ICS 43.040
T 35

中华人民共和国国家标准

GB/T 34590.1—2017

道路车辆　功能安全
第1部分:术语

Road vehicles—Functional safety—
Part 1: Vocabulary

(ISO 26262-1:2011, 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 …… Ⅰ
引言 …… Ⅲ
1　范围 …… 1
2　术语和定义 …… 1
3　缩略语 …… 15
参考文献 …… 17
索引 …… 18

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1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 26262-1:2011《道路车辆　功能安全　第1部分：术语》。

本部分与ISO 26262-1:2011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”；

——2.3　架构　architecture，修改原文中的functions(功能)为requirements(要求)，因为术语“分配”是指将要求指定给架构要素，而不是功能；

——2.32　要素　element，修改原文中的定义内容，明确要素所包含的范围；

——2.55　硬件元器件　hardware part，修改原文中的定义并增加示例内容，便于理解；

——2.66　初始的ASIL等级　initial ASIL，修改原文中的定义内容，ASIL等级是危害分析和风险评估得出的；

——2.69　相关项　item，修改原文中的定义内容，使其定义完整化；

——2.76　多点失效　multiple-point failure，删除原文中的注释，该注释导致过定义和重复定义；

——2.86　乘用车　passenger car，修改原文中的定义内容，与GB 7258—2012《机动车运行安全技术条件》中的定义保持一致；

——2.110　安全措施　safety measure，将原文中的注1内容修改为示例；

——2.117　半形式记法　semi-formal notation，修改原文中的示例内容，SADT指代Structured Analysis and Design Techniques的缩写，而非原文的System Analysis and Design Techniques；

——2.126　特殊用途车辆　special-purpose vehicle，删除原文中的注；

——2.138　验证评审　verification review，修改原文注释2中的内容，明确验证评审的目的。

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、上海海拉电子有限公

司、舍弗勒投资(中国)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、北京兴科迪科技有限公司、联合汽车电子有限公司、大陆汽车投资(上海)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。

本部分参加起草单位:湖南中车时代电动汽车股份有限公司、上汽大众汽车有限公司、郑州宇通客车股份有限公司、东软集团股份有限公司、宁德时代新能源科技有限公司。

本部分主要起草人:李波、尚世亮、薛剑波、蒋军、童菲、曲元宁、杨虎、张立君、史晓密、明月、还宏生、付越、邓湘鸿、范嘉睿、冯亚军、付艳玲、张红霞、李琴、易茂明、张乐敏、卢长军、李春林、邱冬。

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 第 6 章。

图 1　GB/T 34590—2017 概览

道路车辆　功能安全
第1部分:术语

1　范围

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

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、自适应巡航控制系统)有专用的功能性能标准。

2　术语和定义

2.1

分配　allocation

将要求指定给架构**要素**(2.32)。

注:目的不是将一个不可分割的要求分割成多个要求。从一个不可分割的**系统**(2.129)层面的要求到多个较低层面的不可分割的要求的追溯是允许的。

2.2

异常　anomaly

与预期(例如,基于要求、规范、设计文档、用户文档、标准或者经验的预期)偏离的情况。

注:异常可在除**评审**(2.98)、**测试**(2.134)、分析、编译、**组件**(2.15)的使用、或适用文档的使用等过程中被发现,也可在过程中被发现。

2.3

架构　architecture

相关项(2.69)、功能、**系统**(2.129)或**要素**(2.32)的结构的表征,用于识别结构模块及其边界和接口,并包括硬件和软件要素的要求**分配**(2.1)。

2.4

评估　assessment

对**相关项**(2.69)或**要素**(2.32)的特性的检查。

注:执行评估的一方或多方的**独立性**(2.61)水平与每一次评估相关。

2.5

审核　audit

对已实施流程的检查。

2.6

汽车安全完整性等级　automotive safety integrity level;ASIL

四个等级中的每一个等级定义了GB/T 34590中**相关项**(2.69)或**要素**(2.32)的必要的要求和**安全措施**(2.110),以避免不合理的**残余风险**(2.97),D代表最高严格等级,A代表最低严格等级。

2.7

ASIL分解　ASIL decomposition

将安全要求冗余地分配给充分独立的**要素**(2.32),目的是降低分配给相关要素的冗余安全要求的**ASIL**(2.6)等级。

2.8

可用性　availability

在特定时间或给定的期间内,假设所需的外部资源是可用的,在给定条件下,产品处于执行所需功能的状态的能力。

2.9

基线　baseline

在配置管理下,通过变更管理流程,作为进一步开发的基础的一组单一或多个工作成果、**相关项**(2.69)或**要素**(2.32)的版本。

注:参见GB/T 34590.8—2017第8章。

2.10

分支覆盖率　branch coverage

已执行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**(2.127)。

注2:一个if语句总有两个分支即条件真和条件假,其独立于一个else语句。

2.11

标定数据　calibration data

在开发过程中,软件编译后将要应用的数据。

示例:参数(例如,低怠速值、发动机特性曲线图);车辆特定参数(适应值)(例如,节气门极限停止);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。

