



中华人民共和国国家标准

GB/T 43253.4—2023

道路车辆 功能安全审核及评估方法 第4部分：硬件层面

Road vehicles—Functional safety audit and assessment method—
Part 4: Hardware level

2023-11-27 发布

2023-11-27 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 一般要求	1
5 硬件安全要求	2
5.1 目标	2
5.2 审核及评估的输入	2
5.3 审核及评估的要求	2
6 硬件设计	3
6.1 目标	3
6.2 审核及评估的输入	3
6.3 审核及评估的要求	4
7 硬件架构度量的评估	6
7.1 目标	6
7.2 审核及评估的输入	6
7.3 审核及评估的要求	6
8 随机硬件失效导致违背安全目标的评估	7
8.1 目标	7
8.2 审核及评估的输入	7
8.3 审核及评估的要求	7
9 硬件集成和验证	8
9.1 目标	8
9.2 审核及评估的输入	8
9.3 审核及评估的要求	9
10 硬件要素评估	10
10.1 目标	10
10.2 审核及评估的输入	10
10.3 审核及评估的要求	10
附录 A (资料性) 硬件安全要求	13
附录 B (资料性) 硬件设计	16
附录 C (资料性) 硬件架构度量的评估	21

GB/T 43253.4—2023

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

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件是 GB/T 43253《道路车辆 功能安全审核及评估方法》的第 4 部分。GB/T 43253 已经发布了以下部分：

- 第 1 部分：通用要求；
- 第 2 部分：概念阶段和系统层面；
- 第 3 部分：软件层面；
- 第 4 部分：硬件层面。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国汽车标准化技术委员会(SAC/TC 114)归口。

本文件起草单位：中国汽车技术研究中心有限公司、知行汽车科技(苏州)有限公司、北京地平线机器人技术研发有限公司、南京芯驰半导体科技有限公司、英飞凌科技资源中心(上海)有限公司、中国第一汽车集团有限公司、中国长安汽车集团有限公司、东软睿驰汽车技术(上海)有限公司、上海机动车检测认证技术研究中心有限公司、上海禾赛科技有限公司、深圳市大疆卓见科技有限公司、舍弗勒(中国)有限公司、北京长安汽车工程技术研究有限责任公司、北京国家新能源汽车技术创新中心有限公司。

本文件主要起草人：宋炜瑾、蔡香、魏斌、唐沙南、付越、尚世亮、李波、邵海贺、闻继伟、王潇屹、王宇、孙毓阳、赵鑫、刘辉、张晓亮、查小东、李兆麟。

引 言

GB/T 43253《道路车辆 功能安全审核及评估方法》以 GB/T 34590《道路车辆 功能安全》为基础,适用于道路车辆上安全相关的电气/电子(E/E)系统在其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 模型为产品开发的阶段、对象和范围,提供审核及评估参考过程模型。

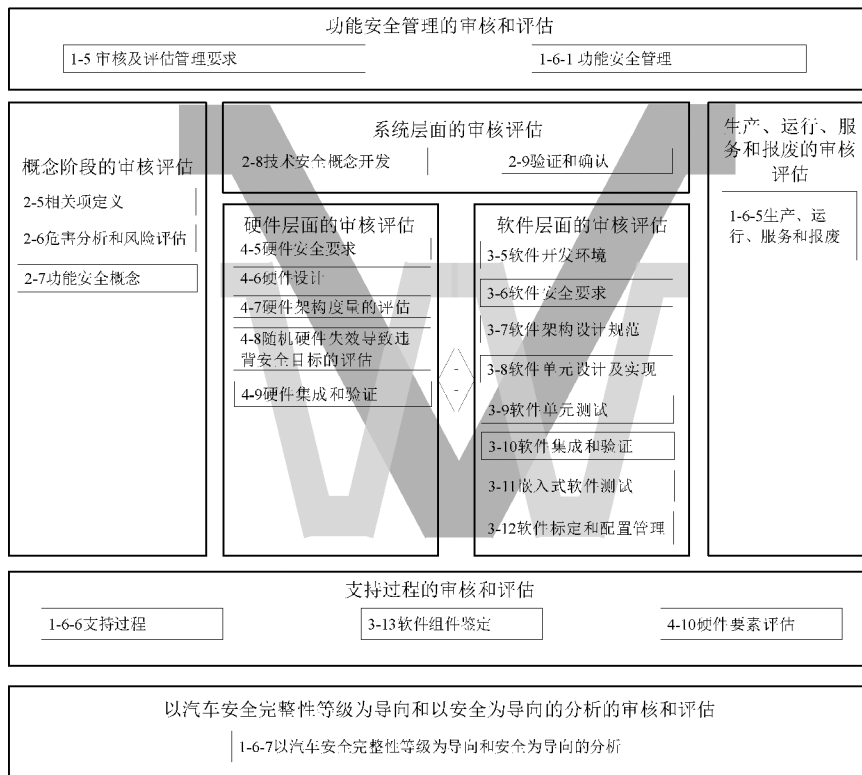


图 1 功能安全审核及评估概览

道路车辆 功能安全审核及评估方法

第4部分：硬件层面

1 范围

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

本文件适用于安装在除轻便摩托车外的量产道路车辆上的包含一个或多个电气/电子(E/E)系统的与安全相关的系统。

本文件不适用于特殊用途车辆上特定的电气/电子(E/E)系统,例如,为残疾驾驶者设计的车辆系统。

2 规范性引用文件

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

GB/T 34590.1~34590.12—2022 道路车辆 功能安全

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

3 术语和定义

GB/T 34590.1—2022 界定的术语和定义适用于本文件。

4 一般要求

GB/T 43253.1—2023 中定义的审核及评估要求适用于本文件。

硬件层面的功能安全审核及评估,主要涉及以下内容:

- 硬件安全要求的定义;
- 硬件设计;
- 硬件架构度量的评估;
- 随机硬件失效导致违背安全目标的评估;
- 硬件集成和验证;
- 硬件要素评估。

通过审核及评估,基于证据判断硬件层面的功能安全开发,符合:

- 硬件安全要求是恰当和完整的;
- 通过设计、验证保证硬件能实现硬件功能安全要求并满足软硬件接口规范;
- 提供基于硬件架构度量的证据,来证明相关项硬件架构设计在安全相关的随机硬件失效探测和控制方面的适用性;
- 确保所开发硬件符合硬件安全要求;
- 确保硬件要素的功能表现足以满足分配的安全要求。