ICS 43.040
T 35

中华人民共和国国家标准

GB/T 34590.3—2017

道路车辆　功能安全
第3部分:概念阶段

Road vehicles—Functional safety—
Part 3: Concept phase

(ISO 26262-3:2011,MOD)

2017-10-14 发布　　2018-05-01 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

目　　次

前　言

GB/T 34590《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 34590的第3部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用重新起草法修改采用ISO 26262-3:2011《道路车辆　功能安全　第3部分：概念阶段》。

本部分与ISO 26262-3:2011的技术性差异及其原因如下：

——修改了本部分的适用范围，由原文的“适用于安装在最大总质量不超过3.5 t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系统”改为“适用于安装在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”；

——关于规范性引用文件，本部分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—2017代替ISO 26262-1:2011；
- 用修改采用国际标准的GB/T 34590.2—2017代替ISO 26262-2:2011；
- 用修改采用国际标准的GB/T 34590.8—2017代替ISO 26262-8:2011；
- 用修改采用国际标准的GB/T 34590.9—2017代替ISO 26262-9:2011。

本部分还做了下列编辑性修改：

——修改了国际标准的引言及其表述和图1的内容。

本部分由全国汽车标准化技术委员会(SAC/TC 114)提出并归口。

本部分负责起草单位：中国汽车技术研究中心、泛亚汽车技术中心有限公司、中国第一汽车股份有限公司、博世汽车部件(苏州)有限公司、舍弗勒投资(中国)有限公司、上海海拉电子有限公司、北京兴科迪科技有限公司、联合汽车电子有限公司、上海汽车集团股份有限公司技术中心、东风汽车公司技术中心、重庆长安汽车股份有限公司。

本部分参加起草单位：上汽大众汽车有限公司、本田技研工业(中国)投资有限公司、上海汽车集团股份有限公司商用车技术中心、上汽通用五菱汽车股份有限责任公司、安徽江淮汽车集团股份有限公司、北京新能源汽车股份有限公司、奇瑞汽车股份有限公司、东风汽车有限公司东风日产乘用车公司。

本部分主要起草人：李波、尚世亮、张立君、薛剑波、童菲、蒋军、曲元宁、史晓密、杨虎、明月、付越、邓湘鸿、范嘉睿、李艳文、冯亚军、付艳玲、边宁、李燕、陈音、张乐敏、盛一芝、宋锦明、匡小军、徐清魁、荣胜军、黄志诚、刘正国、张小帆。

引　言

ISO 26262 是以 IEC 61508 为基础，为满足道路车辆上电子电气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。GB/T 34590 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 GB/T 34590 针对的是电子电气系统的功能安全，但是它也提供了一个框架，在该框架内可考虑基于其他技术的与安全相关系统。GB/T 34590：

a) 提供了一个汽车安全生命周期（管理、开发、生产、运行、服务、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（ASIL）；

c) 应用汽车安全完整性等级（ASIL）定义 GB/T 34590 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、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开发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—2017、GB/T 34590.4—2017、GB/T 34590.5—2017、GB/T 34590.6—2017、GB/T 34590.7—2017 之间的相互关系；

——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—2017 的第 6 章。

图 1　GB/T 34590—2017 概览

道路车辆　功能安全
第3部分:概念阶段

1　范围

GB/T 34590的本部分规定了车辆在概念阶段的要求:

——相关项定义;

——安全生命周期启动;

——危害分析和风险评估;及

——功能安全概念。

本标准适用于安装在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。

本标准不适用于特殊用途车辆上特定的电子电气系统,例如,为残疾驾驶者设计的车辆。

本标准不适用于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。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系统、制动系统、自适应巡航系统)有专用的功能性能标准。

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 34590.1—2017　道路车辆　功能安全　第1部分:术语(ISO 26262-1:2011,MOD)

GB/T 34590.2—2017　道路车辆　功能安全　第2部分:功能安全管理(ISO 26262-2:2011,MOD)

GB/T 34590.8—2017　道路车辆　功能安全　第8部分:支持过程(ISO 26262-8:2011,MOD)

GB/T 34590.9—2017　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 26262-9:2011,MOD)

3　术语、定义和缩略语

GB/T 34590.1—2017界定的术语、定义和缩略语适用于本文件。

4　要求

4.1　一般要求

如声明满足GB/T 34590—2017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—2017 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是可接受的，并且按照 GB/T 34590.2—2017 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—2017 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 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，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他方法，应给出满足相关要求的理由。

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，不依赖于这些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，宜采用具有较高推荐等级的方法。应给出所选的方法组合满足相关要求的理由。

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。

4.3 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，应按照 GB/T 34590.9—2017 第 5 章，遵循分解后的 ASIL 等级。

如果 GB/T 34590—2017 中 ASIL 等级在括号中给出，则对于该 ASIL 等级，相应的子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。

5 相关项定义

5.1 目的

第一个目的是定义并描述相关项，及其与环境和其他相关项的依赖性和相互影响。

第二个目的是为充分理解相关项提供支持，以便执行后续阶段的活动。

5.2 总则

本章为建立相关项的定义列出了要求和建议，相关项的定义包括其功能、接口、环境条件、法规要求和危害等。该定义为执行后续子阶段：“安全生命周期启动”(参见第 6 章)、“危害分析和风险评估”(参见第 7 章)和“功能安全概念”(参见第 8 章)的人员提供了充足的关于相关项的信息。