2.12

候选项　candidate

与已经发布并在运行的相关项或要素的定义和使用条件相同、或具有高度通用性的**相关项**(2.69)或**要素**(2.32)。

注:该定义适用于**在用证明**(2.90)中使用的候选项。

2.13

级联失效　cascading failure

同一个**相关项**(2.69)中,一个**要素**(2.32)的**失效**(2.39)引起另一个或多个要素的失效。

注:级联失效是非**共因失效**(2.14)的**相关失效**(2.22),见图2,失效A。

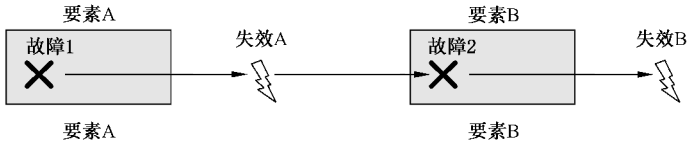

图2　级联失效

2.14

共因失效　common cause failure;CCF

一个**相关项**(2.69)中,由一个单一特定事件或根本原因引起的两个或多个**要素**(2.32)的**失效**

(2.39)。

注：共因失效是非**级联失效**(2.13)的**相关失效**(2.22)。见图 3。

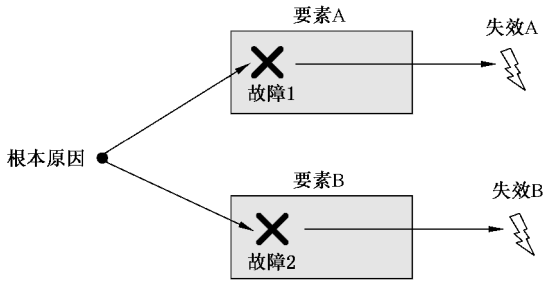

图 3　共因失效

2.15

组件　component

逻辑上和技术上可分的非**系统**(2.129)层面的**要素**(2.32)，由一个以上**硬件元器件**(2.55)或一个到多个**软件单元**(2.125)组成。

注：组件是系统的一部分。

2.16

配置数据　configuration data

在软件构建过程中分配的、控制软件构建过程的数据。

示例：预处理器配置指令；软件构建脚本(例如，XML 配置文件)。

注 1：配置数据不可包含执行代码或注释代码。

注 2：配置数据控制软件的构建，仅由配置数据选择的代码或数据可以包含在执行代码中。

2.17

认可措施　confirmation measure

与**功能安全**(2.51)相关的**认可评审**(2.18)、**审核**(2.5) 或**评估**(2.4)。

2.18

认可评审　confirmation review

由具备所需**独立性**(2.61)级别的评审员，对满足 GB/T 34590 要求的工作成果的确认。

注 1：GB/T 34590.2—2017 提供了一个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。

2.19

可控性　controllability

通过所涉及人员的及时反应，也可能通过**外部措施**(2.38)的支持，避免特定的**伤害**(2.56)或损伤的能力。

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**(2.58)中的参数 C 表示可控性的可能性。

2.20

专用措施　dedicated measure

在评估违背**安全目标**(2.108)的可能性的过程中，用于确保所声明的**失效率**(2.41)的措施。

示例：设计特性，诸如**硬件元器件**(2.55)过度设计(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有关的**失效模式**(2.40)的发生**风险**(2.99)；老化测试；专用的控制计划。

2.21

降级　degradation

通过设计提供**失效**(2.39)发生后的**安全**(2.103)的策略。

注：降级可包含功能缩减，性能降低，或两者均降低。

2.22

相关失效　dependent failures

失效(2.39)同时或相继发生的概率不能表示为每个失效无条件发生概率的简单乘积的失效。

注 1：当 $P_{AB} \neq P_A \times P_B$，失效 A 和失效 B 可被定义为相关失效。

式中：

P_{AB}——失效 A 和失效 B 同时发生的概率；

P_A ——失效 A 发生的概率；

P_B ——失效 B 发生的概率。

注 2：相关失效包含**共因失效**(2.14)和**级联失效**(2.13)。

2.23

可探测的故障　detected fault

在规定的时间内，可通过防止**故障**(2.42)变成潜伏故障的**安全机制**(2.111)探测到的故障。

示例：可被**功能安全概念**(2.52)中定义的专门**安全机制**(2.111)[例如，探测到**错误**(2.36)并通过仪表盘上的报警装置通知驾驶员]探测到的故障。

2.24

开发接口协议　development interface agreement；DIA

客户与供应商之间的协议，该协议规定了双方在相关活动中各自承担的责任、应提供给对方的证据或工作成果。

2.25

诊断覆盖率　diagnostic coverage

硬件**要素**(2.32)**失效率**(2.41)中，由实施的**安全机制**(2.111)探测或控制的失效率所占的比例。

注 1：诊断覆盖率可通过在硬件要素中可能发生的**残余故障**(2.96)或潜伏的**多点故障**(2.77)进行评估。

注 2：该定义可按照 GB/T 34590.5—2017 中给出的等式表述。

注 3：可考虑在**架构**(2.3)中的不同层面所实施的安全机制。

2.26

诊断测试时间间隔　diagnostic test interval

通过**安全机制**(2.111)执行在线诊断测试的时间间隔。

2.27

分布式开发　distributed development

在客户和供应商之间分配整个**相关项**(2.69)、**要素**(2.32)或子系统开发责任的相关项或要素的开发。

注：客户和供应商是合作方中的角色。

2.28

多样性　diversity

以**独立性**(2.61)为目标，满足相同要求的不同解决方案。

示例：多样的程序；多样的硬件。

注：多样性不保证独立性，但是可避免特定类型的**共因失效**(2.14)。

2.29

双点失效　dual-point failure

由两个独立**故障**(2.42)的组合引起，且直接导致违背**安全目标**(2.108)的**失效**(2.39)。

注 1：双点失效是 2 阶的**多点失效**(2.76)。

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**(2.113)，而另一个故障影响到相关的达到或保持**安全状态**(2.102)的**安全机制**(2.111)而导致的失效。

注 3：对于直接违背安全目标的双点失效，两个独立故障的发生是必要的，即不认为导致违背安全目标的**残余故障**(2.96)和**安全故障**(2.101)的组合为双点失效，因为残余故障可以直接导致违背安全目标，与第二个独立故障是否发生没有关系。

