ICS 43.040
CCS T 35

中华人民共和国国家标准

GB/T 34590.7—2022
代替 GB/T 34590.7—2017

道路车辆　功能安全
第7部分：生产、运行、服务和报废

Road vehicles—Functional safety—
Part 7: Production, operation, service and decommissioning

（ISO 26262-7:2018，MOD）

2022-12-30 发布　　2023-07-01 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 …… Ⅴ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 2
4　要求 …… 2
4.1　目的 …… 2
4.2　一般要求 …… 2
4.3　表的诠释 …… 2
4.4　基于 ASIL 等级的要求和建议 …… 3
4.5　摩托车的适用性 …… 3
4.6　载货汽车、客车、专用汽车、挂车的适用性 …… 3
5　生产、运行、服务和报废计划 …… 3
5.1　目的 …… 3
5.2　总则 …… 3
5.3　本章的输入 …… 4
5.4　要求和建议 …… 4
5.5　工作成果 …… 6
6　生产 …… 7
6.1　目的 …… 7
6.2　总则 …… 7
6.3　本章的输入 …… 7
6.4　要求和建议 …… 7
6.5　工作成果 …… 8
7　运行、服务和报废 …… 8
7.1　目的 …… 8
7.2　总则 …… 8
7.3　本章的输入 …… 8
7.4　要求和建议 …… 9
7.5　工作成果 …… 9
附录 A（资料性）　生产、运行、服务和报废的概览和文档流 …… 10
参考文献 …… 12

如需获取标准全文请联系以下：

通讯地址:广州市番禺区石碁镇创运路8号

联系电话：18680502391

E-mail: yuanyf@grgtest.com

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 34590《道路车辆　功能安全》的第7部分。GB/T 34590已经发布了以下部分：

——第1部分：术语；

——第2部分：功能安全管理；

——第3部分：概念阶段；

——第4部分：产品开发：系统层面；

——第5部分：产品开发：硬件层面；

——第6部分：产品开发：软件层面；

——第7部分：生产、运行、服务和报废；

——第8部分：支持过程；

——第9部分：以汽车安全完整性等级为导向和以安全为导向的分析；

——第10部分：指南；

——第11部分：半导体应用指南；

——第12部分：摩托车的适用性。

本文件代替GB/T 34590.7—2017《道路车辆　功能安全　第7部分：生产和运行》，与GB/T 34590.7—2017相比，除结构调整和编辑性改动外，主要技术变化如下：

——标准适用范围由“量产乘用车”更改为“除轻便摩托车外的量产道路车辆”（见第1章，2017年版的第1章）；

——增加了摩托车的适用性要求（见4.5）；

——增加了载货汽车、客车、专用汽车、挂车的适用性要求（见4.6）；

——更改了生产、运行、服务和报废计划的目的（见5.1，2017年版的5.1）；

——更改了生产、运行、服务和报废计划的总则（见5.2，2017年版的5.2）；

——更改了生产、运行、服务和报废计划的前提条件（见5.3.1，2017年版的5.3.1）；

——更改了生产、运行、服务和报废计划的支持信息（见5.3.2，2017年版的5.3.2）；

——更改了计划相关项及其要素的生产过程要考虑的内容（见5.4.1.1，2017年版的5.4.1.1）；

——将“批量试生产”更改为“试生产”（见5.4.2，2017年版的5.4.2）；

——更改了试生产过程和目标批量生产过程的差异目的（见5.4.2.2，2017年版的5.4.2.2）；

——增加了报废的要求、紧急救援服务的要求[见5.4.3.1中的列项c)和d)]；

——将“报警和降级概念”更改为“报警和降级策略”（见5.3.1、5.4.3.1、5.4.3.4，2017年版的6.4.1.1、6.4.1.4）；

——将“维护工具和手段”更改为“工具和设备”（见5.4.3.3，2017年版的6.4.1.3）；

——增加了救援服务信息（见5.4.3.7、5.5.10）；

——更改了生产相关前提条件（见6.3，2017年版的5.3.1）；

——更改了测试设备应按照所采用的质量管理体系进行控制（见6.4.1.4，2017年版的5.4.3.4）；

——更改了运行、服务和报废的目的（见7.1，2017年版的6.1）；

——更改了运行、服务和报废的总则（见7.2，2017年版的6.2）；

——更改了运行、服务和报废的前提条件（见7.3.1，2017年版的6.3.1）。

本文件修改采用 ISO 26262-7:2018《道路车辆　功能安全　第 7 部分:生产、运行、服务和报废》。

本文件与 ISO 26262-7:2018 的技术差异及其原因如下:

——用规范性引用的 GB/T 34590.1—2022 替换了 ISO 26262-1(见第 3 章,ISO 26262-7 的第 3 章),以适应我国国情 ;

——更改了对 T&B 车辆的描述,由“卡车、客车、挂车和半挂车”更改为“载货汽车、客车、专用汽车、挂车”(见 4.6,ISO 26262-7:2018 的 4.6),与 GB/T 3730.1—2022《汽车、挂车及汽车列车的术语和定义　第 1 部分:类型》中规定的车辆类型保持一致。

