ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.4—2006/IEC 61508-4:1998

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 61508-4:1998,IDT)

2006-07-25 发布　　2007-01-01 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—2006/IEC 61508-4:1998
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.5 字数 41 千字
2007年1月第一版 2007年1月第一次印刷
*
书号:155066·1-28710 定价 14.00 元

GB/T 20438.4-2006

前　言

GB/T 20438 由下列 7 部分构成：

——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。

本部分是 GB/T 20438 的第 4 部分。

本部分等同采用国际标准 IEC 61508-4:1998《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》(英文版)。

本部分与 IEC 61508-4:1998 在技术内容上没有差异，为便于使用做了下列编辑性修改：

a) 将“IEC 61508”改为“GB/T 20438”。

b) “本国际标准”一词改为“本标准”。

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和控制标准化技术委员会(SAC/TC124)归口。

本部分由机械工业仪器仪表综合技术经济研究所负责起草。

本部分主要起草人：冯晓升、王莉、梅恪、郑旭、欧阳劲松等。

引　言

由电气和电子器件构成的系统，多年来在许多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（PES））在许多领域中用于非安全目的，但也越来越多地用于安全目的，为使计算机系统技术更有效安全地使用，有必要进行安全方面的指导。

GB/T 20438 针对由电气或电子和可编程电子部件构成的、起安全作用的电气/电子/可编程电子系统（E/E/PES）的整体安全生命周期，提出了一个通用的方法。建立统一方法的目的是为了针对以电子为基础的安全相关系统提出一种一致的、合理的技术方针，主要目标是促进应用领域标准的制定。

在许多情况下，可用多种基于不同技术的防护系统来保证安全（如机械的、液压的、气动的、电气的、电子的、可编程电子的，等等）。从安全战略角度，不仅要考虑各独立系统中所有元器件的问题（如传感器、控制器、执行器等），而且要考虑由所有安全相关系统构成的组合安全相关系统的问题。因此 GB/T 20438对电气/电子/可编程电子（E/E/PE）安全相关系统进行了规定。GB/T 20438 还提出了一个框架，在这个框架内，基于其他技术的安全相关系统也可同时被考虑进去。

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/PES。对每个特定的应用，则根据应用的不同而确定所需的安全量。GB/T 20438 仅是使这些量值规范化。

GB/T 20438

——考虑了当使用 E/E/PES 执行安全功能时，所涉及到的整体安全生命周期、E/E/PES 安全生命周期以及软件安全生命周期的各阶段（如初始构思，整个设计、实现、运行、维护及停用）；

——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。

——有利于促进 E/E/PE 安全相关系统在不同领域中相关标准的制定，各应用领域和交叉应用领域相关标准应在 GB/T 20438 的框架下制定，使之具有高水平的一致性（如基础原理、术语等的一致性）并将既安全又经济。

——为达到 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。

——使用了一个安全完整性等级，此安全完整性等级规定了 E/E/PE 安全相关系统要实现的安全功能的目标安全完整性等级。

——采用了一种基于风险的方案来确定安全完整性等级要求。

——建立了 E/E/PE 安全相关系统的数值目标失效量，这些量都同安全完整性等级相联系。

——建立了危险失效模式中目标失效量的一个下限，此下限是对单一 E/E/PE 安全相关系统的要求。

这些系统运行在：

1）　低要求操作模式下，为了执行它的设计功能，一旦要求时，就把下限设定成平均失效概率为 10^{-5}；

2）　高要求操作模式或者连续操作模式下，下限设定成危险失效概率为 10^{-9}/h。

注：单一 E/E/PE 安全相关系统不一定是单通道结构。

——采用广泛的原理、技术和措施以达到 E/E/PE 安全相关系统的功能安全，但不使用失效-安全的概念，这个概念是在很好定义了失效模式，并且复杂性相对较低时的一个数值。由于 E/E/PE 安全相关系统的复杂性均在 GB/T 20438 范围之内，因此不适用失效-安全的概念。

目　次

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的第1至第7部分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,因此对这些组的标题可不去考虑。

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,尽管它们不适用于简单E/E/PE安全相关系统(见3.4.4),作为基础的安全标准,根据IEC导则104和ISO/IEC导则51中包含的原则,各技术委员会在起草标准时应考虑使用这些标准,因为技术委员会的责任之一是在起草自己标准时凡是适用之处都应贯彻基础安全标准。GB/T 20438同时也可作为独立的标准去使用。