2.30

双点故障　dual-point fault

与另一个独立故障组合而导致**双点失效**(2.29)的一个**故障**(2.42)。

注 1：只有在明确双点失效后才能识别出一个双点故障，例如，通过故障树的割集分析。

注 2：参见**多点故障**(2.77)。

2.31

电子电气系统　electrical and/or electronic system

电子/电气**要素**(2.32)构成的**系统**(2.129)，包括可编程电子要素。

示例：电源；传感器或其他输入装置；通讯路径；执行器或其他输出装置。

2.32

要素　element

系统(2.129)、**组件**(2.15)(硬件、软件)、**硬件元器件**(2.55)或**软件单元**(2.125)。

2.33

嵌入式软件　embedded software

在一个处理**要素**(2.32)上运行的充分集成的软件。

注：该处理要素通常是一个微控制器、一个现场可编程门阵列(FPGA)或者专用集成电路(ASIC)，但是它也可以是一个更复杂的**组件**(2.15)或子系统。

2.34

紧急运行　emergency operation

按**报警和降级概念**(2.140)中所定义的，实现由**故障**(2.42)状态过渡到**安全状态**(2.102)的降级功能。

2.35

紧急运行时间间隔　emergency operation interval

用于支持**报警和降级概念**(2.140)所需要的**紧急运行**(2.34)的特定时间间隔。

注：紧急运行是**报警和降级概念**(2.140)的一部分。

2.36

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 1：错误可由未预见的工作条件引起或由所考虑的**系统**(2.129)、子系统或**组件**(2.15)的内部**故障**(2.42) 引起。

注 2：故障可表现为所考虑**要素**(2.32)内的错误，该错误可最终导致**失效**(2.39)。

2.37

暴露　exposure

处于某**运行场景**(2.83)的状态，在该运行场景下，如果发生所分析的**失效模式**(2.40)，可能导致危害。

2.38

外部措施　external measure

独立于且不同于**相关项**(2.69)的措施，以减少或减轻由相关项导致的**风险**(2.99)。

2.39

失效　failure

要素(2.32)按要求执行功能的能力的终止。

注：不正确的规范是失效的来源。

2.40

失效模式　failure mode

要素(2.32)或**相关项**(2.69)失效的方式。

2.41

失效率　failure rate

硬件**要素**(2.32)的**失效**(2.39)概率密度除以幸存概率。

注：失效率被假设为常数且通常用“λ”表示。

2.42

故障　fault

可引起**要素**(2.32)或**相关项**(2.69)失效的异常情况。

注 1：考虑**永久性故障**(2.88)、间歇性故障和**瞬态故障**(2.135)(尤其软错误)。

注 2：间歇性故障一再发生，然后消失。当一个**组件**(2.15)处于损坏的边缘时，或者例如由于开关的问题，间歇性故障可能会发生。某些**系统性故障**(2.131)(例如时序裕度不足)也可能导致间歇性故障。

2.43

故障模型　fault model

由**故障**(2.42)导致的**失效模式**(2.40)的表现。

注：故障模型一般基于现场经验或可靠性手册。

2.44

故障响应时间　fault reaction time

从**故障**(2.42)探测到进入**安全状态**(2.102)的时间间隔。

参见图 4。

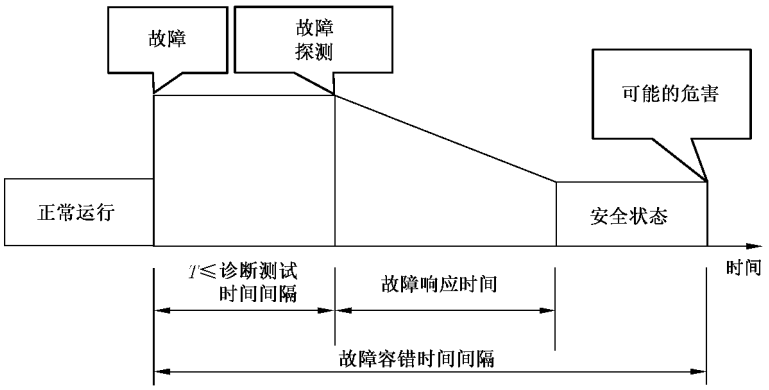

图 4　故障响应时间和容错时间间隔

2.45

故障容错时间间隔　fault tolerant time interval

在**危害事件**(2.59)发生前，**系统**(2.129)中一个或多个**故障**(2.42)可存在的时间间隔。

2.46

现场数据　field data

从**相关项**(2.69)或**要素**(2.32)的使用中获得的数据，包含累加的运行时间、所有的**失效**(2.39)和服务中的异常。

注：现场数据通常来自客户的使用。

2.47

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)。

2.48

形式验证　formal verification

基于以**形式记法**(2.47)定义的**系统**(2.129)所要求的行为，验证系统正确性的方法。

2.49

免于干扰　freedom from interference

两个或两个以上的**要素**(2.32)之间，不存在可能导致违背安全要求的**级联失效**(2.13)。

示例 1：如果要素 2 的**失效**(2.39)不会导致要素 1 失效，则要素 1 免于要素 2 的干扰。

示例 2：如果要素 3 的失效导致要素 4 失效，则要素 3 干扰要素 4。

2.50

功能概念　functional concept

为了实现预期的表现，对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**(2.89)开发的。

2.51

功能安全　functional safety

不存在由**电子电气系统**(2.31)的**功能异常表现**(2.73)引起的**危害**(2.57)而导致**不合理的风险**(2.136)。

2.52

功能安全概念　functional safety concept

为了实现**安全目标**(2.108)，定义**功能安全要求**(2.53)及相关信息，并将要求**分配**(2.1)到架构**要素**(2.32)上，以及定义要素之间的必要交互。

2.53

功能安全要求　functional safety requirement

定义了独立于具体实现方式的**安全**(2.103)行为，或独立于具体实现方式的**安全措施**(2.110)，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**电子电气系统**(2.31)或基于**其他技术**(2.84)的安全相关**系统**(2.129)所执行的安全要求，目的是通过考虑确定的**危害事件**(2.59)，使**相关项**(2.69)达到或保持在**安全状态**(2.102)。