本文件做了下列编辑性修改:

——调整了范围中段落的顺序;

——将规范性引用的 GB/T 34590.12—2022 列在第 2 章清单中;

——删除了 ISO 26262-7:2018 的第 3 章中 ISO 和 IEC 维护的用于标准化的术语数据库网址;

——将 ISO 26262-7:2018 中 5.2 的最后一段更改为列项;

——将 ISO 26262-7:2018 的 5.4.3.1j)更正为 5.4.3.1i);

——删除了 ISO 26262-7:2018 中的章条号 6.3.1、7.5.1。

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、长城汽车股份有限公司、采埃孚汽车科技(上海)有限公司、比亚迪汽车工业有限公司、华为技术有限公司、泛亚汽车技术中心有限公司、耐世特汽车系统(苏州)有限公司、东软睿驰汽车技术(沈阳)有限公司、中国第一汽车集团有限公司、舍弗勒(中国)有限公司、北京华特时代电动汽车技术有限公司、博世汽车部件(苏州)有限公司、戴姆勒大中华区投资有限公司、兴科迪科技(泰州)有限公司、北京宝沃汽车股份有限公司、上海蔚来汽车有限公司、上海金脉电子科技有限公司、上汽大众汽车有限公司、中车时代电动汽车股份有限公司、蜂巢能源科技有限公司、上汽大通汽车有限公司、上海海拉电子有限公司、华霆(合肥)动力技术有限公司、株洲中车时代电气股份有限公司、苏州汇川联合动力系统有限公司、宇通客车股份有限公司。

本文件主要起草人:李波、祁新华、李欣然、付越、马芳平、魏芳、尚世亮、邵海贺、郭晓东、梁瑜、薛剑波、庄萍、曲元宁、吕明、钱秋华、赵田丽、周宇、张会玲、张乐敏、李勇、史晓密、王志鹏、史婷、余建业、郭梦鸽、劳力、陈磊、刘畅、黄雪生。

本文件及其所代替文件的历次版本发布情况为:

——2017 年首次发布为 GB/T 34590.7—2017;

——本次为第一次修订。

引　言

ISO 26262 是以 IEC 61508 为基础，为满足道路车辆上电气/电子系统的特定需求而编写。

GB/T 34590 修改采用 ISO 26262，适用于道路车辆上由电子、电气和软件组件组成的安全相关系统在安全生命周期内的所有活动。

安全是道路车辆开发的关键问题之一，汽车功能的开发和集成强化了对功能安全的需求，并且要求提供满足功能安全目标的证明。

随着技术日益复杂、软件和机电一体化的广泛应用，来自系统性失效和随机硬件失效的风险逐渐增加，这些都在功能安全的考虑范畴之内。GB/T 34590 通过提供适当的要求和流程来降低风险。

为了实现功能安全，GB/T 34590：

a) 提供了一个汽车安全生命周期（开发、生产、运行、服务、报废）的参考，并支持在这些生命周期阶段内对执行的活动进行剪裁；

b) 提供了一种汽车特定的基于风险的分析方法，以确定汽车安全完整性等级（ASIL）；

c) 使用 ASIL 等级来定义 GB/T 34590 中适用的要求，以避免不合理的残余风险；

d) 提出了对于功能安全管理、设计、实现、验证、确认和认可措施的要求；

e) 提出了客户与供应商之间关系的要求。

GB/T 34590 针对的是电气/电子系统的功能安全，通过安全措施（包括安全机制）来实现。GB/T 34590 也提供了一个框架，在该框架内可考虑基于其他技术（例如，机械、液压、气压）的安全相关系统。

功能安全的实现受开发过程（例如，需求规范、设计、实现、集成、验证、确认和配置）、生产过程、服务过程和管理过程的影响。

安全问题与常规的以功能为导向和以质量为导向的活动及工作成果相互关联。GB/T 34590 涉及与安全相关的开发活动和工作成果。GB/T 34590 包含 12 个部分。

——第 1 部分：术语。界定了 GB/T 34590 所应用的术语和定义。

——第 2 部分：功能安全管理。描述了应用于汽车领域的功能安全管理的要求，包括独立于项目的关于所涉及组织的要求（整体安全管理）以及项目特定的在安全生命周期内关于管理活动的要求。

——第 3 部分：概念阶段。描述了车辆在概念阶段进行相关项定义、危害分析和风险评估、功能安全概念的要求。

——第 4 部分：产品开发：系统层面。描述了车辆在系统层面产品开发的要求，包括启动系统层面产品开发总则、技术安全要求的定义、技术安全概念、系统架构设计、相关项集成和测试、安全确认。

——第 5 部分：产品开发：硬件层面。描述了车辆在硬件层面产品开发的要求，包括硬件层面产品开发的概述、硬件安全要求的定义、硬件设计、硬件架构度量的评估、因随机硬件故障而导致违背安全目标的评估、硬件集成和验证。

——第 6 部分：产品开发：软件层面。描述了车辆在软件层面产品开发的要求，包括软件层面产品开发的概述、软件安全要求的定义、软件架构设计、软件单元设计和实现、软件单元验证、软件集成和验证、嵌入式软件测试、可配置软件。

