ICS

T

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

道路车辆 功能安全

第 7 部分：生产和运行

Road vehicles — Functional safety — Part 7: Production and operation

（征求意见稿）

2016.01.15

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

GB/T XXXXX《道路车辆 功能安全》包括十个部分：

——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：生产和运行；

——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。

本部分为GB/T XXXXX的第7部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分修改采用国际标准ISO 26262-7：2011 《道路车辆 功能安全 第7部分：生产和运行》（英文版）。

本部分的附录A为资料性附录。

本部分由国家标准化管理委员会提出。

本部分由全国汽车标准化技术委员会（SAC/TC114）归口。

本部分起草单位：

本部分主要起草人：

引　言

ISO 26262 是以 IEC61508 为基础，为满足道路车辆上特定电子电气系统的需求而编写。

ISO 26262 适用于道路车辆上特定的由电子、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。

安全是未来汽车发展的关键问题之一，不仅在驾驶辅助和动力驱动领域，而且在车辆动态控制和主被动安全系统领域，新的功能越来越多地触及到系统安全工程领域。这些功能的开发和集成将强化对安全相关系统开发流程的需求，并且要求提供满足所有合理的系统安全目标的证明。

随着技术日益复杂、软件内容和机电一体化应用不断增加，来自系统性失效和硬件随机失效的风险逐渐增加。ISO 26262 通过提供适当的要求和流程来避免风险。

系统安全是通过一系列安全措施实现的。安全措施通过各种技术（例如，机械、液压、气压、电子、电气、可编程电子等）实现且应用于开发过程中的不同层面。尽管 ISO 26262 针对的是电子电气系统的功能安全，但是它也提供了一个基于其它技术的与安全相关系统的框架。ISO 26262：

a) 提供了一个汽车安全生命周期(管理、开发、生产、运行、维护、报废)，并支持在这些生命周期阶段内对必要活动的剪裁；

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；

c) 应用汽车安全完整性等级规定 ISO 26262 中适用的要求，以避免不合理的残余风险；

d) 提供了对于确认和认可措施的要求，以确保达到一个充分、可接受的安全等级；

e) 提供了与供应商相关的要求。

功能安全受开发过程(例如包括需求规范、设计、实现、集成、验证、确认和配置)、生产过程、维护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开发活动和工作成果相互关联。ISO 26262涉及与安全相关的开发活动和工作成果。

图1为ISO 26262的整体架构。ISO 26262基于V模型为产品开发不同阶段提供过程参考：

— 阴影"V"表示标准中第 3、4、5、6 和 7 部分之间的关系；

— 以“m-n”方式表示的具体条款中，“m”代表特定部分的编号，“n”代表该部分章条的编号。

示例：“2-6”代表 GB/TXXXX-2 的第六章

图1 GB/T XXXXX概览

道路车辆 功能安全

第 7 部分：生产和运行

1 范围

GB/T XXXXX适用于安装在最大总质量不超过3.5吨的量产乘用车上的包含一个或多个电子电气系统的与安全相关的系统。

GB/T XXXXX不适用于安装在特殊用途车辆上的特定的电子电气系统，例如为残疾驾驶者设计的车辆。

已经完成生产发布的系统及其组件或在本标准发布日期前开发的系统及其组件不适用于本标准。对于在本标准发布前完成生产发布的系统及其组件进行进一步的开发或变更时，仅修改的部分需要按照本标准开发。

本标准针对由电子电气安全相关系统的故障行为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。本标准不针对与触电、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，除非危害是直接由电子电气安全相关系统的故障行为而引起的。

本标准不针对电子电气系统的标称性能，即使这些系统（例如主动和被动安全、制动系统、自适应巡航系统）有专用的功能性能标准。

本部分规定了生产、运行、维护和报废的要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 XXXXX-1:201X，道路车辆 功能安全 第1部分：术语；