1.4　图1表示了GB/T 20438的整体框架,同时明确了在达到E/E/PE安全相关系统功能安全过程中本部分的作用。

2　规范性引用文件

下列文件中的条款通过GB/T 20438的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 20438.1—2006　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(IEC 61508-1:1998,IDT)

GB/T 20438.2—2006　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(IEC 61508-2:2000,IDT)

GB/T 20438.3—2006　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(IEC 61508-3:1998,IDT)

GB/T 20438.5—2006　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(IEC 61508-5:1998,IDT)

GB/T 20438.6—2006　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(IEC 61508-6:2000,IDT)

GB/T 20438.7—2006　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(IEC 61508-7:2000,IDT)

ISO/IEC 2382-14:1998　数据处理　术语　第14部分:可靠性、可维修性和可用性

ISO/IEC导则51:1990　安全方面　在标准中引入安全条款的指南

ISO 8402:1994　质量管理和质量保证　术语

IEC导则104:1997　安全出版物的编写及基本安全出版物和分类安全出版物的应用

IEC 60050(191):1990　国际电工术语(IEV)　第191章:服务质量和可靠性

IEC 60050(315):1975　国际电工术语(IEV)　第351章:自动控制

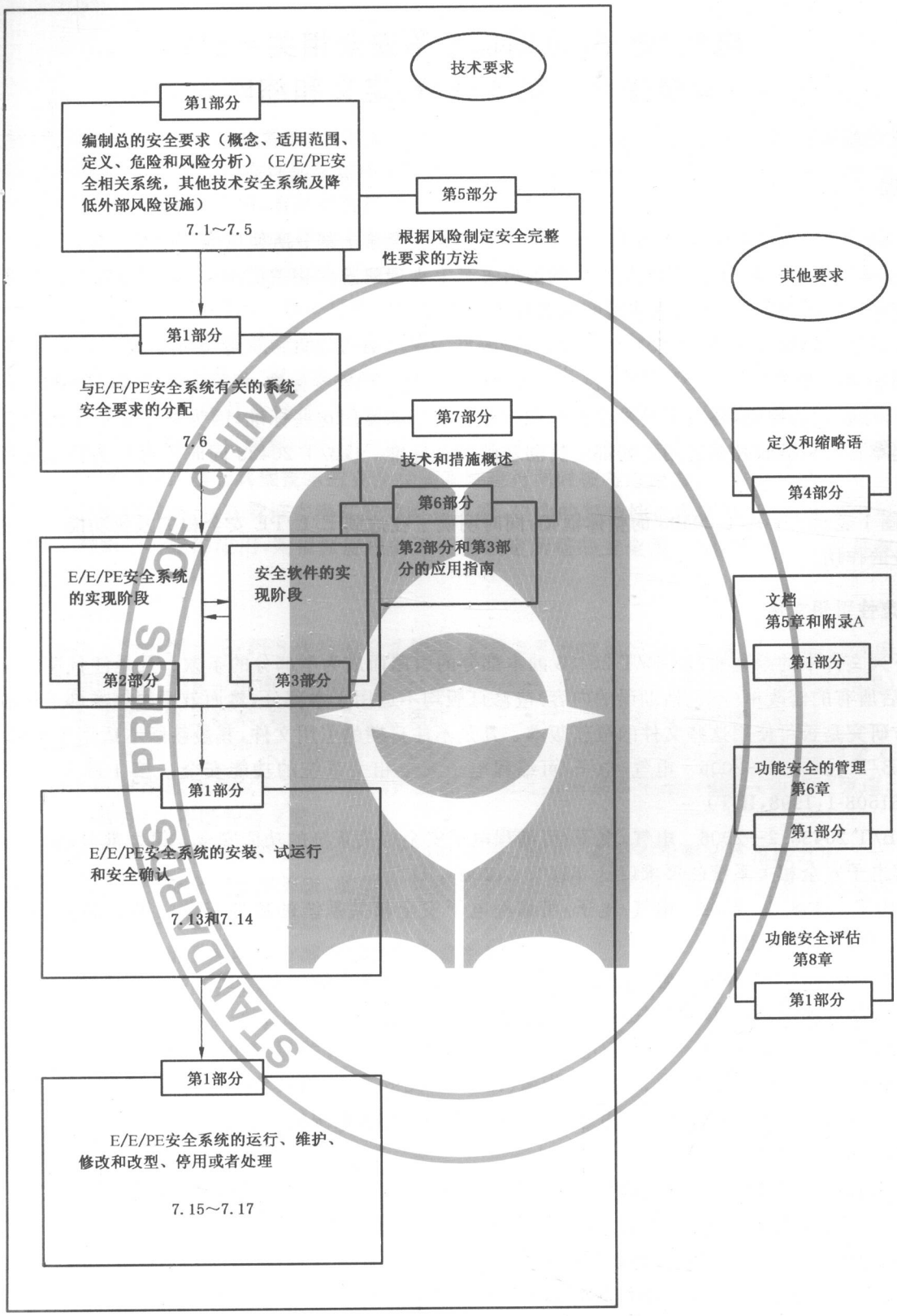


图 1　GB/T 20438 的整体框架

3 定义和缩略语

表1给出了GB/T 20438中使用的缩略语及定义。

表1 GB/T 20438中使用的缩略语

缩略语	全　称	术语定义和(或)解释
MooN	N通道结构中的M(如1oo2为2通道结构中的1)	GB/T 20438.6—2006 附录B
MooND	带诊断的N通道结构中的M	GB/T 20438.6—2006 附录B
ALARP	在合理可行的前提下尽可能低	GB/T 20438.5—2006 附录B
E/E/PE	电气/电子/可编程电子	3.2.6
E/E/PES	电气/电子/可编程电子系统	3.3.3
EUC	受控设备	3.2.3
PES	可编程电子系统	3.3.2
PLC	可编程逻辑控制器	GB/T 20438.6—2006 附录E
SIL	安全完整性等级	3.5.6

3.1 安全术语

3.1.1

伤害　harm

由于对财产或环境的破坏而导致的直接或间接地对人体健康的损害或对人身的损伤。

[ISO/IEC 导则51:1990(修改)]

3.1.2

危险　hazard

伤害的潜在根源。

[ISO/IEC 导则51:1990]

注：该术语包括短时内发生的对人员的威协(如着火或爆炸),以及对人体健康长时间有影响的那些威胁(如有毒物质的释放)。

3.1.3

危险情况　hazardous situation

人暴露于危险的环境。

3.1.4

危险事件　hazardous event

导致伤害的危险情况。

3.1.5

风险　risk

出现伤害的概率及该伤害严重性的组合。

