ICS 43.040
CCS T 35

中华人民共和国国家标准

GB/T 34590.1—XXXX
代替 GB/T 34590.1-2017

道路车辆 功能安全
第1部分：术语

Road vehicles—Functional safety—Part1:Vocabulary

(ISO 26262-1:2018，MOD)

（征求意见稿）

（本草案完成时间：2021年4月1日）

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。

本部分为GB/T 34590-XXXX的第1部分。

本文件代替GB/T 34590.1-2017《道路车辆 功能安全 第1部分:术语》,与GB/T 34590.1-2017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”修改为“除轻便摩托车外的量产道路车辆”，并修改了范围的描述；

——新增第 2 章“规范性引用文件”；

——修改了 3.1 架构、3.3 ASIL 等级分解、3.4 评估、3.5 审核、3.6 汽车安全完整性等级、3.7 可用性、3.10 基线、3.13 分支覆盖率、3.15 标定数据、3.17 级联失效、3.18 共因失效、3.21 组件、 3.22 配置数据、 3.24 认可评审、3.28 降级 degradation、3.29 相关失效、3.31 可探测的故障、 3.32 开发接口协议、3.33 诊断覆盖率、3.35 诊断测试时间间隔、3.36 分布式开发、3.37 多样性、3.38 双点失效、3.40 电气/电子系统、3.41 要素、3.42 嵌入式软件、3.43 紧急运行、 3.44 紧急运行时间间隔、3.46 错误、3.48 暴露、 3.50 失效、 3.51 失效模式、3.54 故障、3.58 故障模型、3.59 故障响应时间间隔、3.61 故障容错时间间隔、3.63 形式记法、3.64 形式验证、3.68 功能安全概念、3.69 功能安全要求、3.70 硬件架构度量、3.71 硬件元器件、3.78 独立性、3.79 非相关失效、3.80 非形式记法、3.82 检查、3.83 预期功能、3.84 相关项、3.85 潜伏故障、3.90 基于模型的开发、3.91 修改、3.96 多点失效、3.97 多点故障、3.99 新开发、3.100 非功能性危害、3.102 运行模式、3.103 运行时间、3.104 运行场景、3.105 其他技术、3.108 可感知故障、3.109 永久性故障、3.110 阶段、3.115 在用证明、3.118 随机硬件失效、3.120 合理预见的、3.122 冗余、3.125 残余故障、3.127 评审、3.131 安全状态、3.133 安全活动、3.136 安全档案、3.137 安全文化、3.139 安全目标、 3.140 安全经理、3.141 安全措施、 3.142 安全机制、3.145 安全相关功能、3.147 安全相关的特殊特性、3.148 安全确认、3.154 严重度、3.155 单点失效、3.156 单点故障、3.161 子阶段、3.163 系统、 3.167 技术安全概念、3.169 测试、3.180 验证、3.181 验证评审、3.182 走查、3.183 报警和降级策略、3.184 值得信赖的、3.185 工作成果等 92 个术语的定义。

——新增了 3.2 ASIL 等级能力、3.8 基础失效率、3.9 基础车辆、3.11 商用车制造商、3.12 车辆上装设备、3.14 客车、3.19 共模失效、3.20 完整车辆、3.26 耦合系数、3.30 相关失效引发源、3.34 诊断点、3.45 紧急运行容错时间间隔、3.47 专业摩托车驾驶员、3.52 失效模式覆盖率、3.55 故障探测时间间隔、3.56 故障处理时间间隔、3.57 故障注入、3.60 故障容错、3.72 硬件基础子元器件、3.73 硬件子元器件、3.87 管理体系、3.89 最长待修复时间间隔、3.92 修改条件/判定覆盖率、3.93 摩托车、3.94 摩托车安全完整性等级、3.95 多核、3.101 观测点、3.111 失效物理学、 3.112 动力输出装置、 3.113 处理要素、3.114 可编程逻辑器件、3.117 质量管理、3.119 随机硬件故障、3.121 重建、3.124 再制造、3.134 安全异常、3.138 独立于环境的安全要素、3.146 安全相关事件、3.151 半挂车、3.152 量产道路车辆、3.162 供应协议、3.166 目标环境、3.170 牵引车、3.171 挂车、3.172 转换器、3.174 卡车、3.175 T&B 车辆配置、3.177 T&B 车辆使用的变化、3.178 整车功能、3.179 车辆运行状态等 50 个术语和定义；

——删除了 GB/T 34590.1-2017 中的 2.1 分配、2.2 异常、2.60 同构冗余、 2.66 初始 ASIL 等级、2.70 相关项开发、2.126 特殊用途车辆等 6 个术语和定义。

——修改缩略语 3 个，新增缩略语 60 个，删除缩略语 6 个。

本部分修改采用ISO 26262-1：2018 《道路车辆 功能安全 第1部分：术语》。

本部分与ISO 26262-1：2018的技术性差异及其原因如下：

——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-XXXX（所有部分）代替 ISO 26262：2018（所有部分）；

——3.14 客车 passenger car，修改原文中的定义内容，与 GB/T 3730.1-2001《汽车和挂车类型的术语和定义》中的定义保持一致；

——3.93 摩托车 motorcycle，修改原文中的定义内容，与 GB/T 5359.1-2019《摩托车和轻便摩托车术语》中的定义保持一致；

——3.107 乘用车 passenger car，修改原文中的定义内容，与 GB/T 3730.1-2001《汽车和挂车类型的术语和定义》中的定义保持一致。

——新增术语 3.186 预期功能安全 safety of the intended functionality;SOTIF 及其定义。

——新增术语 3.187 接受准则 acceptance criteria 及其定义；

——新增术语 3.188 安全度量 safety metric 及其定义；

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：

本文件所代替文件的历次版本发布情况为：

——GB/T 34590.1,2017 年首次发布。

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。

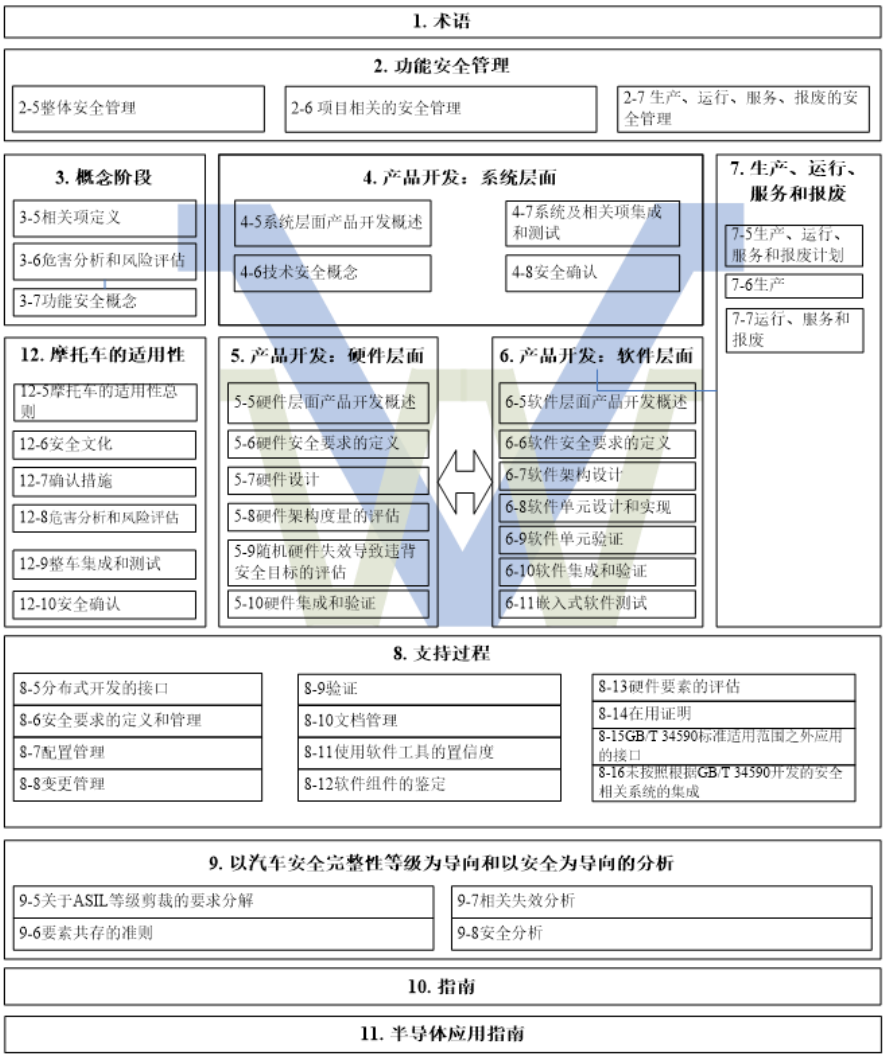

图1　GB/T 34590-XXXX 概览

道路车辆 功能安全
第1部分：术语

1 范围

GB/T 34590的本部分规定了本文件所有部分所应用的术语和定义，以及缩略语。

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。

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-XXXX（所有部分） 道路车辆 功能安全（ISO 26262:2018，MOD）

3 术语和定义

下列术语和定义适用于本文件。

3.1

架构 architecture

相关项(3.84)或**要素**(3.41)的结构的表征，用于识别结构模块及其边界和接口，并包括将要求分配给结构模块。

3.2

ASIL等级能力 ASIL capability

相关项(3.84)或**要素**(3.41)满足假定的、被分配了给定**ASIL**（3.6）等级的**安全**（3.132）要求的能力。

注：作为硬件安全要求的一部分，如果需要，还包括实现分配给**要素**（3.41）的相应随机硬件故障度量目标值（见GB/T 34590.5-XXXX，第8章和第9章）。

3.3

ASIL 等级分解 ASIL decomposition

为有助于实现同一**安全目标**(3.139)，将冗余的**安全**(3.132)要求分配给具有充分**独立性**(3.78)的**要素**(3.41)，以降低分配给相关**要素**(3.41)的冗余的**安全**(3.132)要求的**ASIL**(3.6)等级。

