ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.4—2017/IEC 61508-4:2010
代替 GB/T 20438.4—2006

电气/电子/可编程电子安全相关系统的功能安全　第4部分:定义和缩略语

Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 4:Definitions and abbreviations

(IEC 61508-4:2010,IDT)

2017-12-29 发布　　2018-07-01 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

中 华 人 民 共 和 国
国 家 标 准
电气/电子/可编程电子安全相关系统的
功能安全 第4部分:定义和缩略语
GB/T 20438.4—2017/IEC 61508-4:2010
*
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11月第一版
*
书号:155066·1-57847

目　　次

前　言

GB/T 20438《电气/电子/可编程电子安全相关系统的功能安全》分为七个部分：

——第1部分：一般要求；

——第2部分：电气/电子/可编程电子安全相关系统的要求；

——第3部分：软件要求；

——第4部分：定义和缩略语；

——第5部分：确定安全完整性等级的方法示例；

——第6部分：GB/T 20438.2和GB/T 20438.3的应用指南；

——第7部分：技术和措施概述。

本部分为GB/T 20438的第4部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 20438.4—2006《电气/电子/可编程电子安全相关系统的功能安全　第4部分：定义和缩略语》，与GB/T 20438.4—2006相比，主要技术变化如下：

——增加了“软件支持工具”的术语和定义(见3.2.10和3.2.11)；

——增加了“专用集成电路”的术语和定义(见3.2.15)；

——增加了“系统性安全完整性”和“系统性能力”的术语和定义(见3.5.6和3.5.9)；

——增加了“无关失效”和“无影响失效”的术语和定义(见3.6.13和3.6.14)；

——增加了“平均恢复时间”和“平均维修时间”的术语和定义(见3.6.21和3.6.22)。

本部分使用翻译法等同采用IEC 61508-4:2010《电气/电子/可编程电子安全相关系统的功能安全　第4部分：定义和缩略语》。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本部分起草单位：机械工业仪器仪表综合技术经济研究所、北京国电智深控制技术有限公司、杭州和利时自动化有限公司、西门子(中国)有限公司、施耐德电气(中国)有限公司、上海中沪电子有限公司。

本部分主要起草人：冯晓升、孟邹清、徐皑冬、史学玲、王春喜、左信、罗安、周有铮、唐蓉、白焰、熊文泽、杨柳、梅豪、李佳、邱忠昌、谢亚莲、刘瑶。

本部分所代替标准的历次版本发布情况为：

——GB/T 20438.4—2006。

引　言

由电气和电子器件构成的系统，多年来在许多应用领域中执行其安全功能。以计算机为基础的系统(一般指可编程电子系统)在其应用领域中用于执行非安全功能，并且也越来越多地用于执行安全功能。如果要安全并有效地使用计算机技术，有关决策者在安全方面有充足的指导并据此做出决定是十分必要的。

GB/T 20438 针对由电气和/或电子和/或可编程电子(E/E/PE)组件构成的、用来执行安全功能的系统安全生命周期的所有活动，提出了一个通用的方法。采用统一的方法的目的是为了针对所有以电为基础的安全相关系统提出一种一致的、合理的技术方针。主要目标是促进基于 GB/T 20438 系列标准的产品和应用领域国家标准的制定。

注 1：在参考文献中给出了基于 GB/T 20438 系列标准的产品和应用领域标准的例子(见参考文献[1]，[2]，[3])。

在许多情况下，可用多种基于不同技术(如机械的、液压的、气动的、电气的、电子的、可编程电子的等)的系统来保证安全。因而必须考虑各类安全策略，不仅要考虑单个系统中的所有组件的问题(如传感器、控制器、执行器等)，还要考虑不同安全相关系统组合后的问题。因此当 GB/T 20438 在关注电气/电子/可编程电子(E/E/PE)安全相关系统的同时，也提供了一个框架，在这个框架内，基于其他技术的安全相关系统也可被考虑进去。

在各种应用领域里，存在着许多潜在的危险和风险，包含的复杂性也各不相同，从而需应用不同的 E/E/PE 安全相关系统。对每个特定的应用，将根据特定应用的许多因素来确定所需的安全措施。GB/T 20438 作为基本原则可在未来的产品和应用领域国家标准制定和已有标准的修订中规范这些措施。

GB/T 20438

——考虑了当使用 E/E/PE 系统执行安全功能时，所涉及的整体安全生命周期、E/E/PE 系统安全生命周期以及软件安全生命周期的各阶段(如初始概念、整体设计、实现、运行和维护到退役)；

——针对飞速发展的技术，建立一个足够健壮而广泛的能满足今后发展需要的框架；

——使涉及 E/E/PE 安全相关系统的产品和应用领域的国家标准得以制定；在 GB/T 20438 的框架下，产品和应用领域的国家标准的制定在应用领域和交叉应用领域宜具有高度一致性(如基本原理，术语等)；这将既具有安全性又具有经济效益；

——为实现 E/E/PE 安全相关系统所需的功能安全，提供了编制安全要求规范的方法；

——采用了一种可确定安全完整性要求的基于风险的方法；

——引入安全完整性等级，用于规定 E/E/PE 安全相关系统所要执行的安全功能的目标安全完整性等级；

注 2：GB/T 20438 没有规定每个安全功能的安全完整性等级的要求，也没有规定如何确定安全完整性等级。而是提供了一种基于风险概念的框架和技术范例。

——建立了 E/E/PE 安全相关系统执行安全功能的目标失效量，这些量都同安全完整性等级相联系；

——建立了单一 E/E/PE 安全相关系统执行安全功能时，目标失效量的一个下限值。这些 E/E/PE 安全相关系统运行在：

——低要求运行模式下，下限设定成要求时危险失效平均概率为 10^{-5}；

——高要求运行模式或者连续运行模式下，下限设定成危险失效平均频率为 10^{-9}/h。

注 3：单一 E/E/PE 安全相关系统不一定是单通道架构。

注 4：对于非复杂系统，通过安全相关系统的设计实现更优目标安全完整性是可能的。但对于相对复杂的系统(例如可编程电子安全相关系统)，这些限值代表了目前能够达到的水平。

——基于工业实践中获取的经验和判断，设定了避免和控制系统性故障的要求。即使发生系统性故障的可能性一般不能量化，但 GB/T 20438 允许为一个特定的安全功能做出声明，即如果标准中的所有要求都满足，认为与安全功能相关的目标失效量已达到；

——引入了系统性能力，该能力表明一个组件为满足规定的安全完整性等级要求时，系统性安全完整性的置信度；

——采用多种原理、技术和措施以实现 E/E/PE 安全相关系统的功能安全，但没有明确地使用失效-安全的概念。然而，如果能够满足标准中相关条款的要求，则“失效-安全”的概念和“本质安全”原则可能被应用，并且采用这些概念是可接受的。

电气/电子/可编程电子安全相关系统的功能安全　第4部分:定义和缩略语

1　范围

1.1　GB/T 20438的本部分包括了GB/T 20438.1～GB/T 20438.7所使用的术语和解释。

1.2　这些定义按标题分组,以便从它们的前后关系上去理解这些相关的术语。但这样的分组并不意味着对定义增加了含义。

1.3　GB/T 20438.1、GB/T 20438.2、GB/T 20438.3和GB/T 20438.4是基础的安全标准,虽然它不适用于简单的E/E/PE安全相关系统(见GB/T 20438.4—2017的3.4.3),但作为基础安全标准,各技术委员会可以在IEC指南104和ISO/IEC指南51的指导下制定相关标准时使用。GB/T 20438.1、GB/T 20438.2、GB/T 20438.3和GB/T 20438.4也可作为独立标准来使用。GB/T 20438的横向安全功能不适用于在IEC 60601系列指导下的医疗设备。

1.4　各技术委员会的责任之一,是在其标准的起草工作中尽可能使用基础的安全标准。在本文中,本基础安全标准中的要求、测试方法或测试条件只有在这些技术委员会起草的标准中已明确引用或包含时适用。