注：附录 A 中表 A.1 提供了概念阶段的目的、前提条件和工作成果的概览。

5.3 本章的输入

5.3.1 前提条件

无。

5.3.2 支持信息

可考虑如下信息：

——任何与相关项相关的已有信息，如产品理念、项目梗概、相关专利、预试验结果、来自前代相关项的文档、其他独立的相关项的相关信息。

5.4 要求和建议

5.4.1 应给出相关项的功能性和非功能性的要求，以及相关项与其环境之间的依赖性。

注 1：在定义了相关项的安全目标和各自的 ASIL 等级后，这些要求可归类为是与安全相关的。

注 2：所需的信息对于相关项的定义来说是一个必要的输入，即使该信息不是与安全相关的。如果不具备所需的信息，则可由本章的要求来促成该信息的生成。

该信息包括：

a) 功能概念，其描述了目的和功能，包括相关项的运行模式和状态；

b) 运行条件和环境约束；

c) 法规要求（特别是法律和法规），国家标准和国际标准；

d) 由相似的功能、相关项或要素实现的行为（如果存在）；

e) 相关项的预期行为的假设；及

f) 行为不足，包括已知的失效模式和危害，造成的潜在后果。

注：可包括关于类似相关项的已知的与安全相关的事件。

5.4.2 定义相关项的边界、接口以及提出与其他相关项和要素交互关系的假设时，应考虑：

a) 相关项内部的要素；

注：要素也可基于其他技术。

b) 相关项的行为对其他相关项或要素的影响的假设，即相关项的环境；

c) 该相关项与其他相关项或要素的相互作用；

d) 其他相关项、要素和环境要求本相关项提供的功能；

e) 本相关项要求其他相关项、要素和环境提供的功能；

f) 功能在所涉及的系统和要素间的分配；及

g) 影响相关项功能的运行场景。

5.5 工作成果

相关项定义，由 5.4 的要求得出。

6 安全生命周期启动

6.1 目的

安全生命周期启动的第一个目的是对新的相关项开发和对现有相关项的修改进行区分（参见 GB/T 34590.2—2017 图 2）。

安全生命周期启动的第二个目的是在对现有相关项的修改的情况下定义将要实施的安全生命周期

活动(参见 GB/T 34590.2—2017 图 2)。

6.2 总则

基于相关项定义,通过区分相关项为新的开发还是对现有相关项的修改来启动安全生命周期。对于现有相关项的修改的情况,进行安全相关活动的剪裁。

6.3 本章的输入

6.3.1 前提条件

应具备如下信息:

——相关项定义,按照 5.5。

6.3.2 支持信息

可考虑如下信息:

——相关项的定义未包含的、有助于进行影响分析的任何现有信息。

示例:产品概念、变更要求、实施计划、在用证明。

6.4 要求和建议

6.4.1 确定开发类别

应确定相关项是否为一个新的开发,或对现有相关项或其环境的修改:

a) 对于新开发的情况,紧接着应根据第 7 章进行危害分析和风险评估。

b) 对于现有相关项或其环境进行修改的情况,应按照 6.4.2 确定适用的生命周期子阶段和活动。

注:在用证明可适用于修改的情况(参见 GB/T 34590.8—2017 第 14 章)。

6.4.2 现有相关项修改的情况下的影响分析和可能的安全生命周期剪裁

6.4.2.1 为了识别和描述对相关项或其环境的预期修改,及评估这些修改带来的影响,应进行影响分析。

注 1:对相关项的修改包括设计修改和实现方式的修改。设计修改可来自需求的修改(如功能或性能提高或成本优化)。实现方式的修改不影响相关项的定义或性能,仅影响实现方式的特性。

示例:实现方式的修改可来自软件的修正,或使用新的开发工具或生产工具。

注 2:如果配置数据或标定数据的修改会影响相关项的功能,则该修改被认为是对相关项的修改。

注 3:相关项所处环境的修改可能是由于相关项安装在一个新的目标环境内(如其他车辆变型)或与相关项相互作用的(或在其周边的)其他相关项或要素的升级。

6.4.2.2 影响分析应识别和指出因相关项的修改、相关项先前和未来的使用条件之间的修改所带来的影响,包括:

a) 运行场景和运行模式;

b) 与环境的接口;

c) 安装特性,如在车上的位置、车辆配置和变型;及

d) 一系列环境条件,如温度、海拔、湿度、振动、电磁干扰和燃油类型。

6.4.2.3 应识别并描述修改对功能安全的影响。

6.4.2.4 应识别并描述需要更新的受影响的工作成果。

6.4.2.5 安全活动应根据适用的生命周期阶段进行剪裁。

6.4.2.6 剪裁应基于影响分析的结果。

6.4.2.7 按照 GB/T 34590.2—2017 中 6.4.3,剪裁的结果应包含在安全计划中。

6.4.2.8 应重新生成受到影响的工作成果。

注：受到影响的工作成果包括确认计划(参见 GB/T 34590.4—2017)。

6.4.2.9 如果缺少工作成果或工作成果不满足 GB/T 34590—2017，则应确定为满足 GB/T 34590—2017 的要求所必需的活动。

6.5 工作成果

6.5.1 影响分析，由 6.4.2.1～6.4.2.4 的要求得出。

6.5.2 安全计划(细化的)，由 6.4.2.5～6.4.2.9 的要求得出。

7 危害分析和风险评估

7.1 目的

危害分析和风险评估的目的是识别相关项中因故障而引起的危害并对危害进行归类，制定防止危害事件发生或减轻危害程度的安全目标，以避免不合理的风险。

7.2 总则

危害分析、风险评估和 ASIL 等级的确定用于确定相关项的安全目标以避免不合理的风险。为此，根据相关项中潜在的危害事件，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它们的 ASIL 等级。ASIL 等级是通过对影响因子：严重度、暴露概率和可控性的预估确定的，影响因子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。