注1：ASIL等级分解是设计过程中**ASIL**(3.6)等级剪裁方法的基础(GB/T 34590.9中定义为关于**ASIL**(3.6)等级剪裁的要求分解)。

注2：根据GB/T 34590.9，ASIL等级分解不适用于随机硬件失效要求。

注3：冗余安全(3.132)要求的**ASIL**(3.6)等级降低也存在一些例外，如，**认可措施**(3.23)保持与**安全目标**(3.139)相同的等级。

3.4

评估 assessment

对**相关项**(3.84)或**要素**(3.41)的特性是否实现GB/T 34590目标的检查。

3.5

审核 audit

针对过程目标对已实施过程的检查。

3.6

汽车安全完整性等级 Automotive Safety Integrity Level；ASIL

四个等级中的一个等级，用于定义**相关项**(3.84)或**要素**(3.41)需要满足的GB/T 34590中的要求和**安全措施**(3.141)，以避免不合理的**风险**(3.176)，其中，D代表最高严格等级，A代表最低严格等级。

注：QM(3.117)不是一个ASIL等级。

3.7

可用性 availability

在定义的生命周期内，产品在给定条件下按照要求提供规定功能的能力。

3.8

基础失效率 base failure rate；BFR

在给定用例中作为**安全**（3.132）分析输入的硬件**要素**（3.41）**失效率**（3.53）。

3.9

基础车辆 base vehicle

在安装**车辆上装设备**（3.12）之前，原始设备制造商（OEM）的**T&B车辆配置**（3.175）。

注：车辆上装设备（3.12）可安装在包括所有驾驶相关**系统**（3.163）（发动机、传动系、底盘、转向、制动、驾驶室和驾驶员信息）的基础车辆上。

示例：带有动力系统和驾驶室的**卡车**（3.174）底盘、带动力系统的滚动底盘。

3.10

基线 baseline

已批准的可作为变更基础的一组单一或多个**工作成果**（3.185）、**相关项**（3.84）或**要素**（3.41）的版本。

注1：见GB/T 34590.8，第8章。

注2：基线通常置于配置管理之下。

注3：在**生命周期**（3.86）中，通过变更管理流程，基线被用作进一步开发的基础 。

3.11

车辆上装制造商 body builder；BB

将**卡车**（3.174）、**客车**（3.14）、**挂车**（3.171）和**半挂车**（3.151）（T&B）的车身、 货运工具或设备增加到**基础车辆**（3.9）上的组织。

注1：T&B车身包括**卡车**（3.174）驾驶室、**客车**（3.14）车身、步入式车厢等。

注2：货运工具包括货箱、平板床、汽车运输架等。

注3：设备包括作业设备和机械，如水泥搅拌机、倾卸床、雪铲、升降机等。

3.12

车辆上装设备 body builder equipment

安装在T&B**基础车辆**（3.9）上的机械、车身或货运工具。

3.13

分支覆盖率 branch coverage

在测试中，已执行计算机程序的控制流分支所占的比率。

注1：100%分支覆盖率意味着100%**语句覆盖率**(3.160)。

注2：一个if语句总有两个分支，即条件为true和条件为false，不依赖于else语句是否存在。

3.14

客车 bus

在设计和技术特性上用于载运乘客及其随身行李的商用车辆,包括驾驶员座位在内座位数超过9座。客车有单层的或双层的，也可牵引一**挂车**（3.171）。

[来源：GB/T 3730.1—2001，2.1.2.1]

3.15

标定数据 calibration data

在开发过程中，软件构建后将用作软件参数值的数据。

示例：参数（例如，低怠速值、发动机万有特性图）、车辆特定参数（适应值，例如，节气门限位）、变量编码（例如，国家代码、左舵/右舵）。

注：标定数据不包含可执行代码或注释代码。

3.16

候选项 candidate

与已经发布并在运行的**相关项**(3.84)或**要素**（3.41）的定义和使用条件相同、或具有高度通用性的**相关项**(3.84)或**要素**（3.41）。

注：该定义适用于**在用证明**（3.115）中使用的候选项。

3.17

级联失效 cascading failure

由一个根本原因（来自**要素**（3.41）内部或外部）导致某个**相关项**（3.84）的**要素**（3.41）的**失效**（3.50），进而引起相同或不同**相关项**(3.84)的另一个**要素**(3.41)或多个**要素**(3.41)的**失效**(3.50)。

注：级联失效是**相关失效**（3.29），其可能是导致**共因失效**（3.18）的根本原因之一。见图2。

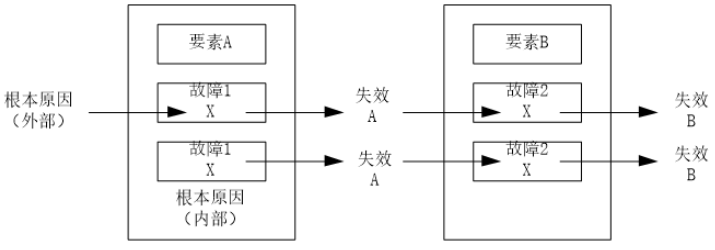

图2　级联失效

3.18

共因失效 common cause failure；CCF

由单一特定事件或根本原因直接导致一个**相关项**(3.84)中两个或多个**要素**(3.41)的**失效**(3.50)，该事件或根本原因可来自所有这些**要素**(3.41)的内部或外部。

注：共因失效是**非级联失效**（3.17）的**相关失效**（3.29），见图3。

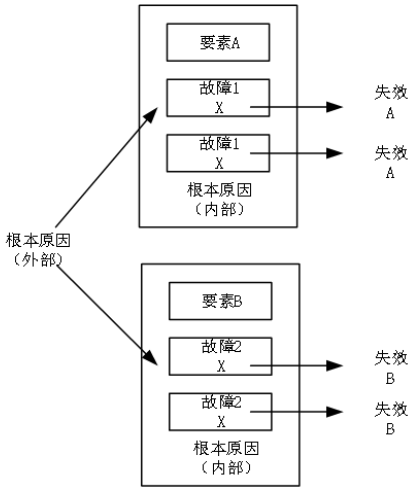

图3　共因失效

3.19

共模失效 common mode failure；CMF

多个**要素**(3.41)以相同方式失效的一种**共因失效**（3.18）。

注：以相同方式**失效**(3.50)并不意味着这些失效必须是完全一样的。**失效模式** (3.51)接近到什么程度才能归为共模失效，需要根据实际情况而定。

示例1：某**系统**(3.163)具有两个互为比较的温度传感器。如果两个温度传感器之间的温差大于或等于 5℃时，将其作为**故障**（3.54）处理，**系统**(3.163)进入**安全状态**（3.131）。某个共模失效使得两个温度传感器以两者之间温差小于5℃的形式失效，从而无法探测到。

示例2：在 CPU 锁步**架构**（3.1）中，两个 CPU 的输出将会进行周期性的比较，两个 CPU 需要以完全相同的方式失效才会导致**失效**（3.50）不被探测到。在这种情况下，共模失效使两个 CPU 以完全相同方式失效。

示例3：由于多个元器件不符合其过电压规范而导致的过压**失效**（3.50）是一种共模失效。

3.20

完整车辆 complete vehicle

完全组装的具有**车辆上装设备**（3.12）的**T&B基础车辆**（3.9）。

示例：垃圾收集车、**自卸卡车**（3.174）。

3.21

组件 component

由一个以上**硬件元器件**(3.71)或一个到多个**软件单元**(3.159)组成的逻辑上或技术上可分的非系统层面的**要素**(3.41)。

示例：微控制器。

注：组件是**系统**(3.163)的一部分。

3.22

配置数据 configuration data

在要素构建过程中分配的且控制要素构建过程的数据。

示例1：预处理器变量设置，用于从源代码导出出编译时间变量。

示例2：用于控制构建工具或工具链的 XML 文件。

注1：配置数据控制软件构建。配置数据用于从代码库已经定义的现有代码变量中选择代码；被选取代码变量的功能将包含在执行代码中。

注2：由于配置数据仅仅用于选择代码变量，因此配置数据不包含**相关项**（3.84）使用时的执行代码和注释代码。

3.23

认可措施 confirmation measure

与**功能安全**(3.67)相关的**认可评审**(3.24)、**审核**(3.5)或**评估**(3.4)。

3.24

认可评审 confirmation review

确认**工作成果**（3.185）能够提供充分且具有说服力的证据，证明其促成了考虑GB/T 34590相关目的和要求的**功能安全**（3.67）的实现。

注1：GB/T 34590.2提供了一份完整的认可评审清单。

注2：认可评审的目的是确保符合GB/T 34590。

3.25

可控性 controllability

通过所涉及人员的及时反应（可能具备**外部措施**(3.49)的支持）避免特定的**伤害**(3.74)或者损伤的能力。

注1：所涉及人员可包括驾驶员、乘客或车辆外部的邻近人员。

注2：危害分析和风险评估(3.76)中的参数C表示可控性的可能性。

3.26

耦合系数 coupling factors

多个**要素**（3.41）间的共同特征或关系，这种共同特征或关系会导致这些要素**失效**（3.50）的相关性。

3.27

专用措施 dedicated measure

在评估违背**安全目标**(3.139)的可能性的过程中，用于确保所声明的**失效率**(3.53)的措施。

示例：设计特性，诸如**硬件元器件**(3.71)过设计（例如，电应力或热应力分级）或者物理分隔（例如，印刷电路板上的触点间隔）；对来料进行专门的抽样测试，以降低与违背**安全目标**(3.139)有关的**失效模式**(3.51)的发生**风险**(3.128)；老化测试；专用的控制计划。