1.5　图1表示了GB/T 20438的整体框架,同时明确了本部分在实现E/E/PE安全相关系统功能安全过程中的作用。

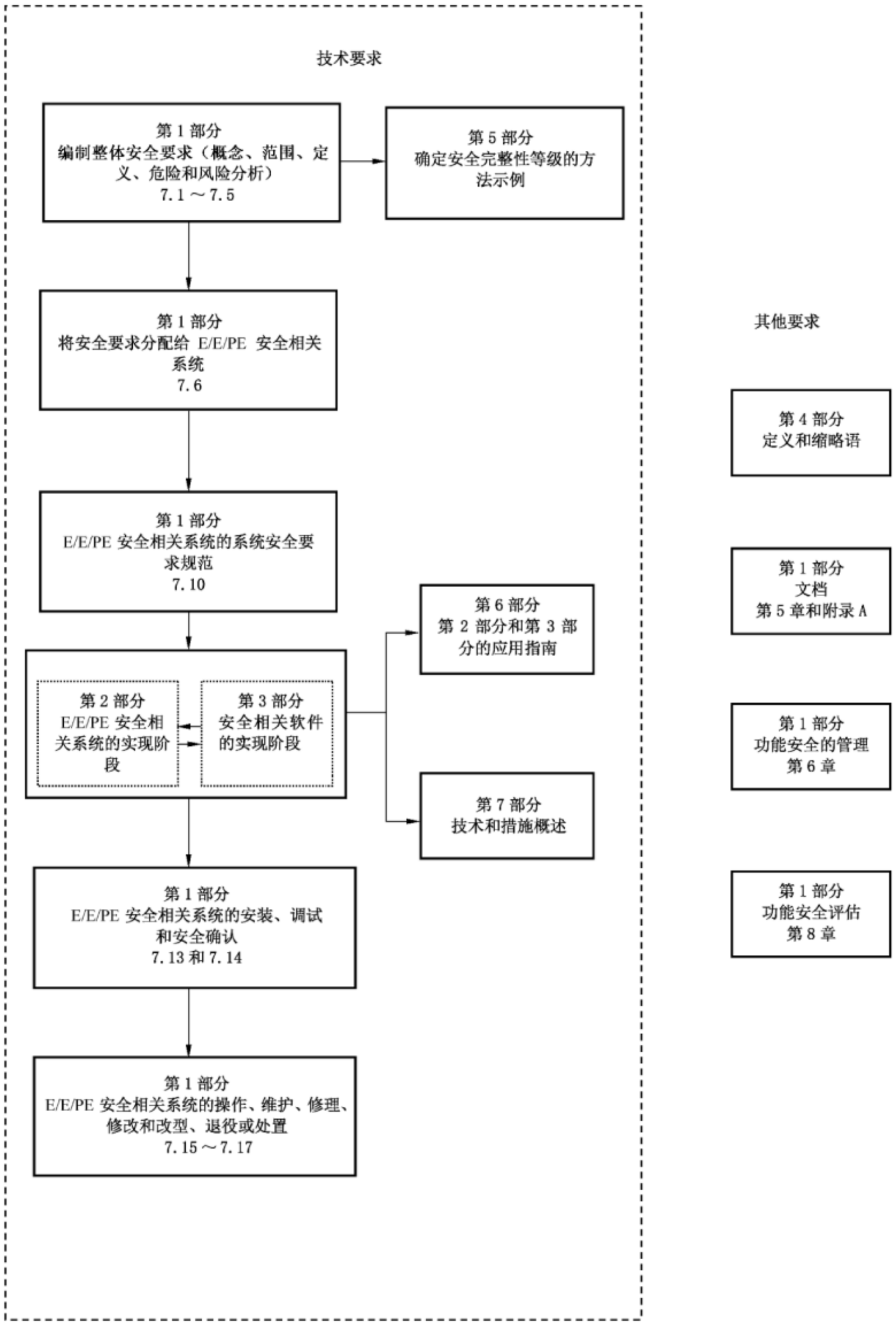


图 1　GB/T 20438 的整体框架

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。

IEC Guide 104:1997 安全出版物的编写及基础安全出版物和多专业共用安全出版物的应用导则(The preparation of safety publications and the use of basic safety publications and group safety publications)

IEC/ISO Guide 51:1999 涉及安全的内容 将安全内容纳入标准的指南(Safety aspects—Guidelines for their inclusion in standards)

3 定义和缩略语

表1给出了GB/T 20438中使用的定义和缩略语。

表1 GB/T 20438使用的缩略语

缩略语	全 称	术语的定义和/或解释
ALARP	合理可行的低	GB/T 20438.5—2017的附录C
ASIC	专用集成电路	3.2.15
CCF	共因失效	3.6.10
CPLD	复杂可编程逻辑器件	
DC	诊断覆盖率	3.8.6
(E)EPLD	(电)可擦写可编程逻辑器件	
E/E/PE	电气/电子/可编程电子	3.2.13，示例:E/E/PE安全相关系统
E/E/PE (system)	电气/电子/可编程电子系统	3.3.2
EEPROM	电可擦写可编程只读存储器	
EPROM	可擦写可编程只读存储器	
EUC	受控设备	3.2.1
FPGA	现场可编程门阵列	
GAL	通用阵列逻辑	
HFT	硬件故障裕度	GB/T 20438.2—2017的7.4.4
MooN	N取M通道架构(如1oo2是2取1架构，两个通道中任一通道都可执行安全功能)	GB/T 20438.6—2017的附录B
MooND	带诊断的N取M通道架构	GB/T 20438.6—2017的附录B
MTBF	平均失效间隔时间	3.6.19，注3
MTTR	平均恢复时间	3.6.21
MRT	平均修理时间	3.6.22
PAL	可编程阵列逻辑	

表 1（续）

缩略语	全　　称	术语的定义和/或解释
PE	可编程电子	3.2.12
PE system	可编程电子系统	3.3.1
PFD	要求时危险失效概率	3.6.17
PFDavg	要求时危险失效平均概率	3.6.18
PFH	危险失效平均频率[h^{-1}]	3.6.19
PLA	可编程逻辑阵列	
PLC	可编程逻辑控制器	GB/T 20438.6—2017 的附录 E
PLD	可编程逻辑器件	
PLS	可编程逻辑序列	
PML	可编程宏逻辑	
RAM	随机存储器	
ROM	只读存储器	
SFF	安全失效分数	3.6.15
SIL	安全完整性等级	3.5.8
VHDL	超高速集成电路硬件描述语言	GB/T 20438.2—2017 的附录 F，注 5

3.1　安全术语

3.1.1

伤害　harm

人身损伤、人的健康损害、财产或环境的损害。

[ISO/IEC 导则 51:1999，定义 3.3]

3.1.2

危险　hazard

伤害的潜在根源。

[ISO/IEC 导则 51:1999，定义 3.5]

注：这个术语包括短时间对人身的伤害（如着火和爆炸），以及那些对人身健康长时间的损害（如有毒物质释放）。

3.1.3

危险状况　hazardous situation

人、财产或环境暴露于一个或多个危险源环境的情况。

[改写 ISO/IEC 导则 51:1999，定义 3.6]

3.1.4

危险事件　hazardous event

可能导致伤害的事件。

注：危险事件是否导致伤害取决于人、财产或环境是否遭受危险情况的后果，以及事件发生后，如果会对人产生伤害，人是否能避免该事件的后果。

3.1.5

伤害事件　harmful event

危险状况或危险事件已产生了伤害的事件。

注：考虑到危险事件，采用 ISO/IEC 导则 51 中 3.4 的定义。

3.1.6

风险　risk

伤害发生的概率与该伤害严重程度的组合。

[ISO/IEC 导则 51:1999，定义 3.2]

注：对这一概念更多的讨论见 GB/T 20438.5—2017 附录 A。

3.1.7

可容忍风险　tolerable risk

根据当前社会发展水平，在给定的范围内能够接受的风险。

[ISO/IEC 导则 51:1999，定义 3.7]

注：参见 GB/T 20438.5—2017 的附录 C。

3.1.8

残余风险　residual risk

采取防护措施以后仍存在的风险。

[ISO/IEC 导则 51:1999，定义 3.9]

3.1.9

EUC 风险　EUC risk

由 EUC 或由 EUC 与 EUC 控制系统相互作用而产生的风险。

注 1：本部分所说的风险是指与特定的危险事件相伴的风险。在这种危险事件中用 E/E/PE 安全相关系统和其他风险降低措施来提供必要的风险降低(即与功能安全相关的风险)。

注 2：GB/T 20438.5—2017 的图 A.1 说明了 EUC 风险。确定 EUC 风险的主要目的是在还未考虑 E/E/PE 安全相关系统和其他风险降低措施之前建立一个风险参考点。

注 3：这个风险评估将包括相关人的因素。

3.1.10

目标风险　target risk

针对特定的危险，考虑了 EUC 风险，及 E/E/PE 安全相关系统和其他风险降低措施后，所要达到的风险。

3.1.11

安全　safety

没有不可接受的风险。

[ISO/IEC 导则 51:1999，定义 3.1]

3.1.12

功能安全　functional safety

整体安全中与 EUC 和 EUC 控制系统相关的部分，它取决于 E/E/PE 安全相关系统和其他风险降低措施正确执行其功能。

3.1.13

安全状态　safe state

达到安全时 EUC 的状态。

注：从潜在的危险条件到最终的安全状态，EUC 可能不得不经过几个中间的安全状态。有时，仅当 EUC 处于连续控制下才存在一个安全状态。这样的连续控制可能是短时间的或是不确定的一段时间。

3.1.14

合理可预见的误用　reasonably foreseeable misuse

由容易预见的人的行为导致的未按照供方预期的方式使用产品、过程和服务。

[ISO/IEC 导则 51:1999,定义 3.14]

3.2　设备和装备

3.2.1

受控设备　equipment under control;EUC

用于制造业、流程工业、运输业、制药业或其他行业的设备、机器、装置或成套设备。

注：EUC 控制系统与 EUC 是分开的并且是截然不同的。

3.2.2

环境　environment

针对特定的应用,在需要考虑的事项下和在任何安全生命周期阶段,对于实现功能安全会产生影响的所有相关变量。

注：可能包括,例如,物理环境、运行环境、法律环境和维护环境。

3.2.3

功能单元　functional unit

能够完成规定目的的软件、硬件或两者相结合的实体。

[ISO/IEC 2382-1，01-01-40]