7.3 本章的输入

7.3.1 前提条件

应提供以下信息：

——相关项定义，按照 5.5。

7.3.2 支持信息

可考虑如下信息：

——影响分析，如果适用(参见 6.5.1)；及

——其他独立相关项的相关信息(来自外部)。

7.4 要求和建议

7.4.1 危害分析和风险评估的启动

7.4.1.1 应基于相关项的定义进行危害分析和风险评估。

7.4.1.2 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前代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。

示例：如果通过电子稳定性控制(ESC)提供更多的控制是可用的并且充分独立的，则其能减轻底盘系统失效的影响。

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。

7.4.2 场景分析及危害识别

7.4.2.1 场景分析

应对相关项的故障行为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，既要考虑正确使用车辆的情况，也要考虑可预见的不正确使用车辆的情况。

注：运行场景描述了期望相关项以一种安全的方式进行工作的边界范围。例如：不期望普通乘用车在越野路面高速行驶。

7.4.2.2 危害识别

7.4.2.2.1 应通过使用足够的技术手段系统地确定危害。

注：使用诸如头脑风暴、检查列表、质量历史记录、FMEA 和现场研究等技术提取相关项层面的危害。

7.4.2.2.2 应以能在整车层面观察到的条件或行为来定义危害。

注 1：通常，每一个危害有多种与相关项的功能实现相关的潜在原因，但在危害分析和风险评估中，对于危害的条件或行为进行定义时，不需要考虑这些原因，这些原因是从相关项的功能行为得出的。

注 2：仅考虑与相关项自身相关的危害，假设其他充分独立的系统（外部措施）均正确工作。

7.4.2.2.3 危害事件应由运行场景和危害的相关组合确定。

7.4.2.2.4 应识别危害事件的后果。

注：如果相关项层面的失效导致该相关项丧失多个功能，则场景分析和危害识别需考虑由相关项或整车的故障行为组合而导致的危害事件。

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”“助力转向”及“前向照明”。

7.4.2.2.5 如果在 7.4.2.2 中所识别出的危害超出 GB/T 34590—2017 的范围（参见第 1 章），应注明需要采用适当的措施来减轻或控制这些危害并通报给相关责任者。

注：由于这些危害超出 GB/T 34590—2017 的范围，因此不需要进行危害分类。

7.4.3 危害事件分类

7.4.3.1 应对在 7.4.2.2 中识别出的所有的危害事件进行分类，除了超出 GB/T 34590—2017 范围的。

注：如果难以对一个给定的危害进行严重度、暴露概率或可控性的分级，则在分级时需要保持谨慎，即不论何时有任何疑问，给出一个较高的 ASIL 等级而不是较低的 ASIL 等级。

7.4.3.2 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。应根据表 1 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。简明损伤定级（AIS）的描述可用于界定严重度，参见附录 B。关于严重度的不同类型和事故的资料性示例参见附录 B。

注 2：严重度等级的评估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评估。

注 3：对被评估中的场景，严重度预估需要考虑事件发生的合理顺序。

注 4：严重度的确定基于目标市场中有代表性的个体样本。

表 1 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

7.4.3.3 如果经过危害分析，确定相关项的故障行为的后果明显局限于物质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。如果一个危害的严重度等级为 S0，则无需分配 ASIL 等级。

7.4.3.4 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。应按照表 2 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：暴露概率的确定基于目标市场中有代表性的运行场景样本。

注 3：暴露概率的相关细节和示例参见附录 B。

表 2 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

7.4.3.5 当预估暴露概率时，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个车辆上（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。

7.4.3.6 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几乎不可能发生或难以置信的场景，无需跟进。应记录排除这些场景的理由。如果一个危害的暴露概率等级被指定为 E0，则无需分配 ASIL 等级。

示例：E0 可用于“不可抗力”风险的情况（参见附录 B 中 B.3）。

7.4.3.7 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潜在处于风险的人员对该危害事件的可控性。应按照表 3 为可控性指定一个 C0、C1、C2 或 C3 的可控性等级。

注 1：从 C1 到 C3 等级，两个相邻 C 等级间的概率差异是一个数量级。

注 2：可控性评估指预估驾驶员或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。因此，使用级别分别为 C1、C2、和 C3 的参数 C，对避免伤害的可能性进行分类。假设驾驶员在正常的条件下驾驶（例如：他/她不疲劳），经过相应的驾驶员培训（他/她有驾驶执照）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。表 B.4 列出了一些示例，用于对这些等级做出解释。考虑合理地可预见的误操作。

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移出自身，或被该危害场景中的其他人员移出的概率的预估。当考虑可控性时，注意涉险人员可能不熟悉相关项的运行。

注 4：当可控性涉及多个交通参与者的行为时，可控性的评估可基于带有故障相关项的车辆的可控性，以及其他参与者的可能的行为。

表 3 可控性等级

等级	C0	C1	C2	C3
描述	可控	简单可控	一般可控	难以控制或不可控

7.4.3.8 如果相关项失效的危害不影响车辆的安全运行（例如一些驾驶员辅助系统），可控性等级可为 C0。如果已经有专门法规规定了针对一个既定危害的功能表现，则该危害的可控性等级可为 C0，此外，也可通过应用现有的经验认为达到了充分的可控性，通过讨论而定义为 C0 等级。如果一个危害的可控性等级为 C0，则无需分配 ASIL 等级。