3.28

降级 degradation

相关项（3.84）或**要素**（3.41）的功能缩减、性能降低或两者均有的状态，或向该状态的过渡。

3.29

相关失效 dependent failures

不具有统计独立性的**失效**(3.50)，即**失效**(3.50)组合发生的概率不等于所有考虑的独立**失效**(3.50)发生概率的乘积。

注1：相关失效可以同时或在足够短的时间间隔内发生，从而产生同时**失效**（3.50）的影响。

注2：相关失效包括**共因失效**(3.18)和**级联失效**(3.17)。

注3：给定的**失效**（3.50）是**级联失效**（3.17）还是**共因失效**（3.18），可取决于**要素**（3.41）的层次结构。

注4：给定的**失效**（3.50）是**级联失效**（3.17）还是**共因失效**（3.18），可取决于**要素**（3.41）的时序行为。

注5：相关失效可包括**软件失效**（3.50），即使其**失效**（3.50）概率不被计算。

3.30

相关失效引发源 dependent failure initiator；DFI

通过**耦合系数**（3.26），导致多个**要素**（3.41）失效的单一根本原因。

注1：在DFA过程中，识别出作为相关性候选项的**耦合系数**（3.26）。

注2：**要素**（3.41）的**失效**（3.50）可以同时或有序发生。

示例1：**耦合系数**(3.26)：使用同一 RAM 的两个软件单元。根本原因：一个软件单元非预期地损坏了第二个软件单元使用的数据。

示例2：**耦合系数**(3.26)：在车辆同一舱室内工作的两个 ECU。根本原因：不需要的/不期望的水侵入该特定的舱室内，导致浸泡并引发两个 ECU 的**失效**（3.50）。

示例3：**耦合系数**(3.26)：使用同一 3.3V 电源的两个微控制器。根本原因：3.3V 电源的过压，损坏了两个微控制器。

3.31

可探测的故障 detected fault

在规定时间内通过**安全机制**（3.142）可以探测到的**故障**（3.54）。

注：规定的时间可以是**故障探测时间间隔**（3.55）或**多点故障探测时间间隔**（3.98）。

3.32

开发接口协议 development interface agreement；DIA

客户与供应商之间的协议，该协议规定了与**相关项**（3.84）或**要素**（3.41）开发相关的各方在待开展的活动、待评审的证据或待交换的**工作成果**（3.185）方面所承担的责任。

注：DIA适用于开发阶段，而**供应协议**（3.162）适用于生产阶段。

3.33

诊断覆盖率 diagnostic coverage；DC

由实施的**安全机制**(3.142)探测或控制的失效率占硬件**要素**(3.41)**失效率**(3.53)或硬件**要素**(3.41)某一**失效模式**(3.51)**失效率**(3.53)的百分比。

注1：诊断覆盖率可通过在硬件**要素**（3.41）中可能发生的**残余故障**(3.125)或潜伏的**多点故障**(3.97)进行评估。

注2：可考虑在**架构**（3.1）中不同层级实施的**安全机制**（3.142）。

注3：除非明确提及，否则在确定**安全机制**（3.142）的诊断覆盖率时，不会考虑安全相关硬件**要素**（3.41）的**安全故障**（3.130）的比例。

3.34

诊断点 diagnostic points

要素（3.41）的输出信号，用来观察**故障**（3.54）的探测或校正。

注：诊断点也称为“警报”或“**错误**（3.46）标志”或“校正标志”。

示例：回读信息。

3.35

诊断测试时间间隔 diagnostic test time interval

安全机制(3.142)执行在线诊断测试之间的时间间隔，包括在线诊断测试的执行时间。

注：见图5。

3.36

分布式开发 distributed development

在某个**相关项**(3.84)或**要素**(3.41)开发中，分配客户和供应商在整个**相关项**(3.84)或**要素**(3.41)的开发责任。

注：客户和供应商是合作方中的角色。

3.37

多样性 diversity

以实现**独立性**(3.78)为目标，满足相同要求的不同解决方案。

注1：多样性不保证独立性，但是可避免某些类型的**共因失效**（3.18）。

注2：多样性可以是应用的技术解决方案 （例如：多样的**硬件组件** (3.21)，多样的**软件组件**(3.21) ）或技术手段（例如：多样的编译器）。

注3：多样性是实现**冗余**（3.122）的一种方式。

示例：多样的程序；多样的硬件。

3.38

双点失效 dual-point failure

由两个独立硬件**故障**(3.54)的组合引起，且直接导致违背**安全目标**(3.139)的**失效**(3.50)。

注1：双点失效是2阶的**多点失效**(3.96)。

注2：GB/T 34590中提到的双点失效包括这些失效，即：有一个故障影响到安全相关**要素**(3.144)，而另一个故障影响到相应的用来达到或保持**安全状态**(3.131)的**安全机制**(3.142)而导致的失效。

3.39

双点故障 dual-point fault

与另一个非相关**故障**(3.54)组合而导致**双点失效**（3.38）的一个**故障**(3.54)。

注1：一个双点故障只有在一个双点失效明确后才能被识别，例如，通过故障树的割集分析。

注2：见**多点故障**(3.97)。

3.40

电气/电子系统 electrical and/or electronic system ; E/E

由电气和/或电子**要素**（3.41），包括可编程电子要素所构成的**系统**（3.163）

注：电气/电子系统的一个**要素**(3.41)可能是另一个电气/电子系统。

示例：电源、传感器或其他输入设备、通讯路径、执行器或其他输出设备。

3.41

要素 element

系统（3.163）、**组件**（3.21）(硬件或软件)、**硬件元器件**（3.71）或**软件单元**（3.159）。

注1：当使用“软件要素”或“硬件要素”时，分别表示仅是软件的要素或仅是硬件的要素。

注2：要素也可以是一个**独立于环境的安全要素**(3.138)。

3.42

嵌入式软件 embedded software

在一个**处理要素**（3.113）上运行的充分集成的软件。

3.43

紧急运行 emergency operation

相关项（3.84）的一种**运行模式**（3.102），用于对**故障**（3.54）作出反应后提供**安全**（3.132），直到过渡到**安全状态**（3.131）。

注1：见图4和图5。

注2：在探测到**故障**（3.54）后，如果不能直接或及时地进入**安全状态**（3.131），又或**安全状态**（3.131）不能被保持时，**安全机制**（3.142）可以将**相关项**（3.84）过渡到紧急运行模式以提供**安全**（3.132），直到过渡并保持在**安全状态**（3.131）。

注3：报警和降级策略（3.183）中描述了紧急运行和相关**紧急运行容错时间间隔**（3.45）。

注4：降级（3.28）可以是紧急运行概念的一部分。

示例：紧急运行可以被定义为故障容错**相关项**（3.84）的**错误**（3.46）响应的一部分。

3.44

紧急运行时间间隔 emergency operation time interval；EOTI

保持**紧急运行**（3.43）的时间间隔。

注1：见图4和图5。

注2：报警和降级策略（3.183）中描述了紧急运行和相关**紧急运行容错时间间隔**（3.45）。

注3：暂时保持**紧急运行**（3.43）以提供**安全**（3.132），直到过渡到**安全状态**（3.131）。

3.45

紧急运行容错时间间隔 emergency operation tolerance time interval；EOTTI

在无不合理**风险**（3.128）的情况下，能够维持**紧急运行**（3.43）的特定时间间隔。

注1：见图4。

注2：紧急运行容错时间间隔是**紧急运行时间间隔**（3.44）的最大值。

注3：基于紧急运行容错时间间隔中规定的有限运行时间，**紧急运行**（3.43）能被认为是安全的。

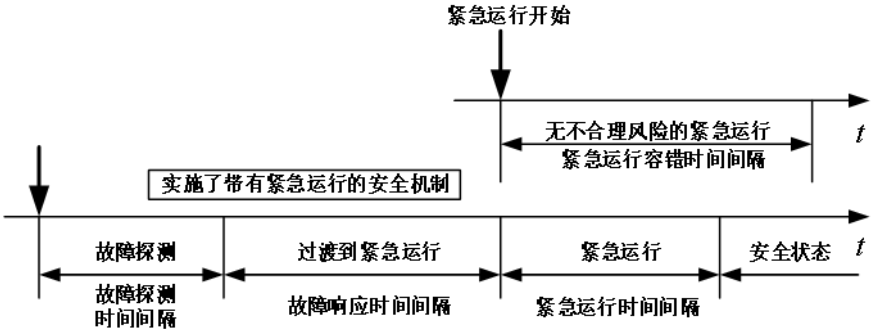

图4　紧急运行容错时间间隔

3.46

错误 error

计算的、观测的、测量的值或条件与真实的、规定的、理论上正确的值或条件之间的差异。

注：错误可由所考虑的**系统**（3.163）或**组件**（3.21）内的**故障**（3.54）引起。

3.47

专业摩托车驾驶员 expert rider

由能够根据对实际**摩托车**（3.93）的操作评估**可控性**（3.25）分级的人员担任的角色。

注1：专业摩托车驾驶员要求具备：

——评估可控性的**技能**（3.25），包括评估的知识；

——实施摩托车试验的能力；及

——基于具有代表性的摩托车驾驶员的驾驶能力来评估**摩托车**（3.93）**可控性**（3.25）特性的知识。

注2：有关使用专业摩托车驾驶员的信息，见GB/T 34590.12-XXXX，附录C。

3.48

暴露　exposure

处于某**运行场景**(3.104)的状态，在该运行情况下，如果发生所分析的**失效模式**(3.51)，可能导致危害。

注：危害分析和风险评估（3.76）中的参数E代表**运行场景**(3.104)的潜在暴露度。

3.49

外部措施　external measure

独立于且不同于**相关项**（3.84）的措施，以降低或减轻由**相关项**（3.84）导致的**风险**（3.128）。

3.50

失效 failure

由于**故障**（3.54）出现导致**要素**（3.41）或**相关项**（3.84）预期行为的终止。

注：终止可能是永久或暂时的。

3.51

失效模式 failure mode

要素（3.41）或**相关项**（3.84）未能提供预期行为的方式。

3.52

失效模式覆盖率 failure mode coverage；FMC

硬件要素（3.41）某一**失效模式**（3.51）的**失效率**（3.53）中被实施的安全机制探测或控制的比例。

3.53

失效率 failure rate

硬件**要素**（3.41）的**失效**（3.50）概率密度除以幸存概率（可靠度）。

注：失效率被假设为常数且通常用“λ”表示。

3.54

故障 fault

能够引起**要素**(3.41)或**相关项**(3.84)失效的异常情况。

注1：考虑永久性故障、间歇性故障和**瞬态故障**(3.173)（尤其是软错误）。

注2：当子系统处于**错误**（3.46）状态时，可能导致**系统**（3.163）发生故障。

注3：间歇性故障时而发生，然后又消失。这种故障可能发生在一个**组件**(3.21)濒临损坏时，或者例如开关内部功能异常导致其发生。某些**系统性故障**(3.165)（例如时序紊乱）也可能导致间歇性故障。