——第7部分：生产、运行、服务和报废。描述了车辆在生产、运行、服务和报废的要求，包括生产、运行、服务和报废计划及具体要求。

——第8部分：支持过程。描述了对支持过程的要求，包括分布式开发的接口、安全要求的定义和管理、配置管理、变更管理、验证、文档管理、使用软件工具的置信度、软件组件的鉴定、硬件要素评估、在用证明、GB/T 34590适用范围之外应用的接口、未按照GB/T 34590开发的安全相关系统的集成。

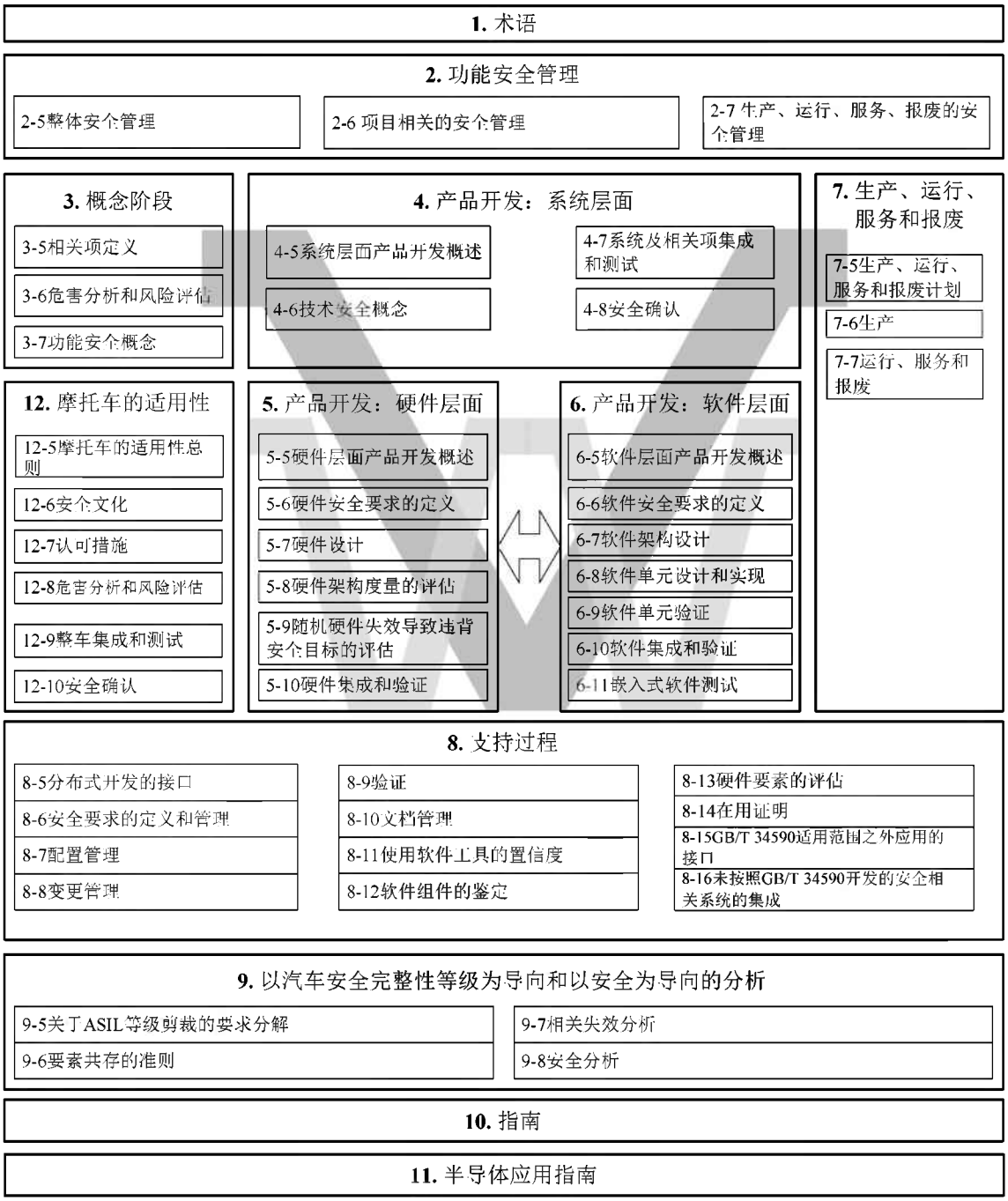
——第9部分：以汽车安全完整性等级为导向和以安全为导向的分析。描述了关于ASIL剪裁的要求分解、要素共存的准则、相关失效分析、安全分析等活动的要求。

——第10部分：指南。目的是增强对GB/T 34590其他部分的理解，提供了GB/T 34590中的关键概念、安全管理的精选话题、概念阶段和系统开发、安全过程的要求结构(流程和顺序)、硬件开发、独立于环境的安全要素、在用证明的示例、ASIL的分解、带安全相关可用性要求的系统、关于“所使用软件工具的置信度”的分析、安全相关的特殊特性、故障树的构建和应用等方面的指南。