注：在 IEV191-01-01 中,常用"项(item)"一词代替功能单元,一个项有时可能包括人员在内。

3.2.4

应用　application

涉及 EUC 的任务,而不是涉及 E/E/PE 系统的任务。

3.2.5

软件　software

用于数据处理系统操作的智能创作,包括程序、规程、数据、规则以及相关的文档。

注 1：软件独立于其记录媒体。

注 2：不包含注 1 的情况下,该定义与 ISO/IEC2382-1 不同之处在于增加了一个词"数据"。

3.2.6

系统软件　system software

是可编程电子系统的软件的一部分,涉及可编程装置自身的功能和提供的服务。而不像应用软件那样规定执行 EUC 安全相关任务的功能。

注：参见 GB/T 20438.7。

3.2.7

应用软件　application software

应用数据　application data

配置(组态)数据　configuration data

是可编程电子系统的软件的一部分,规定了执行 EUC 相关任务的功能而不是可编程装置自身的功能和提供的服务。

3.2.8

已有软件　pre-existing software

并非特定为当前工程或安全相关系统而开发的已有的软件组件。

注：这种软件可能是商业化的产品,也可能是某些机构为早先的产品或系统开发的。已有软件可能是也可能不是按 GB/T 20438 的要求开发的。

3.2.9

数据　data

适合于计算机通信、解释或处理的，以某种方式表示的信息。

注 1：数据可能采用静态信息的形式（如设定点或地理信息表达的配置）或采用指令的形式来规定已有功能的顺序。

注 2：示例参看 GB/T 20438.7。

3.2.10

软件在线支持工具　software on-line support tool

能直接影响运行中的安全相关系统的软件工具。

3.2.11

软件离线支持工具　software off-line support tool

支持软件开发生命周期某个阶段并且不能直接影响运行中的安全相关系统的软件工具。软件离线支持工具分成下面三类：

——T1

不产生直接或间接贡献于安全相关系统可执行代码（包括数据）的输出；

注 1：T1 的例子包括：文本编辑器，或需求支持工具，或设计支持工具，且该工具没有自动代码生成能力；配置控制工具。

——T2

支持设计或可执行代码的测试或验证，如果工具出错，则不能发现错误，但不会在可执行软件中直接产生错误。

注 2：T2 的例子包括：测试环境发生器；测试覆盖率测量工具；静态分析工具。

——T3

产生能够直接或间接贡献于安全相关系统可执行代码的输出。

注 3：T3 的例子包括：当源代码程序与形成的目标代码之间的关系不明显时使用的优化编译器；将可执行的运行时软件包结合进可执行代码的编译器。

3.2.12

可编程电子　programmable electronic；PE

以计算机技术为基础，可以由硬件、软件及其输入和（或）输出单元构成。

注：这个术语包括以一个或多个中央处理器（CPUs）及相关的存储器等为基础的微电子装置。

举例：下列均是可编程电子装置：

——微处理器；

——微控制器；

——可编程控制器；

——专用集成电路（ASICs）；

——可编程逻辑控制器（PLCs）；

——其他以计算机为基础的装置（例如智能传感器、智能变送器、智能执行器）。

3.2.13

电气/电子/可编程电子　electrical/electronic/programmable electronic ；E/E/PE

基于电气（E）和/或 电子（E）和/或 可编程电子（PE）的技术。

注：本术语试图覆盖所有的在电原理下运行的装置或系统。

举例：电气/电子/可编程电子装置包括：

——机电装置（电气）；

——固态非可编程电子装置（电子）；

——以计算机技术为基础的电子装置（可编程电子）；见 3.2.12。

3.2.14

有限可变语言　limited variability language

采用文本、图形，或两者兼有的方法进行编程的软件编程语言，仅限于商业和工业的可编程电子控制器的应用编程。

举例：以下是有限可变语言，引自 GB/T 15969.3(文献 8)和其他资料，作为 PLC 系统的应用程序。

——梯形图：一种图形语言，由一系列输入符号(表示装置的行为，如常开触点和常闭触点)与输出符号(表示如继电器的动作)用线(指示电流流动)相连接而构成；

——布尔代数：具有可增加某些助记符指令能力的，基于布尔运算符如与(AND)、或(OR)和非(NOT)的低级语言；

——功能块图：除布尔运算符外，可使用更复杂的功能，如数据传输文件、块传输读/写，移位寄存器和顺序器指令等。

——顺序功能图：有顺序的程序的图形表示，由相互联系的步、动作和带转换条件的有向线构成。

3.2.15

专用集成电路　application specific integrated circuit；ASIC

为专用功能而设计和制造的集成电路，其功能由产品开发者规定。

注：ASIC 作为一个独立术语包括下列所有类型的集成电路：

——全定制 ASIC：设计和制造与标准集成电路类似，但具有由产品开发者定义的功能性。

标准集成电路是大批量生产的，并能用于不同的应用。功能性、确认、生产和生产测试由半导体厂商独立处理。

在布局层面，人工控制和优化通常是为了减少所需面积。不是为安全相关系统设计的。生产过程、生产技术的频繁变化是为了优化成本和产品成品率。使用特殊工艺制造的元件数量或掩模版本不是公开的。

——基于核的 ASIC：基于预先布局、设计或生成的宏核，并由附加的逻辑支持的 ASIC。

例 1：预先布局的宏是指标准的微处理器核、外围元件、通信接口、模拟块、专用功能 I/O 单元。

例 2：预先设计的宏(被称为知识产权，即 IP)是指例 1 中类似元件的各种变化，具有不同的由高级硬件描述语言(VHDL，Verilog)构成的设计数据。

例 3：生成的宏包括嵌入式 RAM、ROM、EEPROM 或 FLASH(闪存)。基于设计规则生成的块被认为是正确的。预先布局或生成的宏是工艺专用的，但可能被移植到不同的技术。在大多数情况下，宏核不同于初始的分立的现成元件(不同的工艺，由第三方提供)。

——基于单元的 ASIC：以取自单元库的逻辑基本要素(如 AND，OR，Flip-Flop，Latch)为基础的 ASIC。包括逻辑基本要素和互联线的门级网表，通常是用综合工具从高级硬件描述语言中产生的。逻辑基本要素的功能和时间特性是在单元库内表现的。这些参数被用来驱动综合工具，也用于仿真。另外，用布局工具进行单元布局和互联布线。

——门阵列：预先制造的带有固定数量单元的硅元件，该单元对不同成分提供公共的起始点。其功能性由预先制造的单元之间的连接矩阵(金属层)决定。设计过程近似于基于单元的 ASIC，但布局的步骤由连接已存在的单元的布线步骤所取代。

——现场可编程门阵列(FPGA)：标准集成电路，使用一次性或可重复编程的元件来规定功能块之间的连接以及配置单个功能块的功能特性。由于可编程元件的特性，在生产期间不可能完全测试一次性可编程 FPGAs。

——可编程逻辑器件(PLD)：标准集成电路，具有中低复杂度，使用一次性可编程或电可擦除元件(熔丝)来规定组合逻辑——典型的是基于 AND 或 OR 乘积项——以及配置存储元件。由于其规则的结构，在同步电路设计中 PLD 提供可预测的时序和可保证的最高工作频率。典型的 PLD 有 PAL，GAL，PML，(E)EPLD，PLA，PLS。

——复杂可编程逻辑器件(CPLD)：在一个芯片上有多个类似 PLD 块，由可编程的互连矩阵(crossbar)相连接。在多数情况下，可编程逻辑元件是可重复编程的(EPROM 或 EEPROM)。