3.55

故障探测时间间隔 fault detection time interval；FDTI

从**故障**(3.54)发生到被探测到的时间间隔。

注1：见图5。

注2：故障探测时间间隔的确定独立于**诊断测试时间间隔**(3.35)。

示例：由于使用了**错误**(3.46)计数器的原因（即：**故障**(3.54)必须被该诊断测试探测到多于一次，才会触发**错误**(3.46)响应），某一诊断测试的故障探测时间间隔可能会长于**诊断测试时间间隔**(3.35)。

注3：故障探测时间间隔、**诊断测试时间间隔**(3.35)和**故障响应时间间隔**(3.59)是基于**故障**(3.54)探测的**安全机制**(3.142)的相关特性。

注4：如果故障探测时间间隔加上**故障响应时间间隔**(3.59)短于相应的**故障容错时间间隔**(3.61)，则该**故障**(3.54)可以被相应的**安全机制**(3.142)及时处理。

3.56

故障处理时间间隔 fault handling time interval；FHTI

故障探测时间间隔(3.55)和**故障响应时间间隔**(3.59)的总和。

注1：FHTI是**安全机制**(3.142)的一种属性。

注2：见图5。

3.57

故障注入 fault injection

评估**要素**(3.41)内**故障**(3.54)影响的方法，该方法通过注入**故障**(3.54)、**错误**(3.46)、或**失效**(3.50)从而通过**观测点**(3.101)对注入后的响应进行观测。

注：故障注入可以在不同的抽象层面进行，包括**相关项**(3.84)层面或**要素**(3.41)层面，这取决于范围、可行性、可

观测性和所需细节的层面。取决于目的，可以在安全生命周期的不同阶段，考虑不同的**故障模型**(3.58)，进行故障注入。

示例1：在运行期间注入**故障**(3.54)，以验证作为探测**潜伏故障**(3.85)策略一部分的某个**安全机制**(3.142)正在正常工作。

示例2：在进行集成测试时，通过硬件调试端口或专用软件命令注入**故障**(3.54)来测试软硬件接口(HSI)。

示例3：在硬件组件层面对卡滞**故障**(3.54)或瞬态故障进行仿真，以验证**安全机制**(3.142)的**诊断覆盖率**(3.33)，或识别出可引起**错误**(3.46)或**失效**(3.50)的**故障**(3.54)。

3.58

故障模型 fault model

由**故障**(3.54)导致的**失效模式**(3.51)的表现。

注：故障模型用于评估特定**故障**(3.54)的后果。

3.59

故障响应时间间隔 fault reaction time interval；FRTI

从探测到**故障**(3.54)到进入**安全状态**(3.131)或进入**紧急运行**(3.43)的时间间隔。

注：见图4和图5。

3.60

故障容错 fault tolerance

在一个或多个特定**故障**(3.54)存在的情况下，实现特定功能的能力。

注：特定功能可能是**预期功能**(3.83)。

3.61

故障容错时间间隔 fault tolerant time interval ；FTTI

在**安全机制**（3.142）未被激活情况下，从**相关项**（3.84）内部**故障**（3.54）发生到可能发生**危害事件**（3.77）的最短时间间隔。

注1：安全相关的时间间隔见图5。

注2：该最短时间间隔是通过评估所有**危害事件**（3.77）得到的，其可以取决于**危害**（3.75）的特征。

注3：FTTI与**相关项**（3.84）的**功能异常表现**（3.88）而引起的**危害**（3.75）有关。FTTI是源于该**危害**（3.75）的**安全目标**（3.139）的一个相关属性。

注4：在故障容错时间间隔内，如果**相关项**（3.84）保持在**安全状态**（3.131）或过渡到**安全状态**（3.131）或过渡到**紧急运行**（3.43），则表明**安全机制**（3.142）及时对**故障**（3.54）进行了处理。

注5：**危害事件**(3.77)的发生取决于存在的**故障**(3.54)并且车辆处于**故障**(3.54)可影响车辆行为的场景中。

示例：制动**系统**(3.163)中的**失效**（3.50）在实施制动之前可能不会导致**危害事件** (3.77)。

注6：虽然仅在**相关项**(3.84)层面定义FTTI，但在**要素**(3.41)层面可以定义**最长故障处理时间间隔**(3.56)和故障处理后要求达到的状态，以支持**功能安全概念**(3.68)。

注7：当**诊断测试时间间隔**(3.35)比**故障探测时间间隔**(3.55)足够短时，**故障探测时间间隔**(3.55)可包括多个**诊断测试时间间隔**(3.35)用于消除**错误**(3.46)抖动。

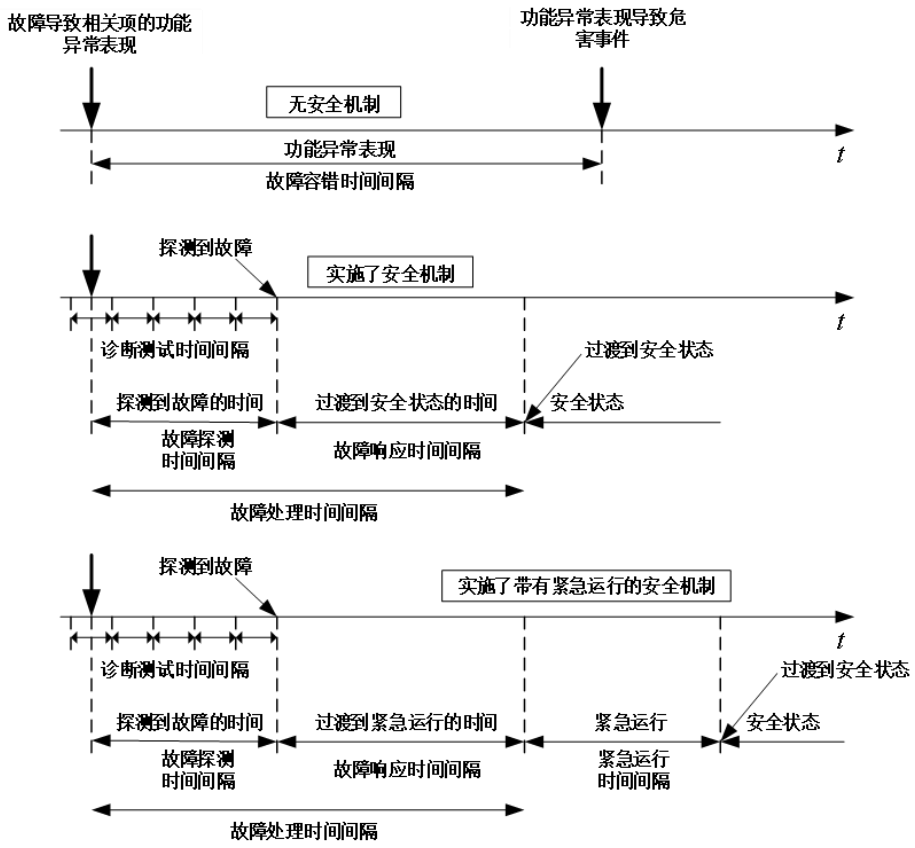

图5　安全相关时间间隔

3.62

现场数据　field data

从**相关项**(3.84)或**要素**(3.41)的使用中获得的数据，包含累积运行时间、所有的**失效**(3.50)和服务中的**安全异常**(3.134)。

注：现场数据通常来自客户的使用。

3.63

形式记法　formal notation

语法和语义上完整定义的描述方法。

示例：Z 记法（Zed）、符号模型检查（NuSMV）、工程样机验证系统（PVS）、Vienna 开发方法（VDM）、数学公式。

3.64

形式验证　formal verification

基于**形式记法**(3.63)针对**相关项**(3.84)或**要素**(3.41)的功能或属性的定义，验证其正确性的方法。

3.65

免于干扰　freedom from interference

两个或两个以上的**要素**（3.41）之间，不存在可能导致违背**安全**（3.132）要求的**级联失效**(3.17)。

示例1：如果**要素**（3.41）2 的**失效**(3.50)不会导致**要素**（3.41）1 失效，则**要素**（3.41）1 免于**要素**（3.41）2 的干扰。

示例2：如果**要素**（3.41）3 的失效导致**要素**（3.41）4 失效，则**要素**（3.41）3 干扰**要素**（3.41）4。

3.66

功能概念　functional concept

实现预期表现所需的各预期功能及其交互的定义。

注：功能概念是在**概念阶段**(3.110)开发的。

3.67

功能安全 functional safety

不存在由**电气/电子系统**（3.40）的**功能异常表现**(3.88)引起的**危害**(3.75)而导致**不合理的风险**(3.176)。

3.68

功能安全概念 functional safety concept

为了实现**安全目标**(3.139)，定义**功能安全要求**（3.69）及相关信息，并将要求分配到**架构**（3.1）中的**要素**（3.41）上，以及定义要素之间的必要交互。

3.69

功能安全要求 functional safety requirement

定义了独立于具体实现方式的**安全**（3.132）行为，或独立于具体实现方式的**安全措施**（3.141），包括安全相关的属性。

注1：功能安全要求可以是由安全相关的**电气/电子系统**（3.40）或基于**其他技术**(3.105)的安全相关**系统**（3.163）所执行的安全要求，目的是通过考虑确定的**危害事件**(3.77)，使**相关项**(3.84)达到或保持在**安全状态**(3.131)。