——第11部分：半导体应用指南。提供了GB/T 34590其他部分针对半导体开发的参考，包括半导体组件及其分区、特定半导体技术和应用案例、如何使用数字失效模式进行诊断覆盖率评估、相关失效分析、数字组件定量分析、模拟组件的定量分析、PLD组件定量分析等方面的指南。

——第12部分：摩托车的适用性。描述了GB/T 34590其他部分对摩托车适用性的要求，包括对摩托车适用性的一般要求、安全文化、认可措施、危害分析和风险评估、整车集成与测试、安全确认。

GB/T 34590基于V模型为产品开发的不同阶段提供参考过程模型，图1为GB/T 34590的整体架构。



注 1：阴影“V”表示 GB/T 34590.3—2022、GB/T 34590.4—2022、GB/T 34590.5—2022、GB/T 34590.6—2022、GB/T 34590.7—2022 之间的相互关系。

注 2：对于摩托车：

——GB/T 34590.12—2022 的第 8 章支持 GB/T 34590.3—2022；

——GB/T 34590.12—2022 的第 9 章和第 10 章支持 GB/T 34590.4—2022。

注 3：以“*m*-*n*”方式表示的具体章条中，“*m*”代表特定部分的编号，“*n*”代表该部分章的编号。

示例：“2-6”代表 GB/T 34590.2—2022 的第 6 章。

图 1　GB/T 34590 概览

道路车辆　功能安全
第7部分：生产、运行、服务和报废

1　范围

本文件规定了车辆生产、运行、服务和报废的要求及相关计划活动。

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/电子系统，例如，为残疾驾驶者设计的车辆系统。

注：其他专用的安全标准可作为本文件的补充，反之亦然。

已经完成生产发布的系统及其组件或在本文件发布日期前正在开发的系统及其组件不适用于本文件。对于在本文件发布前完成生产发布的系统及其组件进行变更时，本文件基于这些变更对安全生命周期的活动进行裁剪。未按照本文件开发的系统与按照本文件开发的系统进行集成时，需要按照本文件进行安全生命周期的裁剪。

本文件针对由安全相关的电气/电子系统的功能异常表现而引起的可能的危害，包括这些系统相互作用而引起的可能的危害。本文件不针对与触电、火灾、烟雾、热、辐射、毒性、易燃性、反应性、腐蚀性、能量释放等相关的危害和类似的危害，除非危害是直接由安全相关的电气/电子系统的功能异常表现而引起的。

本文件提出了安全相关的电气/电子系统进行功能安全开发的框架，该框架旨在将功能安全活动整合到企业特定的开发框架中。本文件提供了为实现产品功能安全的技术开发要求，也提供了组织具备相应功能安全能力的开发流程要求。

本文件不针对电气/电子系统的标称性能。

附录A概述了本文件的目标、前提条件和工作成果。

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—2022　道路车辆　功能安全　第1部分：术语（ISO 26262-1：2018，MOD）

GB/T 34590.2—2022　道路车辆　功能安全　第2部分：功能安全管理（ISO 26262-2：2018，MOD）

注：GB/T 34590.2—2022被引用的内容与ISO 26262-2：2018被引用的内容没有技术上的差异。

GB/T 34590.3—2022　道路车辆　功能安全　第3部分：概念阶段（ISO 26262-3：2018，MOD）

注：GB/T 34590.3—2022被引用的内容与ISO 26262-3：2018被引用的内容没有技术上的差异。

GB/T 34590.4—2022　道路车辆　功能安全　第4部分：产品开发：系统层面（ISO 26262-4：2018，MOD）

注：GB/T 34590.4—2022被引用的内容与ISO 26262-4：2018被引用的内容没有技术上的差异。

GB/T 34590.5—2022 道路车辆 功能安全 第5部分：产品开发：硬件层面(ISO 26262-5：2018，MOD)

注：GB/T 34590.5—2022被引用的内容与ISO 26262-5：2018被引用的内容没有技术上的差异。

GB/T 34590.8—2022 道路车辆 功能安全 第8部分：支持过程(ISO 26262-8：2018，MOD)

注：GB/T 34590.8—2022被引用的内容与ISO 26262-8：2018被引用的内容没有技术上的差异。

GB/T 34590.9—2022 道路车辆 功能安全 第9部分：以汽车安全完整性等级为导向和以安全为导向的分析(ISO 26262-9：2018，MOD)

注：GB/T 34590.9—2022被引用的内容与ISO 26262-9：2018被引用的内容没有技术上的差异。

GB/T 34590.12—2022 道路车辆 功能安全 第12部分：摩托车的适用性(ISO 26262-12：2018，MOD)

