ICS 43.040
CCS T 35

中华人民共和国国家标准

GB/T 34590.12—XXXX

道路车辆 功能安全
第12部分：摩托车的适用性

Road vehicles — Functional safety —Part 12: Adaptation for motorcycles

(ISO 26262-12:2018,Road vehicles — Functional safety —Part 12:Adaptation of ISO 26262 for motorcycles，MOD)

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 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

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。

GB/T 34590-XXXX《道路车辆 功能安全》分为以下部分：

——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。

本文件为GB/T 34590-XXXX的第12部分。

本文件使用重新起草法修改采用了ISO 26262-12:2018《道路车辆 功能安全 第12部分:ISO 26262对摩托车的适用性》。

本文件与ISO 26262-12：2018的技术性差异及其原因如下：

——关于规范性引用文件，本文件做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第 2 章“规范性引用文件”中，具体调整如下：

- 用修改采用国际标准的GB/T 34590.1-XXXX代替ISO 26262-1：2018；
- 用修改采用国际标准的GB/T 34590.2-XXXX代替ISO 26262-2：2018；
- 用修改采用国际标准的GB/T 34590.3-XXXX代替ISO 26262-3：2018；
- 用修改采用国际标准的GB/T 34590.4-XXXX代替ISO 26262-4：2018；
- 用修改采用国际标准的GB/T 34590.5-XXXX代替ISO 26262-5：2018；
- 用修改采用国际标准的GB/T 34590.6-XXXX代替ISO 26262-6：2018；
- 用修改采用国际标准的GB/T 34590.7-XXXX代替ISO 26262-7：2018；
- 用修改采用国际标准的GB/T 34590.8-XXXX代替ISO 26262-8：2018；
- 用修改采用国际标准的GB/T 34590.9-XXXX代替ISO 26262-9：2018。

——10.4.3.4 中，“压力测试”修改为“压力测试（例如：高负荷测试、高环境测试）”；

本文件还做了下列编辑性修改：

——将国际标准中的“本国际标准”改为“本文件”；

——删除国际标准的前言；

——修改了国际标准的引言及其表述。

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/TC114）归口。

本文件起草单位：

本文件主要起草人：

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，以及对提供证据证明满足功能安全目标的需求。

随着技术日益复杂、软件和机电一体化应用不断增加，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-XXXX（所有部分）：

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；及

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。它也提供了一个框架，在该框架内可考虑基于其它技术（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，包括需求规范、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。

图1为GB/T 34590的整体架构。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：

——阴影”V”表示 GB/T 34590.3-XXXX、GB/T 34590.4-XXXX、GB/T 34590.5-XXXX、GB/T 34590.6-XXXX、GB/T 34590.7-XXXX 之间的相互关系；

——对于摩托车：

- GB/T 34590.12-XXXX的第8章支持GB/T 34590.3-XXXX；
- GB/T 34590.12-XXXX的第9章和第10章支持GB/T 34590.4-XXXX。

——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-XXXX 的第 6 章。

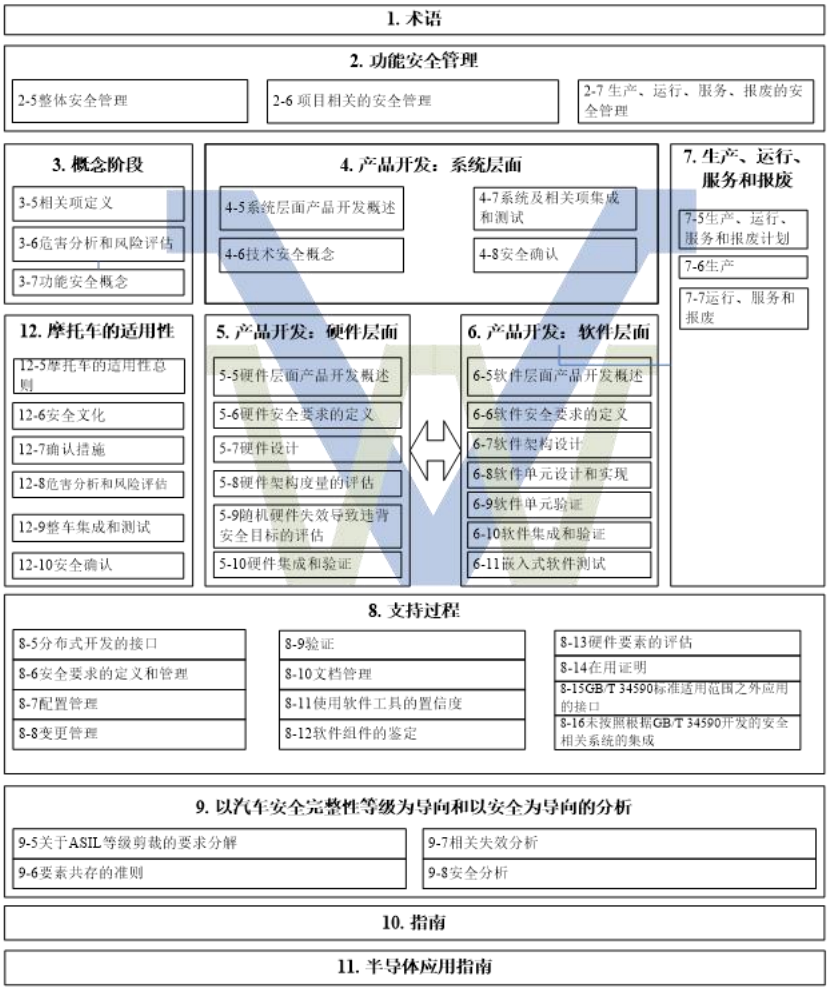


图1　GB/T 34590-XXXX 概览

道路车辆 功能安全
第12部分：摩托车的适用性

1 范围

本文件规定了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；及

——安全确认。

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。

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剪裁。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剪裁。

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。本文件规定了为实现产品功能安全的技术开发要求，也规定了组织应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。

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

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

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

GB/T 34590.4-XXXX 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)

GB/T 34590.5-XXXX 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)

GB/T 34590.6-XXXX 道路车辆功能安全 第6部分：产品开发：软件层面(ISO 26262-6:2018,MOD)

GB/T 34590.7-XXXX 道路车辆功能安全 第7部分：生产、运行、服务和报废(ISO 26262-7:2018,MOD)

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

GB/T 34590.9-XXXX 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)

3 术语、定义和缩略语

GB/T 34590.1-XXXX界定的术语、定义和缩略语适用于本文件。

4 要求

4.1 目的

本章规定了：

a) 如何声明满足 GB/T 34590-XXXX；

b) 解释 GB/T 34590-XXXX 中所使用的表格；及

c) 解释各条款基于不同的 ASIL 等级的适用性。

4.2 一般要求

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

a) 已经按照本文件对安全活动进行剪裁，并表明这些要求不适用；或

b) 不满足要求的理由存在且是可接受的，并且按照本文件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 XXXXX-XXXX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

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应按照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它方法替代,此种情况下，应给出满足相关要求的理由。如果能给出不选择所有所列条目也能满足相关要求的理由，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

若无其它说明，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 XXXXX-9第5章的要求，应遵循分解后的ASIL等级。

如果GB/T 34590-XXXX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

对于适用于本文件要求的摩托车的相关项或要素，本文件的要求代替其他部分的相应要求。

4.6 卡车、客车、挂车和半挂车的适用性

对卡车、客车、挂车和半挂车的特殊规定以（T&B）来表示。

5 摩托车的适用性总则

5.1 目的

本章的目的是给出GB/T 34590对于摩托车适用性的概述。

5.2 总则

摩托车上的电子电气系统应满足GB/T 34590.2 ～GB/T 34590.9的要求。然而，如4.5所述，某些要求可能需要一定程度的剪裁才能适用于摩托车。在这些情况下，这些被剪裁的要求代替了GB/T 34590中的相应要求。

本文件所述的对摩托车的特殊要求对应GB/T 34590.2-XXXX，5.4.2、GB/T 34590.2-XXXX，6.4.9、GB/T 34590.3-XXXX第6章、GB/T 34590.3-XXXX附录B、GB/T 34590.4-XXXX，7.4.4和GB/T 34590.4-XXXX第8章的要求。