注2：功能安全要求的定义可独立于产品开发概念**阶段**（3.110）中使用的技术。

注3：安全相关的属性包括**ASIL等级**（3.6）信息。

3.70

硬件架构度量 hardware architectural metrics

用于评估**硬件架构**（3.1）**安全**（3.132）有效性的度量。

注：**单点故障**（3.156）度量和**潜伏故障**（3.85）度量都是硬件架构度量。

3.71

硬件元器件 hardware part

硬件组件(3.21)在第一层级分解时的一部分。

示例：微控制器的 CPU、电阻、微控制器的闪存阵列。

3.72

硬件基础子元器件 hardware elementary subpart

安全（3.132）分析中考虑的**硬件子元器件**（3.73）的最小部分。

示例：ALU 的触发器及其逻辑锥、寄存器。

3.73

硬件子元器件 hardware subpart

硬件元器件(3.71)中可按逻辑分割的，且代表第二层级或更高层级分解的一部分。

示例：微控制器中的 CPU 的 ALU，CPU 的寄存器组。

3.74

伤害 harm

对人身健康的物理损害或破坏。

3.75

危害 hazard

由**相关项**(3.84)的**功能异常表现**(3.88)而导致的**伤害**(3.74)的潜在来源。

注：该定义仅限于GB/T 34590；危害的一个更通常定义是**伤害**(3.74)的潜在来源。

3.76

危害分析和风险评估 hazard analysis and risk assessment；HARA

为了避免**不合理的风险**(3.176)，对**相关项**(3.84)的危害事件(3.77)进行识别和归类的方法以及定义防止和减轻相关**危害**（3.75）的**安全目标**(3.139)和**ASIL等级**(3.6)的方法。

3.77

危害事件 hazardous event

危害(3.75)和**运行场景**(3.104)的组合。

3.78

独立性 Independence

两个或者多个**要素**(3.41)间不存在会导致违背**安全**(3.132)要求的**相关失效**(3.29),或从组织上分隔执行某一活动的各方。

注：ASIL等级分解(3.3)或**认可措施**(3.23)包括对独立性的要求。

3.79

非相关失效 independent failures

同时或相继失效的概率可表示为无条件失效概率的简单乘积的**失效**（3.50）。

注：非相关失效可以包括软件**失效**（3.50）即使其失效概率未被计算。

3.80

非形式记法 informal notation

非完整语法定义的描述方法。

注：不完整的语法定义意指语义也没有完整的定义。

3.81

继承 inheritance

在开发过程中，某些要求的属性以一种未改变的方式传递到下一细节层面。

3.82

检查 inspection

为发现**安全异常**（3.134）而依据一个正式的流程对**工作成果**（3.185）进行的考查。

注1：检查是**验证**（3.180）的一种方式。

注2：检查不同于**测试**（3.169），检查通常不包括对**相关项**（3.84）或**要素**（3.41）的操作。

注3：一项正式的检查流程通常包括预先定义的步骤、检查列表、核对人员及对结果的**评审**（3.127）。

3.83

预期功能 intended functionality

针对**相关项**（3.84）定义的除**安全机制**（3.142）外的行为。

注：上述行为是在整车层面定义的。

3.84

相关项 item

适用于GB/T 34590，实现整车层面功能或部分功能的**系统**（3.163）或系统组合。

注：见**整车功能**（3.178）。

3.85

潜伏故障 latent fault

在**多点故障探测时间间隔**（3.98）内，未被**安全机制**（3.142）探测到且未被驾驶员感知到的**多点故障**（3.97）。

3.86

生命周期 lifecycle

相关项(3.84)从概念到报废的全部**阶段**(3.110)。

3.87

管理体系 management system

一个组织用来实现其目标的政策、程序及流程。

3.88

功能异常表现 malfunctioning behaviour

失效(3.50)或与设计意图相悖的**相关项**(3.84)非预期表现。

3.89

最长修复时间间隔 maximum time to repair time interval

可以维持在**安全状态**（3.131）的特定时间间隔。

注1：当**安全状态**(3.131)无法保持到车辆剩余使用寿命结束时，最长待修复时间是一个相关特性。

注2：从**安全状态**（3.131）中恢复的条件在**报警和降级策略**（3.183）中进行描述。

注3：若相关，则最长待修复时间间隔在**报警和降级策略**（3.183）中进行描述。

3.90

基于模型的开发 model-based development；MBD

一种使用模型来描述待开发**要素**（3.41）行为或属性的开发。

注：根据模型使用的抽象层次，该模型可用于仿真或代码生成或二者均可。

3.91

修改 modification

以现有**相关项**（3.84）为基础创建新**相关项**（3.84）。

注：在GB/T 34590中，为剪裁**生命周期**（3.86）对复用的部分使用“修改”。变更用于**相关项**（3.84）的**生命周期**（3.86）过程中，而修改用于由已有的相关项生成新的**相关项**（3.84）。

3.92

修改条件/判定覆盖率 modified condition/decision coverage；MC/DC

在控制流中已执行的、可以独立影响判定结果的全部单一条件结果的百分比。

注：MC/DC是一种建立在**分支覆盖率**（3.13）之上的代码覆盖率分析。因此，它也要求所有的代码块和所有的执行路径都经过测试。

3.93

摩托车 motorcycle

由动力装置驱动的具有两个或三个车轮的道路车辆，其最高设计车速大于50 km/h，或满足以下条件之一：

——若使用内燃机，其排量大于 50 ml;

——若使用电力驱动，其电机的最大连续额定功率总和大于 4 kW。

——但不包括如下类别：

——最大设计车速、整车整备质量、外廓尺寸等指标符合相关国家标准和规定的，专供残疾人驾驶的机动轮椅车；

[来源：GB/T 5359.1—2019，2.1]

3.94

摩托车安全完整性等级 motorcycle safety integrity level；MSIL

四个等级中的一个等级，用于定义**相关项**(3.84)或**要素**(3.41)需要满足的GB/T 34590中的风险降低要求以及转换为**ASIL**（3.6）等级后的**安全措施**（3.141），以避免摩托车特定应用的**相关项**（3.84）或**要素**（3.41）的不合理的**残余风险**（3.126），D代表最高严格等级，A代表最低严格等级。

3.95

多核 multi-core

包括两个或多个能彼此独立运行的硬件**处理要素**（3.113）的硬件**组件**（3.21）。

3.96

多点失效 multiple-point failure

由几个独立的硬件**故障**（3.54）组合引发，直接导致违背**安全目标**（3.139）的**失效**（3.50）。

3.97

多点故障 multiple-point fault

在未被探测且未被感知到的情况下，与其他独立**故障**（3.54）组合可能导致一个**多点失效**(3.96)的一个**故障**（3.54）。

注：一个多点故障仅在识别出(例如，通过故障树的割集分析)**多点失效**(3.96)后才能被辨认出来。

3.98

多点故障探测时间间隔 multiple-point fault detection time interval

在可导致一个**多点失效**（3.96）前，将**多点故障**（3.97）探测出来的时间间隔。

3.99

新开发 new development

开发一个具有先前未定义功能的**相关项**（3.84）或**要素**（3.41）的过程，或开发一个现有功能的新的实现方式的过程，或两者都有。

3.100

非功能性危害 non-functional hazard

由**电气/电子系统**（3.40）、基于**其他技术**(3.105)的安全相关**系统**（3.163）或**外部措施**（3.49）的**功能异常表现**（3.88）以外的因素导致的**危害**（3.75）。

3.101

观测点 observation points

用来观察**故障**（3.54）潜在影响的**要素**（3.41）的输出信号。

示例：存储器的输出。

3.102

运行模式 operating mode

源自**相关项**（3.84）或**要素**（3.41）的使用和应用中功能状态的一些条件。

示例：系统（3.163）关闭；**系统**（3.163）激活；**系统**（3.163）非激活；降级运行；**紧急运行**（3.43）；**安全状态**（3.131）。

3.103

运行时间 operating time

相关项（3.84）或**要素**（3.41）工作（包括降级模式）的累积时间。

3.104

运行场景 operational situation

在车辆生命周期中可能发生的场景。

示例：高速行驶、斜坡驻车、维护。

3.105

其他技术 other technology

不同于GB/T 34590规定范围内的电气/电子技术的技术。

示例：机械技术、液压技术。

注：其他技术可在**安全**（3.132）要求（见GB/T 34590.3-XXXX和GB/T 34590.4-XXXX）分配过程中、在**功能安全概念**（3.68）（见GB/T 34590.3-XXXX，第7章和图2）的定义中被考虑，或作为**外部措施**（3.49）被考虑。

3.106

分区 partitioning

为实现某种设计，而对功能或**要素**（3.41）的分隔。

注：分区可用于抑制**故障**（3.54）以避免**级联失效**（3.17）。为实现分区设计**要素**（3.41）间的**免于干扰**（3.65），可引入额外的非功能性要求。

3.107

乘用车 passenger car

设计和制造上主要用于载运乘客及其随身行李和/或临时物品的汽车，包括驾驶人座位在内最多不超过9个座位。它也可以牵引一辆中置轴挂车。

[来源：GB/T 3730.1—2001，2.1.1]

3.108

可感知故障 perceived fault

可间接感知到的**故障**（3.54）（通过整车层面的异常行为）。

3.109

永久性故障 permanent fault

发生并持续直到被移除或修复的**故障**(3.54)。

注：直流(DC)**故障**(3.54),例如卡滞故障和桥接**故障**(3.54)是永久性故障。

3.110

阶段 phase

GB/T34590.3、GB/T34590.4、GB/T34590.5、GB/T34590.6和GB/T34590.7中定义的**安全**(3.132)**生命周期**(3.86)的阶段。