[ISO/IEC 导则51:1990(修改)]

注：对这一概念的进一步讨论见GB/T 20438.5—2006附录A。

3.1.6

允许风险　tolerable risk

根据当今社会的水准,在给定的范围内能够接受的风险。

注：见GB/T 20438.5—2006附录B。

3.1.7

残余风险　residual risk

采取防护措施以后仍存在的风险。

3.1.8

安全　safety

不存在不可接受的风险。

3.1.9

功能安全　functional safety

与 EUC 和 EUC 控制系统有关的整体安全的组成部分，它取决于 E/E/PE 安全相关系统、其他技术安全相关系统和外部风险降低设施功能的正确行使。

3.1.10

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。

3.1.11

合理的可预见的误用　reasonable foreseeable misuse

由于产品、过程或服务加上人的行为习惯而导致的，或者作为人的行为习惯的一个结果有可能发生的，未按照供方要求的条件和用途对产品、过程和服务的使用。

3.2　**设备和装置**

3.2.1

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。

注：在 IEV 191-01-01 中，常用“项目(item)”一词代替功能单元，一个项目有时可能包括人员在内。

[ISO/IEC 2382-14-01-01]

3.2.2

软件　software

包括程序、规程、数据、规则以及相关的数据处理系统操作文档在内的智能创作。

注 1：软件与其记录媒体无关。

注 2：该定义不带有注 1 与 ISO 2382-1 不同，而且完整的定义与 ISO 9000-3 不同之处在于增加了一个词“数据”。

3.2.3

受控设备　equipment under control；EUC

用于制造、加工、运输、制药或其他活动的设备、机器、器械或成套装置。

注：EUC 控制系统与 EUC 是不同的并且是分开的。

3.2.4

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：本文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 E/E/PE 安全相关系统、其他技术安全相关系统和外部风险降低设施被用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—2006 的图 A.1 简要说明了 EUC 风险。确定 EUC 风险的主要目的是在未使用 E/E/PE 安全相关系统、其他技术安全相关系统和外部风险降低设施之前建立一个风险参考点。

注 3：风险评估应包括相关的人的因素。

3.2.5

可编程电子　programmable electronic;PE

可编程电子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(CPU)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(ASIC);

——可编程逻辑控制器(PLC);

——其他以计算机为基础的装置(智能传感器、变送器、执行器)。

3.2.6

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:

——电-机装置(电气);

——使用电晶体的非可编程电子装置(电子);

——以计算机技术为基础的电子装置(可编程电子)(见 3.2.5)。

3.2.7

有限可变语言　limited variability language

能力范围局限于应用的,用于工商业可编程电子控制器的,文本的或图形的软件编程语言。

举例:

下列引自 IEC 61131-3 和其他地方的有限可变语言,用来表示 PLC 系统的应用程序。

——梯形图:一种图形语言,由线条(指出电流流向)将一系列输入符号(代表相似装置的行为,如常开接点和常闭接点)和输出符号(代表相似继电器的行为)连接构成。

——布尔代数:带有增加某些记忆指令能力的、基于布尔运算符(如 AND、OR 和 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、移位寄存器和序列发生器指令等。

——顺序功能图:有顺序的程序的图形表示,由相互联系的步骤、动作和带转换条件的定向连接线构成。

3.3　**系统:一般概念**

3.3.1

系统　system

按照设计相互作用的一组元素,可能包括相互作用的硬件、软件和人等。系统中的某一元素也可自成一个另外的系统,称为子系统,子系统可以是控制系统也可以是被控系统。

注 1:人可以是系统的一部分(另见 3.4 注 5)。

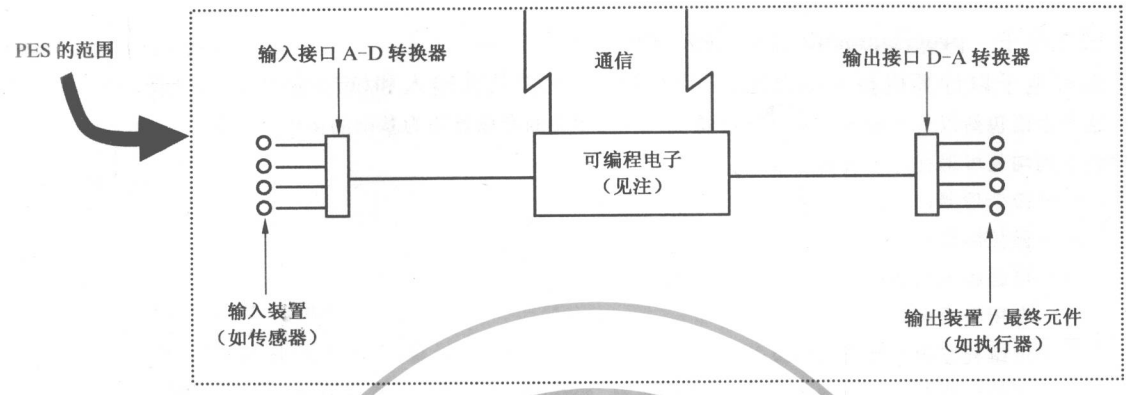
注 2:本定义不同于 IEV351-01-01。

3.3.2

可编程电子系统　programmable electronic system;PES

基于一个或多个可编程电子装置的控制、防护或监视系统,包括系统中所有的元素,诸如电源、传感器和其他输入装置,数据高速公路和其他通信路径,以及执行器和其他输出装置(见图 2)。

注:图 2a)所示为一个 PES 的结构。图 2b)所示为 GB/T 20438 中表示 PES 的方式,在这里可编程电子被表示成与 EUC 及其接口中的传感器和执行器不同的一个单元。但在 PES 中,可编程电子可能出现在许多地方。图 2c)所示为一个 PES 具有两个分立的可编程电子单元。图 2d)所示为一个 PES 具有两个并联的可编程电子单元(即双通道),且只有单个传感器和单个执行器。



a）PES 基本结构

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）具有双可编程电子装置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）

