ICS 25.040
N 10

中华人民共和国国家标准

GB/T 20438.5—2006/IEC 61508-5:1998

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

Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 5:Examples of methods for the determination of safety integrity levels

(IEC 61508-5:1998,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

目　　次

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 5 部分。

本部分等同采用国际标准 IEC 61508-5:1998(第 1 版)《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》(英文版)。

本部分附录 A、附录 B、附录 C、附录 D、附录 E 为资料性附录。

本部分与 IEC 61508-5:1998 在技术内容上没有差异，为便于使用作了下列编辑性修改：

a) 将“IEC 61508”改为“GB/T 20438”。

b) 本“国际标准”一词改为“本标准”。

c) 删除国际标准中 1.2 中注 2，因为此注所表述的是 IEC 61508 在美国和加拿大等国的应用情况，与我国的实际不符，所以删除。

d) 用小数点“.”代替作为小数点的逗号“,”。

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/TC 124)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：王莉、梅恪、冯晓升、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的使用，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。建立统一的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，不仅要考虑各系统中元器件的问题（如传感器、控制器、执行器等），而且要考虑构成组合安全相关系统的所有安全相关系统。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生命周期的各阶段（如初始构思，整个设计、实现、运行和维护到停用）。

——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/PES 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。

——采用了一种可确定安全完整性等级要求的基于风险的方案。

——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。

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

1　范围

1.1　本部分提供以下信息:

——风险的基础概念和风险与安全完整性之间的关系(见附录A);

——提供能确定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的安全完整性等级的一系列方法(见附录B、附录C、附录D和附录E)。

1.2　方法的选择应依赖应用领域和特定环境。附录B、附录C、附录D和附录E列出了定性和定量的方法并为说明基础的原理已进行简化。这些附录已包括在说明一系列方法的通用原理中但不提供明确的计算。如使用附录中提到的方法需查询有关原始材料。

注:如想获取更多附录B、附录D和附录E中说明的方法的有关信息,参见参考文献中的[4]、[2]和[3]。对于附加的方法的描述参见参考文献中的[5]。

1.3　GB/T 20438.1、GB/T 20438.2、GB/T 20438.3和GB/T 20438.4是基础安全标准,虽然它们不适用于简单的E/E/PE安全相关系统(见GB/T 20438.4—2006 3.4.4),作为基础标准,可以在IEC导则104和ISO/IEC导则51的指导下,由相关的技术委员会使用。对于每个技术委员会,都有责任在其制定的标准中使用基础标准。同时,GB/T 20438也是一个可独立使用的标准。

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,其随后所有的修改单(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:对电气/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 20438.4—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(IEC 61508-4:1998,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导则51:1990　安全方面　在标准中引入安全条款的指南