注：GB/T34590.3、GB/T34590.4、GB/T34590.5、GB/T34590.6和GB/T34590.7分别定义了阶段：

——概念；

——**系统**(3.163)层面产品开发；

——硬件层面产品开发；

——软件层面产品开发；

——生产、运行、服务和报废。

3.111

失效物理学 physics of failure ; PoF

基于**失效**(3.50)机制研究可靠性的科学方法。

注1：PoF通常应用于计算机辅助工程(CAE)环境中的耐久性模拟。

注2：在评估新技术和设计的可靠性时，失效物理学分析可能有优势，因为不需要多年的现场**失效**(3.50)历史来进行可靠性预测。

3.112

动力输出装置 power take-off; PTO

卡车(3.174)或**牵引车**(3.170)为操作设备提供动力源的接口。

示例：操作液压泵、真空泵、举升机、翻斗车、水泥搅拌机的接口。

3.113

处理要素 processing element ; PE

提供一系列数据处理功能的**硬件元器件**(3.71)，通常包括一个寄存器集、一个执行单元和一个控制单元。

示例1：由 4 个核组成的硬件**组件**(3.21)可以被描述为具有 4 个处理要素。

示例2：可以将 GPU 中的流多处理器视为处理要素。

3.114

可编程逻辑器件 programmable logic device; PLD

在制造时具有未定义的电路功能，并在集成到更高级别的**要素**(3.41)时进行配置的硬件**组件**(3.21)或**硬件元器件**(3.71)。

3.115

在用证明 proven in use argument

基于对**候选项**(3.16)应用的**现场数据**(3.62)的分析，证明该**候选项**(3.16)的任何**失效**(3.50)可能损害**相关项**(3.84)**安全目标**(3.139)的可能性符合适用**ASIL**(3.6)等级要求的证据。

3.116

在用证明可信度 proven in use credit

通过**在用证明**(3.115)对一组给定的**生命周期**(3.86)**子阶段**(3.161)及相应**工作成果**(3.185)的替代。

3.117

质量管理 quality management; QM

用来指导和控制组织的针对质量的协调活动。

注：QM不是一个**ASIL**(3.6)等级，但可以在**危害分析和风险评估**(3.76)中定义。

3.118

随机硬件失效 random hardware failure

在硬件**要素**(3.41)的生命周期中,发生的服从概率分布的不可预测的**失效**(3.50)。

注1：可在合理的精度内预测随机硬件失效率。

注2：对于本文件准而言，**失效物理学**(3.111)方法论(SAE J1211、JEDEC JEP122等）定义的物理硬件**失效**(3.50)可视为随机硬件失效。

3.119

随机硬件故障 random hardware fault

服从概率分布的硬件**故障**(3.54)

3.120

合理可预见的 reasonably foreseeable

技术上可能的、且具有可信或可测量发生率的。

注：预期的误用可以理解为合理可预见事件的子类。

3.121

重建 rebuilding

改变T&B的原始配置，以便执行不同的任务。

注：重建可以包括 **T&B 车辆配置**(3.175)的**修改**(3.91)。

3.122

冗余 redundancy

除了足以实施所需功能或足以表达信息的方法外，还存在其他方法。

注1：GB/T 34590中使用了冗余，以实现**安全目标**(3.139)或特定**安全**(3.132)要求、或者表达安全相关信息。

注2：冗余可以同质实现，也可以多样性实现。

示例1：重复的功能**组件**(3.21)是冗余的一个实例，其目的是增加**可用性**(3.7)或用于**故障**(3.54)探测。

示例2：对表示安全相关信息的数据增加奇偶检验位，为**故障**(3.54)探测提供了冗余。

3.123

回归策略 regression strategy

用于验证**相关项**(3.84)或**要素**（3.41）中一个已实施的变更不会影响到未变更的、已存在的和先前验证过的部分或特性的策略。

3.124

再制造 remanufacturing

按照原始规范，用新的或修复后的零件对已使用一段时间的T&B车辆进行拆卸和翻修。

3.125

残余故障 residual fault

发生在硬件**要素**（3.41）中，可导致违背**安全目标**（3.139）的**随机硬件故障**（3.119）中未被**安全机制**（3.142）覆盖的部分。

注：此处假设硬件**要素**（3.41）的**安全机制**(3.142)仅覆盖了其**故障**(3.54)的一部分。

示例：如果一系列与安全相关且不安全的**故障**(3.54)，有 60%的子集被覆盖，那么该组**故障**(3.54)剩余的 40%称为残余故障。

3.126

残余风险 residual risk

实施**安全措施**（3.141）后剩余的**风险**（3.128）。

3.127

评审 review

按照评审目的，为实现预期的**工作成果**（3.185）目标而对工作成果（3.185）进行的检查。

注：从开发**阶段**（3.110）的角度看，包括**验证评审**（3.181）和**认可评审**（3.24）。

3.128

风险 risk

伤害（3.74）发生的概率及其**严重度**（3.154）的组合。

3.129

鲁棒性设计 robust design

在无效的输入或有压力的环境条件下，具有正确工作的能力的设计。

注：对鲁棒性可作如下理解：

——对于软件，鲁棒性是指应对异常输入和条件的能力；

——对于硬件，鲁棒性是指在设计范围和使用寿命内对环境压力的承受能力和稳定能力；及

——在GB/T 34590上下文中，鲁棒性是在边界处提供安全行为的能力。

3.130

安全故障 safe fault

不会显著增加违背**安全目标**（3.139）的概率的**故障**（3.54）。

注1：如GB/T 34590.5-XXXX附录B所示，非安全相关和**安全相关要素**（3.144）都可能有安全故障。

注2：单点故障（3.156）、**残余故障**（3.125）和**双点故障**(3.39)不视为安全故障。

注3：除非在**安全**（3.132）概念中表明具有相关性，否则，大于2阶的**多点故障**（3.97）可被认为是安全故障。

3.131

安全状态 safe state

相关项（3.84）在**失效**（3.50）的情况下，没有不合理**风险**（3.128）的**运行模式**（3.102）。

注1：见图5。

注2：虽然可将正常运行视为安全，但GB/T 34590中仅针对**失效**（3.50）情况定义安全状态。

示例：示例：关闭模式（对于非容错性的**系统**（3.163））。

3.132

安全 safety

没有**不合理的风险**（3.176）。

3.133

安全活动 safety activity

在**安全**（3.132）**生命周期**（3.86）的一个或多个**阶段**（3.110）或**子阶段**（3.161）进行的活动。

3.134

安全异常 safety anomaly

偏离预期并可能导致**伤害**（3.74）的情况。

注：安全异常可在**评审**（3.127）、**测试**（3.169）、分析、编译、**组件**（3.21）的使用、或适用文档的使用等过程中被发现。

示例：偏差可以是在需求、规范、设计文档、用户文档、标准或经验方面。

3.135

安全架构 safety architecture

用来实现**安全**（3.132）要求的一系列**要素**（3.41）以及它们之间的交互。

3.136

安全档案 safety case

实现**相关项**（3.84）或**要素**（3.41）**功能安全**（3.67）、收集整理开发过程中安全活动的**工作成果**（3.185）证据来满足**功能安全**（3.67）的论据。

注：安全档案可被扩展，以涵盖GB/T 34590范围外的**安全**（3.132）问题。

3.137

安全文化 safety culture

组织中持久的价值观、态度、动机和认知，即：在决策和行为中，**安全**（3.132）优先于与之冲突的目标。

注：见 GB/T 34590.2-XXXX，附录B。

3.138

独立于环境的安全要素 safety element out of context；SEooC

不是在特定的**相关项**（3.84）定义下开发的**安全相关要素**（3.144）。

注：一个SEooC的安全要素可以是一个**系统**（3.163），**系统**（3.163）组合，一个**软件组件**（3.157），一个**软件单元**（3.159），一个硬件**组件**（3.21），或一个**硬件元器件**（3.71）。

示例：可集成到不同 OEM **系统**（3.163）中的基于假设安全要求的通用雨刮**系统**（3.163）。

3.139

安全目标 safety goal

作为整车层面**危害分析和风险评估**（3.76）结果的最高层面的**安全**（3.132）要求。

注：一个安全目标可能与几种**危害**（3.75）有关，几个安全目标可能与一种单一的**危害**（3.75）有关。

3.140

安全经理 safety manager

对实现**功能安全**（3.67）所必需的活动，负责监督和确保其开展的人员或组织。

注：在**相关项**（3.84）开发的不同层面，每个涉及的公司可按照内部矩阵组织对任务的划分，指派一个或多个不同人员。

3.141

安全措施 safety measure

用来避免或控制**系统性失效**(3.164)，探测或控制**随机硬件失效**(3.118)，或减轻它们有害影响的活动或技术解决方案。

注：安全措施包括**安全机制**(3.142)。

示例：FMEA 或未使用全局变量的软件。

3.142

安全机制 safety mechanism

为了保持**预期功能**(3.83)或者达到/保持某种安全状态，由电气/电子系统的功能/**要素**(3.41)或者**其他技术**(3.105)来实施的技术解决方案，以探测并减轻/容许**故障**(3.54)、或者控制/避免**失效**(3.50)。

注1：在**相关项**(3.84)中实施安全机制以避免**故障**(3.54)导致**单点失效**(3.155)和防止**故障**(3.54)成为**潜伏故障**(3.85)。