GB/T XXXXX-2:201X，道路车辆 功能安全 第2部分：功能安全管理；

GB/T XXXXX-3:201X，道路车辆 功能安全 第3部分：概念阶段；

GB/T XXXXX-4:201X，道路车辆 功能安全 第4部分：产品开发：系统层面；

GB/T XXXXX-5:201X，道路车辆 功能安全 第5部分：产品开发：硬件层面；

GB/T XXXXX-6:201X，道路车辆 功能安全 第6部分：产品开发：软件层面；

GB/T XXXXX-8:201X，道路车辆 功能安全 第8部分：支持过程；

GB/T XXXXX-9:201X，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；

3 术语， 定义和缩略语

GB/T XXXXX-1给出的术语、定义和缩略语适用于本部分。

4 要求

4.1 一般要求

如声明满足GB/T XXXXX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 XXXXX-2 的要求，已经计划安全活动的剪裁并表明这些要求不适用，或，

b) 不满足要求的理由存在且可接受的，并且按照 GB/T XXXXX-2 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。上一阶段工作成果作为“前提条件”的这一信息应具备。如果条款的某些要求是依照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，但在某些案例中，GB/T XXXXX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。

4.2 对表格的诠释

表属于规范性表还是资料性表取决于上下文。在实现满足相关要求时，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（在最左侧栏以顺序号标明，如 1,2,3），或

b) 一个选择的条目（在最左侧栏以数字后加字母标明，如 2a，2b，2c）。

对于连续的条目，全部方法应按照ASIL等级推荐予以使用。除了所列出的方法外，如果应用所列出方法以外的其它方法，应给出满足相关要求的理由。

对于选择性的条目，按照ASIL等级指示的要求，应采用适当的方法组合，不依赖于组合的方法是否在表中列出。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，则应采用具有更高推荐等级的方法。应给出组合方法满足相关要求的理由。

注：在表中所列出的方法的理由是充分的。但是，这并不意味着有偏袒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，未推荐或反对该方法。

4.3 基于 ASIL 等级的要求和建议

若无其它说明，对于ASIL A, B, C和D等级，应满足每一子章条的要求或建议。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 XXXXX-9第5章的要求，应遵循分解后的ASIL等级。

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

5 生产

5.1 目的

本章的第一个目的是为安装在道路车辆上的安全相关要素或相关项开发和维护一个生产过程。

第二个目的是通过生产过程中负责的相关生产者、人员或组织（汽车生产商、供应商、二级供应商等）实现此过程中的功能安全。

5.2 总则

在相关项或要素的生产过程中，符合在开发阶段制定的、与这些相关项或要素安全相关的特殊特性，对实现功能安全是必要的。安全相关特殊特性的示例有：特定的过程参数（例如： 温度范围或紧固扭矩）、材料特性、制造公差或配置。

此阶段通过将这些安全相关特殊特性包含在生产计划和生产控制中，定义了确保在生产过程中实现功能安全的要求。

本章的要求和建议适用于相关项、系统或要素的生产和在车上的安装。

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、维护和报废的相关需求规范，按照GB/T XXXXX-4, 7.5.4 和GB/T XXXXX-5, 7.5.4；