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

3　定义和缩略语

见GB/T 20438.4。

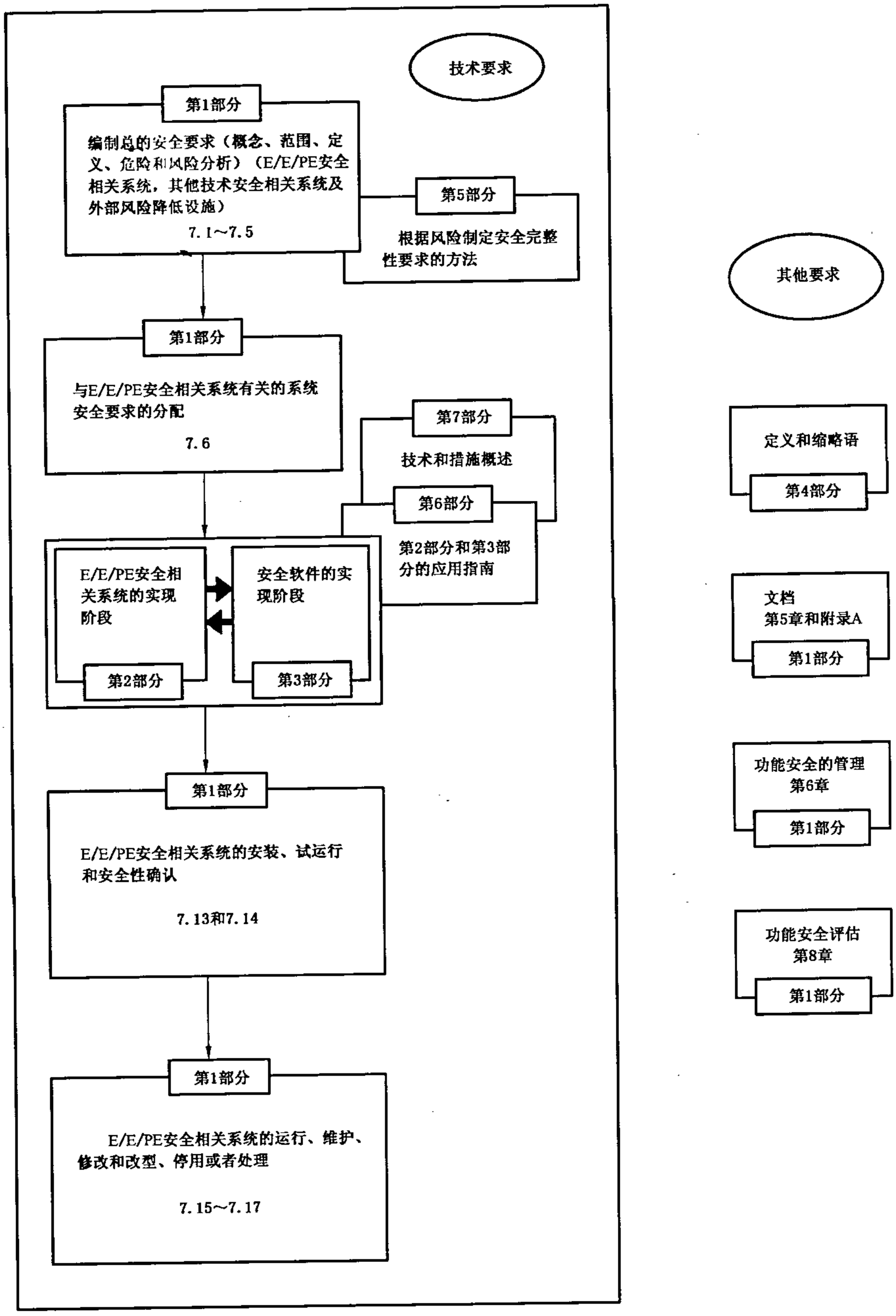


图 1　GB/T 20438 的总体框架

附 录 A
（资料性附录）
风险和安全完整性的通用概念

A.1 一般要求

本附录提供风险和风险与安全完整性之间关系基本概念的有关信息。

A.2 必要的风险降低

必要的风险降低(见 GB/T 20438.4—2006 中的 3.5.14)是降低风险来保证在特定情况下不超过允许风险(可以定性[1)]或定量[2)]说明)。必要的风险降低的概念在开发 E/E/PE 安全相关系统的安全要求方面非常重要(特别是安全要求中的安全完整性部分)。确定特定危险事件的允许风险的目的是说明危险事件的频率(或概率)和其特定后果哪一个更合理。安全相关系统应为减少危险事件的频率(或概率)和/或危险事件的后果而设计。

允许风险应依据许多因素(如伤害的严重程度、暴露在危险中的人数、一个人/多人暴露在危险中的频率和持续时间)决定。重要的因素应是暴露在危险中的人的感觉和视觉。对于一个特定应用允许风险的构成,应考虑以下一系列输入:

——相关权威安全法规的导则。

——与应用有关的不同团体的讨论与协议。

——工业标准和导则。

——国际讨论和协议;国家标准和国际标准在确定特定应用的允许风险基准中起到越来越重要的作用。

——来自咨询机构的最好的独立工业、专家和科学的建议。

——通用的和直接与特定应用有关的法律要求。

A.3 E/E/PE 安全相关系统的作用

E/E/PE 安全相关系统可满足必要的风险降低,以便符合允许风险的要求。

安全相关系统:

——实现所要求的安全功能,使受控设备达到安全状态或保持受控设备的安全状态;并

——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实现所要求的安全功能的必需的安全完整性。

注 1:定义的第一部分规定安全相关系统必须完成安全功能要求规范中规定的安全功能,例如安全功能要求规范可能说明当温度达到 x,阀 y 应打开,允许水流入管道中。

注 2:定义的第二部分规定安全功能应由对应用而言具有置信度的安全相关系统来完成,以达到允许风险。

一个人可能会是 E/E/PE 安全相关系统的一个完整部分。如一个人可作为 EUC 通过屏幕显示来获取信息,并根据这一信息完成安全操作。

E/E/PE 安全相关系统可在低要求操作模式或高要求操作模式或连续操作模式下操作。

A.4 安全完整性

安全完整性定义为在规定的条件下、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

1) 在达到允许风险的过程中,需要建立必要的风险降低,IEC 61506-5 中的附录 D 和附录 E 给出了定性方法,尽管必要的风险降低引用的例子是隐含的组合而非明显说明的。

2) 例如,导致规定后果的危险事件,其发生频率不能大于 10^{8} 次/h。

率(见 GB/T 20438.4—2006 中的 3.5.2)。安全完整性与执行安全功能的安全相关系统的性能有关(执行的安全功能将在安全功能要求规范中说明)。

安全完整性可认为由下列两个因素组成:

——硬件安全完整性。这部分安全完整性与在危险的失效模式下的随机硬件失效有关(见 GB/T 20438.4—2006 中的 3.5.5)。安全硬件安全完整性规定等级的成就可在一个合理的水平下精确估计,并将其要求用组合概率的通用法规在子系统中进行分配。可能需要使用冗余结构来达到足够的硬件安全完整性。

——系统安全完整性。这部分安全完整性与在危险的失效模式下的系统失效有关(见 GB/T 20438.4—2006 中的 3.5.4)。尽管与系统失效有关的平均失效率可估计,但从设计失效和共同原因失效获得的失效数据即失效的分布难以预计。这样便增加了特定情况下失效概率计算的不确定性(例如安全防护系统的失效概率),因此需做出选择最佳技术的判定将不确定性最小化。不必注意减少随机硬件失效概率的措施可能对系统失效的概率产生影响这一情况。像同一硬件的冗余通道的技术一样,它在控制随机硬件失效方面非常有效,但在减少系统失效方面作用非常有限。

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所要求的安全完整性必须在相应等级以保证:

——安全相关系统的失效频率足够低以防止危险事件频率超过要求的允许风险,和/或

——安全相关系统将失效后果修改至满足允许风险要求的范围内。

图 A.1 说明风险降低的通用概念。通用模式假定:

——有一个 EUC 和 EUC 控制系统。

——有关联的人为因素问题。

——安全防护特性包括:

1) 外部风险降低设施;

2) E/E/PE 安全相关系统;

3) 其他技术安全相关系统。

注:图 A.1 是说明通用原理的通用风险模型。特定应用的风险模式需考虑 E/E/PE 安全相关系统和/或其他技术安全相关系统和/或外部风险降低设施实际取得的必要的风险降低中的特定方式来开发。因此相关的风险模型可能不同于图 A.1。

图 A.1 中的各种风险为:

——EUC 风险:EUC、EUC 控制系统和有关人为因素的特定危险事件中存在的风险——在确定这一风险时未考虑指定的安全防护特性。

——允许风险:根据当今社会水平所能接受的风险(见 GB/T 20438.4—2006 中的 3.1.6)。

——残余风险:标准文本中,残余风险是使用了附加外部风险降低设施、E/E/PE 安全相关系统和其他技术安全相关系统(见 GB/T 20438.4—2006 中的 3.1.7)后,存在于 EUC、EUC 控制系统、人为因素的特定危险事件中的风险。

EUC 风险是一种与 EUC 本身有关的风险功能,但也考虑 EUC 控制系统带来的风险降低。为防止对 EUC 控制系统提出不合理的安全完整性要求,GB/T 20438 对可提出的要求进行了限制(见 GB/T 20438.1—2006 中的 7.5.2.5)。

必要的风险降低是通过所有安全防护性能的结合获得的。图 A.1 表示了从 EUC 风险的开始点获得特定允许风险的必要的风险降低。

A.5 风险和安全完整性

正确区分并完全理解风险和安全完整性是非常重要的。风险是对一个特定危险事件出现的概率和结果的估量,可以对不同情况的风险进行评价(EUC 风险、要求满足允许风险的风险、实际风险(见图 A.1))。允许风险根据社会基础和有关社会和政治因素的考虑来确定。安全完整性只应用于 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，并作为这些系统/功能在规定安全功能方面取得必要的风险降低的概率的措施。一旦确定了允许风险，并估计了必要的风险降低，就可分配安全相关系统的安全完整性要求(见 GB/T 20438.1—2006 中的 7.4、7.5 和 7.6)。