注 2：功能安全要求的定义可独立于产品开发概念**阶段**(2.89)中使用的技术。

注 3：安全相关的属性包括 **ASIL 等级**(2.6)信息。

2.54

硬件架构度量　hardware architectural metrics

用于**评估**(2.4)硬件**架构**(2.3)**安全**(2.103)有效性的度量。

注：**单点故障**(2.122)度量和**潜伏故障**(2.71)度量都是硬件架构度量。

2.55

硬件元器件　hardware part

硬件**组件**(2.15)的一部分。

示例：微控制器的 CPU、电阻、电容。

2.56

伤害　harm

对人身健康的物理损害或破坏。

2.57

危害　hazard

由**相关项**(2.69)的**功能异常表现**(2.73)而导致的**伤害**(2.56)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的潜在来源。

2.58

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

为了避免**不合理的风险**(2.136)，对**相关项**(2.69)的**危害事件**(2.59)进行识别和归类的方法以及定义防止和减轻相关危害的**安全目标**(2.108)和 **ASIL 等级**(2.6)的方法。

2.59

危害事件　hazardous event

危害(2.57)和**运行场景**(2.83)的组合。

2.60

同构冗余　homogeneous redundancy

对一个要求的多个完全相同的实现。

2.61

独立性　independence

不存在会导致违安全要求的两个或多个**要素**(2.32)间的**相关失效**(2.22),或从组织上分隔执行活动的各方。

注:根据定义,**ASIL 分解**(2.7)或**认可措施**(2.17)包括独立性要求。

2.62

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**(2.39)。

2.63

非形式记法　informal notation

非完整语法定义的描述方法。

示例:以图形或图表的方式描述。

注:不完整的语法定义指语义学也没有完整的定义。

2.64

非形式验证　informal verification

不属于半形式或**形式验证**(2.48)的**验证**(2.137)方法。

示例:设计**评审**(2.98);建模评审。

2.65

继承　inheritcunce

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。

2.66

初始的 ASIL 等级　initial ASIL

由**危害分析和风险评估**(2.58)得出的或由先前 **ASIL 分解**(2.7)得出的 **ASIL**(2.6)等级。

注:初始的 ASIL 等级是 **ASIL 分解**(2.7)或 ASIL 等级进一步分解的起点。

2.67

检查　inspection

为发现异常而依据一个正式的流程对工作成果进行的考查。

注 1:检查是**验证**(2.137)的一种方式。

注 2:检查不同于**测试**(2.134),检查通常不包括对**相关项**(2.69)或**要素**(2.32)的操作。

注 3:发现的异常经常通过重做予以解决,随后对重做的成果重新检查。

注 4:一项正规的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**(2.98)。

2.68

预期功能　intended functionality

为**相关项**(2.69)、**系统**(2.129)或**要素**(2.32)定义的不包含**安全机制**(2.111)的行为。

2.69

相关项　item

适用于 GB/T 34590—2017,实现车辆层面功能或部分功能的**系统**(2.129)或系统组。

2.70

相关项开发　item development

实现**相关项**(2.69)的完整过程。

2.71

潜伏故障　latent fault

未被**安全机制**(2.111)探测到且在**多点故障探测时间间隔**(2.78)内未被驾驶员感知的**多点故障**(2.77)。

2.72

生命周期　ifecycle

相关项(2.69)从概念到报废的全部**阶段**(2.89)。

2.73

功能异常表现　malfunctioning behaviour

失效(2.39)或与设计意图相悖的**相关项**(2.69)非预期表现。

2.74

基于模型的开发　model-based development

一种使用模型描述**要素**(2.32)功能行为的开发。

注:根据模型使用的层次,该模型可用于仿真和代码生成。

2.75

修改　modification

经过授权的**相关项**(2.69)的变更。

注 1: 在 GB/T 34590 中,为剪裁**生命周期**(2.72)对复用的部分使用"修改"。

注 2: 变更用于**相关项**(2.69)的生命周期过程中,而修改用于由已有的相关项生成新的相关项。

2.76

多点失效　multiple-point failure

由几个独立的**故障**(2.42)组合引发,直接导致违背**安全目标**(2.108)的**失效**(2.39)。

2.77

多点故障　multiple-point fault

与其他独立故障组合而导致一个**多点失效**(2.76)的单独**故障**(2.42)。

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

2.78

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

在可导致一个**多点失效**(2.76)前,将**多点故障**(2.77)探测出来的时间间隔。

2.79

新开发　new development

开发一个具有先前未定义功能的**相关项**(2.69)的过程,或开发一个对现有功能的新的实现方式的相关项的过程,或两者都有。

2.80

非功能性危害　non-functional hazard

由**电子电气系统**(2.31)、基于**其他技术**(2.84)的安全相关**系统**(2.129)或**外部措施**(2.38)的不正确功能之外的其他因素导致的**危害**(2.57)。

2.81

运行模式　operating mode

相关项(2.69)或**要素**(2.32)的可感知的功能状态。

示例:**系统**(2.129)关闭;系统激活;系统非激活;降级运行;**紧急运行**(2.34)。

2.82

运行时间　operating time

相关项(2.69)或**要素**(2.32)工作的累积时间。

2.83

运行场景　operational situation

在车辆生命周期中可发生的场景。

示例: 行驶;驻车;维护。

2.84

其他技术　other technology

不同于 GB/T 34590 规定范围内的电子电气技术的技术。

示例：机械技术；液压技术。

注：其他技术可在安全要求(参见 GB/T 34590.3—2017 和 GB/T 34590.4—2017)**分配**(2.1)过程中、在**功能安全概念**(2.52)(参见 GB/T 34590.3—2017 第 8 章和图 2)中定义，或作为**外部措施**(2.38)被考虑。