3.3　系统-通用

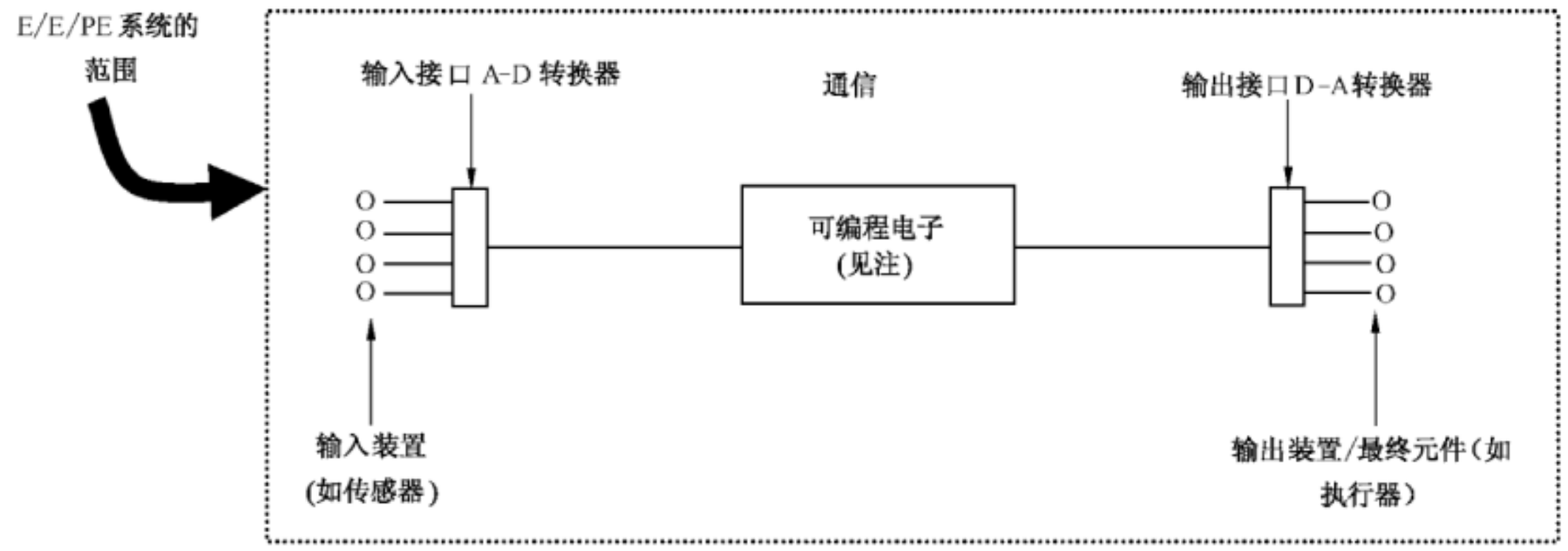
3.3.1

可编程电子系统　programmable electronic system；PE system

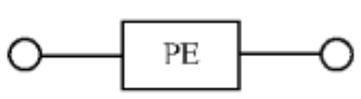
基于一个或多个可编程电子装置的控制、保护或监视系统，包括系统中所有的组件，如电源、传感器

和其他输入装置,数据总线和其他通信路径,以及执行器和其他输出装置(见图 2)。

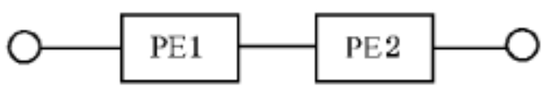
注:PES 的结构如图 2 a)。图 2 b)是阐述 GB/T 20438 中 PES 在 EUC 和其接口中具有不同于传感器、执行器的可编程电子单元的方式,但是,在 PES 中可编程电子可能存在于多处。图 2 c)表示具有两个分立的可编程电子单元的 PES。图 2 d)表示具有双重可编程电子单元(即双通道)的 PES,但共用一个传感器和一个执行器。



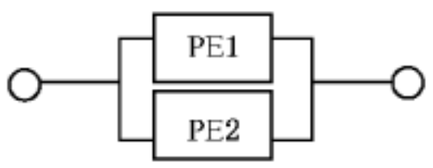
a) 基本的 PES 结构



b) 具有单个可编程电子装置的单个 PES(即由一个单通道可编程电子装置构成的一个 PES)



c) 具有按串联方式连接的双可编程电子装置的单个 PES(如智能传感器和可编程控制器)



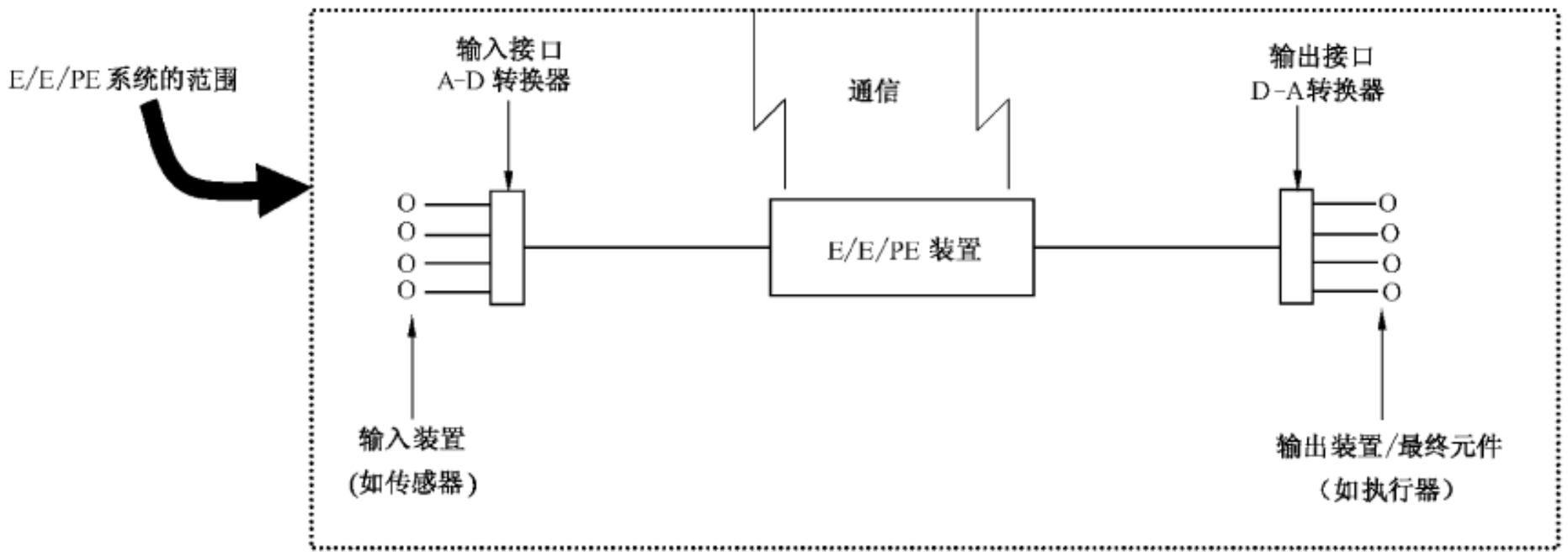
d) 具有双可编程电子单元但共享传感器和最终元件的单个 PES(即由两个可编程电子通道构成的一个 PES)

图 2 可编程电子系统

3.3.2

电气/电子/可编程电子系统 electrical/electronic/programmable electronic system;E/E/PE system

基于一个或多个电气/电子/可编程电子(E/E/PE)装置的控制、保护或监视系统,包括系统中所有的组件,如电源、传感器和其他输入装置,数据总线和其他通信路径,以及执行器和其他输出装置(见图 3)。



注:E/E/PE 装置是图示的中间部分,但这样的装置在 E/E/PE 系统中可能存在于多处

图 3 电气/电子/可编程电子系统(E/E/PE 系统)—结构和术语

3.3.3

EUC 控制系统　EUC control system

响应来自过程和(或)操作者的输入信号,并产生输出信号使 EUC 按预期方式工作的系统。

注:EUC 控制系统包括输入装置和最终元件。

3.3.4

架构　architecture

在一个系统中硬件和软件组件的特定配置。

3.3.5

软件模块　software module

由程序和/或数据声明组成的构件,并且能与其他类似构件相互作用。

3.3.6

通道　channel

独立执行一个组件安全功能的一个或一组组件。

举例:两通道(或双通道)配置是指具有两个能独立执行相同功能的通道构成的配置。

注:该术语可用来描述一个完整的系统或一个系统的一部分(如传感器或最终元件)。

3.3.7

多样性　diversity

执行一个要求功能的不同方法。

注:可用不同的方法或不同的设计途径来达到多样性。

3.4　系统-安全相关

3.4.1

安全相关系统　safety-related system

所指的系统应满足以下两项要求:

——执行要求的安全功能足以实现或保持 EUC 的安全状态;并且

——自身或与其他 E/E/PE 安全相关系统、其他风险降低措施一起,能够实现要求的安全功能所需的安全完整性。

注 1:该术语是指这样的系统,即所谓安全相关系统是,它们及与其他风险降低措施一起,实现必要的风险降低量,以满足所要求的可容忍风险。见 GB/T 20438.5—2017 的附录 A。

注 2:安全相关系统能在检测到可导致危险事件的情况时采取适当的动作以防止 EUC 进入危险状态。安全相关系统的失效将包含于导致危险的事件中。尽管可能存在具备安全功能的其他系统,但所指定的安全相关系统可仅靠其自身能力达到要求的可容忍风险。安全相关系统一般被分为安全相关控制系统和安全相关保护系统。

注 3:安全相关系统可以是 EUC 控制系统的组成部分,也可用传感器和/或执行器与 EUC 连接。即可通过 EUC 控制系统(也可能通过分开的和独立的附加系统)或者利用分开的、独立的、安全专用的安全相关系统执行安全功能达到要求的安全完整性等级。

注 4:安全相关系统可:

a)　用于防止危险事件发生(即安全相关系统一旦执行其安全功能则避免伤害事件发生);

b)　用于减轻伤害事件的影响,即通过减轻后果的办法来降低风险;

c)　同时具有 a)和 b)的功能组合。

注 5:人也可作为安全相关系统的一部分。例如,人可以接收来自可编程电子装置的信息,并根据接收信息执行安全动作,或通过可编程电子装置执行安全动作。

注 6:安全相关系统包括执行规定安全功能所需的全部硬件、软件以及支持服务(如电源)[因此,传感器,其他输入装置,最终元件(执行器)和其他输出装置都包括在安全相关系统中]。

