ICS 43.020

T40

中华人民共和国国家标准

GB/T XXXXX—XXXX

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）

（征求意见稿）

2016.05.05

XXXX－XX－XX 发布

XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

前　言

GB/T XXXXX《道路车辆 功能安全》包括十个部分：

——第1部分：术语；

——第2部分：功能安全管理；

——第3部分：概念阶段；

——第4部分：产品开发：系统层面；

——第5部分：产品开发：硬件层面；

——第6部分：产品开发：软件层面；

——第7部分：生产和运行；

——第8部分：支持过程；

——第9部分：以汽车安全完整性等级为导向和以安全为导向的分析；

——第10部分：指南。

本部分为GB/T XXXXX的第1部分。

注：本部分涵盖GB/T XXXXX的第5-10部分的术语。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分修改采用国际标准ISO 26262-1：2011 《道路车辆 功能安全 第1部分：术语》（英文版）。

本部分由国家标准化管理委员会提出。

本部分由全国汽车标准化技术委员会（SAC/TC114）归口。

本部分起草单位：

本部分主要起草人：

引　言

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

ISO 26262 适用于道路车辆上特定的由电子、电气和软件组件组成的安全相关系统在安全生命周期内的所有活动。

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

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

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

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

b) 提供了一种汽车特定的基于风险的分析方法以确定汽车安全完整性等级；

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

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

e) 提供了与供应商相关的要求。

功能安全受开发过程(例如包括需求规范、设计、实现、集成、验证、确认和配置)、生产过程、维护过程和管理过程的影响。

安全问题与常规的以功能为导向和以质量为导向的开发活动和工作成果相互关联。ISO 26262 涉及与安全相关的开发活动和工作成果。

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

— 阴影"V"表示标准中第 3、4、5、6 和 7 部分之间的关系；

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

示例：“2-6”代表 ISO 26262-2 的第六章

图 1 ISO 26262 概览

道路车辆 功能安全

第 1 部分：术语

1 范围

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

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

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

本标准针对由电子电气安全相关系统的故障行为而引起的可能的危害，包括这些系统相互作用而引起的可能的危害。本标准不针对与触电、火灾、烟雾、热、辐射、毒性、易燃性、反应性、腐蚀性、能量释放等相关的危害和类似的危害，除非危害是直接由电子电气安全相关系统的故障行为而引起的。

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

本部分规定了GB/T XXXXX所有部分应用到的术语、定义和缩略语。

2 术语、定义和缩略语

下列术语、定义和缩略语适用于本文件。

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：条件真和条件假（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

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

注：该定义用于**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。

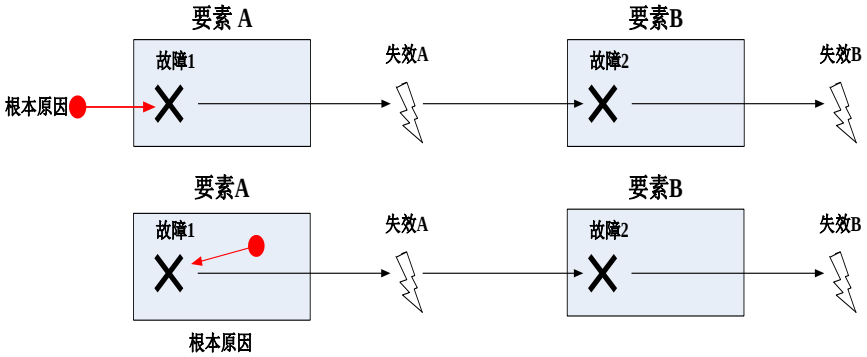

图 2 级联失效

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源引起的两个或多个**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。

