单元验证方法是否是基于 GB/T 34590.6—2022 中表 7 要求的基于 ASIL 等级的验证方法的组合。未选用的验证方法是否有合适的理由
3	是否按照 GB/T 34590.6—2022 中表 8 的要求得到单元测试用例？选择的单元测试用例开发方法是否与软件单元设计与实现（软件详细设计）中的 ASIL 定义保持一致？	检查软件单元验证的测试用例是否依照 GB/T 34590.6—2022 中表 8 的要求基于 ASIL 等级得出并检查单元测试用例评审检查单及记录
4	是否按照 GB/T 34590.6—2022 中表 9 的要求确定了软件验证的结构覆盖率？软件单元验证的结构覆盖率是否与单元设计与实现中的 ASIL 定义保持一致？软件单元验证结构覆盖率是否与标准推荐 ASIL 保持一致？测试结果是否能够提供证据说明单元验证活动满足已定义的软件单元设计及实现（软件详细设计）层级的结构覆盖度？	确认软件单元验证的覆盖率，需求覆盖率尽量做到全覆盖，如果有无法覆盖的需求，需要说明理由 **示例 1**：按照 GB/T 34590.6—2022 中表 9 列出的度量对结构覆盖率进行测定，如语句覆盖率、分支覆盖率、MC/DC（修订的条件/判定覆盖），如果认为已实现的结构覆盖率不充分，应定义额外的测试用例或提供基于其他方法的理由。对于设计及实现覆盖度指标，宜采用工具分析获得。对于无法达成的指标要求，需要说明理由。 **示例 2**：覆盖率＝（至少被执行一次的 Item 数）/Item 的总数。
5	是否按要求对软件单元验证过程中所有的缺陷进行了管理，并跟踪至关闭？	a) 检查软件缺陷管理记录，确认针对软件单元验证工作进行了总结，确认软件验证是否完成； b) 确认测试中所有的问题被记录、跟踪，直至关闭。对于遗留的问题，需要进行评估，确保不影响后续的验证活动，且符合已定义的软件单元验证结束准则

表 E.1　软件单元验证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	是否对通过软件单元验证的软件范围进行了分析，其是否包含定义的功能和性能？对于未定义的功能，是否评估了风险或执行了解决措施？	检查软件单元验证策略： 确认建立了软件单元设计及实现和软件单元验证的追溯关系，确保软件单元验证覆盖了单元设计及实现的所有内容，没有与软件单元设计及实现无关的测试内容
7	是否对软件单元验证环境进行了分析？如果软件单元环境与目标环境不一致，是否给出了对应措施？	检查软件单元验证的测试环境和工具，记录相关的配置信息。如果软件单元验证与目标环境不一致，需要分析差异，定义在目标环境下的附加测试 **示例**：软件单元验证可在不同环境中进行，例如，MIL、SIL、PIL、HIL 等。
8	是否按照 GB/T 34590.8—2022 第 9 章的要求，对已制定的单元验证计划进行了验证？验证中发现的问题是否均已关闭？未关闭的问题是否明确了对应措施，并符合测试结束准则？	检查测试计划、测试报告，测试不符合项整改办法，整改后是否执行了回归测试等？ 验证方法包括了测试，也包括评审、分析等