2.85

分区　partitioning

为实现某种设计，而对功能或**要素**(2.32)的分隔。

注：分区可用于抑制**故障**(2.42)以避免**级联失效**(2.13)。为实现分区设计要素间的**免于干扰**(2.49)，可引入额外的非功能性要求。

2.86

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。

2.87

可感知的故障　perceived fault

在规定的时间间隔内由驾驶员推断出的**故障**(2.42)。

示例：故障可直接通过明显的**系统**(2.129)表现或性能的限制而感知。

2.88

永久性故障　permanent fault

发生并持续直到被移除或修复的**故障**(2.42)。

注：直流(DC)故障，例如卡滞故障和桥接故障是永久性故障。**系统性故障**(2.131)主要表现为永久性故障。

2.89

阶段　phase

在 GB/T 34590 特定部分中定义的安全**生命周期**(2.72)的阶段。

注：GB/T 34590 中的阶段在特定的部分中定义，例如：GB/T 34590.3—2017、GB/T 34590.4—2017、GB/T 34590.5—2017、GB/T 34590.6—2017 和 GB/T 34590.7—2017 分别定义了阶段：

——概念；

——系统层面产品开发；

——硬件层面产品开发；

——软件层面产品开发；

——生产和运行。

2.90

在用证明　proven in use argument

通过分析**候选项**(2.12)应用的**现场数据**(2.46)，得出该候选项会影响**相关项**(2.69)**安全目标**(2.108)的任何**失效**(2.39)的可能性满足适当 **ASIL**(2.6)等级要求的证据。

2.91

在用证明置信度　proven in use credit

通过**在用证明**(2.90)对一组给定的**生命周期**(2.72)**子阶段**(2.128)及相应工作成果的替代。

2.92

随机硬件失效　random hardware failure

在硬件**要素**(2.32)的生命周期中，非预期发生并服从概率分布的**失效**(2.39)。

注：可在合理的精度内预测随机硬件**失效率**(2.41)。

2.93

合理可预见的事件　reasonably foreseeable event

技术上可能并具有置信度或可测发生率的事件。

2.94

冗余　redundancy

对**要素**(2.32)而言,存在除了足够实现其所需功能或表示信息的方法之外的方法。

注:GB/T 34590 中的冗余用于实现**安全目标**(2.108)或特定安全要求,或者表示安全相关信息。

示例 1:复制的功能**组件**(2.15)是冗余的一个实例,其目的是增加**可用性**(2.8)或允许**故障**(2.42)检测。

示例 2:在表示安全相关信息的数据上增加奇偶校验位,是为允许故障检测提供了冗余。

2.95

回归策略　regression strategy

一种用于验证一个已实施的变更不会影响到**相关项**(2.69)或**要素**(2.32)中未变更的、已存在的和先前验证过的部件或特性的策略。

2.96

残余故障　residual fault

发生在硬件**要素**(2.32)中,能导致违背**安全目标**(2.108)且未被**安全机制**(2.111)覆盖的**故障**(2.42)部分。

注:假设硬件要素的安全机制仅覆盖了该故障的一部分。

示例:如果对一个**失效模式**(2.40)声明了低覆盖率(60%),则该失效模式的其余 40%就是残余故障。

2.97

残余风险　residual risk

实施**安全措施**(2.110)后剩余的**风险**(2.100)。

2.98

评审　review

根据评审目的,为实现预期的工作成果目标而对工作成果进行的检查。

注:可用核对表支持评审。

2.99

风险　risk

伤害(2.56)发生的概率及其**严重度**(2.120)的组合。

2.100

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;

——在 GB/T 34590 上下文中,鲁棒性是在边界范围内提供安全行为的能力。

2.101

安全故障　safe fault

不会显著增加违背**安全目标**(2.108)的概率的**故障**(2.42)。

注 1:如 GB/T 34590.5—2017 附录 B 所示,非安全相关和**安全相关要素**(2.113)都可能有安全故障。

注 2:**单点故障**(2.122)、**残余故障**(2.96)和双点故障不视为安全故障。

注 3:除非在安全概念中表明具有相关性,否则,大于 2 阶的**多点故障**(2.77)可被认为是安全故障。

2.102

安全状态　safe state

没有不合理**风险**(2.99)的**相关项**(2.69)的**运行模式**(2.81)。

示例:预期运行模式;降级运行模式;关闭模式。

2.103

安全　safety

没有**不合理的风险**(2.136)。

2.104

安全活动　safety activity

在安全**生命周期**(2.72)的一个或多个**子阶段**(2.128)进行的活动。

2.105

安全架构　safety architecture

用于实现安全要求的一系列**要素**(2.32)以及它们之间的交互。

2.106

安全档案　safety case

将收集了开发过程中安全活动的工作成果作为证据,证明完整地实现了**相关项**(2.69)的安全要求。

注:安全档案可以扩展到包括 GB/T 34590 范围以外的**安全**(2.103)问题。

2.107

安全文化　safety culture

组织内部用于支持安全相关**系统**(2.129)的开发、生产、运行、服务和报废的政策和策略。

注:参见 GB/T 34590.2—2017 附录 B。

2.108

安全目标　safety goal

最高层面的安全要求,是**危害分析和风险评估**(2.58)的结果。

注:一个安全目标可能与几种**危害**(2.57)有关,几个安全目标可能与一种单一的危害有关。

2.109

安全经理　safety manager

在**相关项**(2.69)的开发中,负责**功能安全**(2.51)管理的人员。

2.110

安全措施　safety measure

用以避免或控制**系统性失效**(2.130)、探测**随机硬件失效**(2.92),控制随机硬件失效或减轻它们的有害影响的活动或技术解决方案。

示例:FMEA 和未使用全局变量的软件。

注:安全措施包括**安全机制**(2.111)。

2.111

安全机制　safety mechanism

为了达到或保持某种**安全状态**(2.102),由电子电气系统的功能或**要素**(2.32)或**其他技术**(2.84)来实施的技术解决方案,以探测**故障**(2.42)、控制**失效**(2.39)。