注 7:安全相关系统可基于广泛的技术基础,包括电气、电子、可编程电子、液压和气动等。

3.4.2

其他风险降低措施　other risk reduction measure

不使用 E/E/PE 安全相关系统，并与其分开且截然不同的风险降低或减轻措施。

举例：泄放阀是一种其他风险降低措施。

3.4.3

低复杂 E/E/PE 安全相关系统　low complexity E/E/PE safety-related system

E/E/PE 安全相关系统(见 3.2.13 和 3.4.1)，其中：

——已很好确定了每个单独元件的失效模式；

——能完全确定在故障状况下系统的行为。

注：故障状况下系统的行为可用试验和/或分析的方法确定。

举例：包括一个或几个限位开关，可能还要通过机电式中间继电器控制一个或多个接触器来切断电机电源的系统。就是一个低复杂 E/E/PE 安全相关系统。

3.4.4

子系统　subsystem

安全相关系统顶层架构设计的实体，子系统的危险失效导致安全功能的危险失效。此处的危险失效见 3.6.7(a)。

3.4.5

组件　element

子系统的一部分，由单个或一组元件组成以执行一个或多个组件安全功能。

注 1：一个组件可由硬件和/或软件构成。

注 2：典型的组件是传感器、可编程控制器、最终元件。

3.4.6

冗余　redundancy

对于执行一个要求的功能或对于表示信息而言，存在多于一种的方法。

[基于 GB/T 17215.911]

举例：功能元件加倍和增加奇偶校验位都是冗余的例子。

注 1：冗余主要用于提高可靠性(在给定时间范围内功能正确的概率)或可用性(在特定时间点具有功能的概率)。也可通过像 2oo3 这样的架构来使误动作最小化。

注 2：此定义在 IEV191-15-01 中不完整。

注 3：冗余可能是“活动的(hot or active)”(所有冗余项同时运行)、“待机的(cold or stand-by)”(在同一时间只有一个冗余项运行)、“混合的(mixed)”(在同一时间一个或几个项运行和一个或几个项待机)。

3.5　安全功能和安全完整性

3.5.1

安全功能　safety function

针对特定的危险事件，为实现或保持 EUC 的安全状态，由 E/E/PE 安全相关系统或其他风险降低措施实现的功能。

示例：安全功能的例子包括：

——在要求时执行的功能，作为一种主动行动以避免危险状况(如关闭电机)；和

——采取预防行为的功能(如防止马达启动)。

3.5.2

整体安全功能　overall safety function

针对特定的危险事件，实现或保持 EUC 安全状态的方法。

3.5.3

组件安全功能　element safety function

由组件执行的安全功能的一部分(见 3.5.1)。

3.5.4

安全完整性　safety integrity

在规定的时间段内和规定的条件下,安全相关系统成功执行规定的安全功能的概率。

注 1:安全完整性越高,安全相关系统在要求时未能执行规定的安全功能或未能实现规定的状态的概率就越低。

注 2:有 4 个安全完整性等级(见 3.5.8)。

注 3:在确定安全完整性时,宜包括所有导致非安全状态的失效原因(随机硬件失效和系统性失效),如硬件失效、软件导致的失效和电磁干扰导致的失效。某些类型的失效,尤其是随机硬件失效,可以用危险失效模式下的平均失效频率或安全相关保护系统未能在要求时动作的概率来量化,但是安全完整性还取决于许多不能精确量化只可定性考虑的因素。

注 4:安全完整性由硬件安全完整性(见 3.5.7)和系统性安全完整性(见 3.5.6)构成。

注 5:本定义针对安全相关系统执行安全功能的可靠性(见 IEV 191-12-01 可靠性的定义)。

3.5.5

软件安全完整性　software safety integrity

安全相关系统安全完整性中,与软件造成的危险失效模式下的系统性失效有关的部分。

3.5.6

系统性安全完整性　systematic safety integrity

安全相关系统安全完整性中,与危险失效模式下的系统性失效有关的部分。

注:系统性安全完整性通常不能量化(与通常可量化的硬件安全完整性明显不同)。

3.5.7

硬件安全完整性　hardware safety integrity

安全相关系统安全完整性中,与危险失效模式下的随机硬件失效有关的部分。

注:本术语涉及在危险模式下的失效,即,将削弱其安全完整性的安全相关系统的这类失效。与本术语有关的两个参数是危险失效平均频率和在要求时动作失效的概率。当为保持安全而应该保持连续控制时,使用前一可靠性参数,在安全相关保护系统场合中使用后一可靠性参数。

3.5.8

安全完整性等级　safety integrity level;SIL

一种离散的等级(四个可能等级之一),对应安全完整性量值的范围。安全完整性等级 4 是最高的,安全完整性等级 1 是最低的。

注 1:四个安全完整性等级对应的目标失效量(见 3.5.17)在 GB/T 20438.1—2017 的表 2 和表 3 中规定。

注 2:安全完整性等级用于规定分配给 E/E/PE 安全相关系统安全功能的安全完整性要求。

注 3:安全完整性等级(SIL)并非系统、子系统、组件或元器件的属性。对"SIL n 安全相关系统"(n=1、2、3、4)的正确解释是系统具有支持安全功能的安全完整性等级达到 n 的潜在能力。

3.5.9

系统性能力　systematic capability

当一个组件按组件符合项安全手册的规定应用时,针对规定的组件安全功能,组件的系统性安全完整性满足规定的 SIL 要求的置信度的度量(表示为 SC1～SC4)。

注 1:系统性能力由用于避免和控制系统性故障的要求来确定(见 GB/T 20438.2 和 GB/T 20438.3)。

注 2:相关的系统性失效机理取决于组件的特性。比如一个组件单独由软件构成,则只需考虑软件失效机理。如组件由硬件和软件构成则需要考虑硬件和软件的失效机理。

注 3:当一个组件按组件符合项安全手册的规定应用时,针对规定的组件安全功能,组件具有 SC N 的系统性能力意味着 SIL N 的系统性安全完整性已被满足。

3.5.10

软件安全完整性等级　software safety integrity level

软件组件的系统性能力。该软件组件是安全相关系统的子系统的组成部分。

注：SIL 表示整体安全功能的特性，并不表示支持该功能的单独子系统或组件的特性。与所有组件一样，软件自身也没有 SIL。但是为了方便，也说“SIL n 的软件”，其含义是“对软件置信度(用范围 1～4 表示)的衡量，即当(软件)组件根据该组件符合项安全手册规定的要求应用时，(软件)组件安全功能不会由于相关的系统性失效机理而失效。

3.5.11

E/E/PE 系统安全要求规范　E/E/PE system safety requirements specification

包括安全功能及其安全完整性等级要求的规范。

3.5.12

E/E/PE 系统安全功能要求规范　E/E/PE system safety functions requirements specification

包括安全相关系统必须要执行的安全功能要求的规范。

注 1：这个规范是 E/E/PE 系统安全要求规范(见 GB/T 20438.1—2017 的 7.10 和 7.10.2.6)的一部分(安全功能部分)，包含由安全相关系统必须要执行的安全功能的精确细节。

注 2：只要能清楚地表达安全功能，规范可用文本、流程图、矩阵、逻辑图等形式文档化。

3.5.13

E/E/PE 系统安全完整性要求规范　E/E/PE system safety integrity requirements specification

包括安全相关系统必须要执行的安全功能的安全完整性要求的规范。

注：这个规范是 E/E/PE 系统安全要求规范(见 GB/T 20438.1—2017 的 7.10 和 7.10.2.7)的一部分(安全完整性部分)。

3.5.14

E/E/PE 系统设计要求规范　E/E/PE system design requirements specification

从子系统和组件角度，包含 E/E/PE 安全相关系统设计要求的规范。

3.5.15

安全相关软件　safety-related software

在安全相关系统中用于实现安全功能的软件。

3.5.16

运行模式　mode of operation

安全相关系统运行的方式，可为下列之一：

——低要求模式：仅当要求时才执行将 EUC 导入规定安全状态的安全功能，并且要求的频率不大于每年一次；

注：E/E/PE 安全相关系统只在要求时才对 EUC 或 EUC 控制系统产生影响。如果 E/E/PE 安全相关系统不能执行安全功能，则可能使 EUC 进入安全状态(见 GB/T 20438.2—2017 的 7.4.6)。

——高要求模式：将 EUC 导入规定安全状态的安全功能仅当要求时才执行，并且要求的频率大于每年一次；

——连续模式：安全功能将 EUC 保持在安全状态是正常运行的一部分。

3.5.17

目标失效量　target failure measure

安全完整性要求达到的危险模式失效的目标概率，规定为下列两种之一：

——安全功能在要求时危险失效的平均概率(对于低要求运行模式)；

——危险失效的平均频率[h^{-1}](对于高要求或连续运行模式)；

注：目标失效量的数值在 GB/T 20438.1—2017 的表 2 和表 3 中给出。

3.5.18

必要的风险降低　necessary risk reduction

为保证不超过可容忍风险，由 E/E/PE 安全相关系统、和/或其他风险降低措施实现的风险降低。

3.6 故障,失效和错误(见图 4)