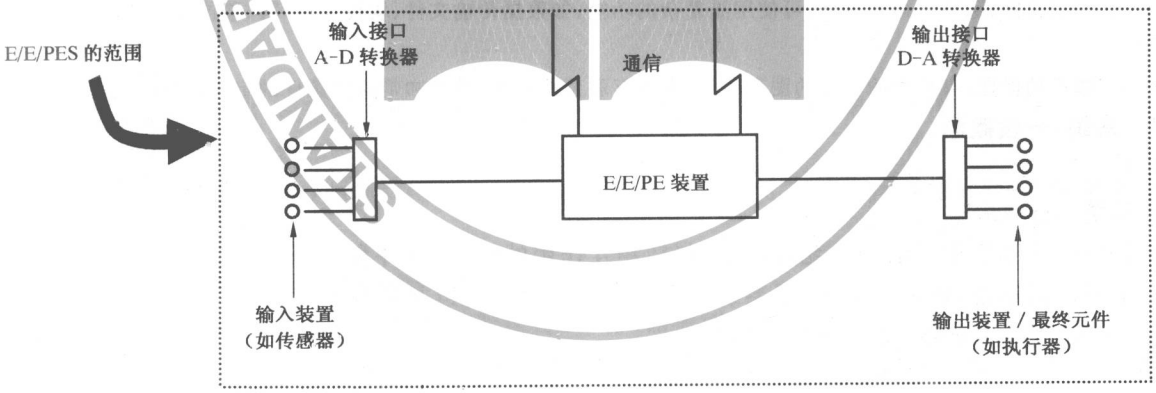
注：可编程电子位于图的中央位置，但在 PES 中可位于几个不同的位置。

图 2　可编程电子系统(PES)：结构和术语

3.3.3

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

基于一个或多个电气/电子/可编程电子(E/E/PE)装置的用于控制、防护或监视的系统，包括系统中所有的元素，诸如电源、传感器和其他输入装置，数据高速公路和其他通信途径，以及执行器和其他输出装置(见图 3)。



注：E/E/PE 装置位于图的中央位置，但在 E/E/PES 中可位于几个不同的位置。

图 3　电气/电子/可编程电子系统(E/E/PES)：结构和术语

3.3.4

EUC 控制系统　EUC control system

对来自过程和(或)操作者的输入信号起反应，产生能使 EUC 按要求的方式工作的输出信号的系统。

注：EUC 控制系统包括输入装置和最终元件。

3.3.5

结构 architecture

在一个系统中硬件和软件元素的特定配置。

3.3.6

模块 module

程序、分立部件、封装程序的一个功能集，或一组归并在一起的分立部件。

3.3.7

软件模块 software module

由规程和(或)数据说明组成的构造，并能与其他这样的构造相互作用。

3.3.8

通道 channel

独立执行一个功能的一个或一组元素。

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1：在通道中的元素可能包括输入/输出模块、逻辑系统(见3.4.5)、传感器和最终元件。

注2：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)。

3.3.9

多样性 diversity

执行一个要求功能的不同方法。

举例：可用不同的物理方法或不同的设计途径来达到多样性。

3.3.10

冗余 redundancy

对于执行一个要求功能的功能单元或对于表示信息的数据而言，除了够用之外还有多余。

举例：功能部件加倍和奇偶校验位的附加都是冗余的例子。

注1：冗余主要用于提高可靠性或可用性。

注2：IEV 191-15-01中的定义不够完整。

[ISO/IEC 2382-14-01-12]

3.4 **系统：安全方面**

3.4.1

安全相关系统 safety-related system

所指的系统：

——必需要能实现要求的安全功能以达到或保持EUC的安全状态；并且

——自身或与其他E/E/PE安全相关系统、其他技术安全相关系统或外部风险降低设施一道，能够达到要求的安全功能所需的安全完整性。

注1：这条术语是指这样的系统，即所谓安全相关系统是指它们，及与外部风险降低设施一道(见3.4.3)达到必要的风险降低量，以满足所要求的允许风险(3.1.6)，另见GB/T 20438.5—2006附录A。

注2：安全相关系统是在接受命令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被包括在导致危险或危害的事件中。尽管存在可能具备安全功能的其他系统，但已指定的安全相关系统仅是指靠其自身能力达到要求的允许风险的安全相关系统。安全相关系统一般分为安全控制系统和安全防护系统，并且具有两种操作模式(见3.5.12)。

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接口，即可通过实现EUC控制系统中的安全功能(也可能通过分开的和独立的附加系统)达到要求的安全完整性等级，或者利用分离、独立、专门的安全相关系统实现安全功能。

注4：安全相关系统可能包括：

a) 被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没有危险事件发生)。

b) 被用来减轻危险事件的影响，即通过减轻后果的办法来降低风险。

c) 同时具有 a)和 b)的组合功能。

注 5：人也可作为安全相关系统的一部分(3.3.1)，例如，人可以接收来自可编程电子装置的信息，并通过可编程电子装置按接收信息要求执行安全动作。

注 6：该术语包括执行安全功能所需的全部硬件、软件以及支持服务(如电源)。(传感器，其他输入装置，最终元件(执行器)和其他输出装置也包括在安全相关系统中。)