注 1:在**相关项**(2.69)中实施安全机制以避免故障导致**单点失效**(2.121)或减少残余失效,并防止故障潜伏。

注 2:如同在**功能安全概念**(2.52)中定义的,安全机制也可是:

a)　能够使相关项过渡到或保持在安全状态;或

b)　能够向驾驶员发出提醒以控制**失效**(2.39)的影响。

2.112

安全计划　safety plan

管理和指导开展项目**安全活动**(2.104)的计划,包括日期、节点、任务、可交付成果、职责和资源。

2.113

安全相关要素　safety-related element

潜在的有助于违背或实现**安全目标**(2.108)的**要素**(2.32)。

注:如果失效-安全要素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。

2.114

安全相关功能　safety-related function

潜在导致违背**安全目标**(2.108)的功能。

2.115

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

相关项(2.69)、**要素**(2.32)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**(2.51)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或要素的开发**阶段**(2.89)中得出。

示例：温度范围、有效期限、紧固力矩、生产公差、配置。

2.116

安全确认　safety validation

基于检查和测试,确认充分实现了**安全目标**(2.108)。

注：GB/T 34590.4—2017 提供了合适的确认方法。

2.117

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)。

2.118

半形式验证　semi-formal verification

基于**半形式记法**(2.117)的**验证**(2.137)。

示例：使用由半形式模型生成的测试向量测试**系统**(2.129)表现与模型是否匹配。

2.119

服务说明　service note

在执行**相关项**(2.69)的维护流程时所考虑的**安全**(2.103)信息文档。

示例：**安全相关的特殊特性**(2.115);所需的安全操作。

2.120

严重度　severity

对可能发生在潜在危害场景中的一个或多个人员的**伤害**(2.56)程度的预估。

注：在**危害分析和风险评估**(2.58)中参数“S”代表潜在伤害的严重度。

2.121

单点失效　single-point failure

由**单点故障**(2.122)引起并直接导致违背**安全目标**(2.108)的**失效**(2.39)。

注 1：单点失效等同于**诊断覆盖率**(2.25)为 0%的**要素**(2.32)的残余**失效**。

注 2：如果为一个硬件要素(例如,微控制器的看门狗)定义了至少一个**安全机制**(2.111),那么,所考虑的硬件要素的**故障**(2.42)都不是**单点故障**(2.122)。

2.122

单点故障　single-point fault

要素(2.32)中没有被**安全机制**(2.111)所覆盖,并且直接导致违背**安全目标**(2.108)的**故障**(2.42)。

注：参见**单点失效**(2.121)。

2.123

软件组件　software component

一个或多个**软件单元**(2.125)。

2.124

软件工具　software tool

在开发**相关项**(2.69)或**要素**(2.32)中所用到的计算机程序。

2.125

软件单元　software unit

软件**架构**(2.3)中的最低层级且可被孤立**测试**(2.134)的**软件组件**(2.123)。

2.126

特殊用途车辆　special-purpose vehicle

由于执行一种专业的或娱乐的功能而需要特殊的车身布置和设备的车辆。

示例：旅居车、装甲车、救护车、殡仪车、拖挂房车、移动吊车。

2.127

语句覆盖率　statement coverage

软件中已执行语句所占的百分比。

2.128

子阶段　subphase

安全**生命周期**(2.72)中某个阶段的细分且其在 GB/T 34590 中有明确的章条描述。

示例：**危害分析和风险评估**(2.58)是安全生命周期的子阶段，在 GB/T 34590.3—2017 第 7 章中进行了描述。

2.129

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**要素**(2.32)。

注 1：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。

注 2：系统中的要素也可能是另一个系统。

2.130

系统性失效　systematic failure

以确定的方式与某个原因相关的**失效**(2.39)，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。

2.131

系统性故障　systematic fault

以确定的方式显现**失效**(2.39)的**故障**(2.42)，只有通过使用流程或设计措施才有可能防止其发生。

2.132

技术安全概念　technical safety concept

技术安全要求(2.133)的定义和为了能够通过系统设计实现功能而将技术安全要求向**系统**(2.129)**要素**(2.32)的**分配**(2.1)。

2.133

技术安全要求　technical safety requirement

为实现相关的**功能安全要求**(2.53)而得出的要求。

注：得出的要求包括减轻失效所需的要求。

2.134

测试　testing

通过计划、准备、运行或演练**相关项**(2.69)或**要素**(2.32)，以验证其满足所定义的要求、探测其**异常**(2.2)、对其行为建立信心的过程。

2.135

瞬态故障　transient fault

发生一次且随后消失的**故障**(2.42)。

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

2.136

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**(2.99)。

2.137

验证　verification

确定某个**阶段**(2.89)或**子阶段**(2.128)的要求是否完整且正确的定义或实现。

2.138

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**(2.137)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**(2.69)或**要素**(2.32)的技术正确性和完整性。

示例：技术**评审**(2.98)、**走查**(2.139)、**检查**(2.67)。

2.139

走查　walk-through

为了发现异常，对**工作成果**(2.142)的系统性检查。

注 1：走查是**验证**(2.137)的一种方法。

注 2：走查与**测试**(2.134)的区别在于，走查通常不涉及**相关项**(2.69)或**要素**(2.32)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进行走查。

示例：在走查过程中，开发者向一个或多个评估员逐步的阐述工作成果。其目的是建立对工作成果的共同理解和识别工作成果中的异常。**检查**(2.67)和走查均属于同级**评审**(2.98)，其中走查的严格性弱于检查。

2.140

报警和降级概念　warning and degradation concept

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**(2.102)的规范。

2.141

值得信赖的　well-trusted

先前使用过且没有已知的**安全**(2.103)**异常**(2.2)。

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**(2.15)。

2.142

工作成果　work product

GB/T 34590 中一个或多个相关要求的结果。

注：包含工作成果的完整信息的独立文档，或工作成果的完整信息的参考列表。

3　缩略语

下列缩略语适用于本文件。

ACC：自适应巡航系统(Adaptive Cruise Control)

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

AIS：简明损伤定级(Abbreviated Injury Scale)

ASIC：专用集成芯片(Application-Specific Integrated Circuit)

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

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)

COTS：商业现成产品(Commercial Off The Shelf)

CPU：中央处理单元(Central Processing Unit)

CRC：循环冗余检验(Cyclic Redundancy Check)