附 录 F
（资料性）
软件集成和验证

软件集成和验证的审核及评估的说明及示例见表 F.1。

表 F.1 软件集成和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	是否基于 GB/T 34590.6—2022 第 10 章的要求，定义了软件集成及验证的方法和策略？	定义软件集成方法和步骤可考虑以下内容： a） 软件集成及验证步骤和集成方式（Top Down 或 Bottom Up）； b） 对于大型软件需要明确集成步骤，可根据软件功能及软件架构明确每次集成的范围和先后顺序； c） 在分步骤集成过程中，可能需要编制“桩函数”，宜在软件集成步骤说明中进行明确； d） 对于复杂软件，宜编制软件集成操作指南，明确集成环境/工具的配置参数； e） 对于小型软件，可考虑“一次性集成”，宜说明原因。 定义软件集成测试策略可考虑以下内容： a） 软件集成测试的测试目标，例如：软件架构层次的需求覆盖度和结构覆盖度； b） 软件集成测试用例的导出方法； c） 软件集成测试的方法组合； d） 软件集成测试的环境，明确软件集成测试环境的配置参数； e） 软件集成测试的缺陷管理流程； f） 软件集成测试中回归测试的策略； g） 软件集成测试的结束准则
2	是否按照 GB/T 34590.6—2022 第 10 章的要求，通过表 10 软件集成验证方法确定了软件集成验证方法的合理组合？	a） GB/T 34590.6—2022 给出了软件集成验证的方法，需要明确软件架构设计的 ASIL，选择的软件集成验证方法需要与标准推荐 ASIL 保持一致。对于未采用的方法，需要说明原因，例如：当未采用 MBD 开发方法，模型和代码之间的背靠背比较测试不适用。 b） 对于选择的验证方法，需要有具体的验证证据，例如：如果选择了静态代码检查方法，并采用工具实施这一活动，需保留静态代码检查结果，如果静态代码检查发现了问题，需在问题解决后，再次执行静态代码检查，以证明发现的问题得到了解决。 c） 对于软件架构、软硬件接口规范和软件需求等，软件集成验证需要有一定的覆盖性，例如：对于软件架构设计中的控制流设计和数据流设计，需要在软件集成验证中有对应的测试用例。 d） 宜明确每条测试用例对应的软件集成验证方法 **注**：具体要求参考 GB/T 34590.6—2022 中的表 10。
3	针对已选择的软件集成及验证方法，是否有相关内容说明相应的软件集成及验证活动执行符合要求？	a） 针对选定的软件集成及验证方法，需要明确执行的方法和工具（例如：故障注入测试与静态代码分析会使用不同的工具）。 b） 如果使用工具执行分析和测试工作，需要维护好相应的输入和输出，并建立好与被验证方面的追溯关系

表 F.1　软件集成和验证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	是否按照 GB/T 34590.6—2022 中表 11 软件集成测试用例的得出方法要求开发了软件集成测试用例？	a）GB/T 34590.6—2022 中给出了软件集成测试用例的得出方法，需要明确软件架构设计的 ASIL，选择的软件集成测试用例导出方法需要与标准推荐 ASIL 保持一致。对于未采用的方法，需要说明原因。 b）基于知识或经验的错误推测方法，虽然标准中为“＋”，如果有条件，宜选择。 c）宜明确每条测试用例对应的软件集成测试用例导出方法。 d）测试用例中宜包含必要的属性：测试用例 ID、测试步骤、预期结果、ASIL 等级、测试用例得出方法、软件集成验证方法 **注**：具体要求参考 GB/T 34590.6—2022 中的表 11。
5	是否按照 GB/T 34590.6—2022 第 10 章要求确定了测试用例在软件架构层级的需求覆盖率和结构覆盖率（包括函数覆盖率和调用覆盖率）？结构覆盖率是否满足 GB/T 34590.6—2022 中表 12 的要求[适用性：本要求适用于 ASIL（A）、（B）、C 和 D 等级]？	a）需要确定软件架构层级的需求覆盖率，软件架构层级的需求覆盖率尽量做到全覆盖，如果的确有无法覆盖的需求，需要说明理由。 b）GB/T 34590.6—2022 给出了软件架构层次的架构覆盖度要求，需要明确软件架构设计的 ASIL，选择的软件架构层次的架构覆盖度需要与标准推荐 ASIL 保持一致。 c）对于架构覆盖度指标，宜采用工具分析获得。对于无法达成的指标要求，需要说明理由 **注**：具体要求参考 GB/T 34590.6—2022 中的表 12。
6	是否建立了软件集成测试用例和软件架构及软件安全要求的追溯关系？是否对软件集成及验证的软件范围进行了验证，其是否包含全部定义的功能和性能？对于未定义的功能，是否评估了风险或执行了解决措施？	a）需要建立软件架构和软件集成验证的双向追溯关系，确保软件集成测试覆盖了软件架构的所有内容，没有与软件架构无关的测试内容。 b）需要建立软件安全要求和软件集成验证的追溯关系，确保软件集成测试覆盖了软件需求的所有内容，没有与软件需求无关的测试内容。 c）对于用于调试或检测的代码，需要进行妥善处理，不影响安全要求
7	是否对软件集成测试及验证环境进行了分析？如果软件集成测试及验证环境与目标环境不一致，是否进行分析并给出了对应措施？	a）软件集成测试可在不同环境中进行，例如：MIL、SIL、PIL、HIL。 b）需要明确软件集成测试的测试环境和工具，记录相关的配置信息。 c）如果软件集成测试与目标环境不一致，需要分析差异，定义在目标环境下的附加测试
8	软件集成及验证是否实施完成？集成及验证中发现的问题是否已关闭？未关闭的问题是否明确了对应措施，并符合测试结束准则？	a）需要针对软件集成及验证的工作进行总结，明确软件集成及验证是否完成。 b）验证中所有的问题需要被记录、跟踪，直至关闭。对于遗留的问题，需要进行评估，确保不影响后续的验证活动，且符合已定义的软件集成测试结束准则

