ICS 43.040
CCS T 35

中华人民共和国国家标准

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

Road vehicles—Functional safety audit and assessment method—Part 1: General requirements

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
4.1　总则 …… 1
4.2　如何使用本文件 …… 1
5　审核及评估管理要求 …… 2
5.1　组织文化要求 …… 2
5.2　审核及评估人员资质要求 …… 2
5.3　审核及评估的输入要求 …… 2
5.4　审核及评估过程要求 …… 3
6　审核及评估技术要求 …… 7
6.1　功能安全管理 …… 7
6.2　概念阶段和系统层面 …… 12
6.3　软件层面 …… 12
6.4　硬件层面 …… 12
6.5　生产、运行、服务和报废 …… 12
6.6　支持过程 …… 15
6.7　以汽车安全完整性等级为导向和安全为导向的分析 …… 24
附录A（资料性）　审核及评估报告示例 …… 28
A.1　功能安全审核及评估概览 …… 28
A.2　审核及评估汇总 …… 29
附录B（资料性）　功能安全管理 …… 31
B.1　整体安全管理的审核及评估 …… 31
B.2　项目相关的安全管理审核及评估 …… 34
B.3　生产、运行、服务、报废的安全管理审核及评估 …… 40
附录C（资料性）　生产、运行、服务和报废 …… 41
附录D（资料性）　支持过程 …… 45
附录E（资料性）　以汽车安全完整性等级为导向和安全分析为导向的分析 …… 63

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1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、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、奇瑞汽车股份有限公司、比亚迪汽车工业有限公司、宁波吉利汽车研究开发有限公司、上海千顾汽车科技有限公司、重庆长安汽车股份有限公司、中国第一汽车集团有限公司、中国长安汽车集团有限公司、知行汽车科技(苏州)有限公司、深圳市大疆卓见科技有限公司、南京芯驰半导体科技有限公司、北京地平线机器人技术研发有限公司、英飞凌科技资源中心(上海)有限公司、苏州博沃创新能源科技有限公司、广州汽车集团股份有限公司、上海集度汽车有限公司、舍弗勒(中国)有限公司、北京百度智行科技有限公司、北京国家新能源汽车技术创新中心有限公司、爱信(苏州)汽车技术中心有限公司杭州分公司。

本文件主要起草人：闻继伟、王潇屹、李波、宋雪莉、李小龙、李齐丽、桂彦、何文、付越、尚世亮、戎辉、王宇、邵海贺、宋炜瑾、刘辉、魏斌、王少璋、周宏伟、蔡香、唐沙南、李俊成、付春晖、孙毓阳、陈勇、郭晓东、徐铱铱、王禺寒、林广义、王梓勋、李鸿鹏、李小锋、胡国强、薛剑波、程周、吴倩、储小勤。

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。

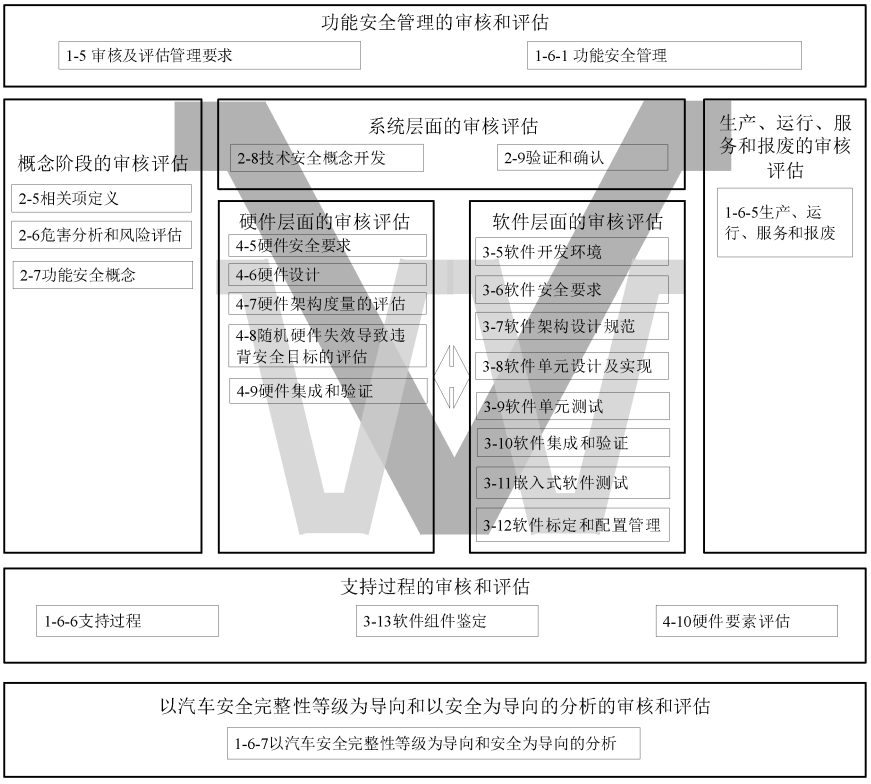

图 1　功能安全审核及评估概览

道路车辆　功能安全审核及评估方法
第1部分:通用要求

1　范围

本文件规定了功能安全审核及评估的通用流程、实施方法及要求。

本文件适用于按照GB/T 34590.1～34590.12—2022开发的,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 43253.2—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

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

4.1　总则

本文件基于GB/T 34590.1～34590.12—2022给出的方法论,按照规定的功能安全审核及评估的流程、实施方法及要求,功能安全审核及评估的检查清单,以判断组织的功能安全流程是否得到了正确的建立及实施,被评估目标(如相关项或要素等)是否实现了功能安全。

注:本文件提供了功能安全审核及评估的检查清单及其示例。

4.2　如何使用本文件

组织可根据本文件建立组织层面的审核及评估流程,制定审核及评估计划、方法和规范,实施审核及评估过程,管理审核及评估问题。

组织在使用本文件时应:

a)　根据审核及评估的对象,参照本文件中的适用要求,定义审核及评估的范围;

b)　根据GB/T 34590.1～34590.12—2022剪裁后的功能安全活动,对本文件的要求和检查清单进

行相应的剪裁；

c) 根据被审核及评估对象的特性，新增或调整检查项；

d) 若对本文件中的已有检查项进行变更或剪裁，需给出恰当的理由。

注 1：本文件所列方法及要求包含功能安全审核和功能安全评估两个方面，但并未区分。如果组织需要单独进行功能安全审核，参考本文件，单独建立组织层面的审核流程，制定审核计划、方法和规范，实施审核过程，管理审核问题。

注 2：组织的内部或外部参照本文件实施审核及评估。

注 3：对于不同 ASIL 等级的检查项，检查项列表中给出了说明；若无其他说明，本文件检查项适用于 ASIL A、B、C 和 D 四个等级。

5 审核及评估管理要求

5.1 组织文化要求

开展审核及评估的相关组织应建立确保有效实施审核及评估的安全文化。良好的安全文化可包含：

a) 在各个开发阶段(例如：概念层面开发阶段、系统层面开发阶段、软件层面开发阶段、硬件层面开发阶段等)，生产、运行、服务和报废阶段及管理过程中执行一个明确的、可追踪的和受控的功能安全审核及评估流程；

b) 明确审核及评估人员的职责与责任，并充分赋予其决策的权利；

c) 制定审核及评估人员的能力提升计划，并按照计划实施能力提升；

d) 任命有审核及评估能力的员工进行审核及评估活动，人员资质要求见 5.2；

e) 制定明确的激励措施(例如奖惩措施)，促进审核及评估有效实施；

f) 应建立、执行并维护持续改进的审核及评估流程，以发现可能导致违反安全的薄弱环节，并提高审核及评估效率。

注：改进方面可为审核及评估的流程、整个生命周期审核及评估的次数、时间点、分阶段审核及评估、审核及评估内容的拆分、人员的配置等。

5.2 审核及评估人员资质要求

组织应按照 GB/T 34590.2—2022 中表 1 的独立性要求指派审核及评估人员。审核及评估人员可来自企业内部、客户或是第三方公司。

审核及评估人员应具备与其职责相匹配的技能水平、能力及资质，至少具备以下知识领域的培训、专业活动经验：

a) 质量体系流程；

b) GB/T 34590.1～34590.12—2022 规定的要求；

c) 本文件规定的功能安全审核及评估的要求；

d) 作为观察者角色，参与过审核及评估过程；

e) 具有被评估对象或相似产品的相关工程经验。

5.3 审核及评估的输入要求

5.3.1 审核及评估的输入

审核及评估的输入应包括如下：

a) 审核及评估的目的说明；

b) 待检查的功能安全工作成果；
c) 审核及评估的计划(可包含在安全计划内)；
d) 产品安全问题或问题清单(如适用)；
e) 审核及评估流程；
f) 审核及评估支持材料(如适用)。
根据审核及评估方要求,被审核及评估方应提供的其他支持材料。
审核及评估的对象工作成果应具备与所进行审核及评估阶段相匹配的成熟度。
注：成熟度的定义由审核及评估方和被审核及评估方在审核及评估计划时进行定义。

5.3.2 审核及评估的授权

审核及评估方应具有支持开展审核及评估范围内所需的权限。

5.4 审核及评估过程要求

5.4.1 审核及评估过程总览

图 2 展示了在分布式开发中审核及评估的过程总览。

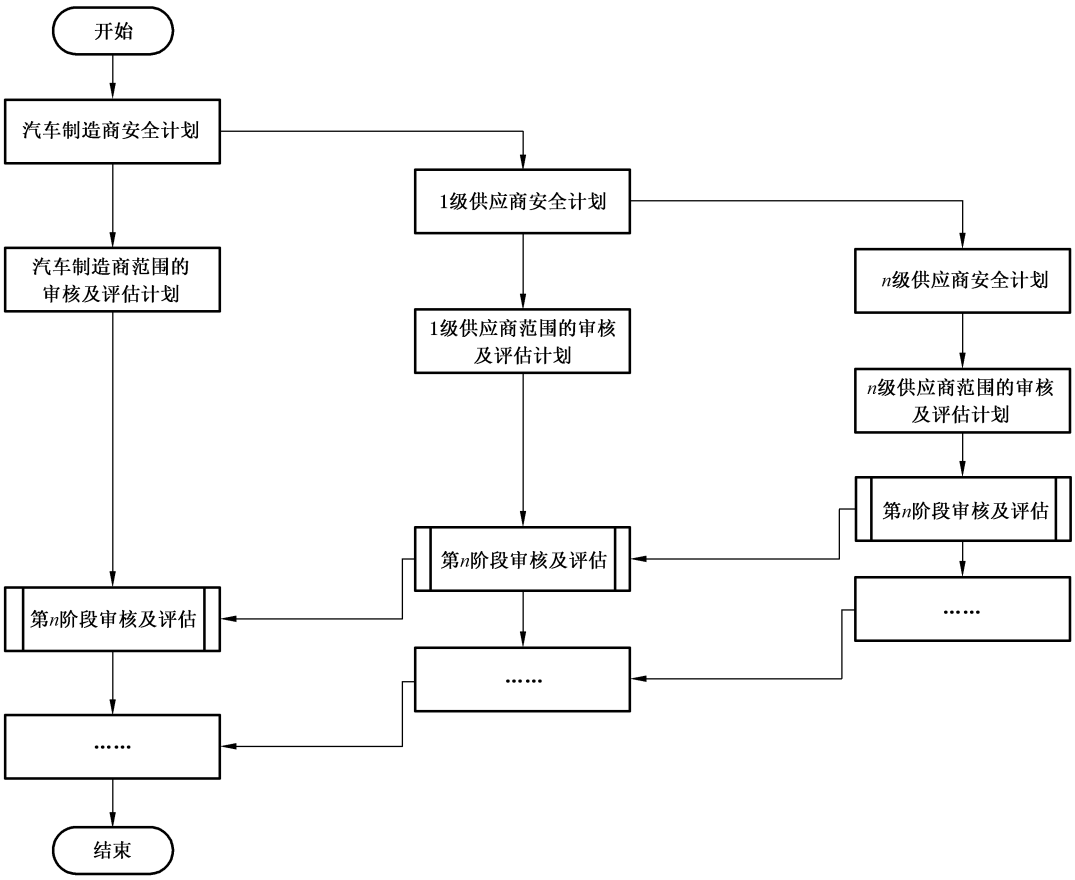

图 2 审核及评估过程总览

在计划阶段，审核及评估方的安全经理应计划审核及评估活动，可包括实施次数、审核及评估范围、责任分工、验收标准、地点及时间等。

审核及评估方所在组织应根据安全计划、相关项或要素的实际情况以及与被审核及评估方达成的协议，细化审核及评估计划。

审核及评估方所在组织应根据审核及评估计划组织和实施审核及评估。

5.4.2 审核及评估过程

5.4.2.1 审核及评估阶段

审核及评估可包含 4 个阶段：

a) 准备阶段；

b) 审核及评估过程阶段；

c) 审核及评估报告阶段；

d) 问题改进及确认阶段(如适用)。

5.4.2.2 准备阶段要求

在准备阶段应至少进行以下活动。

a) 确保审核及评估人员符合 5.2 审核及评估人员资质要求。

b) 计划实施审核及评估所需要的时间和资源等。

c) 制定审核及评估的计划，计划至少包含以下内容：

1) 在适当的管理支持下，确定审核及评估组人员的角色并分配具体的职责；

2) 确定审核及评估的范围；

3) 确定审核及评估的通过准则；

4) 初步制定审核及评估会议的日程。

d) 制定审核及评估所需审核及评估检查清单，检查清单见第 6 章。

e) 制定审核及评估结果记录清单(包含安全问题管理清单)。

5.4.2.3 审核及评估过程要求

图 3 展示了审核及评估阶段的流程。

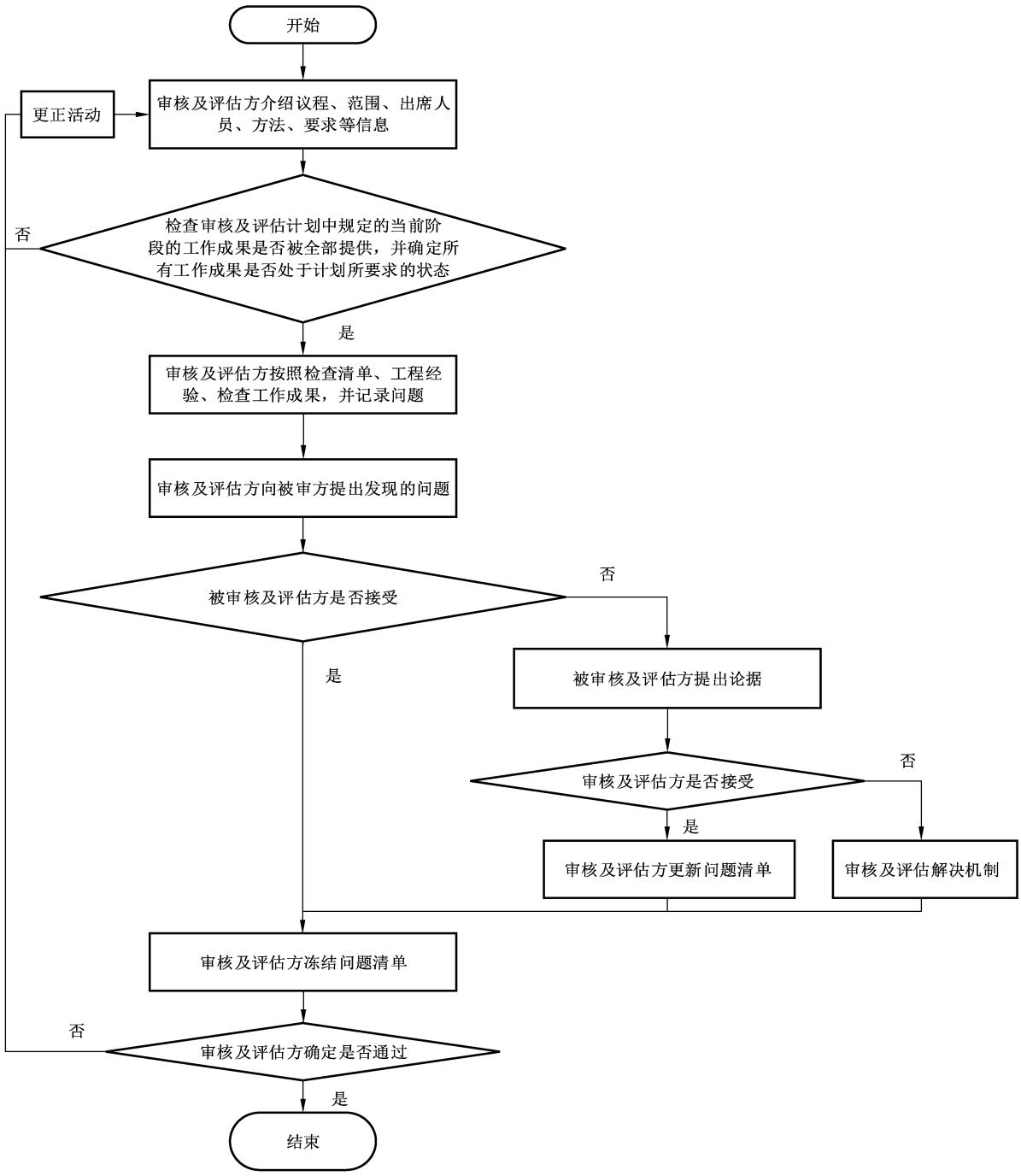

图 3　审核及评估过程

审核及评估方按照以下顺序开展审核及评估。

a）　由审核及评估方进行有关审核及评估规程的概要介绍。介绍可包含会议议程、范围、出席人员、方法、要求等信息。该概要介绍既可作为评审会议的一个部分，也可作为一次单独的会议。

b）　检查审核及评估计划中规定的当前阶段的工作成果是否被全部提供，并确定所有工作成果是否处于计划所规定的状态。

c) 审核及评估方基于本文件检查清单和工程经验检查工作成果，按照准备阶段定义的问题清单形式记录发现的安全问题。各阶段审核及评估技术要求参照第6章审核及评估技术要求。

d) 审核及评估方向被审核及评估方提出发现的问题，如果被审核及评估方接受该问题，则该问题将被纳入问题管理清单；如果被审核及评估方不接受该问题，可提供相关的论据，以支持审核及评估方的重新判断。当双方不能达成一致时，应根据双方建立的争议解决机制进行；

示例：争议解决机制可为以审核及评估人员的意见为准，也可是上升到双方更高级别人员进行决策等。

e) 当所有问题均被讨论完成后，审核及评估方冻结安全问题管理清单。

f) 被审核及评估方按照审核及评估计划和相关流程，制定问题处理措施、责任人、完成日期等信息。

g) 审核及评估方根据审核及评估计划中的通过判定准则给出本次审核及评估结论。如接受，则进行下次审核及评估的计划或结束所有审核及评估；如有条件接受，则定义问题确认机制（可为重新进行该次审核及评估，也可以其他形式确认问题被正常关闭）；如拒绝，则需进行足够的整改活动，并重新计划该次审核及评估。

表1规定了功能安全审核及评估的通过判定准则。

表1 功能安全审核及评估的通过判定准则

结论	通过判定准则
拒绝	存在影响安全目标实现的问题，应经过整改后才能开展后续安全活动
有条件接受	a) 基本达成相关项的功能安全，尽管存在已识别出的未解决的问题； b) 有条件接受的建议应包含与功能安全评估标准的偏差以及这些偏差可被接受的依据
接受	a) 无影响功能安全目标实现的相关问题；或 b) 残余风险非常低，经过适当的整改活动后，即可消除问题
注1：有条件接受是一种过渡状态，可记录有条件接受的条件并在最终发布前验证其是否被满足，即：当满足条件时可最终发布。 **注2**：关于残余风险的可接受程度，可参照已量产应用的类似产品的市场表现。 **注3**：当证明存在有效的运行风险监控措施时，可有助于认为残余风险可接受。 **注4**：审核及评估方需要根据表1规定的通过判定准则指导思想进行通过判定准则的量化指标定义。	

5.4.2.4 审核及评估报告要求

功能安全审核及评估报告用于执行并记录各阶段的功能安全审核及评估活动，并判断功能安全过程的符合性及是否实现功能安全。

功能安全审核及评估的报告应至少包含以下内容。

a) 审核及评估的对象和范围。

b) 审核及评估目的。

c) 审核及评估组成员。

d) 审核及评估的类型。

e) 审核及评估的形式及其局限。

f) 被审核及评估的工作成果等证据。

g) 安全问题管理清单。如适用，还可包括问题解决措施项的状态（待处理或已关闭）、责任人和完成日期（若为待处理）。

h) 审核及评估的结论。

i) 审核及评估的详细内容和结果。

j) 审核及评估证据的存档要求(如适用)。

审核及评估报告示例见附录 A。

5.4.2.5 问题改进阶段要求

被审核及评估方根据问题清单和时间计划,完善并落实问题处理措施。

被审核及评估方应根据审核及评估报告的结论进行安全问题整改,并提交审核及评估方确认整改结果。

审核及评估方应根据安全问题整改结果,进行审核及评估报告修订。

6 审核及评估技术要求

6.1 功能安全管理

6.1.1 目标

本章的目标是对功能安全管理文档进行审核及评估,以检查其内容是否符合功能安全开发的定义及需要。

6.1.2 审核及评估的输入

功能安全管理中需审核及评估的开发流程及对应的输入材料主要包括以下内容(可根据审核及评估范围剪裁)。

a) 整体安全管理:

1) 功能安全规章和流程;

2) 能力管理证据;

3) 质量管理体系证据;

4) 已识别的安全异常报告(如果适用)。

b) 项目相关的安全管理:

1) 相关项层面的影响分析;

2) 要素层面的影响分析(如果适用);

3) 安全计划;

4) 安全档案。

c) 生产、运行、服务、报废的安全管理:关于生产、运行、服务和报废的安全管理证据。

6.1.3 审核及评估的要求

6.1.3.1 整体安全管理的审核及评估要点

对于功能安全规章和流程的审核及评估,应涵盖表 2 所列检查项。

表 2　功能安全规章和流程的审核及评估要点

序号	检查清单
1	功能安全规章和流程是否存在且可用？
2	功能安全规章和流程是否存在版本管理？
3	功能安全规章和流程中是否建立了与实现功能安全相关的其他领域[如预期功能安全、信息安全、非电气/电子(E/E)系统相关安全等]之间的有效沟通渠道？是否合理？
4	功能安全规章和流程中是否明确了功能安全的实现所需资源的提供方案？是否合理？
5	功能安全规章和流程中是否规定了持续改进流程？是否合理？
6	功能安全规章和流程中是否给予负责实现或维护功能安全、执行或支持安全活动的人员以足够的权限来履行他们的职责？是否合理？
7	流程中是否对应 GB/T 34590.1～34590.12—2022 各部分工作成果规定的交付物的要求？
8	交付物的内容是否涵盖 GB/T 43253—2023 定义的评估检查点？

附录 B 中的表 B.1 提供了功能安全规章和流程的审核及评估的说明及示例。

对于能力管理证据和质量管理体系证据的审核及评估，应涵盖表 3 所列检查项。

表 3　能力管理证据和质量管理体系证据的审核及评估要点

序号	检查清单
1	能力管理证据是否存在且可用？
2	能力管理证据文档是否使用了功能安全流程规定的模板？是否存在版本管理？
3	执行安全生命周期活动的人员是否具有与其职责相匹配的技能水平、能力和资质？
4	质量管理体系证据是否存在且可用？

附录 B 中的表 B.2 提供了能力管理证据的审核及评估的说明及示例。

对于已识别的安全异常报告的审核及评估，应涵盖表 4 所列检查项。

表 4　已识别的安全异常报告的审核及评估要点

序号	检查清单
1	已识别的安全异常报告是否存在且可用？
2	安全异常报告是否使用了功能安全流程规定的模板？是否存在版本管理？
3	功能安全异常管理流程是否存在且可用？
4	功能安全异常管理流程是否存在版本管理？
5	功能安全异常管理流程是否可支持及时、有效地分析、评估、解决和管理已识别的安全异常，直至关闭？
6	功能安全异常管理流程中安全异常关闭的要求是否明确？ a)　基于某一依据，实施了充分的安全措施以解决安全异常，且安全措施的有效性得到了验证；或 b)　基于某一依据，将安全异常评估为不构成不合理风险并将其关闭
7	功能安全异常管理流程中，针对关闭安全异常的依据是否具备记录和评审的环节？
8	功能安全异常管理流程中，针对未完成关闭的安全异常是否有及时上报给负责功能安全的人员的路径？

附录 B 中的表 B.3 提供了已识别的安全异常报告的审核及评估的说明及示例。

6.1.3.2 项目相关的安全管理审核及评估要点

对于相关项层面的影响分析和要素层面的影响分析的审核及评估，应涵盖表 5 所列检查项。

表 5 相关项层面的影响分析和要素层面的影响分析的审核及评估要点

序号	检查清单
1	相关项层面的影响分析是否存在且可用？
2	相关项层面的影响分析是否使用了功能安全流程规定的模板？是否存在版本管理？
3	在对相关项或其环境修改的情况下，是否正确识别并描述了应用于相关项的修改（包括设计的修改、实现方式的修改、与环境相关的修改）？
4	在对相关项或其环境修改的情况下，该修改对功能安全的影响的评估是否合理？
5	在对相关项或其环境修改的情况下，受修改影响的安全活动是否合理？
6	要素层面的影响分析是否存在且可用？
7	要素层面的影响分析是否使用了功能安全流程规定的模板？是否存在版本管理？
8	在复用现有要素的情况下，是否识别出运行环境的修改？包括其导致的对要素的修改
9	在复用现有要素的情况下，分配给其的安全要求的符合性是否评估清楚？是否合理？
10	在复用现有要素的情况下，受修改影响的安全活动是否已列出？是否合理？
11	与复用要素有关的现有安全相关文档是否评估清楚？其是否支持将要素集成到相关项，或将要素集成到另一个要素？评估结论是否合理？

附录 B 中的表 B.4 提供了相关项层面的影响分析和要素层面的影响分析的审核及评估的说明及示例。

对于安全计划的审核及评估，应涵盖表 6 所列检查项。

表 6 安全计划的审核及评估要点

序号	检查清单
1	安全计划是否存在且可用？
2	安全计划是否使用了功能安全流程规定的模板？是否存在版本管理？
3	安全经理是否对安全计划进行维护并监控安全活动的进度按照安全计划进行？
4	安全活动的执行责任，是否按照 GB/T 34590.2—2022 中 5.4.2.7 和 5.4.4 的要求分配？
5	安全计划是否都被项目计划引用？或包含在项目计划中，并使安全活动是可区分的？
6	安全计划中是否体现了实现功能安全的活动计划和流程计划？
7	安全计划中是否体现了独立于项目的安全活动？
8	如果安全活动被剪裁，安全计划中是否体现了对安全活动的剪裁？
9	如果安全活动被剪裁，安全计划中对安全活动剪裁的理由说明是否充分、存在、可接受？
10	如果按照影响分析结果而对某一安全活动的剪裁，剪裁是否满足表 5 的要求？

表 6　安全计划的审核及评估要点（续）

序号	检查清单
11	如果按照在用证明结果而对某一安全活动的剪裁，剪裁是否满足表 16 的要求？
12	如果按照硬件要素评估而对某一安全活动的剪裁，剪裁是否满足 GB/T 43253.4—2023 中表 13 的要求？
13	如果是由于软件组件鉴定而对某一安全活动进行剪裁，剪裁是否满足 GB/T 43253.3—2023 中表 9 的要求？
14	如果基于考虑所使用软件工具的置信度的依据而对某一安全活动的剪裁，剪裁是否满足表 15 的要求？
15	如果由于要素被开发为独立于环境的安全要素（SEooC）而对某一安全活动进行剪裁，独立于环境的安全要素的开发是否基于一个需求规范，该需求规范是否来自对预期用途和环境的假设，包括其外部接口？
16	如果由于要素被开发为独立于环境的安全要素（SEooC）而对某一安全活动进行剪裁，当安全要素被集成到其目标应用中时，对独立于环境的安全要素的预期用途和应用环境的假设是否进行了验证？
17	针对于 T&B 的相关项的开发：如果某个应用超出了 GB/T 34590.1～34590.12—2022 的范围，且该应用正在与已根据这些标准开发的基础车辆或相关项进行对接，安全活动的剪裁是否满足表 17 的要求？
18	针对于 T&B 的相关项的开发：如果开展安全活动，以确保未按照 GB/T 34590.1～34590.12—2022 开发的系统或组件，满足集成到按照这些标准开发的相关项中所需的功能安全水平，安全活动的剪裁是否满足表 18 的要求？
19	如果适用，安全活动的计划是否完整包含概念阶段计划？
20	如果适用，安全活动的计划是否完整包含系统层面计划？
21	如果适用，安全活动的计划是否完整包含硬件层面计划？
22	如果适用，安全活动的计划是否完整包含软件层面计划？
23	安全计划中是否完整包含支持过程计划？如果适用，是否包含对定义与分布式开发中其他方的安全计划接口的开发接口协议（DIA）的引用？
24	安全计划中是否完整包含集成和验证活动计划？
25	安全计划中是否完整包含安全确认活动计划？
26	安全计划中是否包含认可评审、功能安全审核和功能安全评估的日程安排？
27	如果适用，安全计划是否完整包含了相关失效分析的计划？
28	如果适用，安全计划是否完整包含了候选项的在用证明分析的计划？
29	如果适用，安全计划是否完整包含了软件工具鉴定的计划？
30	安全活动的计划是否包括：目标；对其他活动或信息的依赖性；负责执行活动的人员；执行活动所需的资源、起始时间、结束时间和持续时间；相应工作成果的识别？
31	当修改相关项和现有相关项环境时，或当复用要素时，GB/T 34590.1～34590.12—2022 的参考安全生命周期是否根据相应影响分析的结果进行剪裁？
32	当修改相关项和现有相关项环境时，或当复用要素时，安全计划中是否相应地识别、描述和返工需要创建或更新的受影响的工作成果？
33	当修改相关项和现有相关项环境时，或当复用要素时，如果其安全文档不符合 GB/T 34590.1～34590.12—2022，安全计划中是否明确必要的活动以符合标准中的相应要求？

表 6　安全计划的审核及评估要点（续）

序号	检查清单
34	安全计划是否在每个阶段开始时进行了更新和细化？
35	安全计划要求的工作成果是否保持最新状态？
36	如果是分布式开发，则客户和供应商是否均有针对各自的安全活动制定安全计划？
37	如果缺乏来自相关先前子阶段的信息，是否在缺乏信息也不会导致功能安全方面的不合理风险的情况下才开始后续子阶段？
38	每一项安全计划所要求的工作成果是否分别服从配置管理、变更管理以及文档管理？纳入管理时间是否不迟于“产品开发：系统层面”阶段的启动时间？

附录 B 中的表 B.5、表 B.7、表 B.8 提供了安全计划的审核及评估的说明及示例。

对于安全档案的审核及评估，应涵盖表 7 所列检查项。

表 7　安全档案的审核及评估要点

序号	检查清单
1	安全档案是否存在且可用？
2	安全档案是否使用了功能安全流程规定的模板？是否存在版本管理？
3	安全档案的建立是否依照安全计划？
4	安全档案中提供的论证是否合理且充分？
5	安全档案中参考的工作成果是否存在且充分完整？
6	安全档案中参考的工作成果是否有可追溯性？
7	安全档案中参考的工作成果内部或成果之间是否无矛盾点？
8	安全档案中参考的工作成果是否满足如下要求？即：既没有导致违背安全目标的问题，或存在的问题是可控的并且有计划得到解决

附录 B 中的表 B.6 提供了安全档案的审核及评估的说明及示例。

6.1.3.3　生产、运行、服务、报废的安全管理审核及评估要点

对于生产、运行、服务和报废的安全管理证据的审核及评估，应涵盖表 8 所列检查项。

表 8　关于生产、运行、服务和报废的安全管理证据审核及评估要点

序号	检查清单
1	关于生产、运行、服务和报废的安全管理证据是否存在且可用？
2	关于生产、运行、服务和报废的安全管理证据是否使用了功能安全流程规定的模板？是否存在版本管理？
3	实现并维护相关项在生产、运行、服务和报废阶段的功能安全的责任人是否明确？
4	在相关项及其要素的生产、运行、服务和报废过程中，相关项的功能安全活动计划是否满足 GB/T 34590.7—2022 第 5 章的要求？

表 8　关于生产、运行、服务和报废的安全管理证据审核及评估要点（续）

序号	检查清单
5	在相关项及其要素的生产、运行、服务和报废过程中，相关项的功能安全活动是否满足 GB/T 34590.4—2022 的要求，在系统层面的产品开发期间启动？
6	在相关项及其要素的生产、运行、服务和报废过程中，相关项的功能安全活动是否按照 GB/T 34590.7—2022 第 6 章和第 7 章执行？
7	是否存在实现和保持相关项在生产、运行、服务和报废阶段的功能安全的流程？
8	如果在生产、运行、服务或报废期间相关项有变更，是否对生产发布变更进行管理？

附录 B 中的表 B.9 提供了生产、运行、服务和报废的安全管理的审核及评估的说明及示例。

6.2　概念阶段和系统层面

概念阶段和系统层面的功能安全审核及评估要求，应满足 GB/T 43253.2—2023。

6.3　软件层面

软件层面的功能安全审核及评估要求，应满足 GB/T 43253.3—2023。

6.4　硬件层面

硬件层面的功能安全审核及评估要求，应满足 GB/T 43253.4—2023。

6.5　生产、运行、服务和报废

6.5.1　目标

本章的目标是对“生产、运行、服务和报废”的相关文档进行审核及评估，以检查其内容是否符合功能安全开发的定义及需要。

6.5.2　审核及评估的输入

生产、运行、服务和报废中需审核及评估的开发流程及对应的输入材料主要包括以下内容（可根据审核及评估范围剪裁）。

a）　安排生产、运行、服务和报废的计划：

1）　生产计划的安全相关内容；

2）　生产控制计划（含测试计划）的安全相关内容；

3）　可生产性需求规范；

4）　生产过程能力报告；

5）　服务计划中安全相关的内容；

6）　服务指导说明中安全相关的内容；

7）　用户须知信息中安全相关的内容；

8）　报废指导说明中安全相关的内容；

9）　运行、服务、报废的需求规范；

10）　救援服务指导说明中安全相关的内容。

b）　生产：

1） 控制措施报告；
2） 生产过程能力报告。

c） 运行、服务和报废：现场观察指导说明。

6.5.3 审核及评估的要求

对于生产、运行、服务和报废的审核及评估，应涵盖表 9 所列检查项。

表 9 生产、运行、服务和报废的审核及评估检查清单

序号	检查清单
1	是否计划了相关项及其要素的生产过程？ 包括： ——对生产的要求； ——安全相关的特殊特性； ——要素的处理和管理条件； ——产品开发过程中定义的配置； ——从以前发布的生产计划中获得的经验总结； ——涉及安全相关的特殊特性的生产过程、设备、工具和测试设备的适宜性； ——人员的能力
2	生产计划是否描述了实现相关项或要素的功能安全而要求的生产步骤、顺序和方法？ 包括： ——生产工艺流程和指导说明； ——生产工具和设备； ——可追溯性措施的实施； ——如果适用，专用措施的实施
3	是否已定义一个流程作为生产过程的一部分，以确保正确版本的嵌入式软件及其相关标定数据被写入 ECU 中？
4	是否识别合理可预见的生产过程失效及其对功能安全的影响，并实施恰当的措施以处理相关过程失效？ 包括过程失效模式和影响分析（PFMEA）
5	是否在制定生产控制计划时考虑了对相关项或要素的控制描述（含控制的准则），以及安全相关的特殊特性？
6	是否在生产控制计划中描述控制步骤的顺序和方法，以及必要的测试设备、工具和测试准则？
7	在计划生产时识别的安全要求，是否已经以适当的方式反馈给负责系统、硬件和软件开发的人员？
8	生产、运行、服务和报废的变更，如影响相关项或其要素，是否已经按要求进行管理？
9	是否已制定相关项的运行、服务和报废过程的计划，并考虑以下因素： ——维护和维修的要求； ——为确保车辆安全运行而应具备的用户须知信息的要求； ——报废的要求； ——紧急救援服务的要求； ——报警和降级策略； ——现场监控流程； ——要素处理的条件； ——在生产发布文件中定义的配置； ——参与人员的能力

表 9　生产、运行、服务和报废的审核及评估检查清单（续）

序号	检查清单
10	服务计划是否已描述对相关项或要素的维护活动的顺序和方法，包括维护间隔以及需要的工具？
11	服务指导说明是否描述了如下内容： ——服务的流程、方法、工作步骤和诊断程序； ——工具和设备； ——用于验证安全相关的特殊特性的控制步骤的顺序和方法，以及控制标准； ——相关项或要素的有关配置，包括可追溯性措施； ——车辆允许的相关项或要素的功能关闭，及其所导致的车辆的任何变更； ——当功能关闭和其他变更发生时，需告知驾驶员； ——备件的供应
12	用户信息，包括用户手册，是否提供了正确使用相关项或要素的有关指导说明和警告，如果适用，还应提供如下信息： ——相关功能（即预期使用、状态信息或用户交互）及其运行模式的描述； ——当报警和降级策略表明失效发生时，为确保可控性所需的用户行为的描述； ——当报警和降级策略表明失效发生时，对用户所期望的服务活动的描述； ——关于与第三方产品交互所导致的已知危害的警告； ——为了防止驾驶员误解或误用，安全相关的整车新功能的正确使用的警告
13	报废指导说明是否描述了相关项或其要素在拆卸过程中采用的活动和措施，以确保其安全报废？
14	在运行、服务和报废的计划过程中识别的安全要求，是否已经以适当的方式反馈给负责系统、硬件和软件开发的人员？
15	救援服务信息，是否包括救援指导说明书或紧急救援指南？如果适用，是否提供相关指导说明和警告，以避免救援操作时发生危害？
16	是否实施了与相关项或其要素相关的潜在安全相关事件的现场监控流程，以便： ——提供能用于分析以探测功能安全问题存在的现场数据； ——分析现场数据，以探测功能安全问题的存在； ——启动相关措施，来处理识别到的功能安全问题
17	相关项或其要素的运行、服务和报废是否按照服务计划、服务指导说明和报废指导说明来实施和文档化？
18	相关项或其要素的变更，运行（包括现场监控）、服务或报废流程的变更，是否已按照要求进行管理？
19	其他通用： 输入文档是否存在且可用？ 输入文档是否使用了最新的模板？是否存在版本管理？ 工作成果是否经过了充分的评审？ 评审人是否为要求的评审人？ 评审是基于基线还是基于版本？ 评审意见是否包含评审人的结论？ 评审记录的所有开口项是否都已关闭？
20	是否制定了生产过程及其控制措施？

表 9　生产、运行、服务和报废的审核及评估检查清单（续）

序号	检查清单
21	是否对生产过程(包括安全相关特殊特性的偏差)进行分析,达到以下目的: ——识别过程失效; ——识别由于过程失效导致的对功能安全的潜在影响; ——采取恰当的措施,以确保识别的影响可被避免或减轻; ——验证采取措施的有效性
22	是否针对功能安全,评估并维护了如下几项能力: ——生产过程; ——设备和工具; ——测试设备
23	测试设备是否按照所采用的质量管理体系进行控制?
24	控制是否按照生产控制计划来执行? 相关的控制报告应包含控制时间、受控对象的识别和控制结果
25	是否落实只有在生产发布报告中定义的已被批准的配置才能进行生产,如有任何偏差应得到负责人的授权?
26	在生产阶段发起的生产过程的变更,是否按照 GB/T 34590.8—2022 第 8 章的要求进行管理?
27	是否实施与相关项或其要素相关的潜在安全相关事件的现场监控流程? 以便: ——提供能用于分析以探测功能安全问题存在的现场数据; ——分析现场数据,以探测功能安全问题的存在; ——启动相关措施,来处理识别到的功能安全问题
28	相关项或其要素的运行、服务和报废是否按照服务计划、服务指导说明和报废指导说明来实施和文档化?
29	相关项或其要素的变更,运行(包括现场监控)、及服务或报废流程的变更是否按照 GB/T 34590.8—2022 第 8 章的要求进行管理?