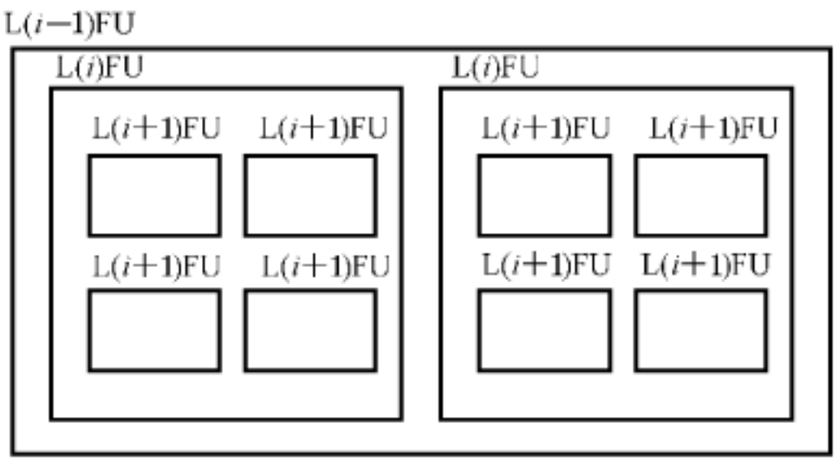
3.6.1

故障 fault

可能导致功能单元执行要求功能的能力降低或丧失的异常状况。

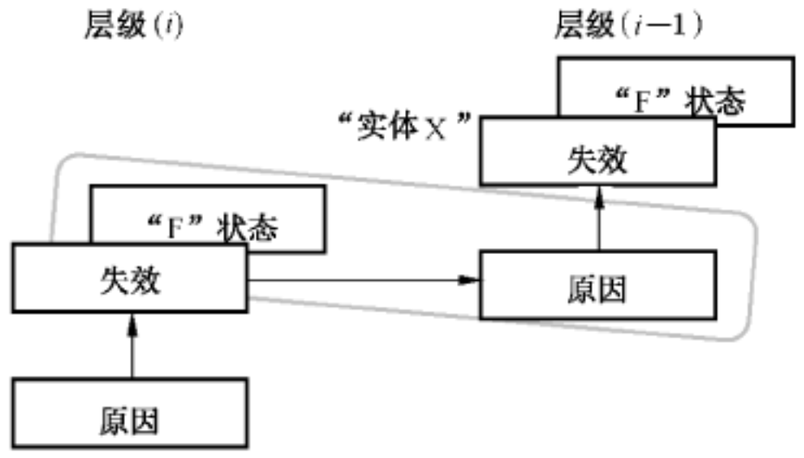
[GB/T 5271.14, 14-01-10]

注:IEV 191-05-01 定义的"故障"是一种以无能力执行要求功能为特征的状态,不包括预防性维护或其他计划的行动期间的无能力或外部资源的缺少产生的无能力。两种观点的表示见图 4。

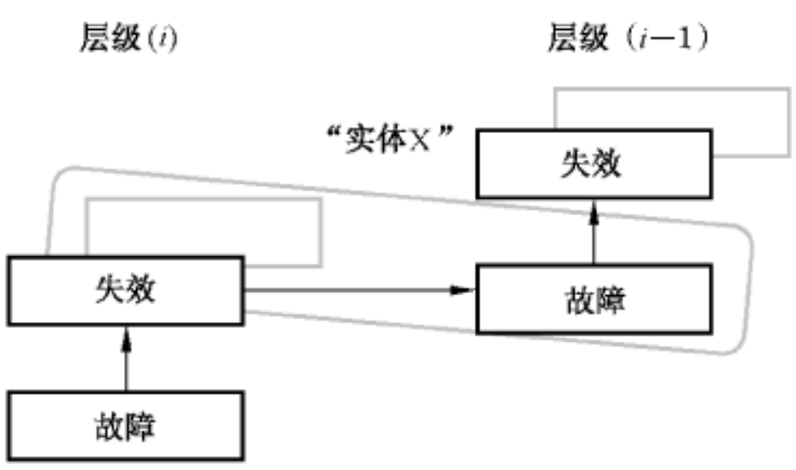


(L=层级;i=1, 2, 3 等;FU=功能单元)

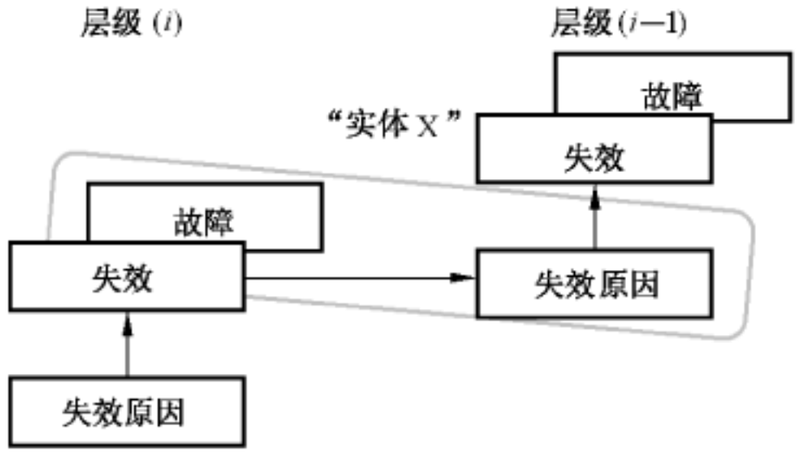
a) 一个功能单元的配置



b) 归纳的观点



c) 来自 GB/T 20438 和 GB/T 5271.14 的观点



d) 来自 IEC 60050(191)的观点

注 1:如 a)所示,可将功能单元看作一个由多层构成的层级结构,每一层都可依次叫做功能单元。在(i)层,"原因"可能是本层功能单元自身错误(偏离正确的值或状态),如不纠正或避免,则可能导致这一功能单元的失效,结果使其进入"F"状态,即不能执行要求的功能(见 b)。(i)层功能单元的"F"状态可能依次表现为($i-1$)层功能单元自身错误,如不纠正或避免,则可能导致这一($i-1$)层功能单元的失效。

注 2:在这个因果链条中,同一件事(实体 X)即可被看作这一层(i)进入"F"状态,结果是该层功能单元的失效,也可看作是($i-1$)层功能单元失效的起因。这个(实体 X)综合了 GB/T 20438 和 GB/T 5271.14 的"故障"的概念,这里强调其原因的概念,如图 c)所示,同时也是 GB/T 2900.13 中的"故障",这里强调其自身状态的概念,如图 d)所示。"F"状态在 GB/T 2900.13 中被叫做故障,但在 GB/T 20438 和 GB/T 5271.14 中没有定义。

注 3:在某些情况下,失效或错误可由外部事件引起,如闪电或静电扰动,而不是由内部故障引起。同样,没有前期失效也可能存在故障(在两处术语中)。比如设计错误就是这种故障的一个例子。

图 4 失效模型

3.6.2

故障避免 fault avoidance

在安全相关系统安全生命周期的任何阶段使用技术和规程以避免引入故障。

3.6.3

故障裕度 fault tolerance

在出现故障或错误的情况下,功能单元继续执行一个要求功能的能力。

[GB/T 5271.14，14-04-06]

注：在 IEV 191-15-05 中的定义仅涉及子项故障。见 3.6.1“故障”术语的注。

3.6.4

失效　failure

功能单元执行一个要求功能的能力的终止，或功能单元以非要求的方式运行。

注 1：本术语基于 IEV 191-04-01，增加了由于软件或规范等的不足而导致的系统性失效。

注 2：图 4 为 GB/T 20438 和 GB/T 2900.13 中故障和失效的关系 。

注 3：应该执行要求的功能以排除特定的行为，以及为要避免的行为规定某些功能。这些行为的出现即失效。

注 4：失效或是随机的(在硬件中)或是系统性的(在硬件或软件中)，见 3.6.5 和 3.6.6。

3.6.5

随机硬件失效　random hardware failure

在硬件中，由一种或几种可能的退化机理而产生的，在随机时间出现的失效。

注 1：在各种元件中，存在以不同速率发生的许多退化机理，在这些元件工作不同的时间之后，这些机理可使制造公差引起元件发生故障，从而使包含许多元件的设备将以可预见的速率，但在不可预见的时间(即随机时间)发生失效。

注 2：随机硬件失效和系统性失效(见 3.6.6)的主要区别是由随机硬件失效导致的系统失效率(或其他合适的度量)可以用合理的精度来量化，但系统性失效无法精确预计，因此系统性失效引起的系统失效率则不能精确地用统计法量化。也就是说，由随机硬件失效引起的系统失效率可以用合理的精度来量化，但是由系统性失效引起的系统失效率不能精确地用统计法量化，因为导致系统性失效的这些事件无法简单预测。

3.6.6

系统性失效　systematic failure

原因确定的失效，只有对设计或制造过程、操作规程、文档或其他相关因素进行修改后，才有可能消除这种失效。

[IEV 191-04-91]