附 录 G
（资料性）
嵌入式软件测试

嵌入式软件测试的审核及评估的说明及示例见表 G.1。

表 G.1 嵌入式软件测试的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否基于 GB/T 34590.6—2022 第 11 章要求，制定了嵌入式软件测试策略？	定义嵌入式软件测试策略可考虑以下内容： a) 嵌入式软件测试的测试目标，例如：软件需求覆盖度； b) 嵌入式软件测试用例的导出方法； c) 嵌入式软件测试的方法组合； d) 嵌入式软件测试的环境，明确嵌入式软件测试环境的配置参数； e) 嵌入式软件测试的缺陷管理流程； f) 嵌入式软件测试中回归测试的策略； g) 嵌入式软件测试的结束准则
2	是否按照 GB/T 34590.6—2022 中表 13 用于执行软件测试的测试环境要求，确定了嵌入式软件测试的测试环境？	a) GB/T 34590.6—2022 给出了嵌入式软件验证的测试环境要求，需要明确软件需求的 ASIL，选择的嵌入式软件测试环境需要与标准推荐 ASIL 保持一致。对于未采用的测试环境，需要说明原因。 b) 需要明确嵌入式软件测试环境的软件测试工具、硬件测试工具的配置参数 **注**：具体要求参考 GB/T 34590.6—2022 中的表 13。
3	是否按照 GB/T 34590.6—2022 中表 14 嵌入式软件的测试方法要求，确定了嵌入式软件测试方法的合理组合？	a) GB/T 34590.6—2022 给出了嵌入式软件测试的测试方法要求，需要明确软件需求的 ASIL，选择的嵌入式软件测试方法需要与标准推荐 ASIL 保持一致。对于未采用的测试方法，需要说明原因。 b) 对于选择的测试方法，需要有具体的测试证据，需要记录测试结果。 c) 宜明确每条测试用例对应的嵌入式软件测试方法 **注**：具体要求参考 GB/T 34590.6—2022 中的表 14。
4	针对已选择的嵌入式软件测试方法，是否有相关内容说明相应的嵌入式软件测试活动执行符合要求？	a) 针对每种选定的嵌入式软件测试方法，需要明确执行的方法和工具（例如：硬件在环方法和电子控制单元网络环境方法可能会使用不同的测试工具）。 b) 对于选择的嵌入式软件测试方法，需要维护好相应的输入和输出，并建立好与被验证方面的追溯关系
5	是否按照 GB/T 34590.6—2022 中表 15 嵌入式软件测试用例的得出方法要求，开发了嵌入式软件测试用例？	a) GB/T 34590.6—2022 给出了嵌入式软件测试的测试用例导出方法，需要明确软件需求的 ASIL，选择的嵌入式软件测试用例导出方法需要与标准推荐 ASIL 保持一致。对于未采用的测试用例导出方法，需要说明原因。 b) 宜明确每条测试用例对应的嵌入式软件测试用例导出方法。 c) 测试用例中宜包含必要的属性：测试用例 ID、测试步骤、预期结果、ASIL 等级、测试用例得出方法、嵌入式软件测试方法 **注**：具体要求参考 GB/T 34590.6—2022 中的表 15。
6	嵌入式软件测试是否实施完成？测试中发现的问题是否均已关闭？未关闭的问题是否明确了对应措施，并符合测试结束准则？	a) 需要针对嵌入式软件测试的工作进行总结，明确嵌入式软件测试是否完成。 b) 测试中所有的问题需要被记录、跟踪，直至关闭。对于遗留的问题，需要进行评估，确保不影响安全功能的执行，且符合已定义的结束准则
7	是否建立了软件安全要求与嵌入式软件测试用例间的追溯关系？是否对嵌入式软件测试的测试结果及覆盖率进行了评估？	a) 需要建立软件安全要求和嵌入式软件测试的双向追溯关系，确保嵌入式软件测试覆盖了软件需求的所有内容，没有与软件需求无关的测试内容。 b) 对于嵌入式软件测试，每条测试用例的测试结果均与软件需求定义的预期需求保持一致