注2：安全机制也可是：

a) 能够使**相关项**(3.84)过渡到或保持在**安全状态**(3.131)；或

b) 如同在**功能安全概念**(3.68)中定义的，能够向驾驶员发出提醒以控制**失效**(3.50)的影响。

3.143

安全计划 safety plan

管理和指导开展项目**安全活动**(3.133)的计划，包括日期、里程碑节点、任务、可交付成果、职责和资源。

3.144

安全相关要素 safety-related element

有潜在可能导致违背安全目标或有助于实现**安全目标**(3.139)的**要素**(3.41)。

注：如果失效-安全**要素**(3.41)可能违背至少一个安全目标，那么该失效-安全要素被认为是与安全相关的。

3.145

安全相关功能 safety-related function

有潜在可能导致违背安全目标或有助于实现**安全目标**(3.139)的功能。

3.146

安全相关事件 safety-related incident

安全相关**失效**（3.50）的发生。

3.147

安全相关的特殊特性 safety-related special characteristic

相关项（3.84）、**要素**（3.41）自身或其生产过程的特性，这些特性的合理可预见偏差可能影响、促使或造成任何潜在的**功能安全**（3.67）降低。

注1：GB/T 18305中定义了特殊特性的术语。

注2：安全相关的特殊特性在**相关项**（3.84）或**要素**（3.41）的开发**阶段**（3.110）中得出。

注3：安全相关的特殊特性不同于安全机制，也不宜和**安全机制**（3.142）混淆。

示例：温度范围、有效期限、紧固力矩、生产公差、配置。

3.148

安全确认 safety validation

基于检查和测试，确保**安全目标**（3.139）是充分的，并已达到且具有足够的完整性等级。

注：GB/T 34590.4-XXXX提供了合适的安全确认方法。

3.149

半形式记法 semi-formal notation

语法定义是完整的，但语义定义可以是不完整的描述方法。

示例：结构化分析与设计技术（SADT）、统一建模语言（UML）。

3.150

半形式验证 semi-formal verification

基于**半形式记法**（3.149）的**验证**(3.180)。

示例：使用由半形式模型生成的测试向量来测试**系统**（3.163）表现与模型是否匹配。

3.151

半挂车 semi-trailer

设计为通过连接到**牵引车**（3.170）上的主销（对牵引车辆施加了很大的垂直载荷）而被牵引的**挂车**（3.171）。

3.152

量产道路车辆 series production road vehicle

旨在用于公共道路且不是原型机的道路车辆。

注：车辆类型分类可能因地区而异。

示例1：普通消费者使用车辆。

示例2：公共用途车辆。

3.153

服务说明 service note

在执行**相关项**(3.84)的维护流程时所考虑的**安全**(3.132)信息文档。

示例：**安全相关的特殊特性**（3.147）；所需的**安全**（3.132）操作。

3.154

严重度 severity

对潜在**危害事件**（3.77）中可能发生的一个或多个人员的**伤害**（3.74）程度的预估。

注：在**危害分析和风险评估**（3.7）中参数“S”代表伤害的潜在严重程度。

3.155

单点失效 single-point failure

由**单点故障**(3.156)引起的**失效**(3.50)。

3.156

单点故障 single-point fault

要素(3.41)中直接导致违背**安全目标**(3.139)的硬件**故障**(3.54)，且该**要素**(3.41)中的**故障**(3.54)未被任何**安全机制**(3.142)覆盖。

注1：见**单点失效**(3.155)。

注2：如果为一个硬件**要素**(3.41)定义了至少一个**安全机制**(3.142)(例如，微控制器的看门狗)，那么，该硬件**要素**(3.41)的**故障**(3.54)均不是单点故障。

3.157

软件组件 software component

一个或多个**软件单元**(3.159)。

3.158

软件工具 software tool

在开发**相关项**(3.84)或**要素**(3.41)中所用到的计算机程序。

3.159

软件单元 software unit

软件**架构**(3.1)中的最低层级且可被独立**测试**(3.169)的**软件组件**(3.157)。

3.160

语句覆盖率 statement coverage

软件中已执行语句所占的百分比。

3.161

子阶段 subphase

GB/T 34590章节中定义的、**安全**(3.132)**生命周期**(3.86)中**阶段**（3.110）的细分。

示例：危害分析和风险评估(3.76)是**安全**(3.132)**生命周期**(3.96)的子阶段，在 GB/T 34590.3-XXXX 第 6 章中进行了定义。

3.162

供应协议 supply agreement

客户和供应商之间的协议，其中规定了各项活动的责任划分，以及各方要执行或交换的与**相关项**（3.84）和**要素**（3.41）生产相关的证据或**工作成果**（3.185）。

注：DIA适用于开发阶段，供应协议适用于生产。

3.163

系统 system

一组至少与一个传感器、一个控制器和一个执行器相关联的**组件**(3.21)或子系统。

注：相关的传感器或执行器可包含在系统中，也可存在于系统之外。

3.164

系统性失效 systematic failure

以确定的方式与某个原因相关的**失效**(3.50)，只有对设计或生产流程、操作规程、文档或其他相关因素进行变更后才可能排除这种失效。

3.165 **系统性故障** systematic fault

以确定的方式显现**失效**(3.50)的**故障**(3.54)，只有通过流程或设计措施的应用才能防止其发生。

3.166

目标环境 target environment

用于执行特定软件的环境。

注：对于应用软件，其目标环境是带有基础软件和操作系统的微控制器。对于**嵌入式软件**（3.42），其目标环境是**系统**（3.163）中的ECU。

3.167

技术安全概念 technical safety concept

技术安全要求（3.168）的定义，**技术安全要求**（3.168）在**系统**（3.163）**要素**（3.41）间的分配，以及为**系统**（3.163）层面**功能安全**（3.67）提供依据的相关信息。

3.168

技术安全要求 technical safety requirement

为实现相关的**功能安全要求**（3.69）而得出的要求。

注：得出的要求包括减轻危害所需的要求。

3.169

测试 testing

为验证**相关项**（3.84）或**要素**（3.41）满足定义的要求、探测其**安全异常**（3.134）、确认要求适用于给定的环境和对其行为建立信心，而进行计划、准备、运行或演练的过程。

3.170

牵引车 tractor

用来牵引**半挂车**（3.151）的**卡车**（3.174）。

3.171

挂车 trailer

设计上需被牵引且总质量的大部分不由牵引车辆承担的道路车辆。

注：挂车可设计用于运输货物、设备或人员。

3.172

转换器 transducer

将一种形式的能量转换成另一种形式的能量的**硬件元器件**(3.71)，其灵敏度决定了其输出能量形式的大小相对于其输入能量形式的大小。

3.173

瞬态故障　transient fault

发生一次且随后消失的**故障**(3.54)。

注：瞬态故障可由电磁干扰引起，其可导致位翻转。软**错误**(3.46)，如单粒子翻转 (SEU)和单粒子瞬态(SET)，均为瞬态故障。

3.174

卡车　truck

设计用于运输货物或在底盘上装有设备的机动车。

注：卡车也可以牵引一辆**挂车**(3.171)。

3.175

T&B 车辆配置　T&B vehicle configuration

T&B的**基础车辆**（3.9）和**车辆上装设备**（3.12）的技术特性，这些特性在运行期间不会发生改变。

注：在**重建**（3.121）时可能发生改变。

示例：轴距，轴荷分布，车轮（车轴数量、驱动轴数量、转向轴数量）。

3.176

不合理的风险　unreasonable risk

按照现行的安全观念，被判断为在某种环境下不可接受的**风险**（3.128）。

3.177

T&B 车辆使用的变化　variance in T&B vehicle operation

在车辆寿命期内受货物或牵引的影响，使用的T&B车辆具有不同的动态特性。

示例：有载荷或无载荷的 T&B，载荷分布变化的 T&B，带或不带**挂车**（3.171）的**卡车**（3.174），带或不带**半挂车**（3.151）的**牵引车**（3.170）（单独的**牵引车**（3.170））。

3.178

整车功能　vehicle function

用户可观察到的、预期通过一个或多个**相关项**（3.84）来实现的车辆行为。

示例：“自动巡航控制”是一种可以使用不同的 ECU 和各种传感器技术（例如雷达、激光雷达、摄像头）实现的车辆功能。

3.179

车辆运行状态　vehicle operating state

与**运行场景**（3.104）结合的**运行模式**（3.102）。

注：车辆的运行状态是由当前行驶情况下(例如以120km/h行驶在高速公路上)特定功能(例如高度自动驾驶)提供的性能所决定的。**危害事件**（3.77）的**ASIL**（3.6）等级（例如特定功能的突然丧失）取决于当前的车辆运行状态（例如高度自动驾驶能力的突然丧失，在高速行驶时就比在低速行驶时更为危险）。如果**系统**（3.163）不在运行中，即当驾驶员在操控车辆时**系统**（3.163）发生失效，则在高速情况下突然丧失高度自动驾驶能力并不是问题。

3.180

验证　verification

确定检查对象是否满足其特定要求。

示例：示例：典型的验证活动可以分为以下几类：

——**验证评审**（3.181），**走查**（3.182），**检查**（3.82）；

——验证**测试**（3.169）；

——仿真模拟；

——原型样机；及

——分析（**安全**（3.132）分析、控制流分析、数据流分析等）。

3.181

验证评审 verification review

确保开发活动结果满足项目要求和/或技术要求的**验证**（3.180）活动。

注1：验证评审的单独要求在GB/T 34590的单独部分中的特定章条中给出。

注2：验证评审的目标是确认**相关项**（3.84）或**要素**（3.41）的技术正确性和完整性。

示例：验证评审类型可以是技术**评审**（3.127）、**走查**（3.182）、**检查**（3.82）。

3.182

走查 walk-through

为了发现**安全异常**（3.134），对**工作成果**（3.185）的系统性检查。

注1：走查是**验证**（3.180）的一种方法。

注2：走查和**测试**（3.169）的区别在于，走查通常不涉及**相关项**（3.84）或**要素**（3.41）的运行。

注3：被发现的任何异常通常通过重做来处理，并对重做的**工作成果**（3.185）进行走查。

示例：在走查过程中，开发者向一个或多个评审员逐步的阐述**工作成果**（3.185）。其目的是建立对工作成果的共同理解和识别**工作成果**（3.185）中的任何**安全异常**（3.134）。**检查**（3.82）和走查均属于同级**评审**（3.127），其中走查的严格性弱于**检查**（3.82）。