注 1：仅修正性维护而不加修改，通常无法消除失效原因。

注 2：通过模拟失效原因可以引出系统失效。

注 3：系统性失效的原因可包括以下情况中的人为错误：

——安全要求规范；

——硬件的设计、制造、安装、运行；

——软件的设计和实现等。

注 4：在本部分中，安全相关系统的失效被分为随机硬件失效(见 3.4.5)和系统性失效。

3.6.7

危险失效　dangerous failure

对执行安全功能有影响的组件和/或子系统和/或系统的失效，其：

a)　在要求时阻止安全功能的执行(要求模式)，或导致安全功能失效(连续模式)以致 EUC 进入危险或潜在危险的状态；或

b)　降低在要求时安全功能正确执行的概率。

3.6.8

安全失效　safe failure

对于执行安全功能有影响的组件和/或子系统和/或系统的失效，其：

a)　导致安全功能的误动作从而使 EUC(或其一部分)进入或保持安全状态；或

b)　增加安全功能的误动作从而使 EUC(或其一部分)进入或保持安全状态的概率。

3.6.9

相关失效　dependent failure

其概率不能表示为引起它的独立事件的无条件概率的简单乘积的失效。

注：仅当：$P(A \text{ and } B) > P(A) \times P(B)$时，两个事件 A 和 B 才是相关的。

3.6.10

共因失效　common cause failure

在多通道系统中由一个或多个事件导致的引起两个或多个独立通道同时失效，从而导致系统失效的一种失效。

3.6.11

偏差　error

计算、观测和测量到的值或条件与真值、规定的或理论上正确的值或条件的差异。

[修改 IEV 191-05-24]

3.6.12

软错误　soft-error

数据内容不正确的变化，但并未改变物理电路。

注 1：当软错误发生并且数据被重写，电路将恢复到初始状态。

注 2：软错误可能发生在存储器、数字逻辑、模拟电路中和传输线路上，主要发生在半导体存储器上，包括寄存器和锁存器。如从制造商处获得该数据。

注 3：软错误是瞬时的并且不宜与软件编程错误混淆。

3.6.13

无关失效　no part failure

不执行安全功能的元器件失效。

注：无关失效不用于 SFF 的计算。

3.6.14

无影响失效　no effect failure

执行安全功能的某个组件失效但不直接影响安全功能。

注 1：按定义，无影响失效不影响安全功能，所以对安全功能的失效率没有贡献。

注 2：无影响失效不用于 SFF 的计算。

3.6.15

安全失效分数　safe failure fraction；SFF

安全相关组件的属性，定义为平均安全失效率加上检测出的平均危险失效率，与平均安全失效率加上平均危险失效率之比。公式如下：

$$SFF=(\sum\lambda_{Savg}+\sum\lambda_{Ddavg})/(\sum\lambda_{Savg}+\sum\lambda_{Ddavg}+\sum\lambda_{Duavg})$$

如失效率是基于一个常数失效率，则公式简化为：

$$SFF=(\sum\lambda_{S}+\sum\lambda_{Dd})/(\sum\lambda_{S}+\sum\lambda_{Dd}+\sum\lambda_{Du})$$

3.6.16

失效率　failure rate

一个实体(单个元器件或系统)的可靠性参数($\lambda(t)$)，即 $\lambda(t)\mathrm{d}t$ 表示该实体在$[0,t]$之间未发生失效情况下，在$[t,t+\mathrm{d}t]$内发生失效的概率。

注 1：数学上，$\lambda(t)$ 是每单位时间 $[t,t+\mathrm{d}t]$上失效的条件概率，其与可靠性函数(即 0～t 内未发生失效的概率)密切相关，可由公式表示：$R(t)=\exp\left(-\int_0^t\lambda(\tau)\mathrm{d}\tau\right)$。反之可由可靠性函数表示：$\lambda(t)=-\frac{\mathrm{d}R(t)}{\mathrm{d}t}\frac{1}{R(t)}$。

注 2：失效率及其不确定度可用传统的统计学由现场反馈数据估算，在使用寿命期间(即老化后至报废前)一个简单项的失效率几乎等于常量，$\lambda(t)\equiv\lambda$。

注 3：在给定区间$[0,T]$内 $\lambda(t)$的平均值，$\lambda_{avg}(T)=\left(\int_0^T\lambda(\tau)\mathrm{d}\tau\right)/T$，不是失效率，因为平均值不能用于计算注 1 中的 $R(t)$，但可解释为在这一期间失效的平均频率(即 PFH，GB/T 20438.6—2017 的附录 B)。

注 4：串联项的失效率是每一个项失效率的和。

注 5：冗余系统的失效率一般不是一个常量。不过，当所有失效能很快被发现，而且是独立的并很快修复，$\lambda(t)$就会很快的收敛于一个近似值λ_{as}，λ_{as}即相当于系统失效率。与注 3 所说的平均失效率不同，平均失效率不需要收敛于近似值。

3.6.17

要求时危险失效概率　probability of dangerous failure on demand；PFD

当 EUC 或 EUC 控制系统发出要求时，执行规定安全功能的 E/E/PE 安全相关系统的安全不可用性(见 GB/T 2900.13)。

注 1：[瞬时]不可用性(按照 GB/T 2900.13)是指一个项在要求的外部资源满足的情况下，在给定的时间点和给定条件下，没有处于执行给定功能的状态的概率。通常用 $U(t)$表示。

注 2：[瞬时]可用性与项在 t 时刻之前经历的状态(运行或失效)无关。它仅表示项在要求时一定能工作，例如在低要求模式下 E/E/PE 安全相关系统的工作。

注 3：如果实施周期性测试，就规定安全功能而言，E/E/PE 安全相关系统的 PFD 是用一种锯齿形曲线表示，在一个大的概率范围内，从刚经过一次测试后的低点到下次测试前的最大值。

3.6.18

要求时危险失效平均概率　average probability of dangerous failure on demand；PFD_{avg}

E/E/PE 安全相关系统在 EUC 或 EUC 控制系统发出要求时执行规定安全功能的平均不可用性(见 GB/T 2900.13)。

注 1：在一个给定时间间隔$[t_1,t_2]$内的平均不可用性用$U[t_1,t_2]$表示

注 2：两种失效会影响 PFD 和 PFD_{avg}：自上次检验测试后发生的未检测到的危险失效和由要求(检验测试和安全要求)本身导致的真实的要求时失效。第一个与时间相关并且由其危险失效率$\lambda_{DU}(t)$表示，而第二个仅与要求的数量相关并由每次要求失效的概率表示(用 γ 表示)。

注 3：因为真实的要求时失效不能通过测试检测到，有必要将他们识别出来并在计算目标失效量时加以考虑。

3.6.19

每小时危险失效平均频率　average frequency of a dangerous failure per hour；PFH

一个 E/E/PE 安全相关系统在一个给定的时间周期内执行规定安全功能时的危险失效平均频率。

注 1：GB/T 20438 不再使用术语“每小时危险失效的概率”，但仍然保留缩略语 PFH，当使用 PFH 时表示的意思是“危险失效平均频率[h^{-1}]”

注 2：从理论的角度看，PFH 是无条件失效强度的平均值，也可称为失效频率，通常用 $w(t)$表示。不宜将 PFH 与失效率混淆(见 GB/T 20438.6—2017 的附录 B)。

注 3：当 E/E/PE 安全相关系统是最终的安全层，PFH 宜根据其不可靠性 $F(T)=1-R(t)$计算(见上面的“失效率”)。当其不是最终的安全相关系统时，PFH 宜根据其不可用性$U(t)$计算(见上面的 PFD)。在第一种情况下，PFH 可近似等于 $F(T)/T$ 和 1/MTTF，在第二种情况下为 1/MTBF。

注 4：当 E/E/PE 安全相关系统仅隐含有能够被快速修复的可揭露失效时，那么收敛的失效率 λ_{as}可以快速达到。它提供了一种对 PFH 的估算。

3.6.20

过程安全时间　process safety time

从 EUC 或 EUC 控制系统中引发潜在危险事件的失效发生，到为阻止在 EUC 中危险事件发生而必须采取的动作完成之间的时间间隔。

3.6.21

平均恢复时间　mean time to restoration ；MTTR

达到恢复的预期时间。

注：MTTR 包括：

——检测失效的时间(a)；和

——开始维修前已过去的时间(b)；和

——维修的有效时间(c)；和

——元件恢复运行前的时间(d)。

(b) 的开始时间是(a)的结束时间 ,(c)的开始时间是 (b)的结束时间,(d)的开始时间是 (c)的结束时间。

3.6.22

平均维修时间　mean repair time;MRT

预期的整体维修时间。

注：MRT 包含 MTTR 中的时间(b)、(c) 和(d)(见 3.6.21)。

3.7　生命周期活动

3.7.1

安全生命周期　safety lifecycle

安全相关系统实现过程中所必需的活动,这些活动从项目的概念阶段开始,直至所有的 E/E/PE 安全相关系统和其他风险降低措施停止使用为止的时间周期。

注 1：严格地讲,用"功能安全生命周期"这个术语更准确,但在本部分中没必要用"功能"这个形容词。

注 2：本部分中使用的安全生命周期模型见 GB/T 20438.1—2017 的图 2、图 3 和图 4。

3.7.2

软件生命周期　software lifecycle

从软件开始构思到软件永久退役期间的活动。

注 1：一个典型的软件生命周期包括需求阶段、开发阶段、测试阶段、集成阶段、安装阶段和修改阶段。

注 2：软件不能进行维护,但可以进行修改。

3.7.3

配置管理　configuration management

系统演变过程中其元件的标识规则,用以控制这些元件的变更并保持在生命周期全过程中的连续性和可追溯性。

注：软件配置管理的细节见 GB/T 20438.7—2017 的 C.5.24。

3.7.4

配置基线　configuration baseline

以可审核的和系统的方式重建软件发布所需的信息,包括:所有源代码、数据、运行时文件、文档、配置文件、以及构成软件发布的安装脚本;有关编译器、操作系统,以及用于创建软件发布的开发工具的信息。