附 录 H
（资料性）
软件标定和配置管理

软件标定和配置管理的审核及评估的说明及示例见表 H.1。

表 H.1 软件标定和配置管理的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否对配置数据进行了定义？ a） 配置数据的有效值； b） 配置数据的目的和用法； c） 范围、比例、单位； d） 配置数据不同要素之间的相互依赖	a） 检查配置数据的定义属性，包括有效值、目的、用法、范围、比例、单位、依赖性等； b） 需要对在要素构建过程中分配的且控制要素构建过程的数据进行定义，如预处理器变量设置，用于从源代码导出编译时间变量；用于控制构建工具或工具链的 XML 文件等 **示例**：软件模块某测试模式开关 TEST，此项打开将会取消部分函数参数和变量的 const 限制和变量的 static 限制方便测试，正式版本需要设置为 STD_OFF（STD_OFF：关；STD_ON：开）。
2	配置数据及其规范是否能够提供证据证明以下内容？ a） 配置数据符合软件架构设计规范； b） 配置数据符合软件单元设计规范； c） 配置数据使用的值在其规定的范围内； d） 配置数据与其他配置数据的兼容性	a） 配置数据规范的定义及内容应符合软件架构设计和软件单元设计，以其为主体，且使用的值在定义的范围内； b） 对配置软件的测试应在软件单元验证、软件集成测试、嵌入式软件测试中进行测试 **示例**：软件架构或软件单元设计规范中已定义好相关数据，配置数据应按其执行。
3	是否规定了配置数据的 ASIL 等级应等于应用于该数据的可配置软件的最高 ASIL 等级？	配置数据的 ASIL 等级应按照其在的可配置软件（软件单元/软件组件）的 ASIL 等级进行匹配，等于应用于该数据的可配置软件的最高 ASIL 等级 **示例**：某传感器模块，其 ASIL 等级为 B，则其配置数据应达到 ASIL B 等级。
4	是否按照 GB/T 34590.8—2022 第 9 章定义了对相关项开发中要使用的配置数据集对可配置软件的验证？	其行为依赖于配置数据的那部分嵌入式软件要针对配置数据集进行验证
5	是否按照以下组合执行了可配置软件的验证？ a） 可配置软件的验证； b） 配置数据的验证； c） 已配置软件的验证	在进行可配置软件的验证时，可通过如下任意一种方式实现： a） 应当在可配置软件的验证验证允许的配置数据的范围，并说明它在配置数据验证中定义的范围； b） 说明在配置数据验证中允许的配置数据范围的符合性，并执行已配置软件的验证
6	是否定义了与软件组件关联的标定数据以确保配置后软件的正确运行和预期性能？ a） 标定数据的有效值； b） 标定数据的目的和用法； c） 范围、比例和单位，以及它们对运行状态的依赖（如果适用）； d） 不同标定数据之间已知的相互依赖； e） 配置数据和标定数据之间的已知的相互依赖	a） 检查标定数据的定义属性，包括有效值、目的、用法、范围、比例、单位、依赖性等； b） 相互依赖可存在于同一标定数据集内的标定数据之间，或者不同标定数据集的标定数据之间，如：不同电子控制单元的软件中执行的应用于相关功能的标定数据； c） 配置数据可对使用标定数据的已配置软件有影响； d） 需要将软件构建后将用作软件参数值的数据进行定义 **示例**：参数（例如，低怠速值、发动机万有特性图）、车辆特定参数（适应值，例如，节气门限位）、变量编码（例如，国家代码、左舵/右舵）。
7	是否规定了标定数据的 ASIL 等级应等于其可能违反的软件安全要求的最高 ASIL 等级？	标定数据的 ASIL 等级应按照其所在的已配置软件（软件单元/软件组件）的 ASIL 等级进行匹配，等于应用于该数据的已配置软件的最高 ASIL 等级 **示例**：某传感器模块，其 ASIL 等级为 B，并已经配置好，则其标定数据（如挡位对应范围）应达到 ASIL B 等级。