注：下列定义与缩略语专用于摩托车并仅在本文件中使用。其已在GB/T 34590.1中描述：

——专业摩托车驾驶员；

——摩托车；

——摩托车安全完整性等级（MSIL）；及

——可控性评级专家组（CCP）。

附录A提供了摩托车实施GB/T 34590.2-XXXX、GB/T 34590.3-XXXX和GB/T 34590.4-XXXX的概览和工作流。

附录B给出了危害分析和风险评估的一般解释。

附录C提供了在传统产品开发环境中考虑摩托车动力学的可控性评估技术的示例。

图2展示了本文件与 GB/T 34590其它部分的关系。

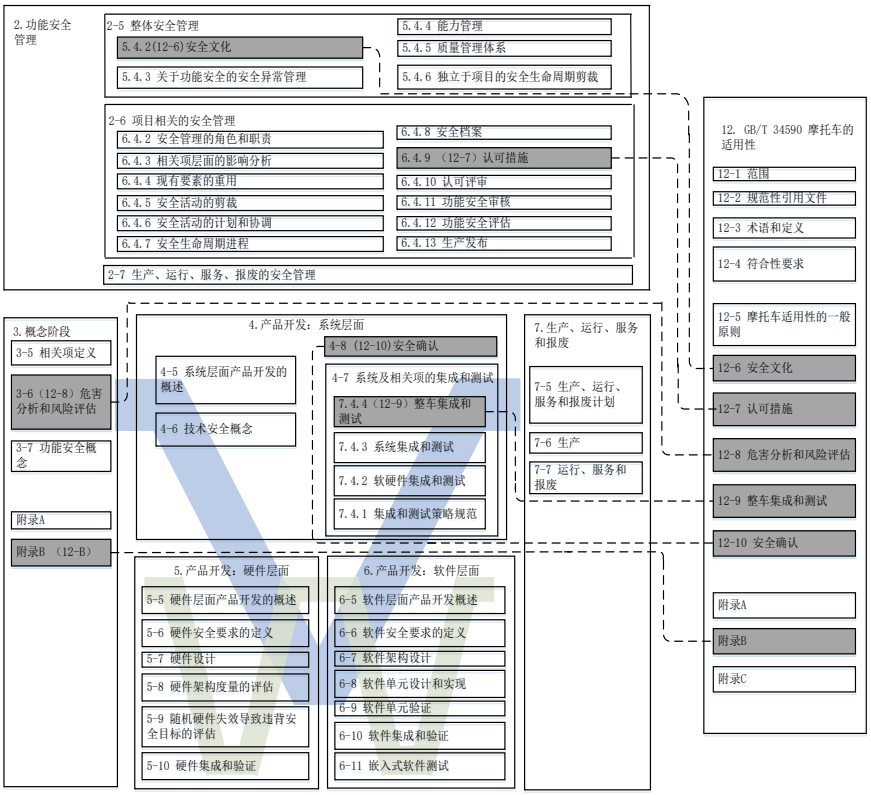


图2　本文件与其他部分间关系的概述

6　安全文化

6.1　目的

提供了对GB/T 34590.2-XXXX第5.4.2条针对摩托车的剪裁。

6.2　要求和建议

6.2.1　组织应创造、培育并保持一种安全文化，以支持并鼓励有效地实现摩托车功能安全。

注：GB/T 34590.2-XXXX附录B提供了构建安全文化的更多细节。

6.2.2　组织应建立、执行并维护组织的专门的规章和流程，以实现且维护功能安全并符合 GB/T 34590 的要求。

注：组织的专门的规章和流程可包括创建并维护通用的计划（例如：通用安全计划）或通用的流程描述。

6.2.3　如果适用，组织应建立并维护功能安全领域、信息安全、及与功能安全实现相关的其他领域之间的有效沟通渠道。

示例1：建立功能安全与信息安全之间的沟通渠道，以便于两者交互相关信息（例如，在识别到信息安全问题可能违反安全目标或安全要求的情况下，或在信息安全要求可能与安全要求冲突的情况下）。

示例2：建立功能安全和质量之间的沟通渠道。

注：功能安全与信息安全潜在交互的指导见GB/T 34590.2-XXXX附录E。

6.2.4　在安全生命周期执行期间，组织应执行要求的安全活动，包括文档的创建和管理（按照 GB/T

34590.8—XXXX，第 10 章的说明)。

6.2.5 组织应为功能安全的实现提供所需的资源。

注：资源包括人力资源、工具、数据库、指南和工作说明。

6.2.6 基于以下几点，组织应建立、执行并维护持续改进的流程：

——从其他相关项安全生命周期的执行过程中学习经验，包括现场经验；及
——将获得的改进应用于后续相关项。

6.2.7 组织应确保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。

7 认可措施

7.1 目的

本章的目的是定义与ASIL相关的认可措施的独立性要求。

7.2 要求和建议

7.2.1 相关项及其要素的功能安全应被认可，基于:

a) 按照表 1 和 GB/T 34590.2-XXXX,6.4.10 的要求，认可评审判断关键工作成果，即表 1 所列工作成果，能否提供充足并令人信服的证据，证明其对实现功能安全的贡献，此过程应考虑 GB/T 34590 相应的目标和要求；

注1：对于摩托车，本文件表1代替GB/T34590.2-XXXX的表1。

注2：对表1中规定的和安全计划中要求的工作成果进行认可评审。

b) 按照表 1 和 GB/T 34590.2-XXXX,6.4.11,功能安全审核判断功能安全所需的流程的实施情况；及

注3：GB/T 34590中定义了功能安全所需的参考流程。与相关项或要素有关的流程通过安全计划中引用或规定的活动来定义。

c) 按照表 1 和 GB/T 34590.2-XXXX,6.4.12，功能安全评估判断相关项实现的功能安全，或所开发的要素对实现功能安全的贡献。

注4：表1中定义的独立性的目的是确保客观、公正的观点，避免利益冲突。本文中所用的“独立性”一词指的是组织独立性。

注5：认可措施指南见GB/T34590.2-XXXX，附录C。

注6：认可措施的结果报告包括所分析的工作成果或流程文档的名称和版本号(见GB/T 34590.8-XXXX，第10章)。

注7：如果在认可措施完成后，相关项发生变更，则需要重新进行或补充相关的认可措施（见GB/T 34590.8-XXXX，8.4.5.2）。

注8：认可措施，如认可评审和功能安全审核，可以与功能安全评估合并、联合，以支持相关项类似变型的处理。

表1 要求的认可措施（包括独立性等级要求）

认可措施	应用于以下的独立性程度[a]				范围
	QM	ASIL A	ASIL B	ASIL C	

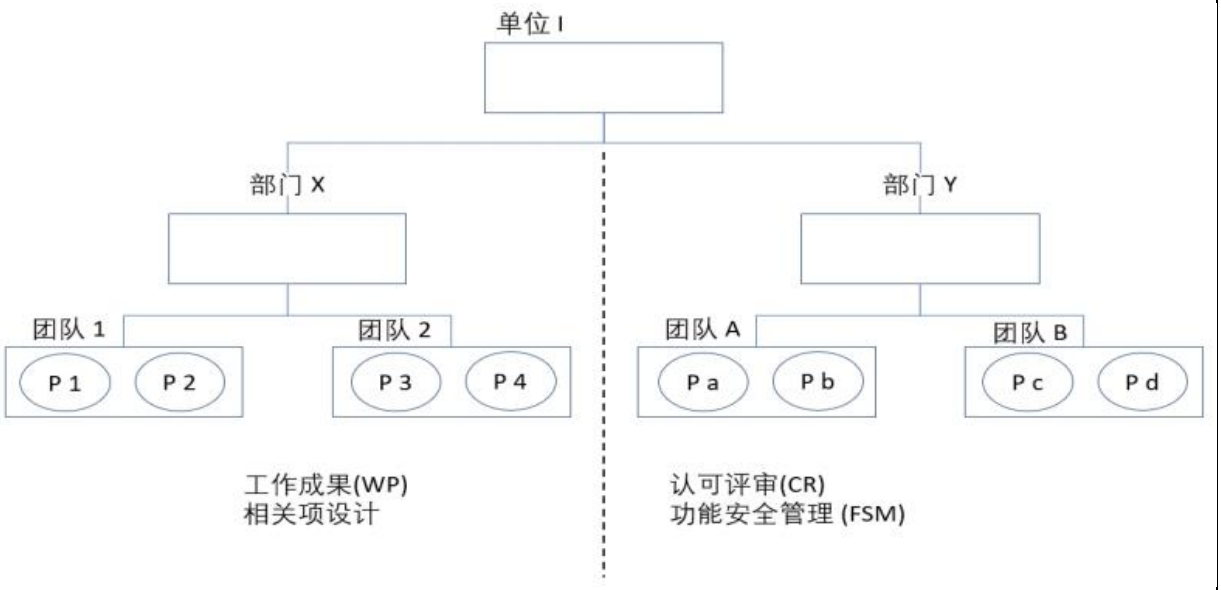
相关项层面对于影响分析的认可评审（见GB/T 34590.2-XXXX，6.5.1）； 独立于工作成果的创建者。	I3	I3	I3	I3	判断按照GB/T 34590.2-XXXX,6.4.3进行的影响分析是否正确识别了相关项是新相关项、对现有相关项的修改或是环境变化的现有相关项。 判断按照GB/T 34590.2-XXXX,6.4.3进行的影响分析是否充分地识别了各种变化引发的功能安全影响；以及要执行的安全活动。
危害分析和风险评估的认可评审（见第8章）； 独立于工作成果的创建者。	I3	I3	I3	I3	判断与危害事件相关的运行场景的选择和危害事件定义是否适当。 判断已确定的ASILs、对于相关项识别的危害事件的质量管理（“QM”）评级和导致没有ASIL的参数(例如C0/S0/E0)是否正确。 判断定义的安全目标是否涵盖已识别的危害事件。
安全计划的认可评审（见GB/T 34590.2-XXXX,6.5.3）； 独立于工作成果的创建者。 **注1：**安全计划的认可评审包括由于现有要素复用而执行的要素层面影响分析的评审（见GB/T 34590.2-XXXX,6.5.2）。 **注2：**安全计划包含候选项在用证明（分析、数据和可信度）及相应的剪裁，若适用（见GB/T 34590.2-XXXX,6.4.6和GB/T 34590.8-XXXX，第14章）。 **注3：**安全计划包括因使用软件工具而引起的剪裁，若适用（见GB/T 34590.2-XXXX,6.4.6 和 GB/T 34590.8-XXXX，第11章）	—	I1	I1	I2	依照全部安全需求中的最高ASIL等级执行。

功能安全概念的认可评审（见GB/T 34590.3-XXXX，第7章），由相应安全分析和相关失效分析的结果支持（分别见GB/T 34590.9-XXXX第8章和GB/T 3459.9-XXXX第7章)； 独立于工作成果的创建者。	—	I1	I1	I2	依照相关项全部安全目标中的最高ASIL等级执行。
技术安全概念的认可评审（见GB/T 34590.4-XXXX，第6章），由相应安全分析和相关失效分析的结果支持（分别见GB/T 34590.9-XXXX第8章和GB/T 34590.9-XXXX第7章） 独立于工作成果的创建者。	—	I1	I1	I2	依照导出技术安全需求的全部功能安全需求的最高ASIL等级执行。 如果已对功能安全概念执行了ASIL 分解,则应考虑分解的 ASIL 结果。
集成和测试策略的认可评审（见GB/T 3459.4-XXXX,第7章）； 独立于工作成果的创建者。	—	I0	I1	I2	依照全部安全需求中的最高ASIL等级执行。
安全确认规范的认可评审（见GB/T 3459.4-XXXX第8章）； 独立于工作成果的创建者。	—	I0	I1	I2	依照全部安全需求中的最高ASIL等级执行。
安全分析和相关失效分析的认可评审（分别见GB/T 34590.9-XXXX第8章和GB/T 34590.9-XXXX第7章）； 独立于工作成果的创建者。	—	I1	I1	I2	依照全部安全需求中的最高ASIL等级执行。
安全档案的认可评审（见GB/T 34590.2-XXXX,6.5.4）； 独立于工作成果的创建者。	—	I1	I1	I2	依照全部安全需求中的最高ASIL等级执行。
按照GB/T 34590.2-XXXX，6.4.11，进行功能安全审核； 独立于相关项开发人员和项目管理。	—	—	I0	I2	依照全部安全需求中的最高ASIL等级执行。
按照GB/T 34590.2-XXXX,6.4.12，进行功能安全评估； 独立于相关项开发人员和项目管理。	—	—	I0	I2	依照全部安全需求中的最高ASIL等级执行。
注：图3展示了一个简化的结构以便更好地理解独立性。在不同的公司，组织的名称可能不同。					
[b]所指的独立性等级是为了表示最低要求。其符号定义如下: ———：对于认可措施无要求和建议； ———I0：宜执行认可措施；但如果执行，应由与负责创建工作成果的人员不同的人员执行； ———I1：认可措施应由与负责创建工作成果的人员不同的人员执行；					