DC：诊断覆盖率(Diagnostic Coverage)

d.c.：直流电路(Direct Current)

DIA：开发接口协议(Development Interface Agreement)
DSC：动态稳定性控制(Dynamic Stability Control)
ECU：电控单元(Electronic Control Unit)
EDC：错误探测和纠错(Error Detection and Correction)
E/E：电子电气系统 (Electrical and/or Electronic system)
EMC：电磁兼容性(Electromagnetic Compatibility)
EMI：电磁干扰(Electromagnetic Interference)
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)
FPGA：可编程门阵列(Field Programmable Gate Array)
FIT：失效率(Failures In Time)
FMEA：失效模式与影响分析(Failure Mode and Effects Analysis)
FTA：故障树分析(Fault Tree Analysis)
HAZOP：危害与可操作性分析(HAZard and Operability analysis)
HSI：软硬件接口(Hardware-Software Interface)
HW：硬件(Hardware)
H&R：危害分析和风险评估(Hazard analysis and Risk assessment)
IC：集成电路(Integrated Circuit)
I/O：输入/输出(Input - Output)
MC/DC：修订的条件/判定覆盖(Modified Condition/Decision Coverage)
MMU：存储器管理单元(Memory Management Unit)
MPU：存储器保护单元(Memory Protection Unit)
MUX：多路转换器(MUltipleXer)
OS：操作系统(Operating System)
PLD：可编程逻辑设备(Programmable Logic Device)
PMHF：随机硬件失效概率度量(Probabilistic Metric for random Hardware Failures)
QM：质量管理(Quality Management)
RAM：随机存储器(Random Access Memory)
ROM：只读存储器(Read Only Memory)
RFQ：报价需求(Request For Quotation)
SIL：安全完整性等级(Safety Integrity Level)
SOP：生产启动(Start Of Production)
SRS：系统需求规范(System Requirements Specification)
SW：软件(Software)
UML：统一建模语言(Unified Modeling Language)
V&V：验证和确认(Verification and Validation)
XML：可扩展标记语言(eXtensible Markup Language)

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] ISO/TS 16949 Quality management systems—Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations

[3] ISO 26262-2:2011 Road vehicles—Functional safety—Part 2: Management of functional safety

[4] ISO 26262-3:2011 Road vehicles—Functional safety—Part 3: Concept phase

[5] ISO 26262-4:2011 Road vehicles—Functional safety—Part 4: Product development at the system level

[6] ISO 26262-5:2011 Road vehicles—Functional safety—Part 5: Product development at the hardware level

[7] ISO 26262-6:2011 Road vehicles—Functional safety—Part 6: Product development at the software level

[8] ISO 26262-7:2011 Road vehicles—Functional safety—Part 7: Production and operation

[9] ISO 26262-8:2011 Road vehicles—Functional safety—Part 8: Supporting processes

[10] ISO 26262-9:2011 Road vehicles—Functional safety—Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses

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

索　引

汉语拼音索引

A

安全 …… 2.103
安全措施 …… 2.110
安全档案 …… 2.106
安全故障 …… 2.101
安全活动 …… 2.104
安全架构 …… 2.105
安全计划 …… 2.112
安全机制 …… 2.111
安全经理 …… 2.109
安全目标 …… 2.108
安全确认 …… 2.116
安全文化 …… 2.107
安全相关的特殊特性 …… 2.115
安全相关功能 …… 2.114
安全相关要素 …… 2.113
安全状态 …… 2.102

B

半形式记法 …… 2.117
半形式验证 …… 2.118
报警和降级概念 …… 2.140
暴露 …… 2.37
标定数据 …… 2.11
不合理的风险 …… 2.136

C

残余风险 …… 2.97
残余故障 …… 2.96
测试 …… 2.134
乘用车 …… 2.86
初始 ASIL 等级 …… 2.66
错误 …… 2.36

D

单点故障 …… 2.122
单点失效 …… 2.121
电子电气系统 …… 2.31
独立性 …… 2.61
多点故障 …… 2.77
多点故障探测时间间隔 …… 2.78
多点失效 …… 2.76
多样性 …… 2.28

F

非功能性危害 …… 2.80
分布式开发 …… 2.27
分配 …… 2.1
分区 …… 2.85
风险 …… 2.99
非相关失效 …… 2.62
非形式记法 …… 2.63
非形式验证 …… 2.64
分支覆盖率 …… 2.10
服务说明 …… 2.119

G

功能安全 …… 2.51
功能安全概念 …… 2.52
功能安全要求 …… 2.53
功能概念 …… 2.50
功能异常表现 …… 2.73
共因失效 …… 2.14
工作成果 …… 2.142
故障 …… 2.42
故障模型 …… 2.43
故障响应时间 …… 2.44

H

合理可预见的事件 …… 2.93
候选项 …… 2.12
回归策略 …… 2.95

J

继承 …… 2.65

级联失效 …… 2.13
技术安全概念 …… 2.132
技术安全要求 …… 2.133
基线 …… 2.9
基于模型的开发 …… 2.74
架构 …… 2.3
检查 …… 2.67
降级 …… 2.21
阶段 …… 2.89
紧急运行 …… 2.34
紧急运行时间间隔 …… 2.35

K

开发接口协议 …… 2.24
可感知的故障 …… 2.87
可控性 …… 2.19
可探测的故障 …… 2.23
可用性 …… 2.8

L

鲁棒性设计 …… 2.100

M

免于干扰 …… 2.49

P

配置数据 …… 2.16
评估 …… 2.4
评审 …… 2.98

Q

汽车安全完整性等级 …… 2.6
其他技术 …… 2.84
潜伏故障 …… 2.71
嵌入式软件 …… 2.33

R

认可措施 …… 2.17
认可评审 …… 2.18
容错时间间隔 …… 2.45
冗余 …… 2.94
软件单元 …… 2.125
软件工具 …… 2.124
软件组件 …… 2.123