附录 C 中的表 C.1 提供了生产、运行、服务和报废的审核及评估的说明及示例。

6.6　支持过程

6.6.1　目标

本章的目标是对“支持过程”的相关文档及活动进行审核及评估,以检查其定义内容是否符合功能安全开发的定义及需要。

6.6.2　审核及评估的输入

支持过程中需审核及评估的开发流程及对应的输入材料主要包括以下内容。

a)　分布式开发的接口:
　　1)　供应商选择报告;
　　2)　开发接口协议;
　　3)　供应商安全计划;
　　4)　功能安全评估报告;

5） 供应协议。

b） 配置管理：配置管理计划。

c） 变更管理：

1） 变更管理计划；

2） 变更需求；

3） 影响分析和变更需求计划；

4） 变更报告。

d） 验证：

1） 验证计划；

2） 验证规范；

3） 验证报告。

e） 文档管理：

1） 文档管理计划；

2） 文档指南要求。

f） 软件工具置信度：

1） 软件工具准则评估报告；

2） 软件工具鉴定报告。

g） 在用证明：

1） 在用证明候选项描述；

2） 在用证明分析报告。

h） GB/T 34590.1～34590.12—2022 适用范围之外应用的接口：基础车辆制造商或供应商指南。

i） 未按照 GB/T 34590.1～34590.12—2022 开发的安全相关系统的集成：安全依据。

6.6.3 审核及评估的要求

对于分布式开发的接口审核及评估，应涵盖表 10 所列检查项。

表 10 分布式开发的接口审核及评估检查清单

序号	检查点
1	供应商选择报告是否对供应商进行能力评估？如果适用，也包含按照 GB/T 34590.1～34590.12—2022 对类似复杂度和 ASIL 等级的相关项和要素的生产能力的评估？
2	供应商选择报告是否包含客户给候选供应商的报价需求(RFQ)？报价需求(RFQ)内容是否完整？
3	双方是否签订了 DIA？
4	DIA 中是否包含客户和供应商安全经理的任命？
5	DIA 中是否按照 GB/T 34590.2—2022 中的 6.4.5 进行安全活动的联合剪裁？
6	DIA 中是否包含客户需开展的安全生命周期的活动和供应商需开展的安全生命周期的活动？
7	DIA 中是否包含需共享的信息和工作成果，包含分配和评审？
8	DIA 是否为每个工作成果定义了责任方？

表 10　分布式开发的接口审核及评估检查清单（续）

序号	检查点
9	DIA 中是否包含目标值的沟通或确认？
10	DIA 中是否包含在客户和供应商合作中所需要的接口相关的流程、方法及工具？
11	DIA 中是否包含哪一方（供应商或者客户）按照 GB/T 34590.4—2022 执行安全确认所达成的协议？
12	DIA 中是否包含按照 GB/T 34590.2—2022，关于由供应商开发的要素或工作成果的功能安全评估活动？
13	DIA 中是否包含供应商关于功能安全评估报告的计划？
14	DIA 中是否包含客户与供应商之间达成的允许客户指定审核人员在供应商的场所进行功能安全审核的协议？
15	DIA 是否为每个工作成果定义了交付路径和交付类型？
16	双方是否都批准了 DIA？
17	如果供应商执行危害分析和风险评估，那么危害分析和风险评估是否提供给客户进行验证和批准？
18	概念阶段的责任方是否按照 GB/T 34590.3—2022 制定功能安全概念？
19	客户是否确保供应商按时收到所需的用于执行开发接口协议中安全活动的信息和数据？
20	供应商是否向客户报告可能增加不符合开发接口协议条款的风险的问题？
21	供应商是否向客户报告在其责任范围内和其分包商责任范围内的开发活动中发生的安全异常？
22	是否分析已识别出的潜在影响供应商交付成果的安全异常，并采取措施予以解决？双方是否就谁来执行所需的行动达成协议？
23	供应商是否确定客户的安全要求是否可行，以及 6.4.1 和 6.4.2 的要求是否满足？若不可行/不满足，客户是否重新检查安全要求并做适当的修改，以确保安全要求定义的正确性？
24	供应商是否向客户传达其职责范围以外但供应商认为为确保实现功能安全所必要的相关项的要素的安全要求？
25	在导出用于当前开发的安全要求时，按照 GB/T 34590.2—2022 中的 5.4.2.6，双方是否都考虑了从之前相似开发中所获得的经验？
26	供应商是否向客户报告安全计划中制定的各项任务和里程碑节点上所取得的进展？
27	供应商和客户是否就报告的内容和提交的日期达成一致？
28	对于分配了安全要求的最高 ASIL 等级为 ASIL（B）、C 或 D 的要素，在 DIA 中是否指定哪个组织按照 GB/T 34590.2—2022 对供应商开发的要素或工作成果执行功能安全评估活动？
29	对于分配了安全要求的最高 ASIL 等级为 ASIL（B）、C 或 D 的要素，在 DIA 中是否规定了供应商功能安全评估活动的计划？
30	对于分配了安全要求的最高 ASIL 等级为 ASIL（B）、C 或 D 的要素，供应商是否向客户提供功能安全评估报告？包括供应商对所开发的要素是否符合来自客户的安全要求的评估？以及所实施的流程是否满足实现功能安全的准则？
31	对于分配了安全要求的最高 ASIL 等级为 ASIL（B）、C 或 D 的要素，是否将供应商的功能安全评估活动的结果提供给客户和供应商？

表 10　分布式开发的接口审核及评估检查清单（续）

序号	检查点
32	供应商是否向客户提供证据，证明能具备并保持 GB/T 34590.2—2022 第 7 章和 GB/T 34590.7—2022 第 5 章和第 6 章所要求的生产过程能力？
33	客户和供应商间的供应协议是否按照 GB/T 34590.2—2022 中的 7.4.2.1 明确功能安全责任，并应定义各方的安全活动
34	供应协议是否规定各方间关于安全相关特殊特性的生产监控记录和从客户退回部件的失效分析结果的访问和交换？
35	供应协议是否规定了关于交换安全相关事件和所需分析的及时的沟通渠道。对于现场问题，是否就按照已建立的现场监控过程对这些事件进行分析？

附录 D 中的表 D.1 提供了分布式开发的接口的审核及评估的说明及示例。

对于配置管理的审核及评估，应涵盖表 11 所列的检查项。

表 11　配置管理的审核及评估检查清单

序号	检查点
1	配置管理策略和计划是否合理？
2	组织架构是否包含所有和配置管理活动相关的人员角色，架构是否正确？
3	配置管理活动是否完整、描述是否清晰？
4	配置管理活动中遵循的规范是否填写完整？内容和规范版本是否正确？
5	配置管理工具环境中是否一一列举配置管理活动中所有使用的工具？
6	基线计划的阶段是否符合配置管理策略的要求？
7	基线名称是否符合配置管理策略的要求？
8	基线计划的时间是否合理且与主计划吻合？
9	基线计划是否按照安全计划的要求？
10	安全计划要求的工作成果及再次生成相关项和要素所需要的工作成果，是否按照配置管理策略，生成基线并存放？
11	在整个安全生命周期中，需要被唯一识别和重生成的工作成果、相关项和要素，在配置管理策略中是否定义其条件或目的？
12	在整个安全生命周期中，是否对配置管理进行维护？

附录 D 中的表 D.2 提供了配置管理的审核及评估的说明及示例。

对于变更管理的审核及评估，应涵盖表 12 所列的检查项。

表 12　变更管理的审核及评估检查清单

序号	检查点
1	变更管理流程是否完整？描述是否清晰？
2	在对工作成果进行变更前，是否计划和启动变更管理流程？
3	是否在变更管理计划中识别要进行变更管理的工作成果、相关项和要素？这些工作成果、相关项和要素是否满足 GB/T 34590.8—2022 中 7.4.3 的要求？
4	是否为已识别出的工作成果、相关项和要素定义实施变更管理流程的日程表？
5	组织架构是否包含所有和变更管理活动相关的人员角色，架构是否正确？
6	变更管理流程中遵循的规范是否填写完整？内容和规范版本是否正确？
7	是否为每个变更需求分配唯一的识别码？
8	每个变更需求是否至少包含以下信息： a)　日期； b)　所需变更的理由； c)　所需变更的准确描述； d)　所需变更基于的配置
9	对于每个变更需求，是否针对以下信息，对所涉及的相关项或要素、接口及关联相关项或要素进行影响分析： a)　变更需求的类型； b)　对需更改的工作成果、相关项和要素及受影响的工作成果、相关项和要素进行的识别； c)　在分布式开发的情况下，所涉及的相关方的识别及其责任； d)　变更对功能安全的潜在影响； e)　变更的实现和验证的日程表
10	变更管理工具环境中是否一一列举变更管理活动中所有使用的工具？
11	变更管理是否受到监控？
12	变更是否重新启动了安全生命周期的适用阶段？
13	变更是否进行了需求评估？
14	变更是否定义了时间节点？
15	变更是否进行了验证？
16	如果变更影响了安全相关功能或特性，是否在发布相关项前，对按照 GB/T 34590.2—2022 中 6.4.9 和 6.4.10 的功能安全评估和适用的认可评审进行了更新？
17	变更记录是否完整？

附录 D 中的表 D.3 提供了变更管理的审核及评估的说明及示例。

对于验证的审核及评估，应涵盖表 13 所列的检查项。

表 13　验证的审核及评估检查清单

序号	检查点
1	验证计划是否与主计划匹配？
2	验证计划是否包含了安全生命周期的每个阶段及子阶段？
3	验证计划的内容是否完整？
4	制定验证计划时是否考虑了所使用验证方法的充分性？
5	制定验证计划时是否考虑了需验证的工作成果的复杂性？
6	制定验证计划时是否考虑了与验证目标材料相关的前期经验？
7	制定验证计划时是否考虑了所使用技术的成熟度，或使用这些技术的风险？
8	验证规范是否对用于验证的方法进行了细化？
9	每条测试用例定义的内容是否完整？
10	对于测试，是否按使用的测试方法对测试用例进行分组？
11	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了评审？
12	是否按照 GB/T 34590.8—2022 中 9.4.1 所做的计划及按照 9.4.2 所做的规范执行验证？
13	验证是否由与待验证的工作成果的完成人不同的人执行？
14	对验证结果的评估所包含的信息是否完整？
15	用于验证的测试设备是否能提供有效的和可重复的结果？是否按照所采用的质量管理体系进行管控？

附录 D 中的表 D.4 提供了验证的审核及评估的说明及示例。

对于文档管理的审核及评估，应涵盖表 14 所列的检查项。

表 14　文档管理的审核及评估检查清单

序号	检查点
1	是否计划了文档管理过程？
2	是否将对 GB/T 34590.1～34590.12—2022 中工作成果进行了文档化管理？
3	文档是否包含相关要求的完整结果信息？
4	整个文档的结构是否考虑了内部流程和工作实践？并进行了适当的组织？
5	文档管理计划是否有记录跟踪？
6	文档指南是否明确文档的撰写要求？
7	文档指南是否定义文档的正式要素？例如应包含题目、作者和批准者、不同修订的唯一标识、变更历史、状态
8	是否能识别当前适用的文档修订(版本)或信息项？

附录 D 中的表 D.5 提供了文档管理的审核及评估的说明及示例。

对于软件工具鉴定的审核及评估，应涵盖表 15 所列的检查项。

表 15　软件工具鉴定的审核及评估检查清单

序号	检查清单
1	安全计划中是否基于考虑所使用软件工具的置信度的依据而按照 GB/T 34590.2—2022 中 6.4.5.1 对某一安全活动进行剪裁？若有，剪裁是否满足 GB/T 34590.8—2022 第 11 章的要求？
2	是否有预先确定的工具在执行其置信度水平评估或鉴定时，独立于特定安全相关项或要素的开发？若有，是否在使用该软件工具前，对预先确定的工具置信度水平的有效性或鉴定的有效性进行验证？
3	使用软件工具时，工具的使用、工具定义的环境和功能约束及其正常运行条件是否和工具评估准则或鉴定相符合？
4	是否有对软件工具使用的计划？
5	对软件工具使用的计划中是否包含： a）　软件工具的识别码和版本号； b）　软件工具的配置； c）　软件工具的使用案例； d）　软件工具执行的环境； e）　当软件工具功能异常并产生相应的错误输出时，会直接违背分配给相关项或要素的全部安全要求的最高 ASIL 等级； f）　如需要，基于确定的置信度水平和 ASIL 等级的软件工具的鉴定方法
6	为了进行软件工具评估，是否收集了软件工具相关信息： a）　软件工具的特征、功能和技术属性的描述； b）　如果适用，用户手册或其他使用指南； c）　工具运行要求的环境描述； d）　如果适用，对异常运行条件下期望的软件工具表现的描述； e）　如果适用，对已知软件工具功能异常，及恰当的安全保护、避免或应急措施的描述；及 f）　在制定软件工具要求的置信度水平过程中，识别出的对软件工具功能异常和相应错误输出的预防或探测措施
7	软件工具准则评估报告对软件工具使用的描述是否包含下述信息： a）　预期的目的； b）　输入和期望的输出； c）　如果适用，使用过程、环境的和功能的约束
8	软件工具准则评估报告中是否分析和评估了软件工具的预期使用，以确定下述内容。 a）　特定软件工具功能异常可引入或不能探测开发中安全相关项或要素中错误的可能性。这是通过工具影响（TI）等级表示的： ——当有论据表明没有这样的可能性时，应选择 TI1； ——在所有其他情况下应选择 TI2。 b）　用于预防软件工具功能异常并产生相应错误输出的措施的置信度，或用于探测软件工具存在功能异常并已产生相应错误输出的措施的置信度。这是通过工具错误探测（TD）等级表示的： ——当对预防或探测出功能异常及其相应错误输出具有高置信度时，应选择 TD1； ——当对预防或探测出功能异常及其相应错误输出具有中等置信度时，应选择 TD2； ——在所有其他情况下应选择 TD3
9	软件工具准则评估报告中是否存在对 TI 或 TD 选择的正确性是不清楚的或可疑的？若有，推荐对 TI 和 TD 进行保守评估

表 15　软件工具鉴定的审核及评估检查清单（续）

序号	检查清单
10	软件工具准则评估报告中基于为 TI 和 TD 等级确定的值，是否按照 GB/T 34590.8—2022 中表 3 来确定所要求的软件工具的置信度水平？
11	软件工具鉴定报告中，对鉴定等级为 TCL3 的软件工具，是否按照 GB/T 34590.8—2022 中表 4 列出的方法进行鉴定？
12	软件工具鉴定报告中，对鉴定等级为 TCL2 的软件工具，是否按照 GB/T 34590.8—2022 中表 5 列出的方法进行鉴定？
13	软件工具鉴定报告中，是否包含以下文档化信息？ a) 软件工具的唯一识别码和版本号； b) 软件工具划分的最高工具置信度等级，及其评估分析参考； c) 对于考虑的使用案例，当软件工具功能异常并产生相应的错误输出时，可能直接违背任何安全要求的预定义的最高 ASIL 等级或特定 ASIL 等级； d) 软件工具被鉴定的配置和环境； e) 执行鉴定的人员或组织； f) 鉴定使用的方法，按照 GB/T 34590.8—2022 中的 11.4.6.1； g) 用于鉴定软件工具的措施结果； h) 如果适用，在鉴定过程中识别出的使用约束和功能异常
14	软件工具鉴定报告中，在使用“使用中积累置信度”方法进行软件工具鉴定时，是否满足以下要求。 a) 仅当具备以下方面的证据时，才应论证软件工具在使用中积累了置信度： ——此前，已经将该软件工具用于相同的目的，具有相似的使用案例、相似的预定运行环境和相似的功能约束中； ——使用中积累置信度的理由是基于充分适当的数据； ——软件工具的定义未改变； ——在之前开发中获得的软件工具功能异常和相应错误输出的发生案例是以系统化方式累计的。 b) 通过考虑以下信息，对给定开发活动中软件工具的先前使用经验进行分析和评估： ——软件工具唯一的识别码和版本号； ——软件工具的配置； ——使用周期和使用相关数据的细节； ——软件工具的功能异常和相应错误输出的详细文档化记录，其中包含引起功能异常和错误输出的条件； ——所监控的先前版本清单，其中列出每个相关版本中解决的功能异常； ——如果适用，对已知缺陷的安全保护、避免措施、应急措施或相应错误输出的探测措施。 c) 使用中积累置信度的论证应仅对所评估的软件工具版本有效
15	软件工具鉴定报告中，在使用“工具开发流程评估”方法进行软件工具鉴定时，是否满足以下要求： a) 用于软件工具开发的流程应满足适当的标准； b) 应基于恰当的国内或国际标准对软件工具开发流程进行评估，同时提供恰当的软件开发流程被应用的证据
16	软件工具鉴定报告中，在使用“软件工具确认”方法进行软件工具鉴定时，是否满足以下要求： a) 确认措施应提供软件工具符合分类中指定用途的特定要求的证据； b) 应对确认中发生的软件工具功能异常及其相应错误输出、其可能的后果信息及避免或探测它们的措施进行分析； c) 应检查软件工具对异常运行条件的响应

附录 D 中的表 D.6 提供了软件工具鉴定的审核及评估的说明及示例。

对于在用证明的审核及评估，应涵盖表 16 所列的检查项。

表 16　在用证明的审核及评估检查清单

序号	检查点
1	是否只有当候选项符合 GB/T 34590.8—2022 中 14.4.2～14.4.5 时才使用了在用证明可信度？
2	是否按照 GB/T 34590.2—2022 中的 6.4.5 计划由在用证明得出在用证明可信度？
3	在用证明可信度是否仅来自于被候选项在用证明覆盖的安全生命周期子阶段和活动？
4	是否按照 GB/T 34590.4—2022 第 8 章在适当层面执行对相关项或要素中的在用证明要素的集成措施？
5	是否按照 GB/T 34590.4—2022 第 9 章执行了对嵌入了在用证明要素的相关项的安全确认？
6	对嵌入了在用证明的要素的相关项，其认可措施是否按照 GB/T 34590.2—2022 中的 6.4.9 和 6.4.10 考虑了在用证明及相关数据？
7	对在用证明的相关项或要素进行任何修改都是否都符合 GB/T 34590.4—2022 中 14.4.4，以保持相应的在用证明可信度？
8	在用证明的候选项描述是否包含之前使用的描述？
9	在用证明的候选项描述是否包含相应的配合要求、形式要求和功能要求？
10	如果适用，在用证明的候选项描述是否包含候选项之前使用时的安全要求及相应的 ASIL 等级？
11	如有，候选项描述是否定义了如何识别候选者，是否建立追溯关系，是否明确了候选项的内部要素和组件目录？
12	在用证明的候选项描述是否依据公司的内部评审流程进行评审？
13	在用证明分析报告是否包含候选项的设计变更和实际变更？如有，按照变更流程审核及评估变更项
14	在用证明分析报告是否包含配置数据或标定数据的变更？如有，按照变更流程审核及评估变更项
15	在用证明分析报告中的候选项是否具有不同安全目标或要求的新型应用？如有，按照变更流程审核及评估变更项
16	在用证明分析报告中候选项是否包含评估期引入的，独立于未来应用的修改？如有，是否提供在用证明状态仍然有效的证据
17	在用证明分析报告是否提供了候选项在服务期内及评估期结束后处于配置管理和变更管理下的证据？
18	在用证明分析报告是否提供了在用证明的目标值？
19	在用证明分析报告是否包含现场问题？如有，问题报告是否记录候选项运行期间，现场中任何由于候选项引起的、具有潜在安全影响的可观察的事件

附录 D 中的表 D.7 提供了在用证明的审核及评估的说明及示例。

对于 GB/T 34590.1～34590.12—2022 适用范围之外应用的接口的审核及评估，应涵盖表 17 所列的检查项。

表 17　GB/T 34590.1～34590.12—2022 适用范围之外应用的接口的审核及评估检查清单

序号	检查点
1	如有，基础车辆制造商或供应商指南是否定义了供应商与集成方的沟通方式？
2	如有，基础车辆制造商或供应商指南是否定义了集成方安全措施的实现方式？如果安全机制和供应商有关，是否与供应商评审安全措施？
3	如有，供应商是否对预期的集成用例及安全要求作出假设？如有例外，是否定义了集成方和供应商的沟通机制？
4	如有，基础车辆制造商或供应商指南是否经过集成方和供应商的联合评审？

附录 D 中的表 D.8 提供了 GB/T 34590.1～34590.12—2022 适用范围之外应用的接口的审核及评估的说明及示例。

对于未按照 GB/T 34590.1～34590.12—2022 开发的安全相关系统的集成审核及评估，应涵盖表 18 所列的检查项。

表 18　未按照 GB/T 34590 开发的安全相关系统的集成审核及评估检查清单

序号	检查点
1	如有，集成方的安全档案中是否有对应依据？
2	如有，集成方是否定义了其他安全标准与 GB/T 34590.1～34590.12—2022 定义的标准的映射关系？是否给出了其他安全标准开发的产品的相关证据，论证开发的产品符合功能安全要求的相关等级？
3	如有，集成方和供应商是否对验证准则达成一致？采取的验证措施是否通过双方的评审讨论？
4	如有，集成方的安全依据是否经过集成方和供应商的充分评审？