注 7：安全相关系统的技术基础范围可以十分广泛，包括电气、电子、可编程电子、液压和气动等。

3.4.2

其他技术安全相关系统 other technology safety-related system

基于电气/电子/可编程电子技术之外的安全相关系统。

举例：安全阀就是一种其他技术安全相关系统。

3.4.3

外部风险降低设施 external risk reduction facility

不使用 E/E/PE 安全相关系统或其他技术安全相关系统，且与上述系统分开并不同的降低或减轻风险的手段。

举例：排放系统、防火墙和堤都是外部风险降低设施。

3.4.4

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

一种 E/E/PE 安全相关系统(见 3.2.6 和 3.4.1)，其中：

——已很好确定了每个单独部件的失效模式；

——能完全确定在故障状况下系统的行为。

注：在故障状况下系统行为可用试验和/或分析的方法确定。

举例：包括一个或几个限位开关，可能还要通过一些承插式机电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简单 E/E/PE 安全相关系统。

3.4.5

逻辑系统 logic system

系统的一部分，用于执行功能逻辑，但不包括传感器和最终元件。

注：GB/T 20438 中使用下列逻辑系统：

——用于机电技术的电气逻辑系统；

——用于电子技术的电子逻辑系统；

——用于可编程电子系统的可编程电子逻辑系统。

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，为达到或保持 EUC 的安全状态，由 E/E/PE 安全相关系统、其他技术安全相关系统或外部风险降低设施实现的功能(见 3.4.1)。

3.5.2

安全完整性 safety integrity

在规定的条件下和规定的时间内，安全相关系统成功实现所要求的安全功能的概率。

注 1：安全相关系统的安全完整性等级越高，安全相关系统不能实现所要求的安全功能的概率就越低。

注 2：安全相关系统有 4 种安全完整性等级(见 3.5.6)。

注 3：在确定安全完整性的过程中，应包括导致非安全状态的所有失效(随机硬件失效和系统失效)的起因，例如硬件失效，软件导致的失效以及由电气干扰引起的失效，其中有些类型的失效，尤其是随机硬件失效，在危险失效模式中，可用失效率这样的量来量化，对一个安全防护系统而言，可以用有要求时不能工作的概率来量化，但是，系统的安全完整性也取决于许多因素，这些因素无法精确定量仅可定性考虑。

注 4：安全完整性由硬件安全完整性(见 3.5.5)和系统安全完整性(见 3.5.4)构成。

注 5：这一定义着重于安全相关系统执行安全功能的可靠性(见 IEV 191-12-01 对可靠性的定义)。

3.5.3

软件安全完整性　software safety integrity

在所有规定条件下和规定时间内表示软件在可编程电子系统中执行其安全功能的可能性的量值。

3.5.4

系统安全完整性　systematic safety integrity

在危险失效模式中与系统失效有关的安全相关系统安全完整性的一部分(见 3.5.2 的注 3)。

注 1:通常无法量化系统的安全完整性(一般可以与硬件安全完整性分开)。

注 2:见 3.5.2、3.5.5 和 3.6.6。

3.5.5

硬件安全完整性　hardware safety integrity

在危险失效模式中与随机硬件失效有关的安全相关系统安全完整性的一部分。

注 1:本术语涉及危险模式中的失效,即安全相关系统的这类失效将削弱其安全完整性,与本术语有关的两个参数是整体危险失效率和在要求时操作失效的概率,当为保持安全而必须保持连续控制时,使用前一可靠性参数,在安全防护系统范围中使用后一可靠性参数。

注 2:见 3.5.2,3.5.4 和 3.6.5。

3.5.6

安全完整性等级　safety integrity level;SIL

一种离散的等级(四种可能等级之一),用于规定分配给 E/E/PE 安全相关系统的安全功能的安全完整性要求。在这里,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:四种安全完整性等级的目标失效量(见 3.5.13)规定于 GB/T 20438.1—2006 的表 2 和表 3 中。

3.5.7

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

一种离散的等级(四种可能等级之一),用于规定在安全相关系统中软件的安全完整性。

注:见 3.5.3 和 3.5.6。

3.5.8

安全要求规范　safety requirement specification

一种技术规定,包括安全相关系统必须要执行安全功能的所有要求。

注:该规范分为下列两种:

——安全功能要求规范(见 3.5.9);

——安全完整性要求规范(见 3.5.10)。

3.5.9

安全功能要求规范　safety function requirement specification

一种技术规定,包括安全相关系统必须要执行的安全功能要求。

注 1:这个规范是安全要求规范的一部分(安全功能部分,见 3.5.8),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。