——I2：认可措施应由独立于负责创建工作成果的团队的人员执行，即由不向同一个直接上级报告的人员执行；及

——I3：认可措施应由来自不同的部门或组织的人员执行，即不向负责发布工作成果的部门领导汇报。

I3=不同部门



I2=不同团队

P1 或 P2 = 工作成果 / 相关项开发

P3 或 p4 = 认可评审

I1=不同人员

P1 = 工作成果 / 相关项开发

P2 = 认可评审

图3　认可评审独立性等级

7.2.2 在相关项开发过程中，实施认可措施的人员应能接触开展安全活动的人员和组织机构，并应得到其支持。

7.2.3 实施认可措施的人员应有权限获取相关信息和工具。

8　危害分析和风险评估

8.1　目的

本章的目的：

a)　规定为进行摩托车特定的危害分析和风险评估而应满足的必要要求；

b)　识别并分类由相关项中的功能异常表现引起的危害事件；及

c)　制定防止危害事件发生或减轻危害程度的安全目标及其按照 MSIL 等级映射的对应 ASIL 等级，以避免不合理的风险。

8.2　总则

由于摩托车的动态行为与GB/T 34590范围内的其他车辆差别很大、且摩托车特定危害事件的可控性可能更强调驾驶员的处置，因此公认的风险评估方法需要进行一定程度的剪裁以最大程度地适应摩托车特定的危害事件。

危害分析、风险评估和MSIL等级的确定用于确定相关项的安全目标。为此，根据相关项的潜在危害事件，对相关项进行评估。通过对危害事件进行系统性的评估确定安全目标及分配给他们的MSIL等级。MSIL等级的确定需要考虑严重度、暴露概率和可控性。严重度、暴露概率和可控性的确定基于相关项的功能行为，因而不一定需要知道相关项的设计细节。

注：摩托车行业的产品开发流程和技术解决方案与汽车行业不同。全球范围内的摩托车行业现有的技术水平（“state-of-the-art”）表明ASIL分级不适用于摩托车。因此使用MSIL分级作为HARA输出。建立MSIL与ASIL的分级间的对应关系是为了应用GB/T 34590其他部分中定义的要求，并适应全球范围内摩托车行业的能力。

8.3 本章的输入

8.3.1 前提条件

应具备以下信息：

——相关项定义，按照 GB/T 34590.3-XXXX，5.5.1。

8.3.2 支持信息

可考虑如下信息：

——其他相关项的相关信息（来自外部）。

8.4 要求和建议

8.4.1 危害分析和风险评估的启动

8.4.1.1 应基于相关项定义进行危害分析和风险评估。

8.4.1.2 在危害分析和风险评估过程中，应对不含内部安全机制的相关项进行评估，即，在危害分析和风险评估过程中不应考虑将要实施或已经在先前相关项中实施的安全机制。

注1：在对相关项进行评估过程中，可用的且充分独立的外部措施是有益的。

注2：相关项中将要或已经实施的安全机制是功能安全概念的一部分。

8.4.2 场景分析和危害识别

8.4.2.1 应对相关项的功能异常表现导致一个危害事件发生时所处的运行场景及运行模式进行描述，包括正确的使用车辆和合理可预见的不正确使用车辆的情况。

注1：运行场景描述了假定相关项是以安全的方式运行的条件。

注2：由相关项非失效情况下的行为导致的危害，不属于本文件的范围。

示例1：普通摩托车不考虑在未经平整或非铺装的路面高速行驶。

示例2：普通摩托车不考虑用于公路赛、越野赛或拉力赛。

8.4.2.2 应基于相关项可能的功能异常表现系统性地确定危害。

注：FMEA方法和HAZOP适用于支持相关项层面的危害识别。这些可以通过头脑风暴、检查表、质量历史记录和现场研究来支持。

8.4.2.3 应在整车层面定义由相关项的功能异常表现导致的危害。

注1：通常，每一个危害有多种与相关项的实现相关的潜在原因，但在危害分析和风险评估中对于功能异常表现的分析，不需要考虑这些原因。

注2：仅考虑相关项的功能异常表现相关的危害，假设其他充分独立的系统（外部措施）均正确工作。

8.4.2.4 如果在本章中所识别出的危害超出了 GB/T 34590 的范围（见第 1 章），应按照组织的特定程序处理这些危害。

注：由于这些危害超出了GB/T 34590的范围，因此本文件未提供有关这些危害的MSIL等级确定与ASIL等级的合规性指导，对此类危害的分类按照适用的安全流程进行。

8.4.2.5 应确定相关的危害事件

8.4.2.6 应识别危害事件的后果

注：如果相关项层面的功能异常表现导致该相关项丧失多个功能，则场景分析和危害识别要考虑其综合影响。

示例：整车供电系统的失效能导致同时丧失一系列功能,包括“发动机扭矩”及“前向照明”。

8.4.2.7 应确保所选择的运行场景列表的详细程度不会导致 MSIL 等级的不适当降低。

注：对一个危害来说，一个非常详细的关于车辆状况、道路条件和环境条件的运行场景列表（见8.4.2.1），会使得用于危害事件分类的场景的颗粒度更为精细。这可以更容易地评估可控性和严重度。然而，大量的不同运行场景可能导致相应地降低各自的暴露等级，从而导致不恰当地降低MSIL等级。可以通过合并类似的场景来避免。

8.4.3 危害事件分类

8.4.3.1 应对在 8.4.2 中识别出的所有的危害事件进行分类，不含超出 GB/T 34590 范围的危害事件。

注：如果难以对一个给定的危害进行严重度（S）、暴露概率（E）或可控性（C）的分级，需要采取保守分级的方法，即，一旦分级存在合理的怀疑，就采用较高的S、E或C等级。

8.4.3.2 对于每一个危害事件，应基于确定的理由来预估潜在伤害的严重度。应按照表 2 为严重度指定一个 S0、S1、S2 或 S3 的严重度等级。

注1：危害事件的风险评估关注的是潜在的处于风险中的每个人受到的伤害情况——包括引起危害事件的车辆的驾驶员或乘客，以及其他潜在的处于风险中的人员，如骑自行车的人员、行人或其他车辆上的人员。附录B中介绍的简明损伤定级（AIS）可用于界定伤害的严重度；此外，附录B中还包括不同类型的严重度和事故的参考示例。如可能的话，适当的摩托车事故数据库可用于为确定严重度提供依据。

注2：严重度的分级可基于对多个伤害的综合性的考量，相比只考虑单一伤害的评估结果而言，这样可能会导致一个较高的严重度等级。

注3：对被评估中的场景，严重度预估应考虑事件发生的合理顺序。

注4：严重度的评级基于涉险人员的代表性样本。

注5：假定已使用车辆用户手册中规定的标准防护装备（如头盔、防护茄克衫、手套和靴子）。

表2 严重度等级

等级	S0	S1	S2	S3
描述	无伤害	轻度和中度伤害	严重的和危及生命的伤害（有存活的可能）	危及生命的伤害（存活不确定），致命的伤害

8.4.3.3 有的运行场景会导致伤害（例如事故），在此运行场景下，其相关项后续的功能异常表现会增加或无法减小所产生的伤害，在这种情况下，严重度的分级可以仅限于初始运行场景（例如事故）和相关项功能异常表现所产生的严重度差异。

示例：在汽车应用中，被考虑的相关项包含用于降低碰撞撞击力的安全气囊功能。如果事故发生时安全气囊未能正常打开，碰撞撞击力可以认为严重度符合 S3 级。如果正常运行的安全气囊能将碰撞撞击力降低到与严重度为 S2 级相对应的水平，则这种差异就将是一个严重度等级。因此，该场景中分配的安全气囊的失效的严重度等级可以设定为 S1。

8.4.3.4 如果经过危害分析和风险评估，确定相关项的功能异常表现的后果明显仅限于物体损坏并不涉及对人员的伤害，则该危害的严重度等级可为 S0。如果一个危害事件的严重度等级为 S0，则无需分配 MSIL 等级。

8.4.3.5 对于每一个危害事件，应基于确定的理由预估每个运行场景的暴露概率。按照表 3，应为暴露概率指定一个 E0、E1、E2、E3 或 E4 的概率等级。

注1：从E1到E4等级，两个相邻E等级间的概率差异是一个数量级。

注2：暴露度的确定基于目标市场中有代表性的运行场景样本。

注3：暴露概率的更多信息和示例见附录B。

表3 关于运行场景的暴露概率等级

等级	E0	E1	E2	E3	E4
描述	不可能	非常低的概率	低概率	中等概率	高概率

8.4.3.6 在预估暴露概率时，不应考虑装备该相关项的车辆数量。

注：暴露概率的评估是基于假设每个车辆都配备有该相关项进行的。这意味着“因为该相关项未装备在每台车辆上（只有一些车辆装备该相关项），所以暴露概率会降低”的观点是不成立的。

8.4.3.7 暴露概率等级 E0 可用于在危害分析和风险评估过程中所建议的那些认为是难以置信的场景，无需进一步探讨。应记录排除这些场景的理由。如果一个危害事件的暴露度等级被指定为 E0，则无需分配 MSIL 等级。

示例：E0 可用于“不可抗力”风险的情况（见 B.3）。

8.4.3.8 对于每一个危害事件，应基于一个确定的理由预估驾驶员或其他处于运行场景的人员对该危害事件的可控性。应按照表 4 为可控性指定一个 C0、C1、C2 或 C3 的可控性等级。

注1：可控性评估是指对人员能够充分控制危害事件以避免特定伤害概率的预估。 因此，使用级别分别为C0，C1，C2和C3的参数C，以对避免伤害的可能性进行分类。表B.4中列出了一些示例，这些示例对这些等级做出解释。评估可以用试验或分析程序进行。

注2：就摩托车而言，假设驾驶员处于正常的状态（例如，驾驶员不疲劳），接受了恰当的驾驶员培训（驾驶员有驾驶执照）、了解摩托车使用的特点并遵守所有适用的法律法规，包括应有的谨慎以避免为其他交通参与者带来风险。