注：GB/T 34590.12—2022被引用的内容与ISO 26262-12：2018被引用的内容没有技术上的差异。

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 要求

4.1 目的

本章规定了：

a) 如何符合GB/T 34590；

b) 如何解释GB/T 34590中所使用的表格；

c) 如何解释各章条基于不同的ASIL等级的适用性。

4.2 一般要求

如声明满足GB/T 34590的要求时，应满足每一个要求，除非有下列情况之一：

a) 按照GB/T 34590.2—2022的要求，安全活动的剪裁已经实施并表明这些要求不适用；或

b) 不满足要求的理由存在且是可接受的，并且按照GB/T 34590.2—2022的要求对该理由进行了评估。

标有“注”或“示例”的信息仅用于辅助理解或阐明相关要求，不应作为要求本身且不具备完备性。

将安全活动的结果作为工作成果，应具备上一阶段工作成果作为“前提条件”的信息。如果章条的某些要求是依照ASIL定义的或可剪裁的，某些工作成果可不作为前提条件。

“支持信息”是可供参考的信息，但在某些情况下，GB/T 34590不要求其作为上一阶段的工作成果，并且可以是由不同于负责功能安全活动的人员或组织等外部资源提供的信息。

4.3 表的诠释

本文件中的表是规范性或资料性取决于上下文。在满足相关要求时，表中列出的不同方法有助于置信度水平。表中的每个方法是：

a) 一个连续的条目(在最左侧列以顺序号标明，如1、2、3)；或

b) 一个选择的条目(在最左侧列以数字后加字母标明，如2a、2b、2c)。

对于连续的条目，高度推荐和推荐的方法按照 ASIL 等级推荐予以使用。高度推荐或推荐的方法允许用未列入表中的其他方法替代，此种情况下，应给出满足相关要求的理由。如果可以给出不选择所有条目也能符合相应要求的理由，则不需要对缺省方法做进一步解释。

对于选择性的条目，应按照指定的 ASIL 等级对这些方法进行适当的组合，而与这些方法在表中是否列出无关。如果所列出的方法对于一个 ASIL 等级来说具有不同的推荐等级，宜采用具有较高推荐等级的方法。应给出选择组合方法或选择单一方法满足相应要求的理由。

注：在表中所列出方法的理由是充分的。但是，这并不意味着有倾向性或对未列到表中的方法表示反对。

对于每种方法，应用相关方法的推荐等级取决于 ASIL 等级，分类如下：

——“++”表示对于指定的 ASIL 等级，高度推荐该方法；

——“+”表示对于指定的 ASIL 等级，推荐该方法；

——“o”表示对于指定的 ASIL 等级，不推荐也不反对该方法。

4.4 基于 ASIL 等级的要求和建议

若无其他说明，对于 ASIL A、B、C 和 D 等级，应满足每一章条的要求或建议。这些要求和建议参照安全目标的 ASIL 等级。如果在项目开发的早期对 ASIL 等级完成了分解，按照 GB/T 34590.9—2022 的第 5 章的要求，应遵循分解后的 ASIL 等级。

如果 GB/T 34590 中 ASIL 等级在括号中给出，则对于该 ASIL 等级，相应的章条应被认为是推荐而非要求。这里的括号与 ASIL 等级分解无关。

4.5 摩托车的适用性

对于适用于 GB/T 34590.12—2022 要求的摩托车的相关项或要素，GB/T 34590.12—2022 的要求替代本文件和 GB/T 34590.2—2022 的相应要求。

4.6 载货汽车、客车、专用汽车、挂车的适用性

本文件对载货汽车、客车、专用汽车、挂车的特殊规定以“T&B”来表示。

5 生产、运行、服务和报废计划

5.1 目的

本章的目的是：

a) 为拟安装在道路车辆上的安全相关的要素或相关项，开发和维护一个生产过程；

注：该目的可以通过组织符合 IATF 16949 或等效标准的要求来实现。这与组织所在安全供应链中的位置及其所生产的安全相关要素的复杂度有关。

b) 为接触安全相关的相关项或要素的用户，开发关于运行、服务（维护和维修）和报废的必要信息，确保在车辆的整个生命周期实现功能安全。

5.2 总则

本章的要求和建议适用于相关项和要素的生产、运行、服务和报废计划，及其在车辆上的安装。

为了实现功能安全，相关项或要素在其生产中，需满足其安全相关的特殊特性。这些特殊特性是在开发阶段被识别出来的。这些安全相关的特殊特性的示例有：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。