3.183

报警和降级策略 warning and degradation strategy

如何将潜在降低的功能向驾驶员报警及如何提供降低的功能以达到**安全状态**（3.131）的定义。

注：报警和降级策略包括：

——触觉、声音或视觉提示的说明，以提醒驾驶员即将发生的**降级**（3.28）；

——与相应的**安全目标**（3.139）相关的一个或多个**安全状态**（3.131）的描述；

——向**安全状态**（3.131）过渡的条件；

——从**安全状态**（3.131）恢复的条件，以及如果适用，相应的**最长待修复时间间隔**（3.89）；及

——如果适用，**紧急运行**（3.43）和相应的**紧急运行容错时间间隔**（3.45）；

3.184

值得信赖的 well-trusted

此前在类似的应用中使用过，且没有已知的**安全异常**（3.134）。

示例：值得信赖的设计原则、值得信赖的工具、值得信赖的硬件**组件**（3.21）。

3.185

工作成果 work product

由GB/T 34590中一个或多个相关要求得出的文档。

注：文档可以是包含工作成果完整信息的单个文档，也可以是包含工作成果完整信息的一系列文档。

3.186

预期功能安全 safety of the intended functionality; SOTIF

不存在由预期功能的不足引起的危害而导致不合理的风险。

3.187

接受准则 acceptance criteria

表征不存在不合理风险水平的准则。

注：接受准则包括两个层面，即危害行为事件接受准则和总体安全风险接受准则。接受准则可以是定性的，也可以是定量的，例如物理参数，即当某特定行为被视为危害行为时，表征该危害行为的参数值，或每小时的最大数，

或最低合理可行（ALARP）原则等。

示例：根据交通统计数据得出每 Xkm 发生一次事故的合理风险水平。

3.188

安全度量 safety metric

为符合安全目标而给定的具体技术参数的量化值（安全度量并非ASIL等级）。

4 缩略语

下列缩略语适用于本文件。

ACC：自适应巡航控制 (Adaptive Cruise Control)

ADC：模数转换器 (Analogue to Digital Converter)

AEC：汽车电子委员会 (Automotive Electronics Council)

AIS：简明损伤定级 (Abbreviated Injury Scale)

ALU：算术逻辑单元 (Arithmetic Logic Unit)

ASIC：专用集成电路 (Application-Specific Integrated Circuit)

ASIL：汽车安全完整性等级 (Automotive Safety Integrity Level)

BB：车辆上装制造商 (Body Builder)

BFR：基础失效率 (Base Failure Rate)

BIST：内建自测试 (Built-In Self-Test)

CAN：控制器局域网络 (Controller Area Network)

CCF：共因失效 (Common Cause Failure)

CCP：可控性评级专家组 (Controllability Classification Panel)

CMOS：互补金属氧化物半导体 (Complementary Metal Oxide Semiconductor)

COTS：商业现成产品 (Commercial Off The Shelf)

CPU：中央处理单元 (Central Processing Unit)

CRC：循环冗余校验 (Cyclic Redundancy Check)

DC:诊断覆盖率 (Diagnostic Coverage)

DAC：数模转换器 (Digital to Analogue Converter)

DFA：相关失效分析 (Dependent Failure Analysis)

DFI：相关失效引发源 (Dependent Failure Initiator)

DIA：开发接口协议 (Development Interface Agreement)

DMA：直接内存访问 (Direct Memory Access)

DMOS：双扩散金属氧化物半导体（高压金属氧化物半导体）（Double diffused Metal Oxide Semiconductor (HV MOS)）

DSP：数字信号处理器 (Digital Signal Processor)

ECC：纠错码 (Error Correction Code)

ECU：电控单元 (Electronic Control Unit)

EDC：检错码 (Error Detection Code)

E/E：电气/电子系统 (Electrical and/or Electronic system)

EEC：对违反安全目标的每个原因的评估 (Evaluation of Each Cause of safety goal violation)

EMC：电磁兼容性 (ElectroMagnetic Compatibility)

EMI：电磁干扰 (ElectroMagnetic Interference)

EOTI：紧急运行时间间隔 (Emergency Operation Time Interval)

EOTTI：紧急运行容错时间间隔 (Emergency Operation Tolerance Time Interval)
ESD：静电放电 (ElectroStatic Discharge)
ESC：电子稳定性控制 (Electronic Stability Control)
ETA：事件树分析 (Event Tree Analysis)
EVR：嵌入式电压调节器 (Embedded Voltage Regulator)
FDTI：故障探测时间间隔 (Fault Detection Time Interval)
FET：场效应晶体管 (Field Effect Transistor)
FHTI：故障处理时间间隔 (Fault Handling Time Interval)
FIT：失效率 (Failures In Time)
FMC：失效模式覆盖率 (Failure Mode Coverage)
FMEA：失效模式与影响分析 (Failure Mode and Effects Analysis)
FPGA：现场可编程门阵列 (Field Programmable Gate Array)
FRTI：故障响应时间间隔 (Fault Reaction Time Interval)
FTA：故障树分析 (Fault Tree Analysis)
FTTI：故障容错时间间隔 (Fault Tolerant Time Interval)
GPU：图形处理单元 (Graphics Processing Unit)
HARA：危害分析和风险评估 (Hazard Analysis and Risk Assessment)
HAZOP：危害和可操作性分析 (HAZard and OPerability analysis)
HSI：软硬件接口 (Hardware-Software Interface)
HS/LS：高边/低边 (High Side/Low Side)
HW：硬件 (HardWare)
IC：集成电路 (Integrated Circuit)
I/O：输入/输出 (Input-Output)
ISA：指令集架构 (Instruction Set Architecture)
LDO：低压差线性稳压器 (Low Drop Output regulator)
LFM：潜伏故障度量 (Latent-Fault Metric)
LS：低边 (Low Side)
LSB：最低有效位 (Least Significant Bit)
MBD：基于模型的开发 (Model Based Development)
MC/DC：修改条件/判定覆盖 (Modified Condition/Decision Coverage)
MCU：多点控制单元 (Multi-point Control Unit)
MMU：存储器管理单元 (Memory Management Unit)
MPU：存储器保护单元 (Memory Protection Unit)
MSIL：摩托车安全完整性等级 (Motorcycle Safety Integrity Level)
MUX：多路转换器 (MUltipleXer)
OEM：原始设备制造商（主机厂） (Original Equipment Manufacturer)
OS：操作系统 (Operating System)
OV：过压 (Over Voltage)
PAL：可编程阵列逻辑 (Programmable Array Logic)
PE：处理要素 (Processing Element)
PLD：可编程逻辑设备 (Programmable Logic Device)
PLL：锁相环 (Phase Locked Loop)
PMHF：随机硬件失效概率度量 (Probabilistic Metric for random Hardware Failures)

PoF：失效物理学 (Physics of Failure)
PPAP：生产件批准程序 (Production Part Approval Process)
PTO：动力输出装置 (Power Take-Off)
QM：质量管理 (Quality Management)
RAM：随机存储器 (Random Access Memory)
RF：残余故障 (Residual Fault)
RFQ：报价需求 (Request For Quotation)
ROM：只读存储器 (Read Only Memory)
RTL：寄存器传输级 (Register Transfer Level)
SEB：单粒子烧毁 (Single Event Burnout)
SEE：单粒子效应 (Single Event Effect)
SEGR：单粒子栅穿 (Single Event Gate Rupture)
SEooC：独立于环境的安全要素 (Safety Element out of Context)
SET：单粒子瞬态 (Single Event Transient)
SEU：单粒子翻转 (Single Event Upset)
SG：安全目标 (Safety Goal)
SMPS：开关模式电源 (Switched Mode Power Supply)
SoC：片上系统 (System on Chip)
SOP：量产 (Start Of Production)
SPFM：单点故障度量 (Single-Point Fault Metric)
SPI：串行外设接口 (Serial Peripheral Interface)
SW：软件 (SoftWare)
T&B：卡车,客车,挂车和半挂车 (Trucks, Buses, trailers and semi-trailers)
TCL ：工具置信度水平 (Tool Confidence Level)
TD ：工具错误探测 (Tool error Detection)
TI： 工具影响 (Tool Impact)
UML：统一建模语言 (Unified Modeling Language)
UV：欠压 (Under Voltage)
XML：可扩展标记语言 (eXtensible Markup Language)
SOTIF：预期功能安全（safety of the intended functionality ）

参 考 文 献

[1] ISO 3779, Road vehicles — Vehicle identification number (VIN) — Content and structure

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

[3] ISO 26262-2:2018, Road vehicles — Functional safety — Part 2: Management of functional safety

[4] ISO 26262-3:2018, Road vehicles — Functional safety — Part 3: Concept phase

[5] ISO 26262-4:2018, Road vehicles — Functional safety — Part 4: Product development at the system level

[6] ISO 26262-5:2018, Road vehicles — Functional safety — Part 5: Product development at the hardware level

[7] ISO 26262-6:2018, Road vehicles — Functional safety — Part 6: Product development at the software level

[8] ISO 26262-7:2018, Road vehicles — Functional safety — Part 7: Production, operation, service and decommissioning

[9] ISO 26262-8:2018, Road vehicles — Functional safety — Part 8: Supporting processes

[10] ISO 26262-9:2018, Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses

[11] ISO 26262-10:2018, Road vehicles — Functional safety — Part 10: Guideline on ISO 26262

[12] ISO 26262-11:2018, Road vehicles — Functional safety — Part 11: Guideline on application of ISO26262 to semiconductors

[13] ISO 26262-12:2018, Road vehicles — Functional safety — Part 12: Adaptation of ISO 26262 for motorcycles

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

[15] ECE/TRANS/WP .29/78/Rev.3+Amend.1 (Consolidated Resolution on the Construction of Vehicles (R.E.3))

[16] TRANS/WP. 29/1045+Amend.1&2

[17] SAE J1211, Physics of Failure methodology

[18] GB/T 3730.1 汽车和挂车类型的术语和定义

[19] ISO 9000:2015, Quality management systems — F

索　引

汉语拼音索引

D

F

G

H

J

K

L

M

O

P

Q

R

S

T

W

X

Y

Z

英文对应索引词

A

B

C

D

L

M

N

O

P

Q

R

S

T

U

V

W