表 H.1　软件标定和配置管理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	是否按照 GB/T 34590.8—2022 第 9 章定义了如何验证标定数据？ a）　定义的标定数据合适并符合软件安全要求； b）　定义的标定数据符合软件架构设计规范； c）　定义的标定数据符合软件单元设计规范； d）　定义的标定数据与其他定义的标定数据是一致且兼容的	a）　标定数据规范的定义及内容应符合软件架构设计和软件单元设计，以其为主体，且使用的值在定义的范围内； b）　标定数据要满足软件安全要求中提出的要求； c）　已定义好的标定数据互相之间应没有影响或不一致，否则需要重新定义； d）　标定数据的验证可包含检查标定数据值的范围或者不同标定数据之间的相互依赖关系
9	是否按照 GB/T 34590.8—2022 第 9 章定义了用于生产发布的标定数据的验证？是否关闭问题？ a）　发布的标定数据符合其规范； b）　嵌入式软件的已标定的、应用特定的变体提供了定义的安全相关功能和特性	a）　标定数据的验证也可在系统层面执行； b）　在小批量生产、量产阶段的标定数据需要进行验证，符合标定数据规范、软件安全需求规范、软件架构设计规范、软件单元设计规范
10	是否定义了数据非预期变化的探测机制？ **注**：具体要求参考 GB/T 34590.6—2022 中的表 C.1。	对于不同 ASIL 等级的软件组件/软件单元的标定数据，应按照其等级，检查是否使用如下方法探测安全相关的标定数据的非预期变化： a）　标定数据合理性检查； b）　标定数据的冗余存储和比较； c）　使用错误检测码检查标定数据
11	是否定义了标定数据应遵循的流程、生成标定数据的工具和验证标定数据的流程？	a）　检查在标定数据规范中应标明标定数据产生、验证的流程，并按此进行执行； b）　生成标定数据所用到的工具需要明确，在软件开发环境文档和标定数据规范中进行定义
12	软件开发环境文档中是否针对软件配置的更新细化内容？	在软件配置时需要按照上述序号 1～序号 11 要求进行明确细化软件开发环境文档，将最初始不明确的地方进行完善