注3：当危害事件与车辆方向和速度的控制无关时，例如肢体卡在运动部件中，该可控性是对涉险人员能够从危害场景中移出自身或被其他人员移出的概率预估。当考虑可控性时，要注意的是涉险人员可能不熟悉相关项的操作，或者可能没有意识到潜在的危害情况的发生。

注4：当可控性涉及多个交通参与者的行为时，可控性评估可以基于带有功能异常相关项的车辆的可控性，以及其他参与者的假定行为。

注5：对于摩托车的危害事件，可控性等级评估在附录C中描述。

注6：在选择合适的可控性等级时，若有适用于相关危害事件的专用法规规定了其功能性能，并有证据（例如真实的使用体验）支撑，则该法规可以作为理由的一部分。

注7：专项法规是指由政府部门规定的要求，可能指定了制造商必须符合的最低性能限制，其车辆才能被批准销售和使用。

表4　可控性等级

等级	C0	C1	C2	C3
类型	可控	简单可控	一般可控	难于控制或不可控

8.4.3.9　如果相关项不可用的危害不影响车辆的安全运行（例如一些驾驶员辅助系统），或者可以通过常规的驾驶员行为来避免事故，则该危害事件的可控性等级可为 C0。如果一个危害事件的可控性等级为 C0，则无需分配 MSIL 等级。

8.4.3.10　每一个危害事件的 MSIL 等级基于严重度、暴露概率和可控性的分级，并按照表 5 来确定。

注：4个ASIL等级：MSIL A、MSIL B、MSIL C和MSIL D，其中MSIL A是最低的安全完整性等级，MSIL D是最高的。

表5　MSIL 等级的确定

严重度等级	暴露概率等级	可控性等级		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

8.4.3.11　在定义安全目标之前应根据表 6 将 MSIL 等级映射到 ASIL 等级，以采用 GB/T 34590 中适用的要求。

注1：除了这4个ASIL等级之外，QM（质量管理）等级表示GB/T 34590不做要求。然而，相应的危害事件可能会影响安全，这种情况下需制定安全要求。QM等级表明质量流程足以管理已识别的风险。

注2：将MSIL等级映射到ASIL等级，以便能以最适当的严格程度用于避免与摩托车运行时使用功能异常的电子电气相关项或与要素相关的不合理的残余风险。

注3：所示的由MSIL等级确定的ASIL等级，显示的是最低的要求。

表6　MSIL 与 ASIL 的对应

MSIL	ASIL

QM	QM
A	QM
B	A
C	B
D	C

8.4.4 安全目标的确定

8.4.4.1 应为具有 ASIL 等级（通过 MSIL 等级映射而来）的每个危害事件确定一个安全目标，该 ASIL 等级从危害分析和风险评估中得出。如果所确定的安全目标是类似的，可将其合并为一个安全目标。

注：安全目标是相关项最高层面的安全要求。安全目标导出功能安全要求，以避免每个危害事件的不合理风险。安全目标不表述为技术解决方案，而表述为功能目的。

8.4.4.2 应将为危害事件所确定的 ASIL 等级（通过 MSIL 等级映射而来）分配给对应的安全目标。如果将类似的安全目标合并为一个安全目标，按照 8.4.4.1，应将最高的 ASIL 等级分配给合并后的安全目标。

8.4.4.3 安全目标连同它们的 ASIL 等级应按照 GB/T 34590.8-XXXX 中第 6 章来定义。

注：安全目标可定义故障容错时间间隔，或物理特性（例如最大的非预期加速度），如果它们与MSIL等级的确定相关。

8.4.4.4 对于与确定 MSIL 等级（如果适用，包括定级为 QM 或没有分配 MSIL 等级的危害事件）相关的危害分析和风险评估过程，应识别其使用到的或从中得出的假设。对于所集成的相关项，应按照第 10 章对这些假设进行确认。

注：如有，在HARA中考虑的假设包括：驾驶员或处于风险中的人员的假定行为以及外部措施的相关假设。

8.4.5 验证

8.4.5.1 应按照 GB/T 34590.8-XXXX 第 9 章对危害分析和风险评估，包括安全目标进行验证，以提供证据证明：

a) 对运行场景和危害识别选择的适用性；
a) 与相关项定义的符合性；
b) 与其他相关项相关的危害分析和风险评估的一致性；
c) 对危害事件覆盖的完备性；
d) 分配了 ASIL 等级（通过 MSIL 等级映射而来）的安全目标与相关危害事件的一致性；及
e) MSIL 等级与 ASIL 等级间映射的一致性。

8.5 工作成果

8.5.1 危害分析和风险评估报告，由 8.4.1～8.4.4 的要求得出。

8.5.2 危害分析和风险评估验证报告，由 8.4.5 的要求得出。

9 整车集成和测试

9.1 目的

本章提供了GB/T 34590.4-XXXX的7.4.4针对摩托车的剪裁。

整车集成是将相关项与车辆上的其他系统的集成以及与整车的集成。

9.2 要求和建议

9.2.1 整车集成

9.2.1.1 应将相关项集成到整车上，并实施整车集成测试。

注：当制定整车层面集成与验证计划时，能考虑车辆在典型和极端车辆状况和环境条件下的正确行为，但应组成一个充分的子集（见GB/T 34590.4-XXXX的表3）。

9.2.1.2 应对相关项与车内通讯网络以及车内供电网络的接口规范进行验证。

9.2.2 整车测试期间的测试目标与测试方法

9.2.2.1 由 9.2.2.2～9.2.2.5 的要求得出的测试目标，应使用对应表格中所列出的适当的测试方法来实现。

注1：这些将支持在整车集成过程中对系统性故障的探测。

注2：基于系统已实施的功能、功能复杂性或分布特性，如有给出足够的理由，在其他集成的子阶段进行测试是可行的。

注3：如果存在对驾驶员安全的担忧，可以选择其他可替代的测试方法或将测试活动移至其他子阶段。

9.2.2.2 功能安全要求在整车层面的正确执行，应使用表 7 中给出的可行的测试方法进行论证。

表7 功能安全要求在整车层面上的正确执行

方法		ASIL等级		
		A	B	C
1a	基于需求的测试[a]	++	++	++
1b	故障注入试验[b]	++	++	++
1c	长期测试[c]	++	++	++
1d	实际使用条件下的用户测试[c,d]	++	++	++

[a] 基于需求的测试是指针对功能性和非功能性要求的测试。

[b] 故障注入测试使用特殊的方法向相关项注入故障。这可以通过特殊测试接口，或者特别准备的要素或通讯设备，在相关项内部完成。该方法经常用于提高安全要求的测试覆盖率，因为在正常运行中安全机制不会被调用。

[c] 长期测试和实际使用条件下的用户测试，类似于来自现场经验的测试，但使用更大的样本量，将普通用户当作测试者，并不局限于之前规定的测试场景，而是在日常生活现实条件下执行。为确保测试人员的安全，如果有必要，这类测试会有限制，例如带有额外的安全措施或停用执行器。对于摩托车来说采取长期测试可能是不可行的。

[d] 对于摩托车来说采取用户测试可能是不可行的。

9.2.2.3 本要求适用于 ASIL(A)、(B)和 C 等级。安全机制在整车层面的正确功能性能、准确性和时序，应使用表 8 中所列的测试方法进行论证。

表8 安全机制在整车层面的正确功能性能、准确性和时序

方法		ASIL等级		
		A	B	C
1a	性能测试[a]	+	+	++
1b	长期测试[b]	+	+	++
1c	实际使用条件下的用户测试[b,c]	+	+	++
1d	故障注入测试[d]	o	+	++
1e	错误猜测法测试[e]	o	+	++
1f	来自现场经验的测试[f]	o	+	++

[a] 性能测试可以验证有关相关项的安全机制的性能(例如:故障出现时，整车层面故障容错时间间隔和车辆的可控性)。

[b] 长期测试和实际使用条件下的用户测试类似于来自现场经验的测试，但使用更大的样本量，将普通用户当作测试者，并不局限于之前规定的测试场景，而是在实际使用条件下执行。为确保测试人员的安全，如果有必要，这类测试会有限制，例如带有额外的安全措施或停用执行器。对于摩托车来说采取长期测试可能是不可行的。

[c] 对于摩托车来说采取用户测试可能是不可行的。

[d] 故障注入测试使用特殊的方法向相关项注入故障。这可以通过特殊测试接口，或者特别准备的要素或通讯设备，在相关项内部完成。该方法经常用于提高安全要求的测试覆盖率，因为在正常运行期间不会触发安全机制。

[e] 错误猜测法测试使用专家知识和经验教训中收集的数据来预测系统错误。然后设计一组包括适当的测试设备的测试以检查这些错误。如果测试者有相似系统的经验时，错误猜测法是一种有效的方法。

[f] 来自现场经验的测试采用从现场收集到得经验和数据。

9.2.2.4 本要求适用于 ASIL(A)、(B)和 C 等级：整车层面外部和内部接口实现的一致性和正确性，应使用表 9 中给出的测试方法进行论证。

注：内部接口是相关项之间或系统之间的接口，外部接口是相关项和整车环境的接口。

表9 整车层面内外部接口实现的正确性

方法		ASIL等级		
		A	B	C
1a	内部接口测试[a]	+	+	++
1b	外部接口测试[a]	+	+	++
1c	通讯和交互测试[b]	+	+	++

[a] 整车层面的接口测试，是对整车系统接口的兼容性测试。这些测试可以通过验证值域、额定值或几何尺寸静态的完成，也可以在整车运行过程中动态的完成。

[b] 通讯和交互测试包括车辆系统在运行期间内针对功能性和非功能性要求的交互测试。

9.2.2.5 本要求适用于 ASIL(A)、(B)和 C 等级。整车层面的鲁棒性水平，应使用表 10 中列出的测试方法进行论证。

表10 整车层面的鲁棒性水平

方法	ASIL等级		
	A	B	C

1a	资源使用测试[a]	+	+	++
1b	压力测试[b]	+	+	++
1c	特定环境条件下的抗干扰性和鲁棒性测试[c]	+	+	++
1d	长期测试[d]	+	+	++

[a] 整车层面的资源使用测试通常在动态环境下进行（如：电子控制单元网络环境、原型车或整车）。测试的问题包括相关项内部资源、功率消耗或其他整车系统的有限资源。

[b] 压力测试验证在高运行负荷或高环境要求下整车能否正确运行。因此，测试可以通过在整车上施加高负荷，或极限的用户输入，或来自于其他系统的极限要求下完成，也可以是极限的温度、湿度或机械冲击测试。