示例：某个专门的法规精确地定义了在失效情况下，车辆系统应具备的力或加速度。

7.4.4 ASIL 等级和安全目标的确定

7.4.4.1 每一个危害事件的 ASIL 等级应根据表 4 使用“严重度”“暴露概率”和“可控性”这三个参数

确定。

注 1：4 个 ASIL 等级：ASIL A、ASIL B、ASIL C 和 ASIL D，其中 ASIL A 是最低的安全完整性等级，ASIL D 是最高的。

注 2：除了这 4 个 ASIL 等级之外，QM(质量管理)等级表示 GB/T 34590—2017 不做要求。

表 4　ASIL 等级确定

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

7.4.4.2　应确保运行场景列表的详细程度选择不会导致相应安全目标的 ASIL 等级不适当的降低。

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(参见 7.4.2.2)，可得到关于多个危害事件的详细分类。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导致相应地降低各自的暴露等级，从而不恰当地降低相应安全目标的 ASIL 等级。

7.4.4.3　应为具有 ASIL 等级的每个危害事件确定一个安全目标，该 ASIL 等级从危害分析中得出。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。

7.4.4.4　应将为危害事件所确定的 ASIL 等级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 7.4.4.3，应将最高的 ASIL 等级分配给合并后的安全目标。

注：如果合并后的安全目标是针对不同场景下的相同的危害，则安全目标的 ASIL 等级是每种场景下所考虑的安全目标中最高的一个。

7.4.4.5　如果一个安全目标可以通过转移到或保持一个或多个安全状态来实现，则应明确说明对应的安全状态。

注：安全状态将在第 8 章中进一步说明。

示例：一个安全状态可以是关闭、锁定、车辆静止，以及在某种失效情况下规定的时间内保持功能。

7.4.4.6　安全目标连同它们的属性(ASIL 等级)应按照 GB/T 34590.8—2017 第 6 章进行定义。

注：安全目标可包括诸如容错时间间隔等特征，或物理特性(例如最大的非预期方向盘转矩，最大的非预期加速度)，如果它们与 ASIL 等级的确定相关。

7.4.5　验证

危害分析、风险评估和安全目标应按照 GB/T 34590.8—2017 第 9 章进行验证，以表明其：

a) 场景(7.4.2.1)和危害(7.4.2.2)的完备性;
b) 与相关项定义的符合性;
c) 与相关危害分析和风险评估的一致性;
d) 对危害事件覆盖的完备性;及
e) 所分配的 ASIL 等级与相关危害事件的一致性。

注:该验证评审检查相关项的危害分析和风险评估的正确性和完备性,即考虑的场景、危害和参数估计(严重度、暴露概率和可控性)。相比之下,根据 GB/T 34590.2—2017 进行的危害分析和风险评估的认可评审,正式地检查危害分析和风险评估的流程是否符合第 7 章的要求。认可评审由一位或多位来自不同的部门或组织的人来执行,而不是相关项的开发人员。

7.5 工作成果

7.5.1 危害分析和风险评估,由 7.4.1.1～7.4.4.2 的要求得出。
7.5.2 安全目标,由 7.4.4.3～7.4.4.6 的要求得出。
7.5.3 危害分析和风险评估以及安全目标的验证评审报告,由 7.4.5 的要求得出。

8 功能安全概念

8.1 目的

功能安全概念的目的是从安全目标中得出功能安全要求,并将其分配给相关项的初步架构要素或外部措施。

8.2 总则

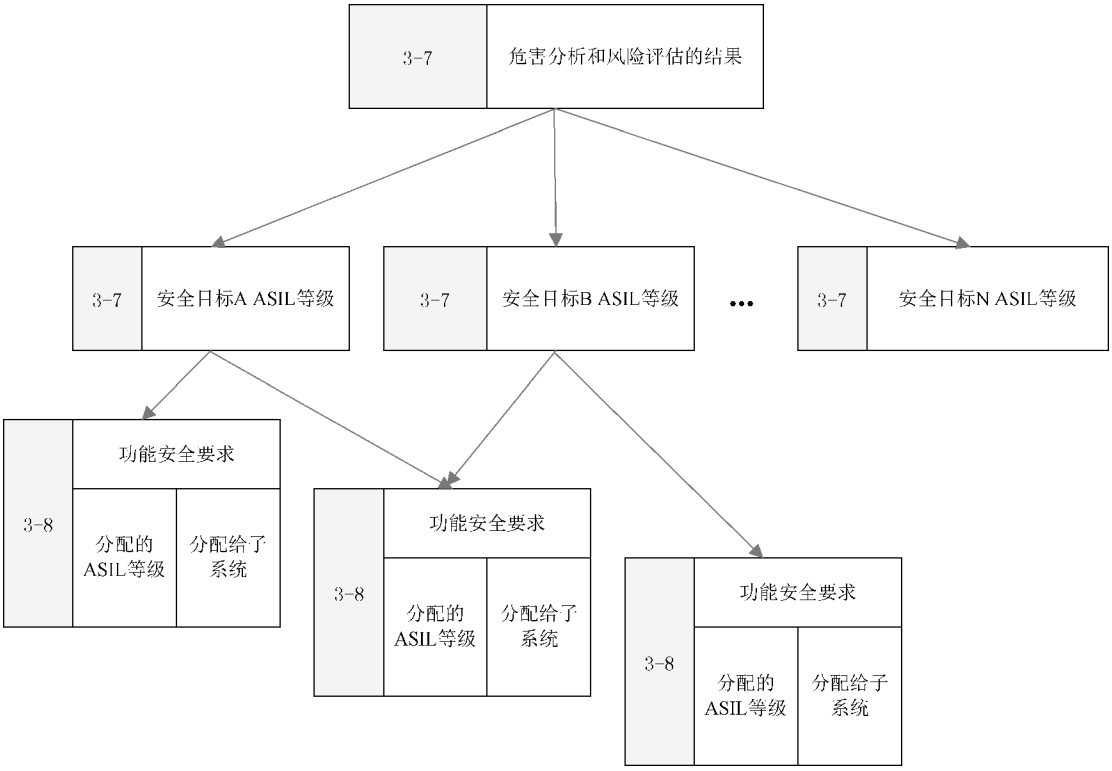
为了满足安全目标,功能安全概念包括安全措施(含安全机制),这些安全措施将在相关项的架构要素中实现,并在功能安全要求中规定。