附录 D 中的表 D.9 提供了未按照 GB/T 34590.1～34590.12—2022 开发的安全相关系统的集成的审核及评估的说明及示例。

6.7　以汽车安全完整性等级为导向和安全为导向的分析

6.7.1　目的

本章的目标是对“以汽车安全完整性等级为导向和安全为导向的分析”的相关文档及活动进行审核及评估，以检查其定义内容是否符合功能安全开发的定义及需要。

6.7.2　审核及评估的输入

为开展以汽车安全完整性等级为导向和安全为导向的分析的审核及评估过程，应具备以下输入及其可能存在的验证报告。

a）　关于 ASIL 等级剪裁的要求分解：

　　1）　整车、系统、硬件或软件层面的架构信息更新；

　　2）　整车、系统、硬件或软件层面作为安全要求和要素属性的 ASIL 等级更新。

b）　要素共存原则：整车、系统、硬件或软件层面要素中各子要素的 ASIL 等级属性的更新。

c）　相关失效分析：

　　1）　整车、系统、硬件或软件层面的相关失效分析；

2） 整车、系统、硬件或软件层面的相关失效分析的验证报告。

d） 安全分析(归纳分析和演绎分析)：

1） 整车、系统、硬件或软件层面的安全分析；

2） 整车、系统、硬件或软件层面的安全分析的验证报告。

6.7.3 审核及评估的要求

对于 ASIL 等级分解的审核及评估，应涵盖表 19 所列的检查项。

表 19 关于 ASIL 分解审核及评估检查清单

序号	检查点
1	进行 ASIL 等级分解时是否考虑了每一个初始的安全要求？
2	初始安全要求是否被分解为冗余安全要求，并由充分独立要素实现？
3	分解后的安全要求自身是否符合初始安全要求？
4	如果在软件层面应用 ASIL 等级分解，是否在系统层面对实施分解后要求的要素间进行充分独立性验证？
5	对于分解后安全要求的 ASIL 等级的标注，是否在括号中给出安全目标的 ASIL 等级？
6	是否应用 GB/T 34590.1～34590.12—2022 允许的 ASIL 等级分解方案进行 ASIL 等级分解？

附录 E 中的表 E.1 提供了针对 ASIL 分解开展审核及评估的说明及示例。

对于实施要素共存的审核及评估，应涵盖表 20 所列的检查项。

表 20 要素共存原则检查清单

序号	检查清单
1	要素共存准则分析所考虑的要素和子要素是否存在分配的安全要求？
2	是否在合适的架构设计层面考虑共存准则？
3	要素共存分析时是否考虑到分配到要素的每个安全要求和要素包含的每个子要素？
4	如果非安全相关的系统架构要素设计和安全相关系统架构要素设计共同存在于同一系统中，是否能证明非安全相关的系统架构要素不直接或间接地违背分配给该要素的任何安全要求，即非安全系统架构要素不干扰系统中安全相关的任何子要素？
5	如果系统中存在执行不同 ASIL 等级要求，包括 QM(X)的安全相关系统架构要素，是否存在证据证明对分配给系统架构要素的每个安全要求，所考虑的系统架构要素不会直接或间接地违背分配给执行更高 ASIL 等级要求的系统架构要素的任何安全要求？否则，是否将共存安全相关子要素的最高 ASIL 等级分配给该子要素？

附录 E 中的表 E.2 提供了针对要素共存准则开展审核及评估的说明及示例。

对于相关失效分析的审核及评估，应涵盖表 21 所列的检查项。

表 21　相关失效分析检查清单

编号	检查清单
1	是否根据安全分析的结果识别出相关失效的潜在可能性？
2	是否评估了每个识别出的相关失效的潜在可能性，以判定其合理性？
3	对每个识别出的相关失效的潜在可能性和合理性评估是否考虑了分析对象（相关项或要素）的不同运行模式和运行情形？
4	如果适用，对每个识别出的相关失效的潜在可能性和合理性评估是否考虑下述这些因素？ ——随机硬件失效； ——开发故障； ——生产故障； ——安装故障； ——售后服务故障； ——环境因素； ——共同外部资源或信息失效； ——特定工况下的压力； ——老化和磨损
5	是否存在相关失效及其影响的合理性的依据？
6	在开发阶段是否发现了相关失效，是否为相关失效定义了合理的解决措施，解决措施是否按照变更管理流程进行了变更？
7	用于解决合理的相关失效的措施是否包括用于预防其根本原因的措施、控制其影响的措施或减少耦合因素的措施这些方面？
8	相关失效的分析细节程度和严格程度，是否可论证达到所要求的独立性或免于干扰的程度？

附录 E 中的表 E.3 提供了针对相关失效分析开展审核及评估的说明及示例。

对于归纳分析和演绎分析的审核及评估，应涵盖表 22 所列的以下检查项。

表 22　归纳分析和演绎分析检查清单

序号	检查清单
1	如适用，安全分析的范围是否包含了下述这些方面？ ——对安全目标和安全概念的确认； ——对安全概念和安全要求的验证； ——对可导致违背安全目标或安全要求的条件及原因的识别，包括故障和失效； ——对探测故障或失效的额外安全要求的识别； ——对探测到的故障或失效所需的响应（行为/措施）的制定； ——对为验证安全目标和安全要求是否得到满足所需的额外措施的识别，包括安全相关的车辆测试
2	是否在对应的开发阶段开展了对应的安全分析？
3	安全分析是否在恰当的开发层面开展？
4	安全分析是否基于对相关故障类型和模式有足够认知？例如：考虑来自外部的故障模式作为支持性信息
5	当适用定性分析的时，是否采用了恰当的定性分析方法？如系统、设计或流程层级的 FMEA、定性 FTA、HAZOP、定性 ETA 等

表 22　归纳分析和演绎分析检查清单（续）

序号	检查清单
6	当适用定量分析时，是否采用了恰当的定性分析方法？如定量 FMEA、定量 FTA、定量 ETA、马尔科夫(Markov)模型、可靠性框图等
7	安全分析是否根据恰当的标准或指南执行？
8	如安全分析采用归纳分析法或演绎分析法，是否按照 GB/T 34590.4—2022 中表 1 的要求开展？
9	分析结果是否表明已符合或违背相关安全目标或安全要求？
10	如果分析结果显示违背了安全目标或安全要求，其内容是否被用于导出新的避免、探测或降低影响的措施？
11	由安全分析得出的措施应作为产品开发的一部分，是否按照相应的标准在各个开发层级得以实现？
12	对于在该层级安全分析中识别到的、未被已有安全目标覆盖的新的风险，是否重新进行了危害分析和风险评估，且相应的变更按照表 8 中变更管理流程检查清单的要求实施？
13	安全分析所用到的故障模式是否和其对应的研发子阶段的详细程度相适应并保持一致？
14	如果必要，是否通过使用故障模式和分析结果来确定额外的安全相关测试用例？
15	安全分析及所有输出是否按照 GB/T 34590.8—2022 第 9 章验证过？
16	定性的安全分析是否系统性地识别哪些会违背安全目标或安全要求的故障或失效？包括相关项或要素本身、相关项或要素与其他相关项或要素之间的交互，以及相关项或要素的使用
17	定性的安全分析是否对每个已识别的故障的后果都进行评估，以确认违背安全目标或安全要求的潜在可能性？
18	定性的安全分析是否识别每个已识别故障的原因？
19	定性的安全分析是否识别或支持识别安全概念的潜在薄弱环节，包括对处理诸如潜在故障、多点故障、共因失效及级联失效这种异常的安全机制的无效性？
20	如果定量分析用于补充定性分析，该分析是否考虑了用于支持硬件架构度量的指标和会违背安全目标和安全要求的硬件随机失效评估的定量数据？
21	如果定量分析用于补充定性分析，该分析是否考虑了系统性地识别那些会违背安全目标或安全要求的故障或失效？
22	如果定量分析用于补充定性分析，该分析是否考虑了安全概念潜在的薄弱点，包括对安全机制的不足进行评估和分级？
23	如果定量分析用于补充定性分析，该分析是否考虑了诊断测试时间间隔，紧急运行时间间隔和从故障探测到修复的时间间隔？
24	从(系统、软件、硬件)安全分析到(系统、软件、硬件)需求规范或(系统、软件、硬件)需求概念的可追溯性是否完整？如适用，相应的变更流程是否完成？

附录 E 中的表 E.4 提供了针对归纳分析和演绎分析开展审核及评估的说明及示例。

附 录 A
（资料性）
审核及评估报告示例

A.1 功能安全审核及评估概览

A.1.1 审核及评估的对象

审核及评估的对象可包括例如被审核/评估的组织名称、被审核/评估对象名称、审核/评估的阶段（如计划/开发/测试/生产等）。

A.1.2 审核及评估的目的

明确本次审核及评估的目的或目标。

A.1.3 参与审核及评估的人员相关信息

参与审核及评估的人员相关信息例如姓名、角色、部门、职责等。

A.1.4 应审人员相关信息

应审人员相关信息例如姓名、角色、部门、职责、项目角色等。

注：审核及评估的应审团队包括项目经理、功能安全经理、系统项目经理、系统集成负责人、系统集成工程师、软件项目经理、软件开发工程师、硬件项目经理、硬件工程师、需求工程师、架构工程师、软件设计工程师、测试经理、测试工程师、质保经理、生产经理等人员。

A.1.5 审核及评估的类型

示例：本次审核及评估的类型为：

[X]初始审核及评估

[ ]复审/复评

……

A.1.6 审核及评估的范围

示例见图 A.1。

章节	部分											
	1	2	3	4	5	6	7	8	9	10	11	12
1～4												
5		√	√			—	—	—	√			
6		√	√	√	—	—	—	√	—			
7			√	—	—	—	—	√	√			
8				—	—	—		√	√			
9					—	—		—				
10					—	—		—				
11						—		—				
12												
13												
…												
附录 C					—	—						
…												

注：√表示范围内；—表示范围外；□表示不要求。

图 A.1　审核及评估的范围示例

A.1.7　审核及评估的策略

示例：本轮功能安全审核采用抽查法。

A.1.8　审核及评估的局限

示例：本轮功能安全审核采用抽查法。由于时间限制，未能对所有工作成果的所有内容进行完整的评估。

A.1.9　审核及评估文件清单

示例：审核及评估文件清单示例见表 A.1。

表 A.1　审核及评估文件清单示例

编号	文件名称	版本	发布日期
1	相关项定义	V1.0	××××年××月××日
2	危害分析和风险评估	V1.0	××××年××月××日
3	……	……	……

A.1.10　审核及评估计划安排

对审核及评估过程中各个活动的前提条件、时间和参与人员进行合理的安排，以确保各个活动有序且充分的开展，达到审核及评估的目的。

A.2　审核及评估汇总

A.2.1　审核及评估问题清单

审核及评估问题清单内容可包括：问题编号、问题对应文档的识别信息（例如文档编号、文档名称或

文档链接)、问题在文档中的位置、问题描述、问题提出人、问题提出时间、问题预期解决时间等信息。

A.2.2 审核及评估的结论

示例：根据审核及评估问题清单和审核及评估的评分规则，本轮审核及评估的结论是：

——[X]接受；

——[ ]有条件接受；

——[ ]拒绝。

审核及评估的结论示例见表 A.2。

表 A.2 审核及评估的结论示例

结论	通过判定准则	示例
拒绝	存在影响安全目标实现的问题，应经过整改后才能开展后续安全活动	SPFM 不符合要求
有条件接受	a) 基本达成相关项的功能安全，尽管存在已识别出的未解决的问题；及 b) 有条件接受的建议应包含与功能安全评估标准的偏差以及这些偏差可被接受的依据	追溯性没有充分保证
接受	a) 无影响功能安全目标实现的相关问题；或 b) 残余风险非常低，经过适当的整改活动后，即可消除问题	—

附 录 B
（资料性）
功能安全管理

B.1 整体安全管理的审核及评估

功能安全规章和流程的审核及评估的说明及示例，见表 B.1。

能力管理证据和质量管理体系证据的审核及评估的说明及示例，见表 B.2。

已识别的安全异常报告的审核及评估的说明及示例，见表 B.3。

表 B.1 功能安全规章和流程的审核及评估的说明及示例

序号	检查清单	说明及示例
1	功能安全规章和流程是否存在且可用？	应检查是否有功能安全规章和流程
2	功能安全规章和流程是否存在版本管理？	应检查功能安全规章和流程是否纳入版本管理，版本变更记录是否清晰
3	功能安全规章和流程中是否建立了与实现功能安全相关的其他领域[如预期功能安全、信息安全、非电气/电子(E/E)系统相关安全等]之间的有效沟通渠道？是否合理？	应检查功能安全规章和流程中是否建立了与实现功能安全相关的其他领域(如预期功能安全、信息安全、非电气/电子系统相关安全等)之间的有效沟通渠道，是否合理。 例如： 1) 安全负责人应在月度定期会议上与质量负责人、信息安全负责人和机械负责人沟通。月度定期会议应明确安全相关问题，并提出持续改进的建议。 2) 由于信息安全事件响应而导致的设计变更，需要参与评估对功能安全的潜在影响
4	功能安全规章和流程中是否明确了功能安全的实现所需资源的提供方案？是否合理？	应检查功能安全规章和流程中是否明确定义了功能安全实现所需资源的提供方案，方案是否合理。 例如：安全负责人应支持安全工具的采购，人力资源的调配，数据库的建立与维护，指南和工作说明
5	功能安全规章和流程中是否规定了持续改进流程？是否合理？	应检查功能安全规章和流程中是否有持续改进流程，是否合理。 例如： 1) 每周与安全小组进行安全沟通： ——交流项目的安全经验； ——沟通独立于项目的安全活动； ——识别系统性安全异常以进行改进； ——讨论找到的解决方案、通用方法和改进可能性； ——识别和管理在后续项目中推出解决方案的方法； ——规划和改进安全培训、流程等。 2) 项目结束后与安全经理召开项目经验总结会议： ——从工程中识别安全异常； ——规划未来的改进。 3) 每月的安全状态报告： ——落实最高管理层的安全意识； ——提高工程团队的安全意识； ——允许对安全要求(如资源)进行长期规划。 4) 与安全没有直接关系的其他改进计划

表 B.1　功能安全规章和流程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	功能安全规章和流程中是否给予负责实现或维护功能安全、执行或支持安全活动的人员以足够的权限来履行他们的职责？是否合理？	应检查功能安全规章和流程中组织结构和人员角色职责和权限的定义，是否合理。 例如：如果存在任何安全异常，项目安全经理有权反对产品发布。安全负责人应协助将安全异常反馈至公司负责人
7	流程中是否对应 GB/T 34590.1～34590.12—2022 各部分工作成果规定的交付物的要求？	例如： 1）　是否定义了软件架构设计规范的开发流程？ 2）　是否定义了软件架构设计规范的模板且在项目中进行了实施？ 3）　软件架构设计规范模板是否与已定义的开发流程保持一致？ 4）　定义的软件架构设计规范模板是否可覆盖下面列出的评估检查点？
8	交付物的内容是否涵盖 GB/T 43253—2023 定义的评估检查点？	根据具体的交付物选择对应的审核及评估要点检查清单

表 B.2　能力管理证据的审核及评估的说明及示例

序号	检查清单	说明及示例
1	能力管理证据是否存在且可用？	应检查是否有能力管理证据且可用。 例如： 1）　能力管理证据中的人员是否在职； 2）　人员职能与组织架构是否匹配
2	能力管理证据文档是否使用了功能安全流程规定的模板？是否存在版本管理？	应检查能力管理证据是否采用的功能安全流程规定的模板，是否纳入版本管理，版本变更记录是否清晰
3	执行安全生命周期活动的人员是否具有与其职责相匹配的技能水平、能力和资质？	应检查执行安全生命周期活动的人员是否具有与其职责相匹配的技能水平、能力和资质。 例如： 为了评估执行满足 GB/T 34590.1～34590.12—2022 的活动所需的技能、能力和资质，可考量以往的专业活动经验，如： 1）　相关项专业领域的知识； 2）　相关项环境方面的专业知识； 3）　管理经验； 4）　生产、运行、服务和报废方面的专业知识
4	质量管理体系证据是否存在且可用？	应检查是否具有质量管理体系且可用。 例如：IATF 16949、ISO 9001 等

表 B.3　已识别的安全异常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	已识别的安全异常报告是否存在且可用？	应检查是否有已识别的安全异常报告
2	安全异常报告是否使用了功能安全流程规定的模板？是否存在版本管理？	应检查安全异常报告是否采用的功能安全流程规定的模板，是否纳入版本管理，版本变更记录是否清晰
3	功能安全异常管理流程是否存在且可用？	应检查是否有功能安全异常管理流程
4	功能安全异常管理流程是否存在版本管理？	应检查功能安全异常管理流程是否纳入版本管理，版本变更记录是否清晰
5	功能安全异常管理流程是否可支持及时、有效地分析、评估、解决和管理已识别的安全异常，直至关闭？	应检查功能安全异常管理流程的合理性，是否可支持及时、有效地分析、评估、解决和管理已识别的安全异常，直至关闭。 例如： 功能安全经理负责所有安全异常，每周组织一次安全会议，在团队内（功能安全工程师、开发工程师、测试工程师、生产功能安全工程师、售后功能安全工程师等）交流安全情况，安全经理将识别到的安全异常上传到相关管理软件或工具中并跟踪状态，指定专人负责关闭异常。这些异常应在产品发布前关闭。识别出的安全异常应在一周内进行分析、评估、解决和管理，直至关闭。如果需要超过一周，应提前通知项目功能安全经理并获得批准
6	功能安全异常管理流程中安全异常关闭的要求是否明确？ a) 基于某一依据，实施了充分的安全措施以解决安全异常，且安全措施的有效性得到了验证；或 b) 基于某一依据，将安全异常评估为不构成不合理风险并将其关闭	应检查功能安全异常管理流程中的安全异常关闭部分，是否可保证其的关闭符合 GB/T 34590.1～34590.12—2022 的要求。 例如：只有在有专门的根本原因分析报告和执行报告的情况下，安全异常才能提前关闭。如果没有合理依据，则无法关闭安全异常
7	功能安全异常管理流程中，针对关闭安全异常的依据是否具备记录和评审的环节？	应检查功能安全异常管理流程中是否规定了关闭安全异常的依据以及评审记录方式。 例如：在相关管理软件或工具中上传关闭安全异常的依据文件，提起相关人评审，评审通过后异常关闭。关闭安全异常的依据和评审信息在系统中记录。对关闭安全异常的依据的评审可作为功能安全评估的一部分
8	功能安全异常管理流程中，针对未完成关闭的安全异常是否有及时上报给负责功能安全的人员的路径？	应检查功能安全异常管理流程中未完成关闭的安全异常的上报路径，是否及时上报给负责功能安全人员。 例如：在相关管理软件或工具中，未完成关闭的安全异常清单，每天通知安全经理，每周通知项目经理。如果此时进行功能安全评估，则负责功能安全评估的人员是需被明确传达安全异常的人员之一

B.2 项目相关的安全管理审核及评估

相关项层面的影响分析和要素层面的影响分析的审核及评估的说明及示例，见表 B.4。

安全计划的审核及评估的说明及示例，见表 B.5。

安全档案的审核及评估的说明及示例，见表 B.6。

表 B.4 相关项层面的影响分析和要素层面的影响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	相关项层面的影响分析是否存在且可用？	应检查是否有相关项层面影响分析
2	相关项层面的影响分析是否使用了功能安全流程规定的模板？是否存在版本管理？	应检查相关项层面的影响分析是否采用的功能安全流程规定的模板，是否纳入版本管理，版本变更记录是否清晰
3	在对相关项或其环境修改的情况下，是否正确识别并描述了应用于相关项的修改，包括设计的修改、实现方式的修改、与环境相关的修改？	应检查在对相关项或其环境修改的情况下，是否正确识别并描述了应用于相关项的修改，包括设计的修改、实现方式的修改、与环境相关的修改
4	在对相关项或其环境修改的情况下，修改对功能安全的影响的评估是否合理？	应检查在对相关项或其环境修改的情况下，修改对功能安全的影响是否合理。 例如：新增车道偏离抑制功能需求：由于新增车道偏离抑制功能，需要在进行危害分析及风险评估等安全分析手段后判断是否有新增或修改功能安全要求，若有，需要在设计及开发阶段进行明确
5	在对相关项或其环境修改的情况下，受修改影响的安全活动是否合理？	应检查在对相关项或其环境修改的情况下，受修改影响的安全活动是否合理。 例如：新增车道偏离抑制功能需求：对于相关项定义、危害分析和风险评估、功能安全概念，及后续系统硬件软件对于 ASIL 等级变更或新增的需求所涉及的工作成果会有影响
6	要素层面的影响分析是否存在且可用？	应检查是否有要素层面的影响分析
7	要素层面的影响分析是否使用了功能安全流程规定的模板？是否存在版本管理？	应检查要素层面的影响分析是否采用的功能安全流程规定的模板，是否纳入版本管理，版本变更记录是否清晰
8	在复用现有要素的情况下，是否识别出运行环境的修改，包括其导致的对要素的修改？	应检查要素层面的影响分析中是否识别出运行环境的修改，包括其导致的对要素的修改
9	在复用现有要素的情况下，分配给其的安全要求的符合性是否评估清楚？是否合理？	应检查要素层面的影响分析中，分配给其的安全要求的符合性是否评估清楚
10	在复用现有要素的情况下，受修改影响的安全活动是否已列出？是否合理？	应检查要素层面的影响分析中，受修改影响的安全活动是否已列出
11	与复用要素有关的现有安全相关文档是否评估清楚？其是否支持将要素集成到相关项，或将要素集成到另一个要素？评估结论是否合理？	应检查要素层面的影响分析中，与复用要素有关的现有安全相关文档是否评估清楚，是否支持将要素集成到相关项，或将要素集成到另一个要素，评估结论是否合理