[c] 在特定环境条件下的抗干扰性和鲁棒性测试，是一种特殊的压力测试，包括电磁兼容性（EMC）和静电放电（ESD）测试（如：见参考文献[4],[5]）。

[d] 长期测试和实际使用条件下的用户测试，类似于来自现场经验的测试，但使用更大的样本量，将普通用户当作测试者，并不局限于之前规定的测试场景，而是在实际使用条件下执行。对于摩托车来说采取长期测试可能是不可行的。

10 安全确认

10.1 目的

本章提供了GB/T34590.4-XXXX的第8章针对摩托车所做的剪裁。

本章的目的是：

a) 提供证据，证明集成到目标车辆的相关项实现了其安全目标；及

b) 提供证据，证明功能安全概念和技术安全概念实现了相关项的功能安全。

10.2 总则

前述验证活动（如：设计验证、安全分析、硬件集成和测试、软件集成和测试、相关项的集成和测试）的目的是提供每项特定活动的结果符合规定要求的证据。

对典型车辆上所集成的相关项的安全确认，目的是为预期使用的恰当性提供证据并确认安全措施对一类或一组车辆的充分性。安全确认基于检查和测试，为安全目标的实现提供了保证。

10.3 本章的输入

10.3.1 前提条件

应具备下列信息：

——危害分析和风险评估，按照 8.5.1；

——功能安全概念，按照 GB/T 34590.3-XXXX,7.5.1。

10.3.2 支持信息

可考虑下列信息：

——技术安全概念（见 GB/T 34590.4-XXXX,6.5.2）；

——相关项定义（见 GB/T 34590.3-XXXX,5.5.1）；及

——安全分析报告（见 GB/T 34590.4-XXXX,6.5.7）。

10.4 要求和建议

10.4.1 安全确认的环境

10.4.1.1 应对整车层面的典型环境下所集成的相关项的安全目标进行确认。

注：如果适用，集成的相关项包括：系统、软件、硬件、其他技术要素和外部措施。

10.4.1.2 为了定义典型环境，应考虑基于车型和车辆配置的典型车辆。

注：危害分析和风险评估报告相关（见8.5.1）可能是选择典型车辆的一个相关输入。

10.4.1.3 安全目标的确认应考虑运行过程变化对技术特性的影响，该因素已经在危害分析和风险评估中进行考虑。

10.4.2 安全确认的规范

10.4.2.1 应定义安全确认规范，包括：

a) 待安全确认的相关项配置，包括其标定数据，按照 GB/T 34590.6-XXXX 附录 C；

注：如果对于每个相关项配置的完整确认是不可行的，那么可选择合理的子集。

b) 安全确认流程、测试案例、驾驶操作和接受准则的定义；及

c) 设备和要求的环境条件。

10.4.3 安全确认的执行

10.4.3.1 如果使用测试进行安全确认，那么可应用与验证测试（见 GB/T 34590.8-XXXX,9.4.2 和 9.4.3）相同的要求。

10.4.3.2 当相关项集成到整车时，应通过评估如下方面对相关项的功能安全实现进行确认，包括：

a) 可控性；

注1：使用运行场景确认可控性，包括预期用途及可预见的误用。

注2：安全确认的一个接受准则是对GB/T 34590.3-XXXX, 7.4.2.5中定义的安全状态有充分的可控性。

注3：单一的可接受准则可能不足以验证某个安全状态。

b) 外部措施的有效性；

c) 其他技术要素的有效性；及

d) 影响危害分析和风险评估（见 8.4.4.4）中 ASIL 等级（通过 MSIL 等级映射而来）的假设只能在最终车辆上进行检查。

示例：假设一个机械组件能够防止或减轻由电气电子系统的功能失效造成的潜在危害，那么这个机械组件防止或减轻危害的有效性只能在整车层面进行确认。

10.4.3.3 应基于安全目标、功能安全要求和预期用途，按计划执行整车层面的确认，使用：

a) 针对每个安全目标的安全确认流程和测试用例，包括详细的通过/未通过准则；及

b) 应用范围。可包括例如配置、环境条件、驾驶场景和操作用例等。

注：可创建操作用例，以助于将安全确认集中在整车层面上。

10.4.3.4 应使用以下方法的适当组合：

a) 已定义了测试流程、测试案例和通过/未通过准则的可重复性测试；

示例1：功能和安全要求的正向测试、黑盒测试、仿真、边界条件下的测试、故障注入、耐久测试、压力测试（例如：高负荷测试、高环境测试）、高加速寿命测试、外部影响模拟。

b) 分析；

示例2：FMEA、FTA、ETA、仿真。

c） 长期测试，例如车辆驾驶日程安排和受控测试车队；

注1：针对目标用户的长期测试对摩托车来说可能是不可行的。

d） 实际使用条件下的用户测试、抽测或盲测、专家小组；及

注2：用户测试对于摩托车来说是不可行的。实际场景可使用模拟条件进行。

e） 评审。

10.4.4 评估

10.4.4.1 需应对安全确认的结果进行评估，以提供证据证明已实施的安全目标实现了相关项的功能安全。

10.5 工作成果

10.5.1 包含安全确认环境描述的安全确认规范，由 10.4.1 和 10.4.2 的要求得出。

10.5.2 安全确认报告，由 10.4.3 和 10.4.4 的要求得出。

附 录 A
（资料性）
GB/T 34590 对摩托车适用性的概览和工作流

A.1 总则

本附录提供了摩托车实施GB/T 34590.2-XXXX、GB/T 34590.3-XXXX和GB/T 34590.4-XXXX的概览和工作流。

A.2 功能安全管理的概览和工作流

表A.1 提供了摩托车功能安全管理的目标、前提条件和工作成果概览。

表A.1 功能安全管理概述

章	目的	前提条件	工作成果
GB/T 34590.2-XXXX 第 5 章:整体安全管理 本文件第 6 章：安全文化	本章旨在确保参与安全生命周期执行的组织，即负责安全生命周期或在安全生命周期内执行安全活动的组织，实现以下目标： a) 建立并维护能够用于支持和鼓励功能安全有效实现，并能够促进与功能安全相关的其他领域有效沟通的安全文化； b) 建立并维护充分的组织的专门的功能安全规章和流程； c) 建立并维护可确保能充分解决识别出的安全异常的流程； d) 建立并维护可确保参与人员的能力与其职责相匹配的能力管理体系；及 e) 建立并维护用以支持功能安全的质量管理体系。 本章是 GB/T 34590 安全生命周期内所有活动的前提条件。	无。	GB/T 34590.2-XXXX，5.5.1 组织的专门的功能安全规章和流程； GB/T 34590.2-XXXX，5.5.2 能力管理证据； GB/T 34590.2-XXXX，5.5.3 质量管理体系证据； GB/T 34590.2-XXXX，5.5.4 已识别的安全异常报告(如果适用)。
GB/T 34590.2-XXXX第6章：项目相关的安全管理 本文件第 7 章：认可措施	本章的目的是，确保参与概念阶段或系统、硬件、软件层面开发阶段的组织实现以下目标: a) 定义与分配与安全活动相关的角色和责任； b) 在相关项层面执行影响分析，以识别相关项是全新的，或是对现有相关项修改，还是对现有相关项的使用环境进行修改；并在有一项或多项修改时，分析所识别出的修改对功能安全的影响； c) 在现有要素复用的情况下，在要素层面执行影响分析，评估复用的要素是否可以满足分配给它的安全要求，并考虑该要素复用的运行环境。	组织的专门的功能安全规章和流程（见 GB/T 34590.2-XXXX，5.5.1）； 能力管理的证据(见 GB/T 34590.2-XXXX，5.5.2)； 质量管理体系的证据（见 GB/T 34590.2-XXXX，5.5.3）。	GB/T 34590.2-XXXX，6.5.1 相关项层面的影响分析； GB/T 34590.2-XXXX，6.5.2 要素层面的影响分析(如果适用)； GB/T 34590.2-XXXX，6.5.3 安全计划； GB/T 34590.2-XXXX，6.5.4 安全档案； GB/T 34590.2-XXXX，6.5.5 认可措施报告； GB/T 34590.2-XXXX，6.5.6

	d) 定义所剪裁的安全活动，提供相应的剪裁理由，并评审所提供的理由； e) 计划安全活动； f) 按照安全计划协调并追踪安全活动的进度； g) 规划分布式开发(参考GB/T 34590.8-XXXX第5章)； h) 在整个安全生命周期内，确保安全活动的正确进程； i) 创建可理解的安全档案，以提供实现了功能安全的证据； j) 判断相关项是否实现了功能安全（即功能安全评估)，或者判断某一要素（即供应商进行的功能安全评估活动)或工作成果(例如认可评审）对于实现功能安全的贡献；及 k) 在开发结束时，基于支持有信心实现功能安全的证据，决定相关项或要素是否能够生产发布。		生产发布报告。
GB/T 34590.2-XXXX第7章 生产、运行、服务和报废的安全管理	本章的目的是定义实现和维护生产、运行、服务和报废相关功能安全的组织和人员的职责。	组织的专门的功能安全规则和流程（见GB/T 34590.2-XXXX的5.5.1)； 能力管理的证据（见GB/T 34590.2-XXXX，5.5.2)； 质量管理体系的证据(见GB/T 34590.2-XXXX，5.5.3)； 生产发布报告(见GB/T 34590.2-XXXX，6.5.6)。	GB/T 34590.2-XXXX，7.5.1关于生产、运行、服务和报废的安全管理证据。