— 硬件专用措施的定义，按照GB/T XXXXX-5，9.5.2；及

— 生产发布报告，按照GB/T XXXXX-4, 11.5.1。

5.3.2 支持信息

可考虑如下信息：

— 生产计划（来自外部）；及

— 生产控制计划（来自外部）

5.4 要求和建议

5.4.1 生产计划

5.4.1.1 应通过相关项评估并考虑以下信息而计划生产过程：

a) 生产要求；

示例：装配指导书 （例如：传感器的标定和设置）；安全相关特殊特性（例如：要素选取的误差范围）

b) 硬件要素的存储条件、运输条件和装卸条件；

示例：要素的允许存储时间。

c) 在生产发布文档中定义了的已批准的配置；

d) 从以前发布的生产计划中得到的关于能力的经验总结；

e) 有关安全相关特殊特性的生产过程、生产手段、工具和测试设备的适宜性；及

f) 人员的能力

5.4.1.2 生产计划应描述为达成相关项、系统或要素的功能安全而要求的生产步骤、次序和方法。包括：

a) 生产工艺流程和指导书；

b) 生产工具和手段

c) 可追溯性措施的实施；及

示例：对要素使用标签。

d) 如果适用，在硬件开发过程中按照GB/T XXXXX-5，9.4.2.4定义的、用于硬件元器件的专用措施的实施；

注：生产过程也包含对相关项进行返工所要求的过程和操作。

5.4.1.3 应定义确保正确的嵌入式软件和相关标定数据被下载到电子控制单元中的流程，该流程作为生产过程的一部分。

示例1：使用校验和，目的是将下载的可执行数据及配置数据的校验和，与该特定车型及车辆配置的正确校验和相比较。

示例2：从下载到电子控制单元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这个特定车辆的标定数据进行对比。

5.4.1.4 当开发生产控制计划时，应考虑相关项、系统或要素的控制描述和控制准则，以及安全相关特殊特性。

5.4.1.5 应在生产控制计划中描述控制步骤的次序和方法，以及必要的测试设备、工具和测试准则。

5.4.1.6 应识别合理的、可预见的过程失效及其对功能安全的影响，并应实施恰当的措施以处理相关过程失效。

5.4.1.7 应对制定生产计划过程中发现的相关项、系统或要素的可生产性（在系统、硬件或软件开发层面上）的安全要求进行定义，并指定给负责开发的人员（参见 GB/T XXXXX-4、GB/T XXXXX-5 和 GB/T XXXXX-6）。

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的插入到电控单元中。

5.4.1.8 如果在生产过程中需要对相关项、系统或要素进行变更，应符合 GB XXXXX-8，第 8 章中所描述的变更管理过程。

5.4.2 批量试生产

5.4.2.1 试生产过程及其控制措施宜与目标生产过程一致。

注：试生产是相关项、系统或要素在生产发布之前的生产。

5.4.2.2 应分析试生产过程和目标生产过程的差异，以识别生产过程的哪个部分能在试生产阶段被评估，以及对目标生产过程的哪个部分需要进行评估。

注：当按照GB/T XXXXX-2，6.4.9.4执行功能安全评估时，如果试生产过程和目标生产过程相同，则可以使用试生产评估的结果（如：生产过程能力的证明）。

示例：差异可能来自生产率、生产次序及方法、或者控制步骤，同时也可能来自必要的生产手段、测试设备和工具。

5.4.3 生产

5.4.3.1 应按计划实施并维护生产过程及其控制措施。

注：对参与生产的人员进行适当的培训是此项实施的一部分

5.4.3.2 应分析发生在生产中的过程失效（包含安全相关特殊特性与其授权范围的偏差）和它们对功能安全的潜在影响，应采取适当的措施并应验证这些措施维护功能安全的能力。