功能安全概念涵盖:

——故障探测和失效减轻;
——向安全状态的过渡;
——容错机制,在此机制下一个故障不直接导致违背一个或多个安全目标,并且使相关项保持在安全状态(无论是否有功能降级);
——故障探测和驾驶员警告,目的是将风险暴露时间降低到一个可接受的时间区间内(例如:发动机故障指示灯,ABS 故障警示灯);及
——仲裁逻辑,从不同功能同时生成的多种请求中选择最合适的控制请求。

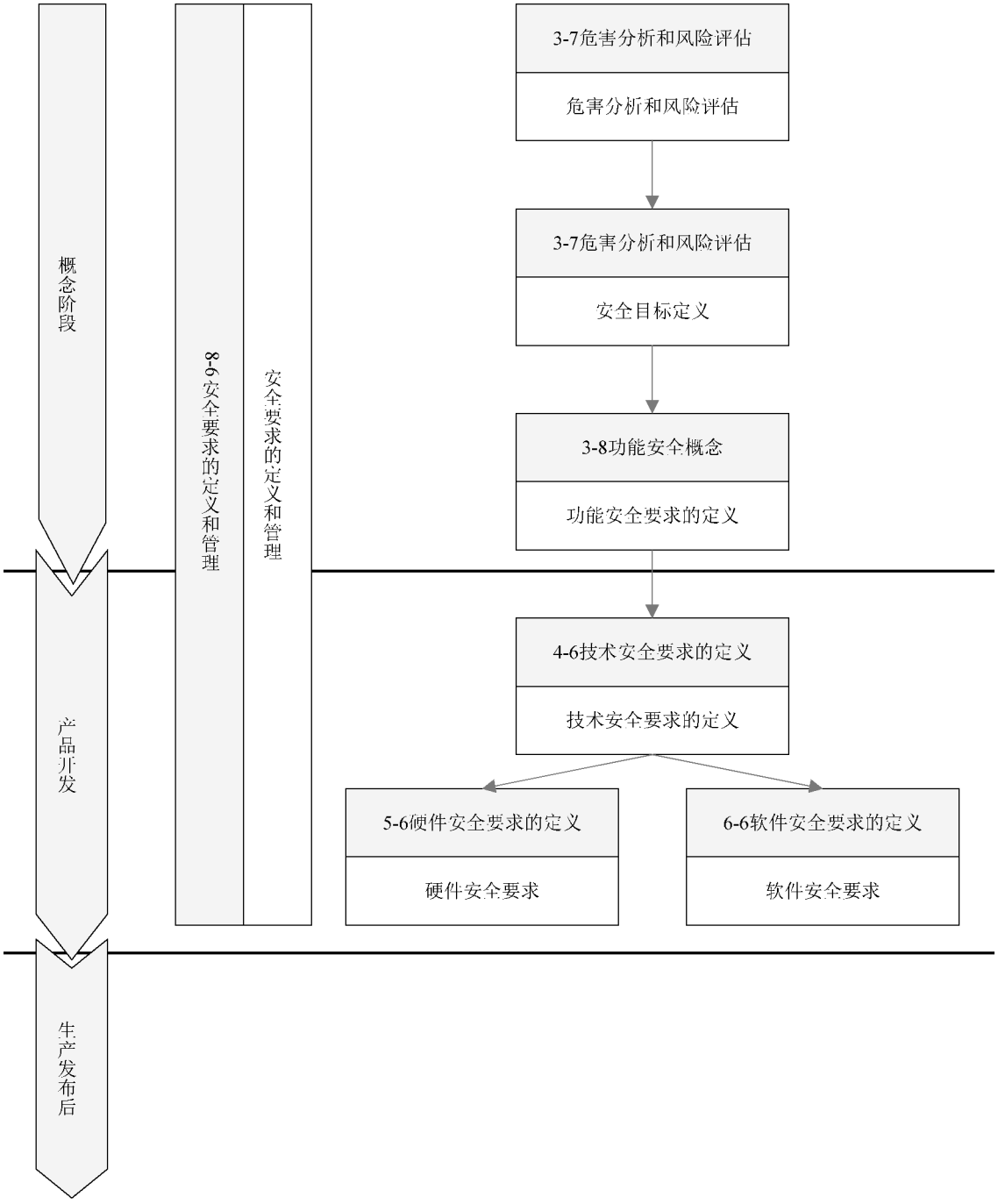
图 2 说明了通过分层的方法,从危害分析和风险评估中得出安全目标,再由安全目标得出功能安全要求。

图 3 给出了 GB/T 34590 相应部分中的安全要求的结构和分布的说明。将功能安全要求分配给初步架构要素。



注：图中 GB/T 34590—2017 每部分的特定章节用以下方式标示：“m-n”，“m”代表部分号，“n”代表章号，例如“3-6”代表 GB/T 34590.3—2017 的第 6 章。

图 2　安全目标和功能安全要求层级



注：图中 GB/T 34590—2017 每部分的特定章用以下方式标示：“m-n”，“m”代表部分号，“n”代表章号，例如“3-6”代表 GB/T 34590.3—2017 的第 6 章。