A.3 概念阶段的概览和工作流

表A.2提供了摩托车概念阶段的目标、前提条件和工作成果的概览。

表A.2 概念阶段概览

章	目的	前提条件	工作成果

GB/T 34590.3-XXXX第5章：相关项定义	本章的目的是： a) 在整车层面对相关项进行定义和描述，包括功能，其与驾驶员、环境和其他相关项的依赖性和交互；及 b) 对充分理解相关项提供支持，以便执行后续阶段的活动。	无。	GB/T 34590.3-XXXX，5.5.1 相关项定义，由GB/T 34590.3-XXXX，5.4的要求得出。
本文件第8章：危害分析和风险评估	本章的目的是： a) 规定为进行摩托车特定的危害分析和风险评估而应满足的必要要求； b) 识别并分类由相关项中的功能异常表现引起的危害事件；及 c) 制定防止危害事件发生或减轻危害程度的安全目标及其按照 MSIL 等级映射的对应 ASIL 等级，以避免不合理的风险。	相关项定义(见 GB/T 34590.3-XXXX，5.5.1)。	8.5.1 危害分析和风险评估报告，由8.4.1～8.4.4的要求得出； 8.5.1 危害分析和风险评估验证报告，由 8.4.5 的要求得出。
GB/T 34590.3-XXXX,第 7 章 功能安全概念	本章的目的是： a) 按照安全目标，定义相关项功能行为或降级的功能行为； b) 按照安全目标，定义用于合理、及时地探测和控制相关故障的约束条件； c) 定义相关项层面的策略或者措施，通过相关项自身、驾驶员或外部措施来实现要求的故障容错，或者充分减轻相关故障的影响； d) 分配功能安全要求给系统架构设计或者外部措施；及 e) 验证功能安全概念和定义安全确认准则。	相关项定义（见 GB/T 34590.3-XXXX,5.5.1）； 危害分析和风险评估报告（见 8.5.1）； 系统架构设计（来自外部）。	GB/T 34590.3-XXXX7.5.1 功能安全概念，由 GB/T 34590.3-XXXX，7.4.1～7.4.3 的要求得出； GB/T 34590.3-XXXX7.5.2 功能安全概念验证报告，由 GB/T 34590.3-XXXX，7.4.4 的要求得出。

A.4 系统层面产品开发的概览和工作流

表A.3提供了对摩托车系统层面产品开发的目标、前提条件和工作成果概览。

表A.3 摩托车系统层面产品开发的概览和工作流

章	目的	前提条件	工作成果
GB/T 34590.4-XXXX 第 5 章，系统层面产品开发的概述	本章的目的是在系统层面提供产品开发的概览。	—	—
GB/T 34590.4-XXXX 第 6 章，技术安全概念	本章的目的是： a) 为实施系统要素和接口的功能、相关性、约束和属性，制定所需的技术安全要求；	功能安全概念，见 GB/T 34590.3-XXXX，7.5.1；	GB/T 34590.4-XXXX，6.5.1 的技术安全要求规范，由 GB/T 34590.4-XXXX，6.4.1

	b) 为系统要素和接口中将要实施的安全机制，制定技术安全要求； c) 验证技术安全要求在系统层级是否符合功能安全要求并与功能安全要求一致； d) 制定满足安全要求且不与非安全相关要求冲突的系统架构设计和技术安全概念； e) 分析系统架构设计，防止故障并为生产和服务得出必要的安全相关特殊特性；及 f) 分析系统架构设计，以防止故障，并导出针对生产和服务必要的安全相关的特殊特性；及 g) 验证系统架构设计和技术安全概念是否合适，以满足相应 ASIL 等级的安全要求。	系统架构设计（来自外部，见 GB/T 34590.3-XXXX,7.3.1）； 其他涉及功能安全的相关项对此相关项的要求（如果适用）	和6.4.2的要求得出； GB/T 34590.4-XXXX，6.5.2 的技术安全概念，由 GB/T 34590.4-XXXX,6.4.3 ～ 6.4.6 的要求得出； GB/T 34590.4-XXXX，6.5.3 系统架构设计规范，由 GB/T 34590.4-XXXX，6.4.3～至 6.4.6 的要求得出； GB/T 34590.4-XXXX，6.5.4 硬软件接口(HSI)规范，由 GB/T 34590.4-XXXX，6.4.7 的要求得出； 生产、运行、服务和报废要求规范，由 GB/T 34590.4-XXXX，6.4.8 的要求得出； GB/T 34590.4-XXXX，6.5.6 针对系统架构设计、软硬件接口规范、针对生产、运行、服务和报废要求规范及技术安全概念的验证报告，由 GB/T 34590.4-XXXX，6.4.9 的要求得出； GB/T 34590.4-XXXX,6.5.7 安全分析报告，由 GB/T 34590.4-XXXX，6.4.4 的要求得出。

GB/T 34590.4-XXXX 第 7 章，相关项的集成和测试 本文件第 9 章， 整车集成与测试	本章的目的是： a) 定义集成步骤并集成系统要素，直到系统完全集成； b) 验证由系统架构层面安全分析定义的安全措施是否得到正确实施；及 c) 提供证据表明所集成的系统要素满足按照系统架构设计的安全要求。	危害分析和风险评估报告得出的安全目标（见GB/T 34590.3-XXXX，6.5.1）； 功能安全概念（见GB/T 34590.3-XXXX,7.5.1）； 技术安全概念（见GB/T 34590.4-XXXX，6.5.2）； 系统架构设计规范（见 GB/T 34590.4-XXXX， 6.5.3）； 硬件软件接口（HSI）规范（见 GB/T 34590.4-XXXX ，6.5.4, GB/T 34590.4-XXXX，6.5.2 以及GB/T 34590.6-XXXX，6.5.2.）	GB/T 34590.4-XXXX，7.5.1 集成和测试策略，由 GB/T 34590.4-XXXX，7.4.1 的要求得出； GB/T 34590.4-XXXX，7.5.2 集成和测试报告，由 GB/T 34590.4-XXXX,7.4.2,7.4.3 和 7.4.4 的要求得出。
本文件第 10 章,安全确认	本章提供GB/T34590.4-XXXX的第8章针对摩托车所做的剪裁。 本章的目的是： a) 提供证据，证明集成到目标车辆的相关项实现了其安全目标；及 b) 提供证据，证明功能安全概念和技术安全概念实现了相关项的功能安全。	危害分析和风险评估报告（见 8.5.1）； 功能安全概念（见GB/T 34590.3-XXXX 的 7.5.1）。	10.5.1包含安全确认环境描述的安全确认规范，由 10.4.1和10.4.2中的要求得出； 10.5.2 安全确认报告，由 10.4.3 和 10.4.4 中的要求得出。

附 录 B
（资料性）
摩托车的危害分析和风险评估

B.1 总则

本附录给出了危害分析和风险评估的一般解释。B.2（严重度）、B.3（暴露概率）和B.4（可控性）中的例子仅供参考，并非穷尽。

对于这种分析方法，风险(R)可以被描述为一个包含三个参数的函数(F)：危害事件发生频率(f)，可控性（C），即，所涉及人员通过及时反应以避免特定的伤害或损坏的能力，以及所产生的伤害或损坏的潜在严重度（S）：

$$R = F\ (f, C, S) \quad \text{(B.1)}$$

发生频率f依次受到两个因素的影响。要考虑的因素之一是人们以何种频度及多长时间能够发现他们自己处于上述危害事件可能发生的场景中。在GB/T 34590中，它被简化成会出现危害事件的运行场景发生概率的度量（暴露度，E）。另一个因素是相关项中故障的发生率，这在危害分析和风险评估中是不考虑的。然而，在危害分析与风险评估中由E, S, C的分级而得出的MSIL等级，确定了相关项最低限度的要求，以控制或减少随机硬件失效的概率，并且避免系统性故障。在风险评估中，不认为相关项的失效率是推理演绎的，因为可通过实现所得出的安全要求来避免不合理的残余风险。

危害分析和风险评估子阶段包括下述三个步骤。

a) 场景分析和危害识别（见 8.4.2）：场景分析和危害识别的目的是识别出可能会导致危害事件的相关项的潜在非预期行为。场景分析和危害识别活动需要一个关于相关项、相关项功能和边界的清晰定义。场景分析和危害识别是基于相关项的行为，因此并不一定需要知道相关项的设计细节。

示例：场景分析和危害识别考虑的要素可包括：

——车辆的使用场景，如高速行驶、城市行驶、停车、越野；

——环境条件，如路面摩擦、侧风；

——合理可预见的驾驶员使用和误用；及

——运行系统之间的交互。

b) 危害事件的分类（见 8.4.3）：危害分类方案包括与相关项危害事件相关的严重度、暴露概率以及可控性的确定。严重度代表对一个特定驾驶场景中的潜在伤害的预估，而暴露概率是由相应的场景来确定的。可控性衡量了驾驶员或其他道路交通参与者在所考虑到的运行场景中避免所考虑到的事故的难易程度。对于每一个危害，基于相关危害事件的数量，该分类将导出严重度、暴露概率和可控性的一个或多个组合。

c) MSIL 等级确定（见 8.4.3）：确定所需的摩托车安全完整性等级。

B.2 严重度示例

B.2.1 总则

评估危害对驾驶员、乘客、车辆周围人员或周边车辆中人员产生的潜在伤害，以确定相应危害的严重度等级，如表B.1所示。

表B.1给出了示例，关于一个给定危害可能导致的后果，以及每一个后果的严重度等级。

由于事故的复杂性以及事故场景的多样性，表B.1中所提供的例子仅代表对事故后果的一个大概估计。它们代表根据过往事故分析所得到的预期值，因此，不能通过这些单独的描述来得出一个普遍有效的结论。

事故统计可用于确定不同类型事故中预期发生的伤害的分布。

在表B.1中，AIS表示伤害等级分类，但仅用于单一伤害。除AIS外，也可以使用其它分类方法，例如最大简明损伤定级（MAIS，Maximum AIS）和创伤严重度评分（ISS，Injury Severity Score）。

特定伤害等级的使用依赖于同期所进行的医学研究的进展情况。因此，不同伤害等级，例如AIS、ISS和NISS的适用性可以随时间而变化（见参考文献[1],[2],[3]）。

B.2.2 AIS等级描述

使用AIS分级来描述严重度。AIS代表受伤的严重程度分级，它由汽车事故医学高级协会（AAAM，Association for the Advancement of Automotive Medicine）发布。该指南的创建使得国际间的严重度比较成为可能。AIS等级分为七级：

——AIS 0：无伤害；

——AIS 1：轻伤，例如皮肤表面伤口、肌肉疼痛、挥鞭样损伤等；

——AIS2：中度伤害，例如深度皮肉伤、脑震荡长达 15 分钟无意识、单纯性长骨骨折、单纯性肋骨骨折等；

——AIS 3: 严重，但未危及生命的伤害，例如无脑损伤的颅骨骨折、没有脊髓损伤的第四颈椎以下脊柱错位、没有呼吸异常的超过一根的肋骨骨折等；

——AIS 4: 严重受伤（危及生命、有生存的可能），例如伴随或不伴随颅骨骨折的脑震荡引起的长达 12 小时的昏迷、呼吸异常；

——AIS 5: 危险伤害（危及生命，生存不确定），例如伴随脊髓损伤的第四颈椎以下脊柱骨折、肠道撕裂、心脏撕裂、伴随颅内出血的超过 12 小时的昏迷等；

——AIS 6:极度危险或致命伤害，例如伴随脊髓损伤的第三颈椎以上脊柱骨折、极度危险的体腔（胸腔和腹腔）开放性伤口等。

表B.1 严重度等级举例

严重度等级（见表 2）	S0	S1	S2	S3
描述	无伤害	轻度和中度伤害	严重的和危及生命的伤害（有存活的可能）	危及生命的伤害（存活不确定），致命的伤害
对单一伤害的参考(根据 AIS 分级)	——AIS 0 及 AIS 1-6 可能性小于 10%； ——不能被归为安全相关的损害。	AIS 1-6 可能性大于 10%（不属于 S2 和 S3）。	AIS 3-6 可能性大于 10%（不属于 S3）。	AIS 5-6 可能性大于 10%。
示例	——自行跌倒/失去平衡；	——以典型的城区车速和路边设施/静止车辆碰撞；	——以典型的主干道车速和路边设施/静止车辆碰撞；	——以典型的高速公路车速和路