S

伤害 …… 2.56
生命周期 …… 2.72
双点故障 …… 2.30
双点失效 …… 2.29
审核 …… 2.5
失效 …… 2.39
失效率 …… 2.41
失效模式 …… 2.40
瞬态故障 …… 2.135
随机硬件失效 …… 2.92

T

特殊用途车辆 …… 2.126
同构冗余 …… 2.60

W

外部措施 …… 2.38
危害 …… 2.57
危害分析和风险评估 …… 2.58
危害事件 …… 2.59

X

系统性故障 …… 2.131
系统性失效 …… 2.130
现场数据 …… 2.46
相关失效 …… 2.22
相关项 …… 2.69
相关项开发 …… 2.70
新开发 …… 2.79
形式记法 …… 2.47
形式验证 …… 2.48
修改 …… 2.75
系统 …… 2.129

Y

严重度 …… 2.120
验证 …… 2.137
验证评审 …… 2.138
要素 …… 2.32
异常 …… 2.2

硬件架构度量 …… 2.54
硬件元器件 …… 2.55
永久性故障 …… 2.88
语句覆盖率 …… 2.127
预期功能 …… 2.68
运行场景 …… 2.83
运行模式 …… 2.81
运行时间 …… 2.82
在用置信度 …… 2.91
诊断覆盖率 …… 2.25
诊断测试时间间隔 …… 2.26
值得信赖的 …… 2.141
专用措施 …… 2.20
子阶段 …… 2.128
走查 …… 2.139
组件 …… 2.15

Z

在用证明 …… 2.90
ASIL 分解 …… 2.7

英文对应词索引

A

allocation …… 2.1
anomaly …… 2.2
architectur …… 2.3
assessment …… 2.4
audit …… 2.5
automotive safety integrity level …… 2.6
ASIL decomposition …… 2.7
availability …… 2.8

B

baseline …… 2.9
branch coverage …… 2.10

C

calibration data …… 2.11
candidate …… 2.12
cascading failure …… 2.13
common cause failure …… 2.14
component …… 2.15
configuration data …… 2.16
confirmation measure …… 2.17
confirmation review …… 2.18
controllability …… 2.19

D

dedicated measure …… 2.20
degradation …… 2.21

dependent failures …… 2.22
detected fault …… 2.23
development interface agreement，DIA …… 2.24
diagnostic coverage …… 2.25
diagnostic test interval …… 2.26
distributed development …… 2.27
diversity …… 2.28
dual-point failure …… 2.29
dual-point fault …… 2.30

E

electrical and/or electronic system，E/E system …… 2.31
element …… 2.32
embedded software …… 2.33
emergency operation …… 2.34
emergency operation interval …… 2.35
error …… 2.36
exposure …… 2.37
external measure …… 2.38

F

failure …… 2.39
failure mode …… 2.40
failure rate …… 2.41
fault …… 2.42
fault model …… 2.43
fault reaction time …… 2.44
fault tolerant time interval …… 2.45
field data …… 2.46
formal notation …… 2.47
formal verification …… 2.48
freedom from interference …… 2.49
functional concept …… 2.50
functional safety …… 2.51
functional safety concept …… 2.52
functional safety requirement …… 2.53

H

hardware architectural metrics …… 2.54
hardware part …… 2.55
harm …… 2.56
hazard …… 2.57
Hazard Analysis and Risk Assessment …… 2.58

hazardous event …… 2.59
homogeneous redundancy …… 2.60

I

independence …… 2.61
independent failures …… 2.62
informal notation …… 2.63
informal verification …… 2.64
Inheritance …… 2.65
initial ASIL …… 2.66
inspection …… 2.67
intended functionality …… 2.68
item …… 2.69
item development …… 2.70

L

latent fault …… 2.71
lifecycle …… 2.72

M

malfunctioning behaviour …… 2.73
model-based development …… 2.74
modification …… 2.75
multiple-point failure …… 2.76
multiple-point fault …… 2.77
multiple-point fault detection interval …… 2.78

N

new development …… 2.79
non-functional hazard …… 2.80

O

operating mode …… 2.81
operating time …… 2.82
operational situation …… 2.83
other technology …… 2.84

P

partitioning …… 2.85
passenger car …… 2.86
perceived fault …… 2.87
permanent fault …… 2.88
phase …… 2.89

proven in use argument …… 2.90
proven in use credit …… 2.91

R

random hardware failure …… 2.92
reasonably foreseeable event …… 2.93
redundancy …… 2.94
regression strategy …… 2.95
residual fault …… 2.96
residual risk …… 2.97
review …… 2.98
risk …… 2.99
robust design …… 2.100

S

safe fault …… 2.101
safe state …… 2.102
safety …… 2.103
safety activity …… 2.104
safety architecture …… 2.105
safety case …… 2.106
safety culture …… 2.107
safety goal …… 2.108
safety manager …… 2.109
safety measure …… 2.110
safety mechanism …… 2.111
safety plan …… 2.112
safety-related element …… 2.113
safety-related function …… 2.114
safety-related special characteristic …… 2.115
safety validation …… 2.116
semi-formal notation …… 2.117
semi-formal verification …… 2.118
service note …… 2.119
severity …… 2.120
single-point failure …… 2.121
single-point fault …… 2.122
software component …… 2.123
software tool …… 2.124
software unit …… 2.125
special-purpose vehicle …… 2.126
statement coverage …… 2.127
subphase …… 2.128

system …… 2.129
systematic failure …… 2.130
systematic fault …… 2.131

T

technical safety concept …… 2.132
technical safety requirement …… 2.133
testing …… 2.134
transient fault …… 2.135

U

unreasonable risk …… 2.136

V

verification …… 2.137
verification review …… 2.138

W

walk-through …… 2.139
warning and degradation concept …… 2.140
well-trusted …… 2.141
work product …… 2.142

中 华 人 民 共 和 国
国 家 标 准
道路车辆 功能安全
第 1 部分：术语
GB/T 34590.1—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：155066·1-57768

GB/T 34590.1-2017