表 B.5　安全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	安全计划是否存在且可用？	应检查是否有安全计划
2	安全计划是否使用了功能安全流程规定的模板？是否存在版本管理？	应检查安全计划是否采用的功能安全流程规定的模板，是否纳入版本管理，版本变更记录是否清晰
3	安全经理是否对安全计划进行维护并监控安全活动的进度按照安全计划进行？	应检查安全计划中安全经理对安全计划的维护方案，对安全活动进度的监控方案。 例如：功能安全经理每周组织一次安全会议，监控安全活动的实施情况，并根据实际进展对安全计划进行维护
4	安全活动的执行责任，是否按照 GB/T 34590.2—2022 中 5.4.2.7 和 5.4.4 的要求分配？	应检查安全计划中安全活动的责任分配，是否按照标准执行。 例如：见表 B.7
5	安全计划是否都被项目计划引用，或包含在项目计划中，并使安全活动是可区分的？	应检查项目计划中，是否引用了安全计划，或者包含了安全计划，并且使安全活动是可区分的
6	安全计划中是否体现了实现功能安全的活动计划和流程计划？	应检查安全计划中是否体现了实现功能安全的活动计划和流程计划，包括下述序号 7～序号 29
7	安全计划中是否体现了独立于项目的安全活动？	应检查安全计划中是否体现了独立于项目的安全活动
8	如果安全活动被剪裁，安全计划中是否体现了对安全活动的剪裁？	如果安全活动被剪裁，应检查安全计划中是否体现了对安全活动的剪裁。 例如：见表 B.8
9	如果安全活动被剪裁，安全计划中对安全活动剪裁的理由说明是否充分、存在、可接受？	如果安全活动被剪裁，应检查安全计划中对安全活动剪裁的理由说明是否充分、存在、可接受？ 例如：见表 B.8
10	如果按照影响分析结果而对某一安全活动的剪裁，剪裁是否满足表 5 的要求？	应检查如果按照影响分析结果而对某一安全活动的剪裁，剪裁是否满足表 5 的要求
11	如果按照在用证明结果而对某一安全活动的剪裁，剪裁是否满足表 16 的要求？	应检查如果按照在用证明结果而对某一安全活动的剪裁，剪裁是否满足表 16 的要求
12	如果按照硬件要素评估而对某一安全活动的剪裁，剪裁是否满足 GB/T 43253.4— 2023 中表 13 的要求？	应检查如果按照硬件要素评估而对某一安全活动的剪裁，剪裁是否满足 GB/T 43253.4—2023 中表 13 的要求
13	如果是由于软件组件鉴定而对某一安全活动进行剪裁，剪裁是否满足 GB/T 43253.3—2023 中表 9 的要求？	应检查如果是由于软件组件鉴定而对某一安全活动进行剪裁，剪裁是否满足 GB/T 43253.3—2023 中表 9 的要求

表 B.5　安全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
14	如果基于考虑所使用软件工具的置信度的依据而对某一安全活动的剪裁，剪裁是否满足表 15 的要求？	应检查如果基于考虑所使用软件工具的置信度的依据而对某一安全活动的剪裁，剪裁是否满足表 15 的要求
15	如果由于要素被开发为独立于环境的安全要素（SEooC）而对某一安全活动进行剪裁，独立于环境的安全要素的开发是否基于一个需求规范，该需求规范是否来自对预期用途和环境的假设，包括其外部接口？	应检查由于要素被开发为独立于环境的安全要素（SEooC）而对某一安全活动的剪裁，独立于环境的安全要素的开发是否基于一个需求规范，该需求规范是否来自对预期用途和环境的假设，包括其外部接口
16	如果由于要素被开发为独立于环境的安全要素（SEooC）而对某一安全活动进行剪裁，当安全要素被集成到其目标应用中时，对独立于环境的安全要素的预期用途和应用环境的假设是否进行了验证？	应检查由于要素被开发为独立于环境的安全要素（SEooC）而对某一安全活动的剪裁，当安全要素被集成到其目标应用中时，对独立于环境的安全要素的预期用途和应用环境的假设是否进行了验证
17	针对于 T&B 的相关项的开发：如果某个应用超出了 GB/T 34590.1～34590.12—2022 的范围，且该应用正在与已根据这些标准开发的基础车辆或相关项进行对接，安全活动的剪裁是否满足表 17 的要求？	应检查针对于 T&B 的相关项的开发：如果某个应用超出了 GB/T 34590.1～ 34590.12—2022 的范围，且该应用正在与已根据这些标准开发的基础车辆或相关项进行对接，安全活动的剪裁满足表 17 的要求
18	针对于 T&B 的相关项的开发：如果开展安全活动，以确保未按照 GB/T 34590.1～ 34590.12—2022 开发的系统或组件，满足集成到按照这些标准开发的相关项中所需的功能安全水平，安全活动的剪裁是否满足表 18 的要求？	应检查针对于 T&B 的相关项的开发：如果开展安全活动，以确保未按照 GB/T 34590.1～34590.12—2022 开发的系统或组件，满足集成到按照这些标准开发的相关项中所需的功能安全水平，安全活动的剪裁是否满足表 18 的要求
19	如果适用，安全活动的计划是否完整包含概念阶段计划？	如果适用，应检查安全活动的计划是否完整包含概念阶段计划，是否满足 GB/T 34590.3—2022 的要求
20	如果适用，安全活动的计划是否完整包含系统层面计划？	如果适用，应检查安全活动的计划是否完整包含系统层面计划，是否满足 GB/T 34590.4—2022 的要求
21	如果适用，安全活动的计划是否完整包含硬件层面计划？	如果适用，应检查安全活动的计划是否完整包含硬件层面计划，是否满足 GB/T 34590.5—2022 的要求
22	如果适用，安全活动的计划是否完整包含软件层面计划？	如果适用，应检查安全活动的计划是否完整包含软件层面计划，是否满足 GB/T 34590.6—2022 的要求
23	安全计划中是否完整包含支持过程计划？如果适用，是否包含对定义与分布式开发中其他方的安全计划接口的开发接口协议（DIA）的引用？	应检查安全计划中是否完整包含支持过程计划，是否满足 GB/T 34590.8—2022 的要求；如果适用，是否包含对定义与分布式开发中其他方的安全计划接口的开发接口协议（DIA）的引用，是否满足 GB/T 34590.8—2022 第 5 章的要求

表 B.5　安全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
24	安全计划中是否完整包含集成和验证活动计划？	应检查安全计划中是否完整包含集成和验证活动计划，是否满足 GB/T 34590.3—2022、GB/T 34590.4—2022、GB/T 34590.5—2022、GB/T 34590.6—2022 和 GB/T 34590.8—2022 第 9 章的要求
25	安全计划中是否完整包含安全确认活动计划？	应检查安全计划中是否完整包含安全确认活动计划，是否满足 GB/T 34590.4—2022 第 8 章的要求
26	安全计划中是否包含认可评审、功能安全审核和功能安全评估的日程安排？	应检查安全计划中是否包含认可评审、功能安全审核和功能安全评估的日程安排
27	如果适用，安全计划是否完整包含了相关失效分析的计划？	如果适用，应检查安全计划是否完整包含了相关失效分析的计划，是否满足 GB/T 34590.3—2022、GB/T 34590.4—2022、GB/T 34590.5—2022、GB/T 34590.6—2022、GB/T 34590.9—2022 第 7 章、GB/T 34590.9—2022 第 8 章的要求
28	如果适用，安全计划是否完整包含了候选项的在用证明分析的计划？	如果适用，应检查安全计划是否完整包含了候选项的在用证明分析的计划，是否满足 GB/T 34590.8—2022 第 14 章的要求
29	如果适用，安全计划是否完整包含了软件工具鉴定的计划？	如果适用，应检查是否完整包含了软件工具鉴定的计划，是否满足 GB/T 34590.8—2022 第 11 章的要求
30	安全活动的计划是否包括：目标；对其他活动或信息的依赖性；负责执行活动的人员；执行活动所需的资源、起始时间、结束时间和持续时间；相应工作成果的识别？	应检查安全活动计划是否包含目标；对其他活动或信息的依赖性；负责执行活动的人员；执行活动所需的资源、起始时间、结束时间和持续时间；相应工作成果的识别
31	当修改相关项和现有相关项环境时，或当复用要素时，GB/T 34590.1～34590.12—2022 的参考安全生命周期是否根据相应影响分析的结果进行剪裁？	当修改相关项和现有相关项环境时，或当复用要素时，应检查安全计划 GB/T 34590.1～34590.12—2022 的参考安全生命周期是否根据相应影响分析的结果进行剪裁
32	当修改相关项和现有相关项环境时，或当复用要素时，安全计划中是否相应地识别、描述和返工需要创建或更新的受影响的工作成果？	当修改相关项和现有相关项环境时，或当复用要素时，应检查安全计划中是否相应地识别、描述和返工需要创建或更新的受影响的工作成果
33	当修改相关项和现有相关项环境时，或当复用要素时，如果其安全文档不符合 GB/T 34590.1～34590.12—2022，安全计划中是否明确必要的活动以符合标准中的相应要求？	当修改相关项和现有相关项环境时，或当复用要素时，如果安全文档不符合 GB/T 34590.1～34590.12—2022，应检查安全计划中是否明确必要的活动以符合标准中的相应要求
34	安全计划是否在每个阶段开始时进行了更新和细化？	应检查安全计划是否在每个阶段开始时进行了更新和细化
35	安全计划要求的工作成果是否保持最新状态？	应检查安全计划要求的工作成果是否保持最新状态

表 B.5　安全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
36	如果是分布式开发，则客户和供应商是否均有针对各自的安全活动制定安全计划？	如果是分布式开发，应检查客户和供应商是否均有针对各自的安全活动制定安全计划
37	如果缺乏来自相关先前子阶段的信息，是否在缺乏信息也不会导致功能安全方面的不合理风险的情况下才开始后续子阶段？	应检查如果缺乏来自相关先前子阶段的信息，是否在缺乏信息也不会导致功能安全方面的不合理风险的情况下才开始后续子阶段
38	每一项安全计划所要求的工作成果是否分别服从配置管理、变更管理以及文档管理？纳入管理时间是否不迟于“产品开发：系统层面”阶段的启动时间？	应检查每一项安全计划所要求的工作成果是否分别服从配置管理、变更管理以及文档管理，纳入管理时间是否不迟于“产品开发：系统层面”阶段的启动时间

表 B.6　安全档案的审核及评估的说明及示例

序号	检查清单	说明及示例
1	安全档案是否存在且可用？	应检查是否有安全档案
2	安全档案是否使用了功能安全流程规定的模板？是否存在版本管理？	应检查安全档案是否采用的功能安全流程规定的模板，是否纳入版本管理，版本变更记录是否清晰
3	安全档案的建立是否依照安全计划？	应检查安全档案与安全计划中安全活动的一致性
4	安全档案中提供的论证是否合理且充分？	应检查安全档案中提供的论证是否合理
5	安全档案中参考的工作成果是否存在且充分完整？	应检查安全档案中参考的成果是否存在且充分完整
6	安全档案中参考的工作成果是否有可追溯性？	应检查安全档案中参考的成果是否有可追溯性
7	安全档案中参考的工作成果内部或成果之间是否无矛盾点？	应检查并确保安全档案中参考的工作成果内部或成果之间无矛盾点
8	安全档案中参考的工作成果是否满足如下要求？即：既没有导致违背安全目标的问题，或存在的问题是可控的并且有计划得到解决	安全档案中参考的工作成果是否满足如下要求，既没有导致违背安全目标的问题，或存在的问题是可控的并且有计划得到解决

表 B.7、表 B.8 为支持表 B.5 的相关示例。

表 B.7　安全计划中安全活动的责任分配示例

角色	职责	姓名	电子邮件	联系方式	所需技能	是否匹配	培训	……
安全经理	——识别需要向安全评估员提供安全档案的项目； ——影响分析和计划所有的安全活动； ——通过剪裁模板，编制项目具体的安全计划； ——在安全生命周期内维护安全计划； ——监控安全活动的流程； ——编制安全报告； ——管理项目相关安全问题； ——协调安全工程师的支持活动； ……	××	××	××	——×年 GB/T 34590、ISO 26262 项目安全经理经验 ……	匹配	—	
安全工程师	——将安全问题上报给安全负责人； ——确保计划中的概念阶段安全活动得到执行并支持安全经理； ——编制相关项定义； ——编制危害分析及风险评估； ——编制功能安全概念； ……							
生产安全工程师	——确保生产过程中要实施的安全相关要素的特殊特性； ——编制生产计划的安全相关内容； ——编制生产控制计划的安全相关内容； ——评审可生产性要求规范； ——评审生产过程能力报告； ——识别生产过程中的安全相关问题并向项目职能安全经理报告； ……							
…	……							

表 B.8　安全活动的剪裁示例

……	工作成果	剪裁原因	剪裁	……
……	要素层面影响分析	新开发项目，不涉及要素复用	是	……

B.3　生产、运行、服务、报废的安全管理审核及评估

关于生产、运行、服务和报废的安全管理的审核及被评估的说明及示例，见表 B.9。

表 B.9　关于生产、运行、服务和报废的安全管理审核及评估的说明及示例

序号	检查清单	说明及示例
1	关于生产、运行、服务和报废的安全管理证据是否存在且可用？	应检查是否有关于生产、运行、服务和报废的安全管理证据
2	关于生产、运行、服务和报废的安全管理证据是否使用了功能安全流程规定的模板？是否存在版本管理？	应检查关于生产、运行、服务和报废的安全管理证据是否使用了功能安全流程规定的模板，是否纳入版本管理，版本变更记录是否清晰
3	实现并维护相关项在生产、运行、服务和报废阶段的功能安全的责任人是否明确？	应检查关于生产、运行、服务和报废的安全管理证据中，是否体现了此阶段的安全责任人，以实现和维护相关项的生产、运行、服务和报废功能安全
4	在相关项及其要素的生产、运行、服务和报废过程中，相关项的功能安全活动计划是否满足 GB/T 34590.7—2022 第 5 章的要求？	应检查在相关项及其要素的生产、运行、服务和报废过程中，相关项的功能安全活动计划是否满足 GB/T 34590.7—2022 第 5 章的要求
5	在相关项及其要素的生产、运行、服务和报废过程中，相关项的功能安全活动是否满足 GB/T 34590.4—2022 的要求，在系统层面的产品开发期间启动？	应检查在相关项及其要素的生产、运行、服务和报废过程中，相关项的功能安全活动是否满足 GB/T 34590.4—2022 的要求，在系统层面的产品开发期间启动
6	在相关项及其要素的生产、运行、服务和报废过程中，相关项的功能安全活动是否按照 GB/T 34590.7—2022 第 6 章和第 7 章执行？	应检查在相关项及其要素的生产、运行、服务和报废过程中，相关项的功能安全活动是否按照 GB/T 34590.7—2022 第 6 章和第 7 章执行。 例如：生产、运行、服务和报废安全工程师应在配置管理下，对生产、运行、服务和报废过程中安全计划要求的安全相关工作成果进行检查。工作成果应正确实施和维护。安全工程师每周检查一次，并做好记录
7	是否存在相关项在生产、运行、服务和报废阶段的功能安全的流程？是否合理？	应检查是否有相关项在生产、运行、服务和报废阶段的功能安全的流程
8	如果在生产、运行、服务或报废期间相关项有变更，是否对生产发布变更进行管理？	应检查在关于生产、运行、服务和报废的安全管理证据中，针对如果在生产、运行、服务或报废期间相关项有变更，生产发布的变更管理方案。 例如：生产发布变更服从于变更管理

附 录 C
（资料性）
生产、运行、服务和报废

生产、运行、服务和报废的审核及评估的说明及示例见表 C.1。

表 C.1 关于生产、运行、服务和报废的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否计划了相关项及其要素的生产过程？ 包括： ——对生产的要求； ——安全相关的特殊特性； ——要素的处理和管理条件； ——产品开发过程中定义的配置； ——从以前发布的生产计划中获得的经验总结； ——涉及安全相关的特殊特性的生产过程、设备、工具和测试设备的适宜性； ——人员的能力	1） 对生产的要求： 装配指导说明（例如：传感器的标定和设置）。 IPC（印刷电路协会）相关标准的要求。 产品对应示例：转向系统的角度传感器的中位标定（即零位标定）偏差小于 0.6°。 2） 安全相关的特殊特性： 特定的过程参数（例如：回流焊的温度范围、紧固扭矩）、材料特性、制造公差和要素的配置。 产品应对示例：BMS 的电路板的回流焊的温度范围。 3） 要素的处理和管理条件： ECU 软件的正确程序设定。 产品对应示例：ECU 的 EOL 验证、ECU 写配置字的序号
2	生产计划是否描述了实现相关项或要素的功能安全而要求的生产步骤、顺序和方法？ 包括： ——生产工艺流程和指导说明； ——生产工具和设备； ——可追溯性措施的实施； ——如果适用，专用措施的实施	1） 生产工艺流程和指导说明： 有三个或更少引脚的元器件的不良焊接点的返工说明。 2） 可追溯性措施的实施： 对要素使用标签
3	是否已定义一个流程作为生产过程的一部分，以确保正确版本的嵌入式软件及其相关标定数据被写入 ECU 中？	1） 使用校验和，目的是将下载的可执行数据及标定数据的校验和，与该特定车辆配置的正确校验和相比较。 2） 从下载到 ECU 中的软件回读零件号，并与物料清单中特定车辆的目标零件号进行对比；同样也回读下载的标定数据并与物料清单中针对该特定车辆的标定数据进行对比
4	是否识别合理可预见的生产过程失效及其对功能安全的影响，并实施恰当的措施以处理相关过程失效？ 包括：过程失效模式和影响分析（PFMEA）	过程失效模式和影响分析（PFMEA）
5	是否在制定生产控制计划时考虑了对相关项或要素的控制描述（含控制的准则），以及安全相关的特殊特性？	—

表 C.1　关于生产、运行、服务和报废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	是否在生产控制计划中描述控制步骤的顺序和方法，以及必要的测试设备、工具和测试准则？	—
7	在计划生产时识别的安全要求，是否已经以适当的方式反馈给负责系统、硬件和软件开发的人员？	在接插件中增加防错功能（波卡纠偏）以确保在装配中它被正确地插入 ECU
8	生产、运行、服务和报废的变更，如影响相关项或其要素，是否已经按要求进行管理？	—
9	是否已制定相关项的运行、服务和报废过程的计划，并考虑以下因素： ——维护和维修的要求； ——为确保车辆安全运行而应具备的用户须知信息的要求； ——报废的要求； ——紧急救援服务的要求； ——报警和降级策略； ——现场监控流程； ——要素处理的条件； ——在生产发布文件中定义的配置； ——参与人员的能力	1）　要素处理的条件： 硬件要素的允许存储时间； ECU 上软件的正确刷写。 2）　在生产发布文件中定义的配置： 在维修过程中，硬件、软件和软件标定数据允许的配置
10	服务计划是否已描述对相关项或要素的维护活动的顺序和方法，包括维护间隔以及需要的工具？	—
11	服务指导说明是否描述了如下内容： ——服务的流程、方法、工作步骤和诊断程序； ——工具和设备； ——用于验证安全相关的特殊特性的控制步骤的顺序和方法，以及控制标准； ——相关项或要素的有关配置，包括可追溯性措施； ——车辆允许的相关项或要素的功能关闭，及其所导致的车辆的任何变更； ——当功能关闭和其他变更发生时，需告知驾驶员； ——备件的供应	1）　工具和设备： 程序设定、传感器标定和诊断设备。 2）　相关项或要素的有关配置，包括可追溯性措施： 对要素使用标签，确保可追溯性。 3）　当功能关闭和其他变更发生时，需告知驾驶员： 通知驾驶员某项辅助功能已经被关闭