	——以典型的步行速度和路边设施/静止车辆碰撞； ——以相当于典型步行速度的速度差后碰（如乘用车撞到摩托车后部）。	——以典型的步行速度和行人/骑自行车的人碰撞； ——以典型的城区/主干道车速低位侧翻，无后续碰撞； ——以典型的城区/主干道车速高位侧翻，无后续碰撞； ——以典型的步行速度侧碰（如乘用车撞到摩托车侧面）； ——以相当于典型城区车速的速度差后碰（如乘用车撞到摩托车后部）； ——以相当于典型步行速度的速度差与迎面驶来的乘用车正碰。	——以典型的城区车速和行人/骑自行车的人碰撞； ——以典型的高速公路车速低位侧翻，无后续碰撞； ——以典型的主干道/高速公路车速高位侧翻，无后续碰撞； ——以典型的城区车速侧碰（如乘用车撞到摩托车侧面）； ——以相当于典型主干道车速的速度差后碰（如乘用车撞到摩托车后部）； ——以相当于典型城区车速的速度差与迎面驶来的乘用车正碰。	边设施/静止车辆碰撞； ——以典型的主干道车速和行人/骑自行车的人碰撞； ——以典型的主干道车速侧碰（乘用车撞到摩托车侧面）； ——以相当于典型高速公路车速的速度差后碰（如乘用车撞到摩托车后部）； ——以相当于典型高速公路车速的速度差与迎面驶来的乘用车正碰。

B.3 暴露概率的示例与解释

对暴露概率的预估需要场景评估，在这些场景中，会出现促成危害发生的相关环境因素。需要评估的场景包括各种驾驶或运行场景。

评估的结果会确定危害场景的暴露概率级别，暴露概率级别有5个，分别为E0（最低暴露概率级别）、E1、E2、E3、E4（最高暴露概率级别）。

那些尽管在危害分析和风险评估中被定义了，但又被认为是不寻常或令人难以置信的场景会被指定为E0。仅仅与E0场景关联的危害的后续评估会被排除在进一步的分析之外。

示例：典型的 E0 示例：

a) 极其不寻常的或不可能同时发生的情况，例如车辆涉及到在高速公路上降落的飞机的事故；及

b) 自然灾害，如地震、飓风、森林大火。

根据场景的持续时间（重叠时间）或发生的频率，指定其余的E1、E2、E3和E4等级给可发生危害的场景。

注1：可依据例如地理位置或使用类型等来分级（见 8.4.3.4）。

危害的暴露度（E）可通过两种方式进行预估。第一种是基于场景的持续时间，第二种是基于场景发生的频率。例如，一个危害可以与一个给定运行场景的持续时间相关，如用在通过交通路口的平均时间；而另一个危害可以与同一个运行场景的发生频率相关，如车辆重复通过交通十字路口的频率。

在第一种情况下，暴露度按照场景的持续时间分级，暴露概率通常根据所考虑的场景下花费的时间与总的运行时间（如上电）的比值来估算。注意，在某些情况下，总运行时间可以是汽车生命周期（包

括下电）。在第二种情况下，一些暴露度的预估通过使用相关驾驶场景的发生频率来确定可能更为合适。一个合适的例子是，在这些情况下，场景发生后的很短的时间间隔内，已存在的电气/电子系统故障会导致危害事件的发生。

表B.2给出了按持续时间分级的驾驶场景和典型的暴露度分级的示例，表B.3给出了按频率分级的驾驶场景示例。

除了这些驾驶场景外，还要考虑该运行场景的具体情况。根据导致危害事件的确切时间和确切位置确定实际的暴露度是必要的。

驾驶场景可能同时具有持续特性和频率特性，如在停车场驾驶。在这种情况下，在表B.2和B.3的例子可能无法得出相同的暴露度等级，所以最合适的暴露度等级是根据对所考虑的运行场景的分析而选取的。

如果失效维持在潜伏状态的时间长度与危害事件预期发生之前的时间长度是相当的，那么暴露概率的预估应考虑这个时间长度。典型的这会涉及到按需动作的设备，比如安全气囊。

在这种情况下，暴露概率可通过$\sigma \times T$来预估：σ是危害事件的发生率，T是失效未被感知的持续时间（可能长达车辆的整个生命周期）。当乘积结果较小时，近似值$\sigma \times T$是有效的。

注2：关于所考虑的失效的持续时间，危害分析和风险评估不考虑作为相关项一部分的安全机制（见8.4.1.2）。

表B.2 基于运行场景持续时间的暴露概率等级

运行场景暴露概率等级（见表 3）	E1	E2	E3	E4
描述	极低概率	低概率	中等概率	高概率
持续时间（平均运行时间的百分比）	无定义	＜1%的平均运行时间	1%～10%的平均运行时间	＞10%的平均运行时间
资料性示例(事件)	——大侧倾角； ——在跳跃/颠簸过程中起动摩托车； ——发动机起动； ——使用撑杆（如支起或放下）； ——紧急制动（如遇到紧急危险）； ——横穿铁路或电车轨道； ——在行车道（如公共道路）上通过障碍物或散落的货物； ——变速换档。	——中等侧倾角； ——加油； ——坡道起步； ——使用转向指示器； ——通过十字路口； ——超车； ——推离中撑； ——制动； ——正常转弯； ——在隧道中； ——用脚支撑以保持摩托车平衡和操纵。	——小侧倾角； ——超车（其他车辆）； ——加速； ——减速； ——发动机怠速，摩托车在撑杆上； ——在交通信号灯或路口处停车。	——略微倾斜或几乎无侧倾角； ——巡航； ——电动摩托车充电； ——停车（包括摩托车使用中撑/撑杆）。

表B.3 基于运行场景频率的暴露概率等级

运行场景暴露概率等级（见表 3）		E1	E2	E3	E4
描述		极低概率	低概率	中度概率	高概率
场景发生的频率		对大多数驾驶员而言，一年发生的频率小于一次	对大多数驾驶员而言，每年发生几次	对普通驾驶员而言，基本上每个月发生一次或多次	平均几乎发生在每次驾驶中
资料性示例	道路类型	——非道路/未分级道路	——山路； ——鹅卵石路（铺装路）； ——回转路。	——机动车道/高速公路（包括带有隔离带的）	——二级公路； ——城区道路。
	路面/骑行条件	——冰雪路面	——在低摩擦路面驾驶（如树叶，碎石，机油，柴油，泥浆）； ——在大雨中驾驶； ——突然的侧风； ——非平整路面； ——大雾。	——在小雨/轻雾中驾驶； ——湿滑路面； ——横穿铁路或电车轨道； ——减速带/波纹减速带。	—
	环境/设施	——在行车道（如公共道路）上通过障碍物或散落的货物	——在隧道中	——交通拥堵； ——在加油站前； ——夜间无照明道路（如在黑暗中驾驶）。	—
	摩托车静止状态	——在跳跃/颠簸过程中起动摩托车	——在修理厂	——加油	——发动机起动； ——使用撑杆（如支起或放下）； ——停车（包括摩托车使用停车架/撑杆）； ——用脚支撑以保持摩托车平衡和操纵； ——发动机怠速，摩托车在撑杆上。

					——在交通信号灯或路口处停车
	驾驶操作	——大侧倾角； ——抬起前轮（带轮）； ——抬起后轮（带轮）。	——中等侧倾角； ——紧急制动（如有潜在危险）； ——低性能摩托车超车； ——从几辆静止或移动的汽车之间穿行； ——侧滑（漂移）动作，偏离预期路线； ——以大侧向加速度转弯； ——稍微抬起前轮； ——稍微抬起后轮。	——小侧倾角； ——坡道起步。	——略微倾斜或几乎无侧倾角； ——使用转向指示器； ——通过十字路口； ——穿过其他车辆； ——超车； ——推离中撑； ——加速； ——制动； ——减速； ——巡航； ——正常转弯； ——电动摩托车充电； ——变速换档。

B.4 可控性示例

为确定一个给定危害的可控性等级，需要预估具有代表性的驾驶员或其他涉及人员为避免伤害发生而能对场景施加影响的可能性。

这种可能性预估包括：如果这个给定的危害将要发生，具有代表性的驾驶员能够保持或者重新控制车辆的可能性，或者在这个危害发生范围内的个体能够通过他们的行动来避免危害的可能性。这种考量基于这样的假设，即危害场景中的个体为保持或者重新控制当前情况采取的必要控制行为，以及所涉及的驾驶员采取有代表性的驾驶行为。

注1：可控性预估可能受到很多因素的影响，包括该目标市场驾驶员的概况，能力水平、个体年龄、驾驶经验、文化背景等。

为了有助于这些评估，表B.4提供了一些发生功能异常的驾驶场景示例，以及可能避免伤害的相应的控制行为的假设。这些场景对应到可控性的分级，明确了用于判断控制能力水平90%和99%的分隔点。