图 3　安全要求的结构

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 5.5；

——危害分析和风险评估，按照 7.5.1；及
——安全目标，按照 7.5.2。

8.3.2 支持信息

可考虑以下信息：
——初步架构设想（来自外部）。

8.4 要求和建议

8.4.1 总则

功能安全要求应按照 GB/T 34590.8—2017 第 6 章进行定义。

8.4.2 功能安全要求的导出

8.4.2.1 功能安全要求应由安全目标和安全状态导出，并考虑初步架构设想。

8.4.2.2 应为每一个安全目标定义至少一项功能安全要求。

注：一项功能安全要求可对几个安全目标有效。

8.4.2.3 如果适用，应考虑以下几点来定义每项功能安全要求：

a) 运行模式；
b) 故障容错时间间隔；
c) 安全状态；
d) 紧急运行时间间隔；及
e) 功能冗余（例如故障容错）。

注：为了制定一套完整有效的功能安全要求，安全分析（例如 FMEA、FTA、HAZOP）可为以上活动提供支持。

8.4.2.4 如果在一个可接受的时间间隔内，不能过渡到安全状态，应规定紧急运行。

示例：当立即关闭系统尚不能达到安全状态的时候，应规定紧急运行。

8.4.2.5 应将报警和降级概念定义为功能安全要求。

注：在报警和降级概念中描述了安全状态的过渡（切换到安全状态和从安全状态中恢复）和过渡条件。

示例 1：通过切换到安全状态进行故障探测和失效减轻。

示例 2：故障探测和驾驶员警告是为了将风险暴露的时间降低到可接受的时间间隔内（例如：发动机故障指示灯、ABS 故障报警灯）。

8.4.2.6 如果为了满足安全目标而对驾驶员或其他潜在涉险人员的必要行动做出了假设，则应进行 a）和 b）：

注：这些行动包括在可控性预测期间被认为是具有可信度的那些行动，以及在实施安全要求之后为满足安全目标所做的任何更进一步的必要行动。

示例：ACC：通过驾驶员踩下加速踏板来撤销制动行为。

a) 在功能安全概念中应定义这些行动；及
b) 在功能安全概念中应定义可供驾驶员或其他潜在涉险人员使用的足够的方法和控制手段。

注 1：对驾驶员的工作任务分析有助于考虑防止驾驶员超负荷，防止驾驶员的惊吓、恐慌、震惊（丧失控制车辆的能力）和模式混淆（关于操作模式的不正确的假设）。

注 2：对警告和降级概念、驾驶员和其他潜在涉险人员的必要行动的定义，应作为用户手册的输入（见 GB/T 34590.7—2017 的 6.4.1）。

8.4.3 功能安全要求的分配

8.4.3.1 功能安全要求应分配给初步架构设想中的要素：

注：冗余度和独立性可通过对相关失效的分析来检查（参见 GB/T 34590.9—2017 第 7 章）。

a) 在分配过程中，ASIL 等级和 8.4.2.3 中所给出的信息应从相关的安全目标或上一级安全要求（若应用了 ASIL 分解）中继承得到；
b) 如果将几个功能安全要求分配给同一个架构要素，且在初步架构中无法证明这些要求是互相独立或者免于干扰，则该架构要素应按照安全要求中最高的 ASIL 等级开发；
c) 如果相关项包含多个系统，则应根据初步架构的设想定义各个系统以及系统之间接口的功能安全要求，这些功能安全要求应分配到各个系统中；
d) 如果在功能安全要求分配期间进行 ASIL 等级分解，则应按照 GB/T 34590.9—2017 第 5 章进行 ASIL 等级分解。

8.4.3.2 如果功能安全概念依赖于其他技术的要素，应：
a) 应导出基于其他技术的要素所实现的功能安全要求，并将其分配给架构中的相关要素；
b) 应定义与其他技术要素的接口相关的功能安全要求；
c) 应通过特定的措施（超出 GB/T 34590—2017 的范围）来保证基于其他技术的要素所实现的功能安全要求；
d) 无需对这些要素分配 ASIL 等级。

注：基于其他技术的要素的充分性体现在确认活动中（参见 GB/T 34590.4—2017）。

8.4.3.3 如果功能安全概念依赖于外部措施，应：
a) 应导出由外部措施实现的功能安全要求并进行沟通；
b) 应定义与外部措施接口的功能安全要求；
c) 若外部措施是由一个或多个电子电气系统实现的，则应使用 GB/T 34590—2017 来表述其功能安全要求；
d) 应确保由外部措施实现的功能安全要求的执行。

注：外部措施的充分性，体现在确认活动中（参见 GB/T 34590.4—2017）。

8.4.4 确认准则

应基于功能安全要求对相关项安全确认的接受准则进行定义。

注：对详细准则和待确认特性列表的进一步要求，参见 GB/T 34590.4—2017 的 6.4.6.2 和 9.4.3.2。

8.4.5 功能安全概念的验证

功能安全概念应按照 GB/T 34590.8—2017 第 9 章进行验证，以表明其与安全目标的一致性和符合性，及减轻或避免危害事件的能力。

注 1：在概念阶段，对减轻或避免危害事件的能力进行验证的方法可与确认方法相同。评估结果可为概念的改进提供指引。然而，需记住的是，GB/T 34590.4—2017 第 9 章里安全确认的基础是一个根据 GB/T 34590 开发的相关项，而且安全确认不能基于概念研究（例如，原型）。