3.7.5

影响分析　impact analysis

确定一个系统中的一个功能或元件的改变将对该系统中其他功能或元件以及其他系统产生影响的活动。

注：软件的内容见 GB/T 20438.7—2017 的 C.5.23。

3.8　安全措施的证实

3.8.1

验证　verification

通过检查和提供客观证据证实规定要求已经被满足。

[修改 ISO 8402,定义 2.7.4]

注：本部分中,验证是指在有关的安全生命周期(整体、E/E/PE 系统和软件)的每个阶段进行的分析、数学论证和/或测试等证明活动,这样,针对具体的输入,其输出能满足该阶段所有方面的目的和要求。

举例:验证活动包括:

——为保证符合阶段的目的和要求,考虑该阶段的具体输入,对其输出(来自所有安全生命周期阶段的文档)进行

复审；

——设计复审；

——对设计的产品进行测试以保证按其规范工作；

——对系统不同部分逐步组装并进行集成测试，并进行环境测试以保证所有部分按规定方式在一起工作。

3.8.2

确认　validation

通过检查和提供客观证据来证明某一具体预期用途的特定要求已被满足。

[修改 ISO 8402，定义 2.18]

注 1：在本部分中有 3 个确认阶段：

——整体安全确认(见 GB/T 20438.1—2017 的图 2)；

——E/E/PE 系统确认(见 GB/T 20438.1—2017 的图 3)；

——软件确认(见 GB/T 20438.1—2017 图 4)。

注 2：确认是证明所考虑的安全相关系统在安装前后全面满足该系统的安全要求规范的活动，比如软件确认意味着用提供客观证据和检查的方法来证明软件满足软件安全要求规范。

3.8.3

功能安全评估　functional safety assessment

通过调查，依据证据来判断一个或多个 E/E/PE 安全相关系统和/或其他风险降低措施实现的功能安全。

3.8.4

功能安全审核　functional safety audit

系统性的、独立的检查，用以确定符合计划安排的功能安全要求的规程是否有效地执行并满意地达到规定目的。

注：功能安全审核可以作为功能安全评估的一部分。

3.8.5

检验测试　proof test

周期性测试，用以检测安全相关系统中危险的隐性失效，在必要时通过维修，把系统复原到“新的”状态或实际上接近这种状态。

注 1：在本部分中使用“检验测试”，但要注意到同义的术语“周期性测试”。

注 2：检验测试的有效性取决于失效覆盖和维修的有效性。在实践中除了低复杂 E/E/PE 安全相关系统外，100% 的隐性失效的检测很难达到。这宜是目标。至少，所有要执行的安全功能，按 E/E/PE 安全相关系统安全要求规范进行检查。如果使用分离通道，则对每个通道分别进行检验测试。对于复杂的组件，可能需进行分析，以证明在 E/E/PE 安全相关系统整体生命周期期间，未被检验测试检测出的隐性危险失效概率可忽略不计。

注 3：检验测试需要一定时间完成。在此时间内 E/E/PE 安全相关系统可能被部分或全部限制。在测试过程中，仅当 EUC 已停机或 E/E/PE 安全相关系统仍能保持在要求时的动作能力，检验测试持续时间可忽略不计。

注 4：在检验测试期间，E/E/PE 安全相关系统可能部分或全部不能响应动作要求。仅在维修时 EUC 已停机或使用其他等效的风险措施来代替时，MTTR 对于 SIL 的计算可以忽略。

3.8.6

诊断覆盖率　diagnostic coverage

DC

通过自动在线诊断测试检测到的危险失效分数。危险失效分数是由检测到的危险失效率除以总危险失效率计算出的。

注 1：危险失效诊断覆盖率是由下式计算的，式中 *DC* 表示诊断覆盖率，λ_{DD} 表示检测到的危险失效率，λ_{Dtotal} 表示总的危险失效率。

$$DC = \sum\lambda_{DD} / \sum\lambda_{Dtotal}$$

注 2：该定义仅在单个元件失效率为常数时适用。

3.8.7

诊断测试间隔　diagnostic test interval

在一个已经规定了诊断覆盖率的安全相关系统中，为检测故障而进行的在线测试的间隔。

3.8.8

检测到的　detected

揭露出的　revealed

显性的　overt

与硬件相关，用诊断测试、检验测试、操作员干预（例如物理检查和人工测试）或通过正常操作所发现的。

举例：这些形容词用于检测到的故障和检测到的失效。

注：由诊断测试检测到的危险失效是一种揭露出的失效，并且当采取了自动或手动的有效的措施可将其归类为安全失效。

3.8.9

未检测到的　undetected

未揭露的　unrevealed

不明显的　covert

与硬件有关，用诊断测试、检验测试、操作员干预（例如物理检查和人工测试）或通过正常操作未发现的。

举例：这些形容词用于未检测到的故障和未检测到的失效。

3.8.10

评估方　assessor

执行功能安全评估的一人、多人或组织，用以判断 E/E/PE 安全相关系统和其他风险降低措施实现的功能安全。

注：见 GB/T 20438.1—2017 的第 8 章。

3.8.11

独立人员　independent person

与整体的、E/E/PE 系统的或软件的安全生命周期特定阶段中的活动分开且不直接负责，但又从事功能安全评估或确认的人。

3.8.12

独立部门　independent department

与对整体的、E/E/PE 系统的或软件的安全生命周期的特定阶段中的活动负责的部门分开，但又从事功能安全评估或确认的部门。

3.8.13

独立组织　independent organization

用管理或其他办法与对整体的、E/E/PE 系统的或软件的安全生命周期特定阶段中的活动负责的组织分开，但又从事功能安全评估或确认的组织。

3.8.14

动画　animation

软件系统（或系统的某一重要部分）的模拟仿真运行，以显示系统行为的主要面貌，例如以适当形式或系统设计的高级表述来表示要求规范。

注：由于动画可以增进人们对规定行为的认识，因此可以提高人们对系统满足要求的置信度。

3.8.15

动态测试　dynamic testing

用系统性的和受控的方式执行软件和/或操作硬件以证明所要求行为的存在以及非要求行为的不

存在。

注：动态测试与静态分析不同，后者不要求执行软件或不要求硬件处于运行之中。

3.8.16

测试用具　test harness

通过把测试用例应用于软件，模拟（达到某个可用的程度）开发中软件或硬件运行环境并记录其响应的设施。

注：测试用具也可能包括测试用例生成器和验证测试结果的设施（自动比对被认为是正确的值或人工分析）。

3.8.17

符合项安全手册　safety manual for compliant items

为确保系统满足 GB/T 20438 标准的要求，针对规定的组件安全功能，提供与组件功能安全有关的所有信息的文档。

3.8.18

经使用证明　proven in use

针对一个组件的特定配置，基于对其运行经验的分析，证明危险的系统性故障的可能性足够低，使得每个使用该组件的安全功能达到其要求的安全完整性等级。

参 考 文 献

[1] GB/T 21109(所有部分) 过程工业领域安全仪表系统的功能安全

[2] GB 28526—2012 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全

[3] GB/T 12668.502 调速电气传动系统 第5-2部分:安全要求 功能

[4] GB/T 20438.5—2017 电气/电子/可编程电子安全相关系统的功能安全 第5部分:确定安全完整性等级的方法示例

[5] GB/T 20438.6—2017 电气/电子/可编程电子安全相关系统的功能安全 第6部分:GB/T 20438.2 和 GB/T 20438.3 的应用指南

[6] GB/T 20438.7—2017 电气/电子/可编程电子安全相关系统的功能安全 第7部分:技术和措施概述

[7] ISO/IEC 2382-1:1993 Information technology—Vocabulary—Part 1: Fundamental terms

[8] GB/T 15969.3—2005 可编程序控制器 第3部分:编程语言

[9] GB/T 17215.911 电测量设备 可信性 第11部分:一般概念

[10] ISO 8402:1994 Quality management and quality assurance—Vocabulary

[11] IEC 60601 (all parts) Medical electrical equipment

[12] GB/T 2900.13—2008 电工术语 可信性与服务质量

[13] GB/T 2900.56—2008 电工术语 控制技术

[14] GB/T 20438.1—2017 电气/电子/可编程电子安全相关系统的功能安全 第1部分:一般要求

[15] GB/T 20438.2—2017 电气/电子/可编程电子安全相关系统的功能安全 第2部分:电气/电子/可编程电子安全相关系统的要求

[16] GB/T 20438.3—2017 电气/电子/可编程电子安全相关系统的功能安全 第3部分:软件要求

[17] GB/T 5271.14—2008 信息技术 词汇 第14部分:可靠性、可维护性与可用性

[18] GB/T 19000—2008 质量管理体系 基础和术语

索　引

汉语拼音索引

英文对应词索引

P

R

S

T

U

V

GB/T 20438.4-2017

*
书号:155066・1-57847