3.5.10

安全完整性要求规范　safety integrity requirement specification

一种技术规定,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。

注:这个规范是安全要求规范的一部分(安全完整性部分,见 3.5.8)。

3.5.11

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。

3.5.12

操作模式　mode of operation

安全相关系统使用的方式，根据其要求产生的频率而言，可为下列两种之一：

——低要求模式：在这种模式下，对一个安全相关系统提出操作要求的频率不大于每年一次和不大于二倍的检验测试频率。

——高要求或连续模式：在这种模式下，对一个安全相关系统提出操作要求的频率大于每年一次或大于二倍的检验测试频率。

注1：高要求或连续模式包括为保持功能安全实现连续控制的安全相关系统。

注2：运行于低要求模式和高要求或连续模式下的安全相关系统的目标失效量在3.5.13中定义。

3.5.13

目标失效量　target failure measure

相对于安全完整性要求要达到预计的危险模式失效概率，规定为下列两种之一：

——按要求执行设计功能的平均失效概率(对于低要求操作模式)。

——每小时危险失效的概率(对于高要求或连续操作模式)；

注：目标失效量的数值在GB/T 20438.1—2006的表2和表3中给出。

3.5.14

必要的风险降低　necessary risk reduction

为保证不超过允许风险，由E/E/PE安全相关系统、其他技术安全相关系统和外部风险降低设施达到的风险降低。

3.6　**故障、失效和错误**

3.6.1

故障　fault

使功能单元执行要求的功能的能力降低或失去其能力的异常状况。

注：IEV 191-05-01定义"故障"是一种无能力执行要求功能的特征状态，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。见图4。

[ISO/IEC 2382-14-01-10]

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中为避免发生故障而使用的技术和规程。

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。

注：IEV 191-15-05中的定义仅指子项目故障，见3.6.1的注。

[ISO/IEC 2382-14-04-06]

3.6.4

失效　failure

功能单元执行一个要求功能的能力的终止。

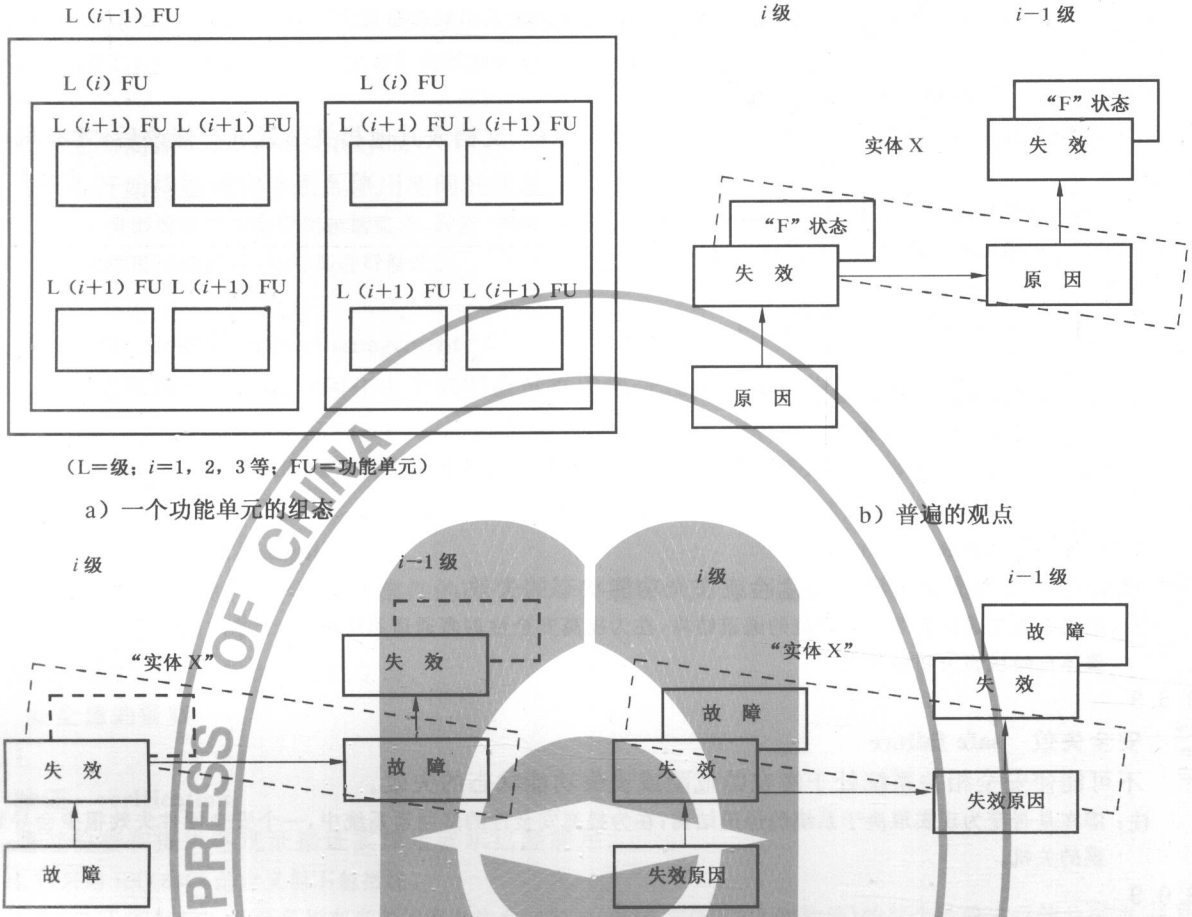
注1：与IEV 191-04-01的定义相同，但增加了注。

[ISO/IEC 2382-14-01-11]