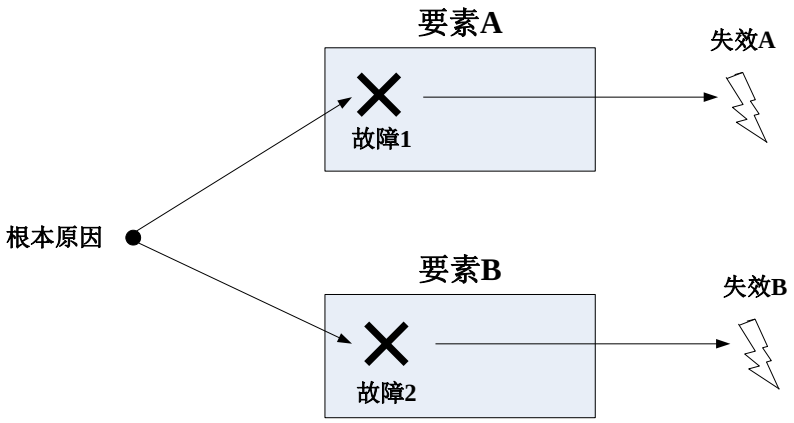

图 3 共因失效

2.20

专用措施 dedicated measure

用来对违背**安全目标**(2.108)的可能性评估中声明的**失效率**(2.41)进行确保的措施。

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。

2.23

可探测的故障 detected fault

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

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。

2.26

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。

2.29

双点失效 dual-point failure

由两个独立**故障**(2.42)的组合引起的、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 XXXXX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用来达到或保持**安全状态**(2.102)的**安全机制**(2.111)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,E/E 系统

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；传感器或其它输入装置；通讯路径；执行器或其它输出装置。

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。

2.44

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。

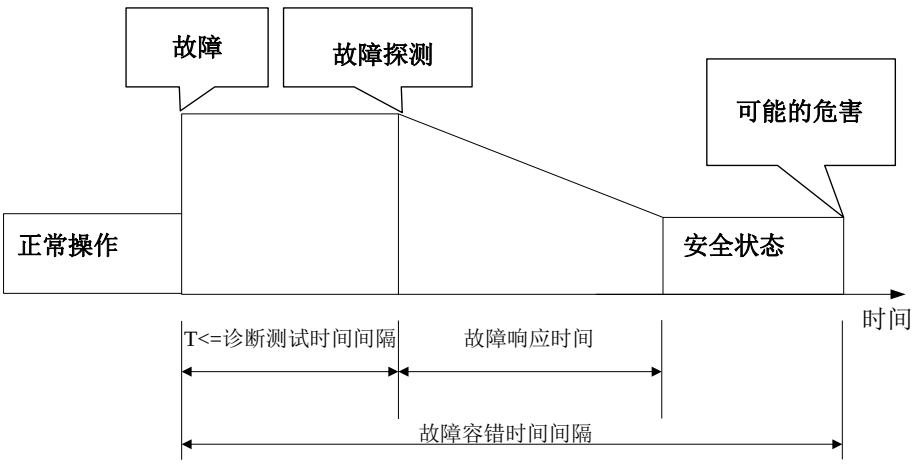

图 4 故障响应时间和容错时间间隔

2.46

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)和维护中的异常。

注：现场数据通常来自于客户的使用。

2.47

形式记法 formal notation

在语法和语义上完整定义的描述方法。

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

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。

2.55

硬件元器件 hardware part

一个硬件**组件**(2.15)的一部分。

示例：微控制器的CPU。

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 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。

2.66

初始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 等级分解**(2.7)得出的 ASIL 等级(2.6)。

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

2.68

预期功能 intended functionality

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

的行为。

2.74

基于模型的开发 model-based development

一种使用模型来描述**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。

2.87

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。

2.92

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:随机硬件**失效率**（2.41）可在合理的精度内来预测。

2.95

回归策略 regression strategy

一种策略，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。

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），并未被**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

采用**安全措施**（2.110）后剩余的**风险**（2.99）。

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

具备在无效输入或压力环境条件下正确工作能力的设计。

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 XXXXX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)概率的**故障**（2.42）。

注1：如GB/T XXXXX-5 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）和双点故障不会是安全故障。

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

2.103

安全 safety

没有**不合理的风险**（2.136）。

2.105

安全架构 safety architecture

用来实现安全要求的一系列**要素**（2.32）以及它们之间的交互。

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。

2.117

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来测试**系统**（2.129）表现与模型是否匹配。

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**（2.42）。

注 2：如果为一个硬件**要素**（2.32）（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**（2.32）的**故障**(2.42)都不是**单点故障**（2.122）。

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。

2.135

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。