本章规定了通过将这些安全相关的特殊特性包含在生产计划和生产控制中，以确保在生产过程中实现功能安全的要求。

本章还规定了与如下内容相关的要求：

——如何描述服务信息和用户信息(包括用户手册)；

——维护工作的计划、执行和监控；

——维修指导说明；

——报废指导说明；

——救援服务的指导说明和有关信息。

5.3 本章的输入

5.3.1 前提条件

应具备如下信息：

——生产、运行、服务和报废需求规范，按照 GB/T 34590.4—2022 的 6.5.5 和 GB/T 34590.5—2022 的 7.5.4；

——硬件专用措施的定义，按照 GB/T 34590.5—2022 的 9.5.2；

——包含在功能安全概念中的报警和降级策略，按照 GB/T 34590.3—2022 的 7.5.1。

5.3.2 支持信息

可以考虑如下信息：

——生产计划(来自外部)；

——生产控制计划(来自外部)；

——在系统、软件或硬件层面的技术规范或设计中的相关内容。

5.4 要求和建议

5.4.1 生产计划

5.4.1.1 应计划相关项及其要素的生产过程，该计划考虑如下内容：

a) 对生产的要求；

示例 1：装配指导说明(例如，传感器的标定和设置)。

示例 2：IPC(印刷电路协会)相关标准的要求。

b) 安全相关的特殊特性；

示例 3：所选要素的公差。

示例 4：坡度传感器的下线标定。

c) 要素的处理和管理条件；

示例 5：硬件要素的允许存储时间。

示例 6：ECU 软件的正确程序设定。

d) 产品开发过程中定义的配置；

e) 从以前发布的生产计划中获得的经验总结；

f) 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；

g) 人员的能力。

5.4.1.2 生产计划应描述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：

a) 生产工艺流程和指导说明；

注：生产流程也可包括要素的返工。

示例 1：有三个或更少引脚的元器件的不良焊接点的返工说明。

b) 生产工具和设备；

c) 可追溯性措施的实施；

示例 2：对要素使用标签。

d) 如果适用，专用措施的实施，按照 GB/T 34590.5—2022 的 9.5.2。

5.4.1.3 应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。

示例 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。

示例 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。

5.4.1.4 应识别可合理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。

示例：过程失效模式和影响分析(PFMEA)。

5.4.1.5 制定生产控制计划时，应考虑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。

5.4.1.6 应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。

5.4.1.7 计划生产时识别的安全要求，应按照 GB/T 34590.2—2022 的第 6 章，以适当的方式反馈给负责系统、硬件和软件开发的人员。

示例：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。

5.4.1.8 生产、运行、服务和报废的变更，如影响相关项或其要素，应按照 GB/T 34590.8—2022 中第 8 章的要求进行管理。

5.4.2 试生产

5.4.2.1 试生产过程及其控制措施宜能代表目标批量生产过程。

注：试生产是生产发布之前相关项或要素的生产。

5.4.2.2 在试生产阶段，可以分析试生产过程和目标批量生产过程的差异，以确定是否具备生产过程能力。

注 1：如果试生产过程和目标批量生产过程相同，可在试生产中获得符合 6.4.1.3 的生产过程能力。

注 2：差异可包括生产率、生产或控制步骤的顺序以及方法、测试设备和工具。

5.4.3 运行、服务和报废的计划

5.4.3.1 应制定相关项的运行、服务和报废过程的计划，并考虑以下因素：

a) 维护和维修的要求；

b) 为确保车辆安全运行而应具备的用户须知信息的要求(见 5.4.3.4)；

c) 报废的要求；

d) 紧急救援服务的要求；

e) 报警和降级策略；

f) 现场监控流程(见 7.4.1.1)；

g) 要素处理的条件；

示例 1：硬件要素的允许存储时间。

示例 2：ECU 上软件的正确刷写。

h) 在生产发布文件中定义的配置；

示例 3：在维修过程中，硬件、软件和软件标定数据允许的配置。

i) 参与人员的能力。

5.4.3.2 服务计划应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。

5.4.3.3 服务指导说明应描述如下内容：

a) 服务的流程、方法、工作步骤和诊断程序；

b) 工具和设备；

示例 1：程序设定、传感器标定和诊断设备。

c) 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；

d) 相关项或要素的有关配置，包括可追溯性措施；

注：如果在服务中进行重刷软件，刷写软件的工具具有确保车辆下载了正确版本软件的功能。

示例 2：对要素使用标签，确保可追溯性。

e) 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；

f) 当功能关闭和其他变更发生时，需告知驾驶员；

示例 3：通知驾驶员某项辅助功能已经被关闭。

g) 备件的供应。

5.4.3.4 用户信息，包括用户手册，应提供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：

a) 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；

b) 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；

c) 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；

d) 关于与第三方产品交互所导致的已知危害的警告；

示例 1：当使用额外第三方的拖载挂车时，需要告知用户泊车辅助将不能检查车辆后方。

e) 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。

示例 2：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。

5.4.3.5 报废指导说明应描述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。

示例：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。

5.4.3.6 在运行、服务和报废的计划过程中识别的安全要求，应按照 GB/T 34590.2—2022 的第 6 章，以适当的方式反馈给负责系统、硬件和软件开发的人员。