示例：这些措施可包括执行更进一步的控制措施、分类、处理和要素的交换。

5.4.3.3 关于功能安全，应评估并维护以下几项的能力：

a) 生产过程；

b) 生产手段；及

c) 工具和测试设备。

注1：过程能力可通过周期性的过程审核或通过对执行过程各步骤的人员的周期性鉴定措施来证明。

注2：过程能力涵盖了维护安全相关特殊特性的能力。

5.4.3.4 测试设备应受到监控仪器及测量仪器的控制。

5.4.3.5 应按照生产控制计划执行控制。相关的控制报告应包含下列信息：控制时间、受控对象的识别和控制结果。

注1：在人工控制的情况下，控制报告包含受控对象的识别和控制结果是充分的。

注2：受控对象的识别可以是车辆识别码、整车级控制措施的生产码、受控组件的零件号或序列号。

注3：控制结果可由单一状态（比如，通过或不通过）或者对搜集的数据进行边界限制评估来组成。

5.4.3.6 除非与生产发布文档的偏差得到责任人的授权，否则应仅按照生产发布文档中定义的批准配置进行生产。生产发布文档可根据授权的偏差进行后续更新。

5.4.3.7 在生产阶段启动的、对生产过程的变更应符合第5章的要求。

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、5.4.1.6 和 5.4.3.2 的要求得出。

5.5.2 生产控制计划的安全相关内容（含测试计划），由 5.4.1.4、5.4.1.5、5.4.3.4 和 5.4.3.6 的要求得出。

5.5.3 控制措施报告，由 5.4.3.5 的要求得出。

5.5.4 如果适用，系统、硬件或软件开发层面关于可生产性需求规范，由 5.4.1.7 的要求得出。

注：此定义可附在相应阶段的相关文档中。

5.5.5 生产过程能力的评估报告，由 5.4.2.2 和 5.4.3.3 的要求得出。

6 运行、服务（维护与维修）和报废

6.1 目的

本章的目的是定义关于相关项、系统或要素的客户信息、维护和维修及拆卸指导说明，以保持车辆整个生命周期内的功能安全。

6.2 总则

本章提供了开发维修指导说明和用户信息的要求，包括用户手册以及对维护工作的计划、执行和监控，并考虑相关项与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”三个阶段。本章仅针对“拆卸前”的活动。

6.3 本章的输入

6.3.1 前提条件

应具备下列信息：

— 生产、运行、服务和报废的需求规范，按照GB/T XXXXX-5, 7.5.4；

— 生产发布报告，按照GB/T XXXXX-4, 11.5.1；以及

— 包含在功能安全概念里的报警和降级概念，按照GB/T XXXXX-3, 8.5.1。

6.3.2 支持信息

可考虑下列信息：

— 维护计划（来自外部）。

6.4 要求和建议

6.4.1 运行、服务（维护与维修）和报废的计划

6.4.1.1 应通过评估相关项并考虑下列信息来计划运行、维修和维护的过程：

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；

c) 报警和降级概念；

d) 现场数据的收集措施和分析措施；

e) 硬件要素的存储、运输和处理的条件；

示例：要素的允许存储时间。

f) 在生产发布文件中定义的已批准的配置；以及

示例：在维修过程中，硬件、软件和软件标定数据的允许配置。

g) 参与人员的能力

6.4.1.2 **维护计划应描述维护步骤或活动的顺序和方法、维护间隔以及维护的必要手段和工具。**

6.4.1.3 **维护计划和维修说明应描述：**

a) 工作步骤、流程、诊断程序和方法；

b) 维护工具和手段；

示例：程序设定、传感器标定/设置和诊断设备。

c) 用于验证安全相关特殊特性的控制步骤的顺序和方法，以及控制准则。

d) 有关相关项、系统或要素的配置，包括可追溯性措施；

注：这包括用来确保车辆下载了正确版本软件的维护工具特性（如果在维护中执行这种操作）。

示例：要素的标签是确保可追溯性的一个方法。

e) 车辆中允许关闭的相关项、系统或要素，及必要的变更；

f) 针对允许关闭和变更的驾驶员信息；以及

示例：通知驾驶员某项辅助功能已经被关闭。

g) 备件的供应。

6.4.1.4 **用户信息，包括用户手册，应对相关项正确使用提供相关使用指导说明和警告，如果适用，还应提供以下信息：**

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) 在通过报警和降级概念表明失效的情况下，为确保可控性所需的客户行为的描述。

c) 在通过报警和降级概念表明失效的情况下，所期望的客户维护活动的描述；

d) 关于与第三方产品交互所导致的已知危害的警告；以及

示例：对于泊车辅助，当使用带第三方挂钩的拖车时，用户需意识到泊车辅助已不能扫描到车辆后方。

e) 关于可能导致驾驶员误解或误用的相关项安全相关创新功能的警告。

示例： 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啮合驻车制动就离开车辆。

6.4.1.5 报废说明应描述在拆卸前所适用的以及防止车辆、相关项或其要素在拆卸、处理或报废过程中违背安全目标所需的活动和措施。

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。

6.4.1.6 在运行、服务（维护和维修）和报废的过程中所引起的系统、硬件或软件层面的安全要求，应被定义并传导给负责开发的人员（参见 GB/TXXXXX-4, GB/TXXXXX-5 and GB/TXXXXX-6）。