示例：减轻或者避免一个危害事件的能力可通过测试、试运行或专家评价来评估，结合原型、研究、专项测试或者仿真等。

注 2：针对该故障的特性（例如，是瞬态的或者是永久的），对减轻或避免危害事件的能力进行验证。

注 3：对于验证，可使用一种基于可追溯性的论证，例如：若相关项符合功能安全要求，则该相关项符合与该要求相关的安全目标。

8.5 工作成果

8.5.1 功能安全概念，由 8.4.1～8.4.4 的要求得出。

8.5.2 功能安全概念验证报告，由 8.4.5 的要求得出。

附 录 A
（资料性附录）
概念阶段概览

表 A.1 提供了概念阶段的目的、前提条件和工作成果的概览。

表 A.1 概念阶段概览

章	目的	前提条件	工作成果
5 相关项定义	第一个目的是定义并描述相关项，及其与环境和其他相关项的依赖性和相互影响。 第二个目的是为充分理解相关项提供支持，以便执行后续阶段的活动	无	5.5 相关项定义
6 安全生命周期启动	安全生命周期启动的第一个目的是对新的相关项开发和现有相关项的修改进行区分（参见 GB/T 34590.2—2017 图 2）。 安全生命周期启动的第二个目的在对现有相关项的修改的情况下定义将要实施的安全生命周期活动（参见 GB/T 34590.2—2017 图 2）	相关项定义	6.5.1 影响分析； 6.5.2 安全计划（细化的）
7 危害分析和风险评估	危害分析和风险评估的目的是识别相关项中因故障而引起的危害并对危害进行归类，制定防止危害事件发生或减轻危害程度的安全目标，以避免不合理的风险	相关项定义	7.5.1 危害分析和风险评估； 7.5.2 安全目标； 7.5.3 危害分析和风险评估以及安全目标的验证评审报告
8 功能安全概念	功能安全概念的目的是从安全目标中得出功能安全要求，并将其分配给相关项的初步架构要素或外部措施	相关项定义； 危害分析和风险评估； 安全目标	8.5.1 功能安全概念； 8.5.2 功能安全概念验证报告

附 录 B
（资料性附录）
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危害事件发生频率(f),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——可控性(C),以及所产生的伤害或损坏的潜在严重度(S)的函数(F):

$$R = F(f, C, S)$$

发生频率 f 依次受到几个因素的影响。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—2017 中,它被简化成危害事件可能发生的驾驶场景的概率的度量(暴露概率 E)。另一个因素是相关项可能导致危害事件的失效率(失效率 λ)。失效率是通过存留在系统中导致危害的随机硬件失效和系统故障来表征:

$$f = E \times \lambda$$

危害分析和风险评估与相关项的设定要求相关联,以避免不合理的风险。

由危害分析和风险评估得出的 ASIL 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 7.4.2):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、及其功能和界限的清晰定义。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详细设计。

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、城市驾驶、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;

——操作系统之间的相互作用。

b) 危害事件的分类(参见 7.4.3):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) ASIL 等级确定(参见 7.4.4):确定所需的汽车安全完整性等级。

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，也可以使用其他分类方法，例如 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[2]，[4]，[5])。

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，见参考文献[2])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：无人员伤亡；

——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 min 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 h 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 h 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

严重程度等级 (见表 1)	S0	S1	S2	S3
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%

表 B.1（续）

严重程度等级（见表 1）	S0	S1	S2	S3
示例	——冲撞路边设施； ——撞倒路边邮筒、围栏等； ——轻微碰撞； ——轻微刮痕损害； ——在进入或退出停车位置时损害； ——没有碰撞或者侧翻的情景下离开道路	——侧面碰撞一个狭窄的静止物体，例如以非常低的速度撞上一棵树（影响到乘员舱）； ——以非常低的速度侧面碰撞轿车（例如侵入乘客舱）； ——以非常低的速度和其他轿车后碰/正碰； ——最小重叠（10%～20%）的碰撞； ——正面碰撞（例如追尾其他车辆、半挂车）没有乘员舱变形	——侧面碰撞一个狭窄的静止物体，例如以低速撞上一棵树（影响到乘员舱）； ——低速侧面碰撞轿车（例如侵入乘客舱）； ——以低速和其他轿车后碰/正碰； ——由于转弯造成的行人或自行车事故（城市路口和街道）	——侧面碰撞一个狭窄的静止物体，例如以中速撞上一棵树（影响到乘员舱）； ——中速侧面碰撞轿车（例如侵入乘客舱）； ——以中速和其他轿车后碰/正碰； ——行人/自行车事故（例如两车道）； ——正面碰撞乘员舱变形（例如追尾其他车辆、半挂车）

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和运行场景。

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）。

首先，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，如

——车辆与另一辆装载危险材料的车的事故

注：这不适用于设计目的本身就是装载危险材料的车；

——车辆涉及到与在高速公路上降落的飞机的事故。

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 7.4.3.4）。

如果暴露按照场景的持续时间分级，暴露概率可以根据时间（所考虑的场景）与总的运行时间（上电）的比值来预估。在特殊情况下，总的运行时间可以是汽车生命周期（包括下电）。表 B.2 给出了持续型工况分级和典型的暴露概率级别的例子。

注 2：一个危害可以与一个给定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场景的频率相关（如车辆重复通过交通路口的频率）。

此外，一些暴露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。在这些情况下，场景发生后的很短的时间间隔内，已存在的系统故障会导致危害事件的发生。表 B.3 给出了驾驶场景和典型的暴露概率级别的例子。

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 和表 B.3 的例子可能无法得出相同的暴露等级，所以最合适的暴露等级是根据对所考虑的驾驶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，则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 3：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（参见 7.4.1.2）。