附 录 I
（资料性）
软件组件鉴定

软件组件鉴定的审核及评估的说明及示例见表 I.1。

表 I.1 软件组件鉴定的审核及评估的说明及示例

序号	检查清单	说明及示例
1	安全计划中是否由于软件组件鉴定而按照 GB/T 34590.2—2022 中的 6.4.5.1 对某一安全活动进行了剪裁？若有，剪裁是否满足 GB/T 34590.8—2022 第 12 章的要求？	检查安全计划中是否由于软件组件鉴定而对某一安全活动进行了剪裁
2	软件组件的软件开发过程是否基于适当的国家或国际标准？	检查软件组件的软件开发过程是否基于适当的国家或国际标准（如 ISO/IEC/IEEE 12207）
3	软件组件的文档是否按 GB/T 34590.8—2022 中 12.4.2.1 软件组件鉴定定义的要求得出？	检查软件组件的文档是否按 GB/T 34590.8—2022 中 12.4.2.1 软件组件鉴定定义的要求得出
4	软件组件鉴定的定义是否包括了软件组件的唯一识别？	检查软件组件鉴定的定义是否包括了软件组件的唯一识别 **示例**：标识软件组件的 ID。
5	软件组件鉴定的定义是否包含当软件组件错误执行时，可能违背的所有安全要求的最高 ASIL 等级？	检查软件组件鉴定的定义中是否包含最高 ASIL 等级
6	软件组件鉴定的定义是否包括了为鉴定软件组件所应执行的活动？	检查软件组件鉴定的定义是否包括了为鉴定软件组件所应执行的活动
7	软件组件鉴定的定义是否包含以下要求？ ——软件组件的要求； ——软件组件预期用途的要求； ——配置描述； ——所需接口、供给接口、共享资源描述（如果适用）； ——软件组件集成的描述； ——异常运行条件下的功能反应； ——对已知异常及相应应急措施的描述	检查软件组件鉴定的定义是否包含以下要求。 a) 软件组件的要求； b) 软件组件预期用途的要求； c) 配置描述； d) 所需接口、供给接口、共享资源描述（如果适用）； e) 软件组件集成的描述； f) 异常运行条件下的功能反应； g) 对已知异常及相应应急措施的描述
8	是否提供了软件组件的鉴定报告，以证明组件的开发过程符合标准的证据，并记录了论证结果？	检查软件组件的鉴定报告是否有提供，是否有证明组件的开发过程符合标准的证据及论证结果记录
9	软件组件鉴定报告是否提供了软件组件的验证结果，以证明符合以下要求，并记录了论证结果？ ——分配给软件组件的要求的测试覆盖率应满足 GB/T 34590.6—2022 第 9 章； ——满足测试用例完整性要求（ASILD 适用），结构覆盖率应按照 GB/T 34590.6—2022 第 9 章来测量； ——既覆盖正常运行条件，也覆盖失效情况下的表现； ——没有导致违背安全要求的已知错误； ——验证结果仅对软件组件未经改变的实现有效	a) 检查软件组件鉴定报告是否提供了软件组件的验证结果，以证明符合要求，并记录了论证结果。 b) 展示对要求的覆盖率，按照 GB/T 34590.6—2022 第 9 章 **注**：该验证是主要基于要求的测试，可使用软件组件开发过程中或在之前的集成测试中执行的基于要求的测试结果。 **示例**：专用鉴定测试套件的应用，对软件组件实施和全部集成期间的所有已执行测试的分析。

表 I.1 软件组件鉴定的审核及评估的说明及示例（续）

序号	检查清单	说明及示例
10	对软件组件的鉴定记录中是否包含下述信息： a) 软件组件的唯一识别； b) 软件组件的唯一配置； c) 执行鉴定的人员或组织； d) 用于鉴定的环境； e) 用于鉴定软件组件的验证措施的结果； f) 分配给软件组件的安全要求的最高 ASIL 等级	检查对软件组件的鉴定记录中是否包含 GB/T 34590.8—2022 中 12.4.2 要求的信息
11	是否按照 GB/T 34590.8—2022 第 9 章的要求验证了软件组件的鉴定结果，以证明是否对软件组件资质评估结果进行验证？	检查是否按照 GB/T 34590.8—2022 第 9 章的要求验证了软件组件的鉴定结果，以证明是否对软件组件资质评估结果进行验证