示例：ECU 中的错误日志功能的软件规范，以便于服务中进行诊断。

5.4.3.7 救援服务信息，包括救援指导说明书或紧急救援指南，如果适用，应提供相关指导说明和警告，以避免救援操作时发生危害。

示例：防止非期望的气囊点爆或电击伤害的信息。

5.5 工作成果

5.5.1 生产计划的安全相关内容，由 5.4.1.1、5.4.1.2、5.4.1.3 和 5.4.1.4 的要求得出。

5.5.2 生产控制计划（含测试计划）的安全相关内容，由 5.4.1.5 和 5.4.1.6 的要求得出。

5.5.3 可生产性需求规范，由 5.4.1.7 的要求得出。

注：此规范可包含在对应阶段的相关文档中。

5.5.4 生产过程能力报告，由 5.4.2.2 的要求得出。

5.5.5 服务计划中安全相关的内容，由 5.4.3.1～5.4.3.3 的要求得出。

5.5.6 服务指导说明中安全相关的内容，由 5.4.3.3 的要求得出。

5.5.7 用户须知信息中安全相关的内容，由 5.4.3.4 的要求得出。

5.5.8 报废指导说明中安全相关的内容，由 5.4.3.5 的要求得出。

5.5.9 运行、服务、报废需求规范，由 5.4.3.6 的要求得出。

注：此规范可包含在对应阶段的相关文档中。

5.5.10 救援服务指导说明中安全相关的内容，由 5.4.3.7 的要求得出。

6 生产

6.1 目的

本章的目的是，通过对相关项及其要素的生产过程负责的有关制造商、个人或组织（如车辆制造商、供应商、子供应商等）来确保在生产阶段（产品发布给生产后）实现功能安全。

6.2 总则

本章的要求和建议适用于相关项及要素的生产，及其在车辆上的安装。

6.3 本章的输入

前提条件应具备如下信息：

——生产发布报告，按照 GB/T 34590.2—2022 的 6.5.6；

——生产计划中安全相关的内容，按照 5.5.1；

——生产控制计划（含测试计划）中的安全相关内容，按照 5.5.2；

——如果适用，可生产性需求规范，按照 5.5.3；

——如果适用，生产过程能力报告，按照 5.5.4。

6.4 要求和建议

6.4.1 生产

6.4.1.1 生产过程及其控制措施，应按照 5.4.1 定义的计划进行执行和维护。

注：这包括对参与生产的人员进行适当的培训。

6.4.1.2 应对生产过程（包括安全相关特殊特性的偏差）进行分析，目的是：

a) 识别过程失效；

b) 识别由于过程失效导致的对功能安全的潜在影响；

c) 采取恰当的措施，以确保识别的影响可以被避免或减轻；

注：这类措施可包括要素的进一步控制措施、整理分类、处理和更换。

d) 验证采取措施的有效性。

6.4.1.3 针对功能安全，应评估并维护如下几项能力：

a) 生产过程；

b) 设备和工具；

c) 测试设备。

注 1：生产过程能力的证据可通过，周期性的过程审核，或者是对每个执行过程步骤的人以及质量管理体系的周期性的资质认证措施来获得。

注 2：过程能力涵盖了维护安全相关特殊特性的能力。

6.4.1.4 测试设备应按照所采用的质量管理体系进行控制。

示例：IATF 16949 中对监控和测量设备的管理要求。

6.4.1.5 控制应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。

注 1：整车层面的受控对象的识别，可以是车辆识别号或生产序列号。

注 2：组件层面的受控对象的识别，可以是零件号或序列号。

注 3：控制结果可以是一个单一状态，如通过或不通过，或者是对采集的数据针对边界条件的评估结果。

6.4.1.6 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。

6.4.1.7 在生产阶段发起的生产过程的变更，应按照 GB/T 34590.8—2022 中第 8 章的要求进行管理。

6.5 工作成果

6.5.1 控制措施报告，由 6.4.1.1、6.4.1.2、6.4.1.5 和 6.4.1.6 的要求得出。

6.5.2 生产过程能力报告，由 6.4.1.3 和 6.4.1.4 的要求得出。

注：生产过程能力可包含在生产件批准程序(PPAP)文档中。

7 运行、服务和报废

7.1 目的

本章的目的是，确保在车辆生命周期的运行、服务(维护和维修)以及报废子阶段中实现功能安全。

7.2 总则

本章提出了对运行、服务和报废的执行与监控的要求，并考虑了相关项的安全相关的特殊特性。

报废过程可分为“拆卸前”“拆卸中”和“拆卸后”三个子阶段。本章针对“拆卸前”的活动提出要求，还包括对“拆卸中”的活动和措施的指导说明。

7.3 本章的输入

7.3.1 前提条件

应具备下列信息：

——生产发布报告，按照 GB/T 34590.2—2022 的 6.5.6；

——服务计划中安全相关的内容，按照 5.5.5；

——服务指导说明中安全相关的内容，按照 5.5.6；

——用户须知信息中安全相关的内容，按照 5.5.7；

——报废指导说明中安全相关的内容，按照 5.5.8；

——如果适用，运行、服务、报废需求规范，按照 5.5.9；

——如果适用，救援服务指导说明中安全相关的内容，按照 5.5.10。

7.3.2 支持信息

可考虑下列信息：

——维护计划(来自外部)。

7.4 要求和建议

7.4.1 运行、服务和报废

7.4.1.1 应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：

a) 提供能用于分析以探测功能安全问题存在的现场数据；

b) 分析现场数据，以探测功能安全问题的存在；

c) 启动相关措施，来处理识别到的功能安全问题。

注 1：现场监控数据可以提供按照 GB/T 34590.8—2022 中第 14 章的在用证明所需的证据，用于在其他环境中进行相关项或要素的后续发布。

注 2：安全相关事件的现场监控过程包括决策过程、定义遏制和纠正措施（例如，召回）以及向利益相关者报告事件。利益相关者可以是组织内部的，如果是分布式开发，也可以是组织外部的。