表 B.2　基于运行场景持续时间的暴露概率分级

运行场景暴露概率分级（见表 2）		E1	E2	E3	E4
持续时间（平均运行时间的百分比）		无定义	<1%平均运行时间	1%～10%平均运行时间	>10%平均运行时间
示例	道路类型	—	——山路，带有不安全的陡峭的斜坡； ——乡间道路的交叉口； ——高速公路的入口匝道； ——高速公路的出口匝道	——单行道（城市街道）	——高速公路； ——二级公路； ——乡间道路
	路面	—	——冰雪路面； ——有很多光滑树叶的路面	——湿滑路面	—
	附近的物体	——在行驶道路（高速公路）上被遗弃的货物或障碍物	——在洗车房； ——靠近拥堵的末端（高速公路）	——在隧道中； ——交通堵塞	—
	车辆静止状态	——车辆处于跨接线启动； ——在修理厂（转动台）	——连接挂车； ——装备车顶行李架； ——车辆正在加油； ——在修理厂（诊断或维修过程中）； ——在升降机上	——车辆在斜坡上（停在坡上）	—
	驾驶操控	——下坡时关闭发动机（山路）	——倒车（从停车位）； ——倒车（城市街道）； ——超车； ——停车（在车中有睡着的人）； ——停车（有挂车连接）	——交通繁忙（频繁起停）	——加速； ——减速； ——转弯（转向）； ——停车（停车场）； ——变换车道（城市街道）； ——停在交通灯前（城市街道）； ——变换车道（高速公路）
	能见度	—	—	晚上没有路灯的道路	—

表 B.3　基于运行场景频率的暴露概率分级

运行场景暴露概率分级(见表 2)		E1	E2	E3	E4
场景频率		对于绝大多数驾驶员小于一年发生一次	对于绝大多数驾驶员一年发生几次	对于一般的驾驶员一个月发生一次或多次	平均几乎发生在每次驾驶中
示例	道路类型	—	——山路,带有不安全的陡峭斜坡	—	—
	路面	—	——冰雪路面	——湿滑路面	—
	附近的物体	—	—	——在隧道中; ——在洗车房; ——交通堵塞	—
	车辆静止状态	——停止,需要重新启动发动机(在铁路道口); ——车辆在被拖的过程中; ——车辆在泵电启动中	——连接挂车; ——装备车顶行李架	——车辆正在加油; ——车辆在斜坡上(停在坡上)	—
	驾驶操控	—	——驾车闪躲,偏离预期的路线	——超车	——从静止开始启动; ——换挡; ——加速; ——制动; ——转弯(转向); ——使用指示器; ——操控车辆进入停车位置; ——倒车

B.4　可控性示例(避免伤害)

确定一个给定危害的可控性等级,需要预估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。

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(这可能与目标市场、个体年龄、手眼配合、驾驶经验、文化背景等有关)。

注:可控性预估可能受到很多因素的影响,包括分析人员的文化背景、车辆的目标市场或该目标市场的驾驶员概况。

为了有助于这些评估,表 B.4 提供了一些驾驶场景的示例,这些示例给出了故障发生后,对应的能够避免伤害的控制行为的假设。这些场景对应到可控性的分级,明确了用于判断参与者控制能力水平 90%和 99%的分隔点。

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

驾驶因素和场景		可控性等级(见表 3)			
		C0	C1	C2	C3
		常规可控	99%或者更多的驾驶员或者交通参与者通常能够避免危害	90%或者更多的驾驶员或交通参与者通常能够避免危害	少于 90%的驾驶员或者交通参与者通常能够或者勉强能够避免伤害
示例	精神注意力不集中的情况	保持既定行驶路线	—	—	—
	非预期的收音机音量增大	保持既定行驶路线	—	—	—
	报警信息-油不够	保持既定行驶路线	—	—	—
	驾驶员辅助系统失效	保持既定行驶路线	—	—	—
	驾驶过程中座椅位置错误调整	—	制动减速/停止车辆	—	—
	车辆启动时转向柱锁止	—	制动减速/停止车辆	—	—
	紧急制动情况下 ABS 失效	—	—	保持既定行驶路线	—
	夜晚无照明道路上中高速行驶中大灯失效	—	—	靠边或停车	—
	高侧向加速度时发动机失效(高速路出口)	—	—	保持既定行驶路线	—
	在低附路面上制动并转向时 ABS 失效	—	—	—	保持既定行驶路线，留在车道里面
	制动失效	—	—	—	制动减速/停止车辆
	车辆中速或高速行驶中，高角速度的不正确转向角(转向角的变化不符合驾驶员的预期)	—	—	—	保持既定行驶路线，留在车道里面
	高速行驶中驾驶员安全气囊误触发	—	—	—	保持既定行驶路线，留在车道里面；制动减速/停车

注 1：对于 C2，一个符合 RESPONSE 3(见参考文献[3])的合理的测试场景是足够的："实际的测试经验表明，每个场景 20 个有效的数据包能提供基本的有效性说明"。如果这 20 个数据包中的每一个都符合测试的通过标准，能够证明 85%的可控性水平(达到一个通常能被人为因素测试接受的 95%的置信度)。这为 C2 预估的合理性提供了适当的证据。

注 2：对于 C1，通过一个测试去提供一个 99%的驾驶员都能够在特定的驾驶环境下"通过"这个测试的理由是不可行的，因为必须要有大量的测试项目作为这个理由的适当的证据。

注 3：由于 C3 等级假定为没有可控性，所以对于这个分类理由不需要提供相关的适当证据。

参 考 文 献

[1] GB/T 20438—2006(所有部分) 电气/电子/可编程电子安全相关系统的功能安全

[2] Abbreviated injury scale; Association of the advancement of Automotive medicine; Barrington, IL, USA Information is also available at www.carcrash.org or http://www.unfallforensik.de/.

[3] Code of Practice for the design and evaluation of ADAS, EU Project RESPONSE 3: Oct. 2006.

[4] 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.

[5] 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.

中 华 人 民 共 和 国
国 家 标 准
道路车辆 功能安全
第 3 部分:概念阶段
GB/T 34590.3—2017
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2017 年 10 月第一版
*
书号:155066·1-57766

GB/T 34590-2017