表 C.1　关于生产、运行、服务和报废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	用户信息，包括用户手册，是否提供了正确使用相关项或要素的有关指导说明和警告，如果适用，还应提供如下信息： ——相关功能（即预期使用、状态信息或用户交互）及其运行模式的描述； ——当报警和降级策略表明失效发生时，为确保可控性所需的用户行为的描述； ——当报警和降级策略表明失效发生时，对用户所期望的服务活动的描述； ——关于与第三方产品交互所导致的已知危害的警告； ——为了防止驾驶员误解或误用，安全相关的整车新功能的正确使用的警告	1）　关于与第三方产品交互所导致的已知危害的警告： 用户应被告知，当使用额外第三方的拖载挂车时，泊车辅助将不能检查车辆后方。 2）　为了防止驾驶员误解或误用，安全相关的整车新功能的正确使用的警告： 相对于手动驻车制动，自动驻车制动的误用可能导致驾驶员没有将驻车制动啮合就离开车辆
13	报废指导说明是否描述了相关项或其要素在拆卸过程中采用的活动和措施，以确保其安全报废？	为避免对报废作业人员造成伤害，在车辆拆卸前对安全气囊进行解除的指导说明
14	在运行、服务和报废的计划过程中识别的安全要求，是否已经以适当的方式反馈给负责系统、硬件和软件开发的人员？	ECU 中的错误日志功能的软件规范，以便于服务中进行诊断
15	救援服务信息，是否包括救援指导说明书或紧急救援指南？如果适用，是否提供相关指导说明和警告，以避免救援操作时发生危害？	防止非期望的气囊点爆或电击伤害的信息
16	是否实施了与相关项或其要素相关的潜在安全相关事件的现场监控流程，以便： ——提供能用于分析以探测功能安全问题存在的现场数据； ——分析现场数据，以探测功能安全问题的存在； ——启动相关措施，来处理识别到的功能安全问题	—
17	相关项或其要素的运行、服务和报废是否按照服务计划、服务指导说明和报废指导说明来实施和文档化？	—
18	相关项或其要素的变更，运行（包括现场监控）及服务或报废流程的变更，是否已按照要求进行管理？	—
19	其他通用： 输入文档是否存在且可用？ 输入文档是否使用了最新的模板？是否存在版本管理？ 工作成果是否经过了充分的评审？ 评审人是否为要求的评审人？ 评审是基于基线还是基于版本？ 评审意见是否包含评审人的结论？ 评审记录的所有开口项是否都已关闭？	—

表 C.1　关于生产、运行、服务和报废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	是否制定了生产过程及其控制措施？	—
21	是否应对生产过程(包括安全相关特殊特性的偏差)进行分析，达到以下目的： ——识别过程失效； ——识别由于过程失效导致的对功能安全的潜在影响； ——采取恰当的措施，以确保识别的影响可被避免或减轻； ——验证采取措施的有效性	—
22	是否针对功能安全，评估并维护了如下几项能力： ——生产过程； ——设备和工具； ——测试设备	—
23	测试设备是否按照所采用的质量管理体系进行控制？	IATF 16949 中对监控和测量设备的管理要求
24	控制是否按照生产控制计划来执行？相关的控制报告应包含控制时间、受控对象的识别和控制结果	—
25	是否落实只有在生产发布报告中定义的已被批准的配置才能进行生产，如有任何偏差应得到负责人的授权？	—
26	在生产阶段发起的生产过程的变更，是否按照 GB/T 34590.8—2022 第 8 章的要求进行管理？	—
27	是否实施与相关项或其要素相关的潜在安全相关事件的现场监控流程？以便： ——提供能用于分析以探测功能安全问题存在的现场数据； ——分析现场数据，以探测功能安全问题的存在； ——启动相关措施，来处理识别到的功能安全问题	—
28	相关项或其要素的运行、服务和报废是否按照服务计划、服务指导说明和报废指导说明来实施和文档化？	—
29	相关项或其要素的变更，运行(包括现场监控)及服务或报废流程的变更是否按照 GB/T 34590.8—2022 第 8 章的要求进行管理？	—

附 录 D
（资料性）
支 持 过 程

本附录给出了GB/T 34590.8—2022支持过程的审核及评估的说明及示例，包括：

a） 分布式开发的接口的审核及评估的说明及示例，见表D.1；
b） 配置管理的审核及评估的说明及示例，见表D.2；
c） 变更管理的审核及评估的说明及示例，见表D.3；
d） 验证的审核及评估的说明及示例，见表D.4；
e） 文档管理的审核及评估的说明及示例，见表D.5；
f） 软件工具鉴定的审核及评估的说明及示例，见表D.6；
g） 在用证明的审核及评估的说明及示例，见表D.7；
h） GB/T 34590.1～34590.12—2022适用范围之外应用的接口的审核及评估的说明及示例，见表D.8；
i） 未按照GB/T 34590.1～34590.12—2022开发的安全相关系统的集成审核及评估的说明及示例，见表D.9。

表D.1 分布式开发的接口的审核及评估的说明及示例

序号	检查点	说明及示例
1	供应商选择报告是否对供应商进行能力评估？如果适用，也包含按照GB/T 34590.1～34590.12—2022对类似复杂度和ASIL等级的相关项和要素的生产能力的评估？	检查是否对供应商能力进行了评估。 说明：供应商选择准则包含： ——供应商质量管理体系的证据； ——供应商以往的表现和质量； ——对供应商功能安全能力（作为投标的一部分）的确认； ——以往按照GB/T 34590.2—2022中6.4.12进行的功能安全评估结果；或 ——来自整车厂开发、生产、质量和物流部门（因其影响功能安全）的推荐
2	供应商选择报告是否包含客户给候选供应商的报价需求（RFQ）？报价需求（RFQ）内容是否完整？	报价需求（RFQ）： a） 符合GB/T 34590.1～34590.12—2022的正式要求； b） 供货范围的定义； 说明：供货范围规定了需要供应商提供的相关项或要素的功能、特性和边界。 c） 如果已存在，基于供应商报价对象的安全目标或相关功能安全要求（包含其分配的ASIL等级）； 说明：如果在选择供应商时ASIL等级未知，则可作出保守的假设。 d） 如果已存在，基于供应商报价对象的要素的失效率目标值和诊断覆盖率目标值（按照GB/T 34590.4—2022中的6.4.5.3）
3	双方是否签订了DIA？	检查双方是否签订了DIA
4	DIA中是否包含客户和供应商安全经理的任命？	—

表 D.1　分布式开发的接口的审核及评估的说明及示例（续）

序号	检查点	说明及示例
5	DIA 中是否按照 GB/T 34590.2—2022 中的 6.4.5 进行安全活动的联合剪裁？	—
6	DIA 中是否包含客户需开展的安全生命周期的活动和供应商需开展的安全生命周期的活动？	说明：活动的联合计划是需要考虑的，包含按照 GB/T 34590.2—2022 给出的功能安全评估和功能安全审核的职责
7	DIA 中是否包含需共享的信息和工作成果，包含分配和评审？	说明 1：这包括对需提供的文档达成一致，以完成客户及供应商的安全档案。 说明 2：交换的信息包含安全相关的特殊特性。 说明 3：对所涉及开发方的活动所必需的工作成果相关部分，可进行识别和交换
8	DIA 是否为每个工作成果定义了责任方？	**示例**：责任可描述为负责、批准、支持、通知、咨询。
9	DIA 中是否包含目标值的沟通或确认？	—
10	DIA 中是否包含在客户和供应商合作中所需要的接口相关的流程、方法及工具？	说明：流程、工具及工具配置的版本和修订可为相关的
11	DIA 中是否包含哪一方（供应商或者客户）按照 GB/T 34590.4—2022 执行安全确认所达成的协议？	说明：如果由供应商执行整车集成和确认，对供应商所需的能力和资源达成一致是重要的，因为安全确认工作需要集成后的车辆（见 GB/T 34590.4—2022）
12	DIA 中是否包含按照 GB/T 34590.2—2022，关于由供应商开发的要素或工作成果的功能安全评估活动？	说明：这些由供应商开发的要素或工作成果的功能安全评估活动，可能是由供应商本身、客户或供应商/客户指定的组织或个人来执行
13	DIA 中是否包含供应商关于功能安全评估活动的计划？	说明：开发接口协议包含报告的最低限度内容、版本和里程碑节点
14	DIA 中是否包含客户与供应商之间达成的允许客户指定审核人员在供应商的场所进行功能安全审核的协议？	—
15	DIA 是否为每个工作成果定义了交付路径和交付类型？	**示例**：DIA 指定了每项工作成果物存放的存储空间的地址。
16	双方是否都批准了 DIA？	说明：检查双方是否都批准了 DIA，DIA 中涉及的相关责任人，如项目经理、功能安全经理、测试经理、软件经理、硬件经理等都已经签字批准
17	如果供应商执行危害分析和风险评估，那么危害分析和风险评估是否提供给客户进行验证和批准？	—
18	概念阶段的责任方是否按照 GB/T 34590.3—2022 制定功能安全概念？	—
19	客户是否确保供应商按时收到所需的用于执行开发接口协议中安全活动的信息和数据？	—

表 D.1　分布式开发的接口的审核及评估的说明及示例（续）

序号	检查点	说明及示例
20	供应商是否向客户报告可能增加不符合开发接口协议条款的风险的问题？	—
21	供应商是否向客户报告在其责任范围内和其分包商责任范围内的开发活动中发生的安全异常？	—
22	是否分析已识别出的潜在影响供应商交付成果的安全异常，并采取措施予以解决？双方是否就谁来执行所需的行动达成协议？	—
23	供应商是否确定客户的安全要求是否可行，以及 6.4.1 和 6.4.2 的要求是否满足？若不可行/不满足，客户是否重新检查安全要求并做适当的修改，以确保安全要求定义的正确性？	—
24	供应商是否向客户传达其职责范围以外但供应商认为为确保实现功能安全所必要的相关项的要素的安全要求？	—
25	在导出用于当前开发的安全要求时，按照 GB/T 34590.2—2022 中的 5.4.2.6，双方是否都考虑了从之前相似开发中所获得的经验？	**示例**：供应商在开发某型车 A 功能，如 ACC 时可考虑其他类似项目如 LCC 中导出功能安全要求的经验。
26	供应商是否向客户报告安全计划中制定的各项任务和里程碑节点上所取得的进展？	说明：应检查供应商是否有向客户报告各项任务和里程碑节点上取得的进展
27	供应商和客户是否就报告的内容和提交的日期达成一致？	—
28	对于分配了安全要求的最高 ASIL 等级为 ASIL(B)、C 或 D 的要素，在 DIA 中是否指定哪个组织按照 GB/T 34590.2—2022 对供应商开发的要素或工作成果执行功能安全评估活动？	**示例**：EPS 按 ASIL D 等级开发，双方在 DIA 中约定由客户对供应商进行功能安全评估。
29	对于分配了安全要求的最高 ASIL 等级为 ASIL(B)、C 或 D 的要素，在 DIA 中是否规定了供应商功能安全评估活动的计划？	说明：计划包括报告的最低限度内容和里程碑节点 **示例**：EPS 按 ASIL D 等级开发，客户和供应商在双方签订的 DIA 中依据安全计划制定的时间节点规定好功能安全评估活动的计划。

表 D.1　分布式开发的接口的审核及评估的说明及示例（续）

序号	检查点	说明及示例
30	对于分配了安全要求的最高 ASIL 等级为 ASIL(B)、C 或 D 的要素，供应商是否向客户提供功能安全评估报告，包括供应商对所开发的要素是否符合来自客户的安全要求的评估，以及所实施的流程是否满足实现功能安全的准则？	—
31	对于分配了安全要求的最高 ASIL 等级为 ASIL(B)、C 或 D 的要素，是否将供应商的功能安全评估活动的结果提供给客户和供应商？	—
32	供应商是否向客户提供证据，证明能具备并保持 GB/T 34590.2—2022 第 7 章和 GB/T 34590.7—2022 第 5 章和第 6 章所要求的生产过程能力？	说明：关于半导体生产的指南，参照 GB/T 34590.11—2022 中的 4.9
33	客户和供应商间的供应协议是否按照 GB/T 34590.2—2022 中的 7.4.2.1 明确功能安全责任，并应定义各方的安全活动？	说明：关于半导体分布式开发的指南，参照 GB/T 34590.11—2022 中的 4.10
34	供应协议是否规定各方间关于安全相关特殊特性的生产监控记录和从客户退回部件的失效分析结果的访问和交换？	说明：这些事项能由质量管理协议充分覆盖
35	供应协议是否规定了关于交换安全相关事件和所需分析的及时的沟通渠道。对于现场问题，是否就按照已建立的现场监控过程对这些事件进行分析？	说明：该分析包括类似相关项和潜在受类似事件影响的其他方

表 D.2　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	配置管理策略和计划是否合理	如适应，参照 ASPICE 配置管理策略，应检查配置管理策略的内容，例如： ——职责； ——工具和存储库； ——配置项准则； ——命名规则； ——访问权限； ——基线准则； ——合并和分支策略； ——配置项修订历史的方法
2	组织架构是否包含所有和配置管理活动相关的人员角色，架构是否正确？	应检查组织架构中配置管理活动的人员角色，以及判断组织架构的正确性

表 D.2　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
3	配置管理过程是否完整、描述是否清晰？	检查配置管理活动是否完整，依据 ASPICE 的配置管理活动，应包括以下内容： ——制订配置管理策略； ——识别配置项； ——建立配置管理系统； ——建立分支管理； ——控制修改和发布； ——建立基线； ——报告配置状态； ——验证关于配置项的信息； ——管理配置项和基线的存储
4	配置管理过程中遵循的规范是否填写完整？内容和规范版本是否正确？	配置管理过程应符合： a)　质量管理体系标准的相关要求； b)　软件开发的特定要求。 说明：ISO/IEC/IEEE 12207 中给出了软件开发的软件配置管理的特定要求
5	配置管理工具环境中是否一一列举配置管理活动中所有使用的工具？	检查配置管理工具环境中配置活动所使用的工具，检查列举的工具完整性
6	基线计划的阶段是否符合配置管理策略的要求？	检查基线计划的阶段与配置管理策略的一致性
7	基线名称是否符合配置管理策略的要求？	检查基线名称与配置管理策略的一致性
8	基线计划的时间是否合理且与主计划吻合？	检查基线计划的时间与主计划的一致性
9	基线计划是否按照安全计划的要求？	检查基线计划与安全计划的一致性
10	输入文档是否存在且可用？	检查输入文档是否存在且完整，如：配置管理计划
11	安全计划要求的工作成果及再次生成相关项和要素所需要的工作成果，是否按照配置管理策略，生成基线并存放？	—
12	在整个安全生命周期中，需要被唯一识别和重生成的工作成果、相关项和要素，在配置管理策略中是否定义其条件或目的？	例如：作为客户-供应商关系里安全活动的一部分，在其交换之前需要创建工作成果、相关项和要素的配置条件或目的
13	在整个安全生命周期中，是否对配置管理进行维护？	—

表 D.3　变更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	变更管理流程是否完整、描述是否清晰？	变更管理流程应包括： a)　变更需求，按照 8.4.2； b)　变更需求分析，按照 8.4.3； c)　变更需求的决策和依据，按照 8.4.4； d)　已接受的变更的实施和验证，按照 8.4.5； e)　文档化，按照 8.4.5。 说明 1：变更管理流程可适用于开发过程中的相应阶段。 说明 2：可在一个变更需求中处理多个变更
2	在对工作成果进行变更前，是否计划和启动变更管理流程？	说明：配置管理和变更管理是相互关联的，定义并维护两个流程间的接口，以确保变更管理的有效性
3	是否在变更管理计划中识别要进行变更管理的工作成果、相关项和要素？这些工作成果、相关项和要素是否满足 GB/T 34590.8—2022 中 7.4.3 的要求？	—
4	是否为已识别出的工作成果、相关项和要素定义实施变更管理流程的日程表？	—
5	组织架构是否包含所有和变更管理活动相关的人员角色，架构是否正确？	检查组织架构是否包含变更管理活动的所有人员角色
6	变更管理流程中遵循的规范是否填写完整？内容和规范版本是否正确？	检查管理活动中遵循的规范内容，如 ASPICE
7	是否为每个变更需求分配唯一的识别码？	—
8	每个变更需求是否至少包含以下信息： a)　日期； b)　所需变更的理由； c)　所需变更的准确描述； d)　所需变更基于的配置	—
9	对于每个变更需求，是否针对以下信息，对所涉及的相关项或要素、接口及关联相关项或要素进行影响分析： a)　变更需求的类型； b)　对需更改的工作成果、相关项和要素及受影响的工作成果、相关项和要素进行的识别； c)　在分布式开发的情况下，所涉及的相关方的识别及其责任； d)　变更对功能安全的潜在影响； e)　变更的实现和验证的日程表	例如：可能的变更类型有解决错误、调整、消除、加强、预防
10	变更管理工具环境中是否一一列举配置管理活动中所有使用的工具？	检查配置管理工具环境中配置活动所使用的工具，检查列举的工具完整性

表 D.3　变更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
11	变更管理是否受到监控？	检查变更是否受到监控
12	变更是否重新启动了安全生命周期的适用阶段？	对工作成果的变更，应重新启动安全生命周期的适当阶段，后续阶段的开展应符合 GB/T 34590.1～34590.12—2022
13	变更是否进行了需求评估？	检查是否依据 GB/T 34590.8—2022 中 8.4.3.1 进行影响分析的结果，对变更需求进行了评估，并且检查授权人员对变更的决定是否接收，或是拒绝，或是推迟变更。 例如：EPS 能接收的信号由转矩变成转角，导致 ADAS 的发送的转向请求信号发生变化，进而会导致 ADAS 的通信矩阵发生变化，且影响控制横向控制策略。这种变更最终需要由授权人员来决定是否同意。典型的授权人员包括： ——项目经理； ——安全经理； ——负责质量保证的人员； ——涉及的开发人员
14	变更是否定义了时间节点？	检查已经接受的变更需求，应决定由谁来开展变更以及变更的最晚时间
15	变更是否进行了验证？	应按计划实施变更和验证变更
16	如果变更影响了安全相关功能或特性，是否在发布相关项前，对按照 GB/T 34590.2—2022 中 6.4.9 和 6.4.10 的功能安全评估和适用的认可评审进行了更新？	—
17	变更记录是否完整？	变更的记录应包含以下信息： a)　按照第 7 章，在合适的层面下，变更的工作成果、相关项和要素的清单，包括配置和版本； b)　开展的变更细节； c)　变更部署的计划日期。 说明 1：对临时变更需求，应明确指出该变更需求的理由和变更持续的时间（如已知）。 说明 2：对被拒绝的变更需求，记录变更需求和拒绝的理由

表 D.4　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	验证计划是否与主计划匹配？	检查验证计划与主计划的一致性
2	验证计划是否包含了安全生命周期的每个阶段及子阶段？	检查在安全生命周期的每个阶段及子阶段都制定了验证计划

表 D.4　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
3	验证计划的内容是否完整？	验证计划的应涵盖以下方面： ——需验证的工作成果内容； ——用于验证的方法，验证方法包括评审、走查、检查、模型检查、模拟、工程分析、证明和测试，典型的验证会使用这些方法和其他方法的组合； ——验证通过和不通过的准则； ——如果适用，验证环境，验证环境可为测试或模拟环境； ——如果适用，用于验证的工具； ——当探测出问题时需采取的行动； ——回归策略。 说明 1：验证环境可为测试环境或模拟环境。 说明 2：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
4	制定验证计划时是否考虑了所使用验证方法的充分性？	—
5	制定验证计划时是否考虑了需验证的工作成果的复杂性？	—
6	制定验证计划时是否考虑了与验证目标材料相关的前期经验？	说明：这包括维修历史及在用证明达到的程度
7	制定验证计划时是否考虑了所使用技术的成熟度，或使用这些技术的风险？	—
8	验证规范是否对用于验证的方法进行了细化？	验证方法的细化： ——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
9	每条测试用例定义的内容是否完整？	每条测试用例的定义应包含以下内容： ——唯一的识别； ——需验证的相关工作成果的版本的参考； ——前提条件和配置； ——如果适用，环境条件； ——输入数据、数据时序及其值； ——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； ——确定测试用例通过和不通过的准则
10	对于测试，是否按使用的测试方法对测试用例进行分组？	分组时宜从以下几个方面考虑： ——所需的测试设备或测试环境； ——逻辑和时间的依赖性； ——资源。 例如：将测试用例分成回归测试用例和完整测试用例

表 D.4　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
11	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了评审？	—
12	是否按照 GB/T 34590.8—2022 中 9.4.1 所做的计划及按照 9.4.2 所做的规范，执行验证？	—
13	验证是否由与待验证的工作成果的完成人不同的人执行？	—
14	对验证结果的评估所包含的信息是否完整？	对验证结果的评估应包含以下信息： ——所验证工作成果的唯一识别； ——验证计划和验证规范的参考； ——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； ——验证结果与期望结果的一致性水平； ——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； ——每个验证步骤未执行的理由
15	用于验证的测试设备是否能提供有效的和可重复的结果，是否按照所采用的质量管理体系进行管控？	—