注2：表B.4中提供的可控性分级示例是假定基于作为道路使用的中等尺寸摩托车。所提供的资料性示例将根据所考虑的摩托车的类型和性能进行评审。

注3：表B.4提供了可能发生的潜在风险，且在评估特定相关项时有必要考虑的参考。

表B.4 驾驶员或者潜在涉险人员可能控制的危害事件示例

可控性等级（见表4）	C0	C1	C2	C3

描述	可控	简单可控	一般可控	难以控制或不可控
驾驶因素和场景	常规可控	超过 99%的具有代表性的驾驶员或交通参与者能够避免伤害	90%到 99%具有代表性的驾驶员或交通参与者能够避免伤害	不到 90%具有代表性的驾驶员或交通参与者能够避免伤害
危害	运行场景（潜在涉险驾驶员/人员的控制行为）			
牵引力丧失（如轮胎失去切向力和径向力）	起步加速（如分离离合器、取消加速）	—	—	在坡道加速过程中，发生停止加速、掉头或制动
非预期加速（如油门加大）	—	—	在拥挤的城区交通中(如制动、分离离合器)	—
非预期减速(如发动机制动）	在拥挤的城区交通中(如：摩托车驾驶员分离离合器，其他车辆使用者可能制动）	在转向操作时（如摩托车驾驶员可能分离离合器）	—	—
非预期（最大）制动（如车轮未抱死）	—	在拥挤的城区交通中(如其他车辆使用者可以制动)	—	在转弯操作时（如掉头，移动重心）
牵引力丧失	在高速公路上巡航行驶时(如制动并向路边转向)	在超车操作中(如制动并转向以取消超车操作)	—	—
非预期后轮抱死	—	行驶至有停车让行标志的路口(如转向并使用前轮制动)	—	—
非预期前轮抱死	—	—	—	当接近一个停车枢纽时（如移动重心） 在转向操作时（如转向，移动重心）
制动能力大幅降低	—	—	当接近一群横穿道路的行人时(如在行人周围转向、降挡、鸣笛，行人可避开摩托车)	—
溜车	在斜坡上（如制动、加速）	—	—	—
前向照明丧失	—	夜间在没有照明的城郊路	—	—

		上行驶（如必要时应减速或停车，如有的话打开其他照明设备，如远光灯）		
转向阻尼丧失	—	在不平整路面以高速公路车速行驶（如增大转向动作，降低车速）	—	—
转向阻尼过大	—	进行超车时(如施加更大的转向力，减速或停车) 在停车场行驶时(如增加转向力，减速或停车)	—	—
非预期俯仰	—	当接近一个停车路口时（如移动重心） 从静止状态加速（如转移重心，减速）	—	—

附 录 C
（资料性）
可控性评级技术示例

C.1 总则

本附录提供了可用于帮助指定摩托车特定危害事件可控性等级的通用技术的一般介绍。本附录还介绍了使用可控性评级专家组（CCP）的概念，即通过考虑评估结果和可控性评估技术输出来指定可控性等级。

本附录未提供如何确定具体危害事件可控性等级的指导，而是针对可用于帮助开展可控性评估的有效方法和技术。

C.2 可控性评级专家组概念

可控性等级的分配可由CCP执行，其成员应在如下领域具有专业知识：

——摩托车可控性评估（由专业驾驶员进行）；

——摩托车动力学；

——电子/电气系统；

——功能安全；或

——驾驶员行为。

摩托车制造商和系统供应商可以根据不同的项目灵活地对CCP成员的数量和构成进行剪裁，并可提供选择CCP成员的合理理由。相关组织可将CCP成员构成的分享作为安全生命周期中任何功能安全计划的活动的一部分。在概念阶段，只要提供合理的理由支持，允许CCP就特定危害事件的可控性分级进行评估。

CCP开展评估可基于危害分析和风险评估过程中对严重度、暴露概率、可控性的分级的共同理解，功能安全目标和可用的文档，具有代表性的驾驶员的能力和其对摩托车的预期使用的理解，以及之前的安全确认测试结果与安全分析。开展危害分析和风险评估，可使用如下描述的单一技术或适当的技术组合，或其他技术，来进行可控性评估。

C.3 评估摩托车危害事件的可控性

可控性评估是指对危害事件发生时，具有代表性的驾驶员能够保持或恢复对摩托车的控制，或者其他潜在处于风险的人员能够充分控制危害事件以避免特定伤害的概率预估。评估可通过测试或分析来完成。

根据以往经验，汽车相关危害事件的可控性最初是基于对具有代表性的驾驶员或其他潜在处于风险的人员的反应来进行评估。条件允许的情况下，可以引入一组具有代表性的驾驶员对系统发生故障时车辆的可控性水平进行评估。

由于摩托车的动态行为和乘用车相比，在确保动态稳定性、预期轨迹和驾驶平顺性方面更加强调人与车的交互作用。所以，评估可控性时通常不太可能使用和汽车行业相同的方法。而且摩托车驾驶员的典型控制行为与乘用车驾驶员有本质不同，因此，有必要对摩托车进行专门的评估。

某一种评估方法是基于真实驾驶员的反馈对可控性进行评估，以了解驾驶员的反应（如掉头、加大油门开度、刹车和重心转移等）如何影响摩托车的动态稳定性、预期轨迹和驾驶平顺性。评估摩托车危害事件可控性的一种普遍接受的方法，是使用专业摩托车驾驶员判断具有代表性的驾驶员对特定的危

害事件如何应对。专业摩托车驾驶员具有经验和技能来处理一些相当极端的危害事件。对专业驾驶员的使用可能需要进行适当限制，以确保他/她的安全。

C.4 专业摩托车驾驶员

本附录并不要求专业摩托车驾驶员通过任何特定标准的认证或持有特定的高级驾驶员资质，而是推荐车辆制造商、测试机构和/或供应商基于他们内部的规程来进行专业摩托车驾驶员的选择,该程序应该将专业摩托车驾驶员的安全列为最高优先级，并且要求采取适当的风险控制措施，以尽量降低对专业驾驶员伤害的风险。公司程序可能包括如何选择专业摩托车驾驶员的指导。以下的资料性示例息可以作为专业摩托车驾驶员的选拔准则。

——具有多年在所有目标群体的相关场景和环境条件下的摩托车驾驶经验；

——具备利用公司特定标准进行可控性评级的知识；

——具备完成评估的经验；

——具备正确传递各类具有代表性的摩托车驾驶员驾驶信息的能力；

——具备在技术背景下讨论测试与结果的技术能力；

——参与企业特定的驾驶员培训课程；或

——持有企业出具的作为专业摩托车驾驶员的正式证明；

C.5 可控性评估技术

由CCP进行的可控性等级分配，可通过采用常规评估技术的适当组合来完成，例如通过一组具有代表性的摩托车驾驶员或专业摩托车驾驶员、使用驾驶模拟器或数学建模技术。如果出现不能确保专业摩托车驾驶员安全的场景，则应分配为最高级的可控性等级(即，甚至是专业摩托车驾驶员也会认为某个特定动作是不可控的)。本附录不指定首选的可控性评估技术,也不对使用哪些评估技术提出具体建议。下列评估技术可供参考：

a) 由一组具有代表性的驾驶员来评估：这仍然是汽车工业中常用的方法，且此类评估对风险降低到可接受程度是有例可循的，即危害事件不会影响摩托车的动态稳定性、预期轨迹和驾驶平顺性(例如，电加热手柄)。

b) 由专业摩托车驾驶员来评估：通过专业摩托车驾驶员进行评估是一种常用的技术。专业摩托车驾驶员可以对一个具有代表性的驾驶员如何应对特定的危害事件做出判断。通过多个专业摩托车驾驶员来评估可控性可能更有效(见 C.6)。

c) 使用驾驶模拟器进行评估：这种方法可以使用具有代表性的驾驶员和驾驶模拟器，该驾驶模拟器能够提供某个系统功能异常场景，逼真的显示摩托车的动态控制特性和驾驶环境。请注意，“模拟器”这个词在此上下文中是指真实驾驶员使用方向把、油门、刹车等等来控制摩托车的物理、机电的动态表现。该模拟器具有合适的控制感觉特性和合适的感知显示器。模拟器的功能可以根据可控性评估的需要进行调整。

d) 使用数学建模及仿真技术进行评估：该计算机仿真方法采用了摩托车动力学和驾驶员/控制器的数学模型。请注意，“模拟”一词在这里是指摩托车和驾驶员/控制器及其动态交互在软件中表示。

C.6 评估可控性

对具有代表性的驾驶员的可控性分级的评估可基于下列各项:

——车辆响应与性能，如表 C.1 所示;

——感知，如表 C.2 所示;或

——控制行为，如表 C.3 所示。

表C.1 车辆响应与性能

高可控 ◄——► 低可控			
车辆的响应和性能没有变化	车辆的响应和性能有轻微变化	车辆的响应和性能有中度变化	车辆的响应和性能有严重变化

表C.2 感知

高可控 ◄——► 低可控			
危害和由此产生的车辆反应是察觉不到的[a]，或对车辆的运行没有影响。(例如:收音机的音量)	危害和由此产生的车辆反应是可以察觉的，但不向驾驶员示警。 驾驶员控制动作的时机会有较小的影响。	危害和由此产生的车辆反应是可以察觉的，并向驾驶员示警。驾驶员控制动作的时机较重要，但不是最关键。	危害和由此产生的车辆反应是可以察觉的，并向驾驶员充分示警。 驾驶员控制动作的时机是至关重要的。
[a] 例如，当车辆之间的相对运动速度很小时，驾驶员可能无法分辨附近的车辆在减速还是自己的车辆在加速。			

表C.3 控制行为

高可控 ◄——► 低可控			
驾驶员无需改变他/她的控制行为[a]	正常的控制补偿动作[b]足以使驾驶员保持对车辆的控制。	驾驶员可能需要调整他/她超出正常控制补偿动作的控制行为，以保持对车辆的控制。	特别的技能和高超的控制力是保持对车辆控制的必要条件。
[a] 这可能包括，例如，必要的控制以保持与前方速度变化车辆的跟车距离。 [b] 正常的控制补偿动作是指控制受到典型扰动(如阵风、粗糙路面等)的摩托车时所需的一系列操纵力、作用力或其他控制动作。			

参 考 文 献

[1] Abbreviated injury scale; Association of the advancement of Automotive medicine; Barrington, IL, USA Information is also available at www.aaam.org [viewed 2018-12-11].

[2] Baker,S.P., O'Neill,B., Haddon,W., Long,W.B., The injury severity score: a method for describing patients with multiple injuries and evaluating emergency care, The Journal of Trauma, Vol.14, No.3, 1974.

[3] Balogh,Z., Offner,P.J., Moore,E.E., Biffl, W.L., NISS predicts post injury multiple organ failure better than ISS, The Journal of Trauma, Vol.48, No.4, 2000 .

[4] ISO11451 (all parts), Road vehicles— Vehicle test methods for electrical disturbances from narrowband radiated electromagnetic energy.

[5] IEC61000-6-1, Electromagnetic compatibility (EMC)— Part6-1: Generic standards— Immunity for residential, commercial and light-industrial environments.