7.4.1.2 相关项或其要素的运行、服务和报废应按照服务计划、服务指导说明和报废指导说明来实施和文档化。

注 1：这包括维修和维护流程的应用，以及此应用的纸质或电子文档的提供。

注 2：包含 T&B 车辆要素的再制造。

注 3：零件的供应、存储和运输按照 5.4.3.1。

7.4.1.3 相关项或其要素的变更、运行（包括现场监控）以及服务或报废流程的变更，应按照 GB/T 34590.8—2022 中第 8 章的要求进行管理。

注：包含 T&B 车辆的再制造。

7.5 工作成果

现场观察指导说明，由 7.4.1.1 的要求得出。

附 录 A
（资料性）
生产、运行、服务和报废的概览和文档流

表 A.1 提供了生产和运行特定阶段的目的、前提条件和工作成果的概览。

表 A.1 生产、运行、服务和报废的概览

章	目的	前提条件	工作成果
5 生产、运行、服务和报废计划	本章的目的有： a) 为拟安装在道路车辆上的安全相关的要素或相关项，开发和维护一个生产过程； 注：该目的可以通过组织符合 IATF 16949 或等效标准的要求来实现。这与组织所在安全供应链中的位置及其所生产的安全相关要素的复杂度有关。 b) 为接触安全相关的相关项或要素的用户，开发关于运行、服务（维护和维修）和报废必要信息，确保在车辆的整个生命周期实现功能安全	——生产、运行、服务和报废需求规范，按照 GB/T 34590.4—2022 的 6.5.5 和 GB/T 34590.5—2022 的 7.5.4； ——硬件专用措施的定义，按照 GB/T 34590.5—2022 的 9.5.2； ——包含在功能安全概念中的报警和降级策略，按照 GB/T 34590.3—2022 的 7.5.1。	5.5.1 生产计划的安全相关内容，由 5.4.1.1、5.4.1.2、5.4.1.3 和 5.4.1.4 的要求得出。 5.5.2 生产控制计划（含测试计划）的安全相关内容，由 5.4.1.5 和 5.4.1.6 的要求得出。 5.5.3 可生产性需求规范，由 5.4.1.7 的要求得出。 5.5.4 生产过程能力报告，由 5.4.2.2 的要求得出。 5.5.5 服务计划中安全相关的内容，由 5.4.3.1～5.4.3.3 的要求得出。 5.5.6 服务指导说明中安全相关的内容，由 5.4.3.3 的要求得出。 5.5.7 用户须知信息中安全相关的内容，由 5.4.3.4 的要求得出。 5.5.8 报废指导说明中安全相关的内容，由 5.4.3.5 的要求得出。 5.5.9 运行、服务、报废需求规范，由 5.4.3.6 的要求得出。 5.5.10 救援服务指导说明中安全相关的内容，由 5.4.3.7 的要求得出。
6 生产	本章的目的是，通过对相关项及其要素的生产过程负责的有关制造商、个人或组织（如车辆制造商、供应商、子供应商等）来确保在生产阶段（产品发布给生产后）实现功能安全。	——生产发布报告，按照 GB/T 34590.2—2022 的 6.5.6； ——生产计划中的安全相关内容，按照 5.5.1； ——生产控制计划（含测试计划）中的安全相关内容，按照 5.5.2； ——如果适用，可生产性需求规范，按照 5.5.3； ——如果适用，生产过程能力报告，按照 5.5.4。	6.5.1 控制措施报告，由 6.4.1.1、6.4.1.2、6.4.1.5 和 6.4.1.6 的要求得出。 6.5.2 生产过程能力报告，由 6.4.1.3 和 6.4.1.4 的要求得出。

表 A.1　生产、运行、服务和报废的概览（续）

章	目的	前提条件	工作成果
7　运行、服务和报废	本章的目的是，确保在车辆生命周期的运行、服务（维护和维修）以及报废子阶段中实现功能安全。	——生产发布报告，按照GB/T 34590.2—2022 的6.5.6； ——服务计划中安全相关的内容，按照 5.5.5； ——服务指导说明中安全相关的内容，按照 5.5.6； ——用户须知信息中安全相关的内容，按照 5.5.7； ——报废指导说明中安全相关的内容，按照 5.5.8； ——如果适用，运行、服务、报废需求规范，按照5.5.9； ——如果适用，救援服务指导说明中安全相关的内容，按照 5.5.10。	现场观察指导说明，由 7.4.1.1 的要求得出。

参 考 文 献

[1] GB/T 34590.6—2022 道路车辆 功能安全 第6部分:产品开发:软件层面

[2] GB/T 34590.10—2022 道路车辆 功能安全 第10部分:指南

[3] GB/T 34590.11—2022 道路车辆 功能安全 第11部分:半导体应用指南

[4] IEC 61508 (all parts) Functional safety of electrical/electronic/programmable electronic safety-related systems

[5] IATF 16949 Quality management system requirements for automotive production and relevant service parts organizations