注2：GB/T 20438和IEV50(191)中，故障和失效的关系见图4。

注3：为了排除特定的行为需要执行必要的功能，并根据要避免的行为来规定某些功能。这些行为的出现就是失效。

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



注1：如a)所示，一个功能单元可看作是一个多层的分级结构，每个级别可叫作一个功能单元。在i级中，一个“原因”本身可能表现为该级功能单元的一个错误(与正确值或正确状态的偏离)，并且如果不纠错或防止发生，则可能引起该功能单元的失效，结果它将进入“F”状态，在这种状态下它不能再执行要求的功能(见b)。i级功能单元的这种“F”状态本身也可表现为$i-1$级功能单元中的一个错误，如不纠错或防止发生也可能引起这个$i-1$级功能单元的一次失效。

注2：在这个原因和影响链中，同一个事物(“实体X”)可被看作是一个i级功能单元的一个状态(“F”状态)，此状态是因它失效才进入的，同样也可把它看作是$i-1$级功能单元的失效原因。“实体X”与GB/T 20438和ISO/IEC 2382-14中“故障”概念相结合强调它的原因方面，如c)所示，与IEC 60050(191)中的“故障”相结合，强调它的状态方面，如d)所示。“F”状态在IEC 60050(191)中称为“故障”，但它在GB/T 20438和ISO/IEC 2382-14中没有定义。

注3：有些情况下，一个失效或一个错误可由外部事件(如闪电或静电噪音)引起，而不是由内部故障引起。同样地，一个故障(在两个术语中)可能在没有预先失效的情况下发生，设计错误就是这类故障的例子。

图4 失效模型

3.6.5

随机硬件失效 random hardware failure

在硬件中，由一种或几种机能退化可能产生的、按随机时间出现的失效。

注1：在各种部件中，存在以不同速率发生的许多机器退化，在这些部件工作不同的时间之后，这些机能可使制造公差引起部件发生故障，从而使包含许多部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：随机失效和系统的失效主要区别是由随机硬件失效导致的系统失效率(或其他合适的量度)可用合理的精确度来预计，但系统失效一直就不能精确预计，因此系统失效引起的系统失效率则不能精确地用统计法量化。

3.6.6

系统失效　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，才有可能排除这种失效。

注1：仅正确维护而不加修改，无法排除失效原因。

注2：通过模拟失效原因可以导致系统失效。

[IEV 191-04-91]

注3：人为错误引起的系统失效的例子有：

——安全要求规范；

——硬件的设计、制造、安装、操作；

——软件的设计和实现等。

注4：在GB/T 20438中，安全相关系统的失效被分为随机硬件失效和系统失效(见3.6.4和3.6.5)。

3.6.7

危险失效　dangerous failure

使安全相关系统处于潜在的危险或丧失功能状态的失效。

注：潜在是否变成事实取决于系统的通道结构，在为提高安全性的多通道系统中，一个危险的硬件失效很少会导致整体危险或丧失功能状态。

3.6.8

安全失效　safe failure

不可能使安全相关系统处于潜在的危险或丧失功能状态的失效。

注：潜在是否变为现实取决于系统的通道结构；在为提高安全性的多通道系统中，一个安全硬件失效很少会导致错误的关机。

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：$P(Z)$是事件Z的概率，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

共同原因失效　common cause failure

一种失效，它是一个或多个事件导致的结果，在多通道系统中引起两个或多个分离通道同时失效，从而导致系统失效。

3.6.11

错误　error

计算、观测和测量到的值或条件与真值、规定的或理论上的正确值或条件的差异。

注：采用IEV 191-05-24的定义但不包括注。

3.6.12

人为错误　human error

失误　mistake

引发非期望结果的人的动作或不动作。

注：在IEV 191-05-25的基础上增加了“不动作”。

[ISO/IEC 2382-14 -01-09]

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生命活动，这些活动发生在从一项工程的概念阶段开始，直至所有