表 D.5　文档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	是否计划了文档管理过程？	计划文档制定和管理过程，以获得文档： ——用于在整个生命周期的每个阶段中有效完成各阶段及验证活动； ——用于功能安全的管理； ——作为认可措施的输入
2	是否将对 GB/T 34590.1～34590.12—2022 中工作成果进行了文档化管理？	—
3	文档是否包含相关要求的完整结果信息？	—
4	整个文档的结构是否考虑了内部流程和工作实践？并进行了适当的组织？	**示例**：文档树。
5	文档管理计划是否有记录跟踪？	如适用，每个工作成果或文档应包含下面的正式要素： ——题目，参照内容的范围； ——作者和批准者； ——文档每个不同修订（版本）的唯一标识； ——变更历史，包含每次变更的作者姓名、日期和简要描述。 ——状态，例如：“草稿”“已发布”

表 D.5　文档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
6	文档指南是否明确文档的撰写要求？	如适用，应检查文档指南要求是否包含： ——准确的和简明的； ——结构清晰的； ——目标使用者容易理解的； ——可验证的； ——可维护的
7	文档指南是否定义文档的正式要素？例如应包含题目、作者和批准者、唯一的标识、变更历史、状态	如适用，每个工作成果或文档应包含下面的正式要素： ——题目，参照内容的范围； ——作者和批准者； ——文档每个不同修订（版本）的唯一标识； ——变更历史，包含每次变更的作者姓名、日期和简要描述。 ——状态，例如："草稿""已发布"等
8	是否能识别当前适用的文档修订（版本）或信息项？	—

表 D.6　软件工具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	安全计划中是否基于考虑所使用软件工具的置信度的依据而按照 GB/T 34590.2—2022 中的 6.4.5.1 对某一安全活动进行剪裁？若有，剪裁是否满足 GB/T 34590.8—2022 第 11 章的要求？	检查安全计划中是否由于软件工具鉴定而对某一安全活动进行了剪裁
2	是否有预先确定的工具在执行其置信度水平评估或鉴定时，独立于特定安全相关项或要素的开发？若有，在使用该软件工具前，是否对预先确定的工具置信度水平的有效性或鉴定的有效性进行验证？	检查是否有预先确定的工具在执行其置信度水平评估或鉴定时，独立于特定安全相关项或要素的开发？若有，是否对预先确定的工具置信度水平的有效性或鉴定的有效性进行验证
3	使用软件工具时，工具的使用、工具定义的环境和功能约束及其正常运行条件是否和工具评估准则或鉴定相符合？	检查使用软件工具时，工具的使用、工具定义的环境和功能约束及其正常运行条件是否和工具评估准则或鉴定相符合
4	是否有对软件工具使用的计划？	检查是否有对软件工具使用的计划

表 D.6　软件工具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
5	对软件工具使用的计划中是否包含： a）　软件工具的识别码和版本号； b）　软件工具的配置； c）　软件工具的使用案例； d）　软件工具执行的环境； e）　当软件工具功能异常并产生相应的错误输出时，会直接违背分配给相关项或要素的全部安全要求的最高 ASIL 等级； f）　如需要，基于确定的置信度水平和 ASIL 等级的软件工具的鉴定方法	检查对软件工具使用的计划中是否包含 GB/T 34590.8—2022 中 11.4.4.1 要求的内容。 a）　软件工具的配置； **示例 1**：通过设定编译器开关和 C 源文件中“# pragma”声明，定义编译器的配置。 b）　软件工具的使用案例； **注 1**：在开展安全生命周期活动时，使用案例可描述用户与软件工具的配合和软件工具功能的应用子集。 **注 2**：使用案例可包含对软件工具配置及软件工具执行环境的要求。 c）　软件工具执行的环境； **示例 2**：执行软件工具所需的资源、基础设施或运行时环境，应用软件工具所需的流程活动或与软件工具输出结果验证相关的后续流程活动。 d）　当软件工具功能异常并产生相应的错误输出时，会直接违背分配给相关项或要素的全部安全要求的最高 ASIL 等级 **注 3**：可根据特定开发确定最高 ASIL 等级，或可根据软件工具通用的用法确定最高 ASIL 等级。在预先假定 ASIL 等级的情况下，对该假设进行验证。
6	为了进行软件工具评估，是否收集了软件工具相关信息： a）　软件工具的特征、功能和技术属性的描述； b）　如果适用，用户手册或其他使用指南； c）　工具运行要求的环境描述； d）　如果适用，对异常运行条件下期望的软件工具表现的描述； e）　如果适用，对已知软件工具功能异常，及恰当的安全保护、避免或应急措施的描述； f）　在制定软件工具要求的置信度水平过程中，识别出的对软件工具功能异常和相应错误输出的预防或探测措施	检查为了进行软件工具评估，是否收集了 GB/T 34590.8—2022 中 11.4.4.2 要求的软件工具相关信息。 a）　如果适用，对异常运行条件下期望的软件工具表现的描述； **示例 1**：异常运行条件可为禁止的编译开关组合、不符合用户手册的环境或不正确的安装。 **示例 2**：异常运行条件下期望的表现可为对输出生成的阻止、用户提示或用户报告。 b）　如果适用，对已知软件工具功能异常，及恰当的安全保护、避免或应急措施的描述； **示例 3**：针对已知的功能异常、编译器编码优化局限或建模中使用受限制的一组构件的使用指南或应急措施。 **示例 4**：安全保护包括通过使用约束防止全部已知的功能异常和问题、探测和报告全部已知的功能异常和问题，也包括提供安全替代技术以开展相应的活动。 c）　在制定软件工具要求的置信度水平过程中，识别出的对软件工具功能异常和相应错误输出的预防或探测措施 **注**：相应错误输出的预防或探测措施可针对软件工具输出中的已知和潜在错误。 **示例 5**：冗余软件工具输出的对比、执行的测试、静态分析或评审、软件工具日志文件的分析、具有已知问题的功能的避免。

表 D.6　软件工具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
7	软件工具准则评估报告对软件工具使用的描述是否包含下述信息： a)　预期的目的； b)　输入和期望的输出； c)　如果适用，使用过程、环境的和功能的约束	检查软件工具准则评估报告对软件工具使用的描述是否包含 GB/T 34590.8—2022 中 11.4.5.1 要求的信息。 a)　预期的目的； **示例 1**：功能的模拟、源代码的生成、嵌入式软件的测试、安全生命周期的剪裁、GB/T 34590.1～34590.12—2022 要求的活动和任务的简单化或自动化。 b)　输入和期望的输出； **示例 2**：后续开发活动输入所需的数据、源代码、模拟结果、测试结果、或 GB/T 34590.1～34590.12—2022 的其他工作成果。 c)　如果适用，使用过程、环境的和功能的约束 **示例 3**：软件工具嵌入到开发过程、不同软件工具使用共享数据及其他使用条件、预防或探测软件工具的功能异常的流程措施。
8	软件工具准则评估报告中是否分析和评估了软件工具的预期使用，以确定： a)　特定软件工具功能异常可引入或不能探测开发中安全相关项或要素中错误的可能性。这是通过工具影响(TI)等级表示的： ——当有论据表明没有这样的可能性时，应选择 TI1； ——在所有其他情况下应选择 TI2。 b)　用于预防软件工具功能异常并产生相应错误输出的措施的置信度，或用于探测软件工具存在功能异常并已产生相应错误输出的措施的置信度。这是通过工具错误探测(TD)等级表示的： ——当对预防或探测出功能异常及其相应错误输出具有高置信度时，应选择 TD1； ——当对预防或探测出功能异常及其相应错误输出具有中等置信度时，应选择 TD2； ——在所有其他情况下应选择 TD3	软件工具准则评估报告中是否按 GB/T 34590.8—2022 中 11.4.5.2 要求分析和评估了软件工具的预期使用。 **注 1**：预防或探测可通过流程步骤、任务或软件工具的冗余、或软件工具自身的合理性检查完成。 **注 2**：如果具备的开发流程中没有系统性措施，则典型适用 TD3，为此，仅能随机探测出软件工具的功能异常及其相应错误输出。 **注 3**：如果用一个软件工具验证另一软件工具的输出，当评估这一软件工具时，考虑软件工具间的相互依赖性，为该软件工具选择一个充分的 TD。例如，工具之间可能因使用了公共组件或者共享资源而存在相互依赖性。 **注 4**：此使用分析的详细程度仅需要允许恰当地确定 TI 和 TD 的等级。 **示例 1**：在按照 GB/T 34590.1～34590.12—2022 对产生的源代码进行验证的情况下，为代码生成器选择 TD1。当不对产生的源代码进行验证时，为代码生成器选择 TD3。 **示例 2**：使用指南防止功能异常，例如编译器对代码构成的错误或不清晰的理解。 **示例 3**：针对用于静态验证源代码中不存在潜在的除零情况的工具，如果为此目的也同时进行了测试，则可为该工具选择 TD2。如果仅通过工具验证不存在除零的情况，可为该工具选择 TD3。
9	软件工具准则评估报告中是否存在对 TI 或 TD 选择的正确性是不清楚的或可疑的？若有，推荐对 TI 和 TD 进行保守评估	**示例**：对 TI 选择的正确性存疑，那么 TI＝2。

表 D.6　软件工具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	软件工具准则评估报告中基于为 TI 和 TD 等级确定的值，是否按照 GB/T 34590.8—2022 中的表 3 来确定所要求的软件工具的置信度水平？	检查 TI 和 TD 等级确定的值得出的 TCL 值是否能与 GB/T 34590.8—2022 中的表 3 对应
11	软件工具鉴定报告中，对鉴定等级为 TCL3 的软件工具，是否按照 GB/T 34590.8—2022 中表 4 列出的方法进行鉴定？	检查对鉴定等级为 TCL3 的软件工具，是否按照 GB/T 34590.8—2022 中表 4 列出的方法进行鉴定。 ——1 d 按照安全标准开发：没有安全标准完全适用于软件工具的开发。相反，可选择安全标准中相关的一组安全要求 **示例**：按照 GB/T 34590.1～34590.12—2022、GB/T 20438、EN 50128 或 RTCA DO-178 开发软件工具。
12	软件工具鉴定报告中，对鉴定等级为 TCL2 的软件工具，是否按照 GB/T 34590.8—2022 中表 5 列出的方法进行鉴定？	检查对鉴定等级为 TCL2 的软件工具，是否按照 GB/T 34590.8—2022 中表 5 列出的方法进行鉴定。 ——1 d 按照安全标准开发：没有安全标准完全适用于软件工具的开发。相反，可选择安全标准中相关的一组安全要求 **示例**：按照 GB/T 34590.1～34590.12—2022、GB/T 20438、EN 50128 或 RTCA DO-178 开发软件工具。
13	软件工具鉴定报告中，是否包含以下文档化信息： a）　软件工具的唯一识别码和版本号； b）　软件工具划分的最高工具置信度等级，及其评估分析参考； c）　对于考虑的使用案例，当软件工具功能异常并产生相应的错误输出时，可能直接违背任何安全要求的预定义最高 ASIL 等级或特定 ASIL 等级； d）　软件工具被鉴定的配置和环境； e）　执行鉴定的人员或组织； f）　鉴定使用的方法，按照 GB/T 34590.8—2022 中的 11.4.6.1； g）　用于鉴定软件工具的措施结果； h）　如果适用，在鉴定过程中识别出的使用约束和功能异常	检查软件工具鉴定报告中，是否包含 GB/T 34590.8—2022 中 11.4.6.2 规定的信息

表 D.6　软件工具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
14	软件工具鉴定报告中，在使用“使用中积累置信度”方法进行软件工具鉴定时，是否满足以下要求： a) 仅当具备以下方面的证据时，才应论证软件工具在使用中积累了置信度： ——此前，已经将该软件工具用于相同的目的，具有相似的使用案例、相似的预定运行环境和相似的功能约束中； ——使用中积累置信度的理由是基于充分适当的数据； ——软件工具的定义未改变； ——在之前开发中获得的软件工具功能异常和相应错误输出的发生案例是以系统化方式累计的。 b) 应通过考虑以下信息，对给定开发活动中软件工具的先前使用经验进行分析和评估： ——软件工具唯一的识别码和版本号； ——软件工具的配置； ——使用周期和使用相关数据的细节； ——软件工具的功能异常和相应错误输出的详细文档化记录，其中包含引起功能异常和错误输出的条件； ——所监控的先前版本清单，其中列出每个相关版本中解决的功能异常； ——如果适用，对已知缺陷的安全保护、避免措施、应急措施或相应错误输出的探测措施。 c) 使用中积累置信度的论证应仅对所评估的软件工具版本有效	检查软件工具鉴定报告中，在使用“使用中积累置信度”方法进行软件工具鉴定时，是否满足 GB/T 34590.8—2022 中 11.4.7 的要求。 a) 仅当具备以下方面的证据时，才应论证软件工具在使用中积累了置信度： ——使用中积累置信度的理由是基于充分适当的数据。 **注**：可从累计使用量中获得数据（例如：时间长度或频率）。 b) 应通过考虑以下信息，对给定开发活动中软件工具的先前使用经验进行分析和评估： ——使用周期和使用相关数据的细节； **示例 1**：软件工具相关使用案例中，使用的软件工具特征及使用频率。 ——如果适用，对已知缺陷的安全保护、避免措施、应急措施或相应错误输出的探测措施 **示例 2**：使用报告的来源可为日志、供应商提供的软件工具版本历史、已发布的勘误表。

表 D.6　软件工具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
15	软件工具鉴定报告中，在使用“工具开发流程评估”方法进行软件工具鉴定时，是否满足以下要求： a）　用于软件工具开发的流程应满足适当的标准； b）　应基于恰当的国内或国际标准对软件工具开发流程进行评估，同时提供恰当的软件开发流程被应用的证据	检查软件工具鉴定报告中，在使用“工具开发流程评估”方法进行软件工具鉴定时，是否满足 GB/T 34590.8—2022 中 11.4.8 的要求。 a）　用于软件工具开发的流程应满足适当的标准。 **注 1**：对于开源开发，那些团体使用的某些标准也可能是适当的。 b）　应基于恰当的国内或国际标准对软件工具开发流程进行评估，同时提供恰当的软件开发流程被应用的证据 **注 2**：该评估涵盖了对软件工具的一个恰当且相关的特征子集的开发。 **示例**：使用基于 Automotive SPICE、ISO/IEC 33000 或 CMMI 的评估方法。
16	软件工具鉴定报告中，在使用“软件工具确认”方法进行软件工具鉴定时，是否满足以下要求： a）　确认措施应提供软件工具符合分类中指定用途的特定要求的证据； b）　应对确认中发生的软件工具功能异常及其相应错误输出、其可能的后果信息，及避免或探测它们的措施进行分析； c）　应检查软件工具对异常运行条件的响应	检查软件工具鉴定报告中，在使用“软件工具确认”方法进行软件工具鉴定时，是否满足 GB/T 34590.8—2022 中 11.4.9 的要求。 a）　确认措施应提供软件工具符合分类中指定用途的特定要求的证据。 **注 1**：确认提供了评估的工具错误不会发生或将被检测到的证据； **注 2**：确认可通过使用用户开发的或工具供应商（如果供应商的测试套件包括用户的工具使用案例）开发的自定义测试套件来实施。 **示例 1**：编程语言标准有助于定义相关编译器的确认要求。 b）　应检查软件工具对异常运行条件的响应 **示例 2**：可预见的误用、不完整的输入数据、不完整的软件工具升级、使用被禁止的配置设置组合。

表 D.7　在用证明的审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否只有当候选项符合 GB/T 34590.8—2022 中的 14.4.2～14.4.5 时才使用了在用证明可信度？	—
2	是否按照 GB/T 34590.2—2022 中的 6.4.5 计划由在用证明得出在用证明可信度？	—
3	在用证明可信度是否仅来自被候选项在用证明覆盖的安全生命周期子阶段和活动？	—

表 D.7　在用证明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 34590.4—2022 第 8 章在适当层面执行对相关项或要素中的在用证明要素的集成措施？	**示例**：某个电控单元的硬件有令人满意的现场记录，且将被100％沿用到某个新的应用。在用证明可信度可被用于该硬件要素开发的子阶段及活动。同样，如果具有令人满意的服役记录的软件 100％被沿用，那么在用证明可信度也可被用于软件子阶段及活动。
5	是否按照 GB/T 34590.4—2022 第 9 章执行了对嵌入了在用证明要素的相关项的安全确认？	—
6	对嵌入了在用证明的要素的相关项，其认可措施是否按照 GB/T 34590.2—2022 中的 6.4.9 和 6.4.10 考虑了在用证明及相关数据？	—
7	对在用证明的相关项或要素进行任何修改都是否都符合 GB/T 34590.4—2022 中的 14.4.4，以保持相应的在用证明可信度？	—
8	在用证明的候选项描述是否包含之前使用的描述？	如适用，检查是否包含关于候选项之前的适用描述。 安全档案； 说明：对未按照 GB/T 34590.1～34590.12—2022 开发的候选项[例如商业现成产品(COTS)，基于 GB/T 34590.1～34590.12—2022 之外的其他安全标准(如 IEC 61508 或 RTCA DO-178)所开发的候选项]，可能不具备安全档案中某些工作成果，则这些成果将被候选项开发中得到的可用数据所替代
9	在用证明的候选项描述是否包含相应的配合要求，形式要求和功能要求？	如果适用，应检查候选项的最低限度信息，这些信息应具备对候选项及其之前适用的描述，包括： ——响应的配合要求，形式要求和功能要求，若适用，并描述候选项的接口和环境特性，物理和尺寸特性，功能和性能特性
10	如果适用，在用证明的候选项描述是否包含候选项之前使用时的安全要求及相应的 ASIL 等级？	若适用，候选项之前适用时的安全要求及相应的 ASIL 等级
11	如有，候选项描述是否定义了如何识别候选者，是否建立追溯关系，是否明确了候选项的内部要素和组件目录？	若有，候选项的识别和追溯，及内部要素或组件的目录
12	在用证明的候选项描述是否依据公司的内部评审流程进行评审？	候选项描述应依据公司内部评审流程进行评审

表 D.7　在用证明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	在用证明分析报告是否包含候选项的设计变更和实施变更？如有，按照变更流程审核及评估变更项	应识别出对候选项及其环境的变更： 说明：候选项的变更是指设计变更和实施变更。要求更改，功能性加强或性能加强可导致设计变更。实施变更不影响候选项的定义或其性能，仅影响其实施特性。软件整改，适用新的开发工具或生产工具可导致实施变更。如有这些变更，应按照变更流程审核及评估变更项
14	在用证明分析报告是否包含配置数据或标定数据的变更？如有，按照变更流程审核及评估变更项	应识别出对候选项及其环境的变更： 说明：配置数据或标定数据的更改如果影响了候选项的表现并与违背安全目标相关，则认为这些变更是对相关项的变更
15	在用证明分析报告中的候选项是否具有不同安全目标或要求的新型应用？如有，按照变更流程审核及评估变更项	应识别出对候选项及其环境的变更： 说明：将候选项用于具有不同安全目标或要求的新应用，将候选项安装于新的目标环境（如车辆变型，环境条件范围），与候选项存在相互作用的组件升级或位于候选项附近的组件升级都可导致候选项环境的变更
16	在用证明分析报告中候选项是否包含评估期引入的，独立于未来应用的修改？如有，是否提供在用证明状态仍然有效的证据？	应识别出在候选项服务后期引入的，独立于未来应用的候选项变更。如果有，应为在用证明的状态仍然有效提供证据
17	在用证明分析报告是否提供了候选项在服务期内及评估期结束后处于配置管理和变更管理下的证据？	应提供候选项在其服务期内及服务期结束后处于配置管理和变更管理管辖下的证据，以便于建立候选项的当前状态
18	在用证明分析报告是否提供了在用证明的目标值？	检查在用证明的目标值： 说明：如果还没有分配任何 ASIL 等级给候选项，可保守的选取 ASIL D 等级。 候选项评估期依据 GB/T 34590.8—2022 中的 14.4.5.2 进行计算
19	在用证明分析报告是否包含现场问题？如有，问题报告是否记录候选项运行期间，现场中任何由于候选项引起的、具有潜在安全影响的可观察的事件	问题报告系统应确保，在候选项运行期间，获取并记录现场中任何由候选项引起的，具有潜在安全影响的可观察到的事故（见 GB/T 34590.7—2022 中的 6.4.2.1）

表 D.8　GB/T 34590—2022 适用范围之外应用的接口的审核及评估的说明及示例

序号	检查清单	说明及示例
1	如有，基础车辆制造商或供应商指南是否定义了供应商与集成方的沟通方式？	基础车辆制造商、相关项或要素的供应商应向集成方沟通信息，识别可修改的系统和组件以及允许的系统安全限制/修改的要求
2	如有，基础车辆制造商或供应商指南是否定义了集成方安全措施的实现方式？如果安全机制和供应商有关，是否与供应商评审安全措施？	如果适用，基础车辆制造商或相关项的供应商应针对要求集成方采取的安全措施进行沟通。 如果安全机制与供应商有关，检查与供应商评审安全措施的记录