示例：为便于在服务中的诊断而存在于ECU中的故障记录功能的定义。

6.4.2 运行、服务（维护与维修）和报废

6.4.2.1 按照 GB/T XXXXX-2, 7.4.2.4 的计划，应实施对相关项功能安全事件的现场监控流程，以用于：

a) 提供现场数据，此现场数据被分析以探测任何可能存在的功能安全问题，如果发现问题，则触发处理.那些问题的动作。以及：

b) 提供在用证明所需的证据（如果计划按照GB/T XXXXX-8第14章使用在用证明）。

6.4.2.2 相关项及其系统或要素的维护、维修和报废宜按照维护计划和维护维修说明实施并形成文档。

注：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。

6.4.2.3 应按照 6.4.1.3 所计划的来实现元器件的供应、储存和运输。

6.4.2.4 如果由于运行、现场监控、维护、维修或报废引起相关项后续生产的变更，那么应符合 GB/T XXXXX-8，第 8 章所描述的变更管理过程。

6.5 工作成果

6.5.1 维护计划中与安全相关的内容，由 6.4.1.1、6.4.1.2 和 6.4.1.3 的要求得出。

6.5.2 维修说明，由 6.4.1.3 的要求得出。

6.5.3 用户须知信息中与安全相关的内容，由 6.4.1.4 的要求得出。

6.5.4 关于现场观察的说明，由 6.4.2.1 的要求得出。

6.5.5 报废说明中与安全相关的内容，由 6.4.1.5 的要求得出。

6.5.6 如果适用，在系统、硬件或软件开发层面与运行、服务和报废相关的需求规范，由 6.4.1.6 的要求得出。

注:此规范可被附加到相应阶段的有关文档中

附录 A

（资料性附录）

生产和运行的概览和文档流程

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 — 产品开发软件层面概览

章	目的	前提条件	工作成果
5 生产	本章的第一个目的是为安装在道路车辆上的安全相关要素或相关项开发和维护一个生产过程。 第二个目的是在生产过程中，通过对此过程负责的相关生产者、人员或组织（汽车生产商、供应商、二级供应商等）实现功能安全。	生产、运行、维护和报废的要求定义，按照GB/T XXXXX-4, 7.5.4 和GB/T XXXXX-5, 7.5.4； 硬件专用措施的定义，按照GB/T XXXXX-5，9.5.2；及 生产发布报告，按照GB/T XXXXX-4, 11.5.1。	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、5.4.1.6和 5.4.3.2 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 5.4.1.4、5.4.1.5、5.4.3.4 和 5.4.3.6 的要求得出。 5.5.3 控制措施报告，由 5.4.3.5 的要求得出。 5.5.4 如果适用，系统、硬件或软件开发层面关于可生产性要求的定义，由 5.4.1.7 的要求得出。 5.5.5 生产过程能力的评估报告，由 5.4.2.2 和 5.4.3.3 的要求得出。
6 运行、服务（维护与维修）和报废	本章的目的是定义关于相关项、系统或要素的客户信息、维护和维修及拆卸指导说明，以保持车辆整个生命周期内的功能安全。	生产、运行、服务和报废的需求规范，按照GB/T XXXXX-5, 7.5.4； 生产发布报告，按照GB/T XXXXX-4, 11.5.1；以及 包含在功能安全概念里的报警和降级概念，按照GB/T XXXXX-3, 8.5.1。	6.5.1 维护计划中与安全相关的内容，由 6.4.1.1、6.4.1.2 和 6.4.1.3 的要求得出。 6.5.2 维修说明，由 6.4.1.3 的要求得出。 6.5.3 用户须知信息中与安全相关的内容，由 6.4.1.4 的要求得出。 6.5.4 关于现场观察的说明，由 6.4.2.1 的要求得出。 6.5.5 报废说明中与安全相关的内容，由 6.4.1.5 的要求得出。