表 D.8　GB/T 34590—2022 适用范围之外应用的接口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	如有，供应商是否对预期的集成用例及安全要求作出假设？如有例外，是否定义了集成方和供应商的沟通机制？	基础车辆制造商、相关项或要素的供应商对预期的集成用例及其安全要求做出假设。如有例外情况，集成方应针对安全要求与基础车辆制造商、相关项或要素的供应商进行沟通 **示例**：在驾驶过程中，车身制造商联系基础车辆制造商请求开启 PTO 功能。车身制造商使用 ISO 13849 开发，双方针对在 ISO 13849 基础上增加的 ASIL 等级达成一致。基础车辆制造商沟通关于 PTO 功能相关的带有 ASIL 等级的安全要求，车身制造商（以商定的性能等级）符合这些要求。基础车辆制造商启用车身制造商所请求的 PTO 功能。
4	如有，基础车辆制造商或供应商指南是否经过集成方和供应商的联合评审？	如果适用，检查基础车辆制造商或供应商指南是否经过了联合评审

表 D.9　未按照 GB/T 34590—2022 开发的安全相关系统的集成审核及评估的说明及示例

序号	检查清单	说明及示例
1	如有，集成方的安全档案中是否有对应依据？	在集成方安全档案中应给出依据，以证明本章应用的合理性 **示例**：供应商遵循安全标准 ISO 13849。
2	如有，集成方是否定义了其他安全标准与 GB/T 34590.1～34590.12—2022 定义的标准的映射关系？是否给出了其他安全标准开发的产品的相关证据，论证开发的产品符合功能安全要求的相关等级？	集成方应定义准则，以论证按照另一安全标准开发的安全相关系统符合所需的功能安全要求的等级 **示例 1**：ASIL 等级和 PL 等级（ISO 13849 中使用的性能等级）之间的映射。 说明：该准则应涉及设计流程、产品设计、认证措施和审批流程 **示例 2**：不同安全标准之间，对于应用方法要求和所需失效率要求的对比。
3	如有，集成方和供应商是否对验证准则达成一致？采取的验证措施是否通过双方的评审讨论？	集成方和供应商应就相关的一系列措施达成一致，以验证是否满足准则。 一系列措施可为： ——待集成系统规范的可用性； ——通过测试报告证明待集成系统符合其要求的证据； ——通过 FMEA、FTA、既定设计模式/配置的应用，对系统性设计故障进行结构化设计分析； ——待集成系统适合其预期用途的证据； ——基于充分的 PPAP（生产件批准程序）审批流程，对组件进行产品发布的证据； ——通过高加速寿命测试、环境测试、超出规范限制的测试、鲁棒性测试进行的设计验证与设计确认测试； ——现场数据分析
4	如有，集成方的安全依据是否经过集成方和供应商的充分评审？	如有，检查集成方的安全依据的评审记录

附 录 E
（资料性）
以汽车安全完整性等级为导向和安全分析为导向的分析

针对 ASIL 等级剪裁的要求分解开展审核及评估的说明及示例，见表 E.1。
关于要素共存的准则的审核及评估的说明及示例，见表 E.2。
关于相关失效分析审核及评估的说明及示例，见表 E.3。
关于归纳分析和演绎分析开展审核及评估的说明及示例，见表 E.4。

表 E.1 针对 ASIL 等级剪裁的要求分解开展审核及评估的说明及示例

序号	检查清单	说明及示例
1	进行 ASIL 等级分解时是否考虑了每一个初始的安全要求？	对不同初始安全要求的 ASIL 等级分解，可能导致将几个安全要求分配给相同的独立要素，此时要素的 ASIL 等级应充分考虑所有分配的安全要求
2	初始安全要求是否被分解为冗余安全要求，并由充分独立要素实现？	可通过相关失效分析证明没有导致违背初始安全要求的合理；或者对于初始安全要求的 ASIL 等级，所识别相关失效的每个原因都被充分的安全措施控制，以证明要素承接分解后安全要求要素之间的充分独立 **示例 1**：使用同构冗余来实现分解的要求（例如，通过复制的设备或复制的软件）并不能解决硬件和软件系统性失效。除非相关失效的分析提供了充分的独立性证据或存在潜在共因可进入安全状态的证据，否则不允许 ASIL 等级的降低。因此，在没有针对特定系统应用背景的相关失效分析的支持下，单靠同构冗余通常不足以降低 ASIL 等级。 **示例 2**：ASIL 等级分解通常不适用于在多通道架构设计中确保通道选择或通道切换的要素。
3	分解后的安全要求自身是否符合初始安全要求？	如果将分解后的安全要求分配给安全机制，则应在评估分解后的要求是否符合初始安全要求时，考虑该安全机制的有效性 **示例**：分配给指定 ECU 的 ASIL D 要求，可能被轻易地分解为分配给 ECU 中简单看门狗的 ASIL D 要求和该 ECU 微处理器的 QM 安全要求。然而，这个简单的看门狗不足以覆盖 ASIL D 要求的微处理器的失效模式。在这种情况下，该看门狗不能有效地满足初始的安全要求。
4	如果在软件层面应用 ASIL 等级分解，是否在系统层面对实施分解后要求的要素间进行充分独立性验证？	**示例**：如将本身为 ASIL C 的软件模块拆分为 ASIL C(C)的监控或安全执行模块和 QM(C)的功能模块后，在系统层面是否会因为 CPU 核分配或权限分配不合理导致访问、写数据等行为时发生违反安全目标的情况。
5	对于分解后安全需求的 ASIL 等级的标注，是否在括号中给出安全目标的 ASIL 等级？	—

表 E.1　针对 ASIL 等级剪裁的要求分解开展审核及评估的说明及示例（续）

序号	检查清单	说明及示例
6	是否应用 GB/T 34590.1～34590.12—2022 允许的 ASIL 等级分解方案进行 ASIL 等级分解	GB/T 34590.1～34590.12—2022 规定的分解方案如下。 a)　应按照下列之一对一个 ASIL D 的要求进行分解： 1)　一个 ASIL C(D)的要求和一个 ASIL A(D)的要求； 2)　一个 ASIL B(D)的要求和一个 ASIL B(D)的要求； 3)　一个 ASIL D(D)的要求和一个 QM(D)的要求。 b)　应按照下列之一对一个 ASIL C 的要求进行分解： 1)　一个 ASIL B(C)的要求和一个 ASIL A(C)的要求； 2)　一个 ASIL C(C)的要求和一个 QM(C)的要求。 c)　应按照下列之一对一个 ASIL B 的要求进行分解： 1)　一个 ASIL A(B)的要求和一个 ASIL A(B)的要求； 2)　一个 ASIL B(B)的要求和一个 QM(B)的要求。 d)　如果需要，ASIL A 只应被分解为一个 ASIL A(A)的要求和一个 QM(A)的要求

表 E.2　要素共存的准则审核及评估的说明及示例

编号	检查清单	说明及示例
1	要素共存准则分析所考虑的要素和子要素是否存在分配的安全要求？	—
2	是否在合适的架构设计层面考虑共存准则？	通常在系统设计、硬件设计或软件架构设计时考虑共存准则
3	要素共存分析时是否考虑到分配到要素的每个安全要求和要素包含的每个子要素？	—
4	如果非安全相关的系统架构要素设计和安全相关系统架构要素设计共同存在于同一系统中，是否能证明非安全相关的系统架构要素不直接或间接地违背分配给该要素的任何安全要求，即非安全系统架构要素不干扰系统中安全相关的任何子要素？	这意味着从该子要素到安全相关子要素的级联失效是不存在的； 级联失效的避免可通过设计措施获得，诸如考虑软件的数据流和控制流，或硬件的输入/输出信号及控制线
5	如果系统中存在执行不同 ASIL 等级要求，包括 QM(X)的安全相关系统架构要素，是否存在证据证明对分配给系统架构要素的每个安全要求，所考虑的系统架构要素不会直接或间接地违背分配给执行更高 ASIL 等级要求的系统架构要素的任何安全要求？否则，是否将共存安全相关子要素的最高 ASIL 等级分配给该子要素？	—

表 E.3　相关失效分析审核及评估的说明及示例

序号	检查清单	说明及示例
1	是否应按照安全分析的结果识别出相关失效的潜在可能性？	基于演绎分析法，例如割集检查或者 FTA 中重复的相同事件；基于归纳分析法，例如在 FMEA 中多次出现的具有相似失效模式的相似元器件或组件
2	是否评估了每个识别出的相关失效的潜在可能性，以判定其合理性？	即是否存在导致相关失效并违背给定要素间所要求的独立性或免于干扰的合理可预见原因。因不存在通用且充分可靠的量化方法，共因失效和级联失效的影响是在定性基础上预估的
3	对每个识别出的相关失效的潜在可能性和合理性评估是否考虑了分析对象（相关项或要素）的不同运行模式和运行情形？	—
4	如果适用，对每个识别出的相关失效的潜在可能性和合理性评估是否考虑下述这些因素？ ——随机硬件失效； ——开发故障； ——生产故障； ——安装故障； ——售后服务故障； ——环境因素； ——共同外部资源或信息失效； ——特定工况下的压力； ——老化和磨损	随机硬件失效示例：共用模块的失效，例如大规模集成电路（微控制器、ASIC 等）的时钟、测试逻辑和内部电压调节器的失效。 ——开发故障示例：需求故障、设计故障、实施故障、因使用新技术导致的故障和做更改时引入的故障。 ——生产故障示例：过程、流程和培训相关的故障；控制计划和特殊特性监控中的故障；软件刷新和下线刷新相关的故障。 ——安装故障示例：线束布置相关的故障；器件间互换性相关的故障；相邻的相关项或要素的失效。 ——服务故障示例：过程、流程和培训相关的故障；问题处理相关的故障；器件间互换性相关的故障和由于反向的不兼容性导致的故障。 ——环境因素示例：温度、振动、压力、湿度/冷凝、污染、腐蚀、毒害、电磁兼容性。 ——共同外部资源或信息失效示例：供电、输入数据、系统间数据总线和通信。 ——特定工况下的压力示例：高工作负载、极端的用户输入或来自其他系统的请求、热冲击和机械冲击
5	是否存在相关失效及其影响的合理性的依据？	合理的相关失效是指通过评估发现了合理可预见原因的失效
6	在开发阶段是否发现了相关失效，是否为相关失效定义了合理的解决措施，解决措施是否按照变更管理流程进行了变更？	—
7	用于解决合理的相关失效的措施是否包括用于预防其根本原因的措施、控制其影响的措施或减少耦合因素的措施这些方面？	**示例**：多样性是可用于预防、降低或探测共因失效的一种措施。
8	相关失效的分析细节程度和严格程度，是否可论证达到所要求的独立性或免于干扰的程度？	可用于证明对相关失效所进行分析的深度和严格程度是否合适的准则包括： ——ASIL 等级； ——安全概念所要求的要素之间的独立程度； ——产品复杂性； ——技术； ——不利环境和其他压力因素的数量和程度

表 E.4　归纳分析和演绎分析开展审核及评估的说明及示例

序号	检查清单	说明及示例
1	如适用，安全分析的范围是否包含了下述这些方面？ ——对安全目标和安全概念的确认； ——对安全概念和安全要求的验证； ——对可导致违背安全目标或安全要求的条件及原因的识别，包括故障和失效； ——对探测故障或失效的额外安全要求的识别； ——对探测到的故障或失效所需的响应（行为/措施）的制定； ——对为验证安全目标和安全要求是否得到满足所需的额外措施的识别，包括安全相关的车辆测试	概要性地检查安全分析是否覆盖了标准要求的范围
2	是否在对应的开发阶段开展了对应的安全分析？	通用检查项，概要性检查是否在合适的时间开展了安全分析活动，其中： ——概念阶段的安全分析一般是进行危害分析和风险评估； ——在系统和软硬件阶段有通用的安全分析，如 FMEA、FTA 等； ——在硬件阶段，则在上述通用的安全分析基础上，还有硬件特有的一些安全分析，如 FMEDA； ——在软件阶段，安全分析也有其特别的一些要求，例如 GB/T 34590.6—2022 附录 E 提供的针对软件架构层级的安全分析和相关失效分析的应用和指引
3	安全分析是否在恰当的开发层面开展？	例如：检查该安全分析确切是在概念阶段，或系统阶段，或软硬件阶段开展的。 ——安全分析是否在选定的抽象层次上保持一致？ 例如：针对系统层的安全分析，检查其是否确切在系统层这个抽象层进行，而非概念层或软硬件层。 ——安全分析是否在选定的抽象层次上完成？ 例如：针对系统层的安全分析，检查其是否确实是在系统层这个抽象层完成，而非概念层或软硬件层

表 E.4　归纳分析和演绎分析开展审核及评估的说明及示例（续）

序号	检查清单	说明及示例
4	安全分析是否基于对相关故障类型和模式有足够认知？例如：考虑来自外部的故障模式作为支持性信息	安全分析依赖于对故障类型和模式有足够认知，接下来的几个检查子项则进一步针对性地检查。 ——是否所有的故障类型和模式都被描述和被应用？ 例如：实施 FMEA 的时候，针对一个特定的要素，相关规范要求的 ——“指引词”是否全部都罗列并被考虑？ 例如：实施硬件 FMEDA 的时候，针对特定的电阻，除了开路故障外，是否需要考虑其短路故障？ ——是否所有故障类型和模式都被系统性的方式所收集？ 例如： 是否有相关的标准，规范和指引？ 是否利用了权威的数据库？ 是否利用了专业的工具？ 是否有对应的流程进行管理？ ——是否所有的相关要素都有故障类型和模式？ 例如：是否遍历了目标架构的所有要素，确保所有相关要素都有故障类型和模式？ ——是否所有的相关要素都考虑了合适的故障类型和模式？ 例如：特定的要素，有些故障类型和模式是不适用的，或者相对于常规的故障类型和模式，需要考虑一些特别的。 ——当采用归纳法执行安全分析时，为了预见潜在的失效，是否考虑所有已知的故障？针对归纳法，例如 FMEA，该类方法是由下而上的方法，由已知的原因识别可能的影响，所以需要重点检查是否考虑了所有已知的故障。 ——当采用演绎法执行安全分析时，为了识别引起失效的潜在故障，是否考虑所有已知的失效和影响？例如 FTA，该类方法是由上而下的方法，由已知的影响探寻可能的原因，所以需要重点检查是否考虑了所有已知的失效和影响。 ——考虑来自外部的故障模式作为支持性信息，例如外部权威的数据库所罗列的故障模式（例如硬件安全分析里，其失效模式会参考西门子 SN 29500）用于安全分析的参考
5	当适用定性分析的时，是否采用了恰当的定性分析方法，如系统、设计或流程层级的 FMEA，定性 FTA，HAZOP，或定性 ETA？	标准罗列了几个典型的定性分析方法，当目标层级确定使用定性方式进行安全分析时，需要检查是否采用了合适的方法。 当没有更合适的软件特定分析方法存在时，也可对软件应用这些定性分析方法。 在系统层级的安全分析，通常定性分析就足够，定量分析只在必要的时候被考虑
6	当适用定量分析时，是否采用了恰当的定量分析方法，如定量 FMEA、定量 FTA、定量 ETA、马尔科夫（Markov）模型或可靠性框图？	标准罗列了几个典型的定量分析方法，当目标层级确定使用定量方式进行安全分析时，需要检查是否采用了合适的方法。 GB/T 34590.9—2022 中的 8.2 指出定量分析用于验证硬件设计是否符合已定义的硬件架构度量评估目标值和因随机硬件失效导致违背安全目标的评估目标值，且要求掌握硬件要素定量失效率的知识

表 E.4　归纳分析和演绎分析开展审核及评估的说明及示例（续）

序号	检查清单	说明及示例
7	安全分析是否根据恰当的标准或指南执行？	a）　**示例**：使用相关行业指南来指导 FMEA 分析的开展；如果适用，使用企业内部的 FTA 标准来指导 FTA 分析开展。 b）　分析的详细程度与设计的详细程度相适应。故障模型取决于分析所基于的设计描述层面（系统、硬件、软件）及所实施的安全要求。 c）　此类标准和指南可包括定义安全分析深度和严谨度的准则。这些准则可取决于特定相关项的 ASIL 等级、复杂性或经验，以及它所应用的领域。 d）　安全分析的目的和范围取决于其所应用的子阶段及颗粒度
8	如安全分析采用归纳分析法或演绎分析法，是否按照 GB/T 34590.4—2022 中表 1 的要求开展？	检查安全分析是否按照 GB/T 34590.4—2022 中的 6.4.4.1 定义安全分析深度和严谨度的准则来开展
9	分析结果是否表明已符合或违背相关安全目标或安全要求？	通过开展安全分析，应能得出结论：当前的设计是否可满足安全目标或安全要求
10	如果分析结果显示违背了安全目标或安全要求，其内容是否被用于导出新的避免，或检测，或降低影响的措施？	安全分析是一个迭代的过程，如果前期的安全分析结果表明违背了安全目标或安全要求的话，则需要进一步根据该结果导出新的措施，直至安全分析的结果符合安全目标或安全要求
11	由安全分析得出的措施应作为产品开发的一部分，是否按照相应的标准在各个开发层级得以实现？	检查所有安全措施是否被正确实现，其中： ——系统层面的措施按照 GB/T 34590.4—2022； ——硬件层面的措施按照 GB/T 34590.5—2022； ——软件层面的措施按照 GB/T 34590.6—2022
12	对于在该层级安全分析中识别到的、未被已有安全目标覆盖的新的风险，是否按照表 2，重新进行了危害分析和风险评估，且相应的变更按照表 12 变更管理的审核及评估检查清单的要求实施？	呼应概念阶段的危害分析和风险评估，确保整个产品开发过程中安全分析的有效迭代。 例如：在系统阶段的安全分析如果发现新的风险，在此前的概念阶段中没有分析到，则触发变更流程，对此前的危害分析和风险评估进行变更，将新识别到的风险纳入其中
13	安全分析所用到的故障模式是否和其对应的研发子阶段的详细程度相适应并保持一致？	子阶段包括 GB/T 34590.5—2022 中的硬件设计、对硬件架构指标的评估以及由于随机硬件失效而导致的违背安全目标的评估，或按照 GB/T 34590.6—2022 进行的软件架构设计。 关于软件架构层面的安全性分析，见 GB/T 34590.6—2022 附录 E
14	如果必要，是否通过使用故障模式和分析结果来确定额外的安全相关测试用例？	当安全分析中采用的故障模式和分析结果不太笃定，或者结果比较接近目标临界值，可适当地设计额外的测试用例来佐证相关的分析
15	安全分析及所有输出是否按照标准 GB/T 34590.8—2022 第 9 章验证过？	和所有其他安全活动的输出一样，安全分析的过程和输出需要按照标准进行确认，手段包括评审、测试、仿真等

表 E.4　归纳分析和演绎分析开展审核及评估的说明及示例（续）

序号	检查清单	说明及示例
16	定性的安全分析是否系统性地识别哪些会违背安全目标或安全要求的故障或失效？包括相关项或要素本身，相关项或要素与其他相关项或要素之间的交互，以及相关项或要素的使用	为了识别完整的故障和失效，针对目标层级，既要考虑要素其本身，其跟外部的交互（接口、边界），及其具体的用法，从内部到外部，整体考虑
17	定性的安全分析是否对每个已识别的故障的后果进行评估，以确认违背安全目标或安全要求的潜在可能性	是否遍历了所有故障，并对其造成的后果进行评估
18	定性的安全分析是否识别对每个已识别故障的原因？	是否遍历了所有故障，识别其原因
19	定性的安全分析是否识别或支持识别安全概念的潜在薄弱环节？包括对处理诸如潜在故障、多点故障、共因失效及级联失效这种异常的安全机制的无效性？	—
20	如果定量分析用于补充定性分析，该分析是否考虑了用于支持硬件架构度量的指标和会违背安全目标和安全要求的硬件随机失效评估的定量数据？	—
21	如果定量分析用于补充定性分析，该分析是否考虑了系统性地识别那些会违背安全目标或安全要求的故障或失效？	—
22	如果定量分析用于补充定性分析，该分析是否考虑了安全概念潜在的薄弱点，包括对安全机制的不足进行评估和分级？	—
23	如果定量分析用于补充定性分析，该分析是否考虑了诊断测试时间间隔，紧急运行时间间隔和从故障探测到修复的时间间隔？	—
24	从（系统、软件、硬件）安全分析到（系统、软件、硬件）需求规范或（系统、软件、硬件）需求概念的可追溯性是否完整？如适用，相应的变更流程是否完成？	如适用，关注（系统、软件、硬件）需求规范或（系统、软件、硬件）需求概念的变更记录是否追溯到相应的安全分析条目