注：分配需重复以便使设计最优化以满足各种要求。

安全相关系统在获取必要的风险降低方面所起的作用由图 A.1 和图 A.2 来说明。

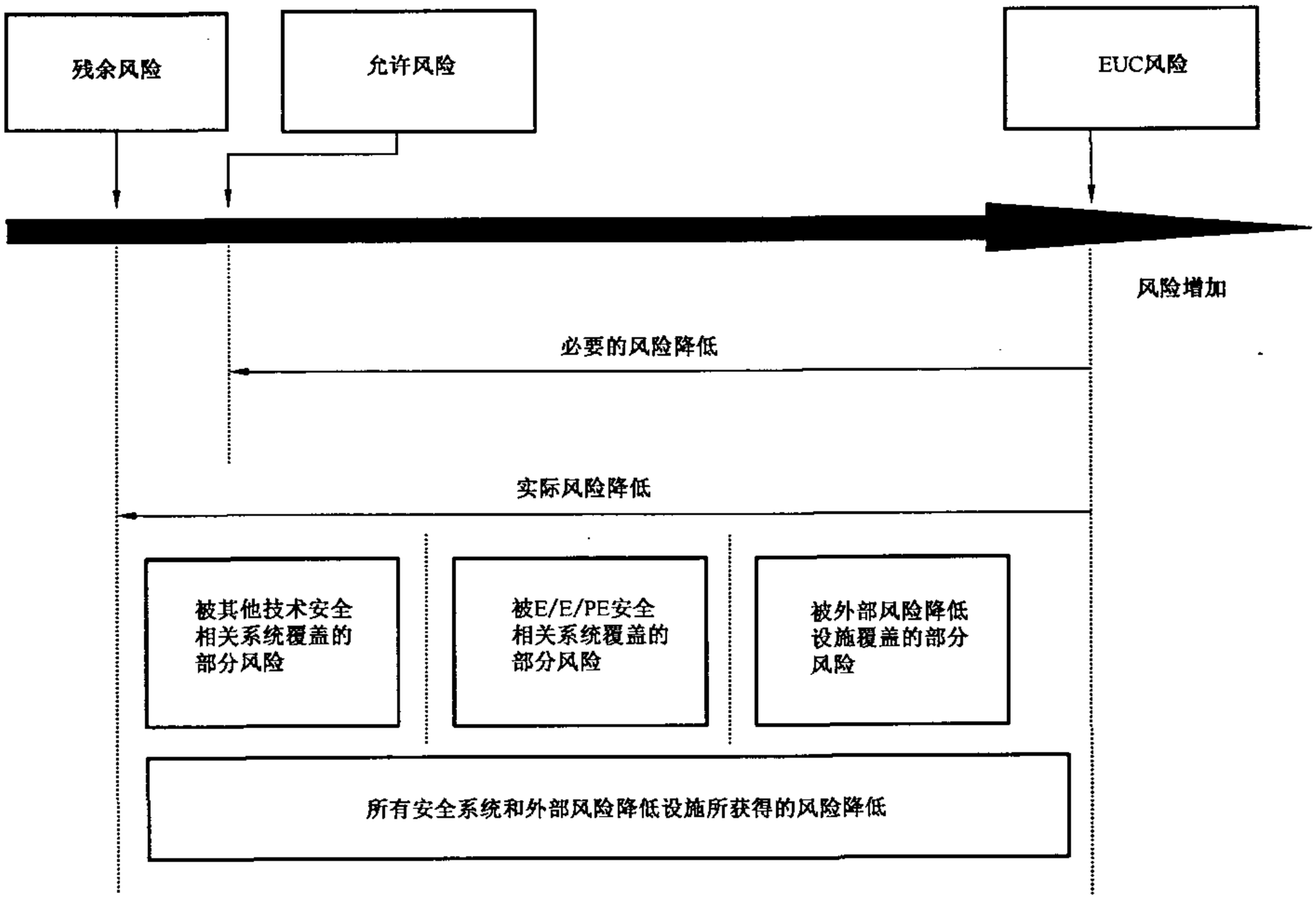


图 A.1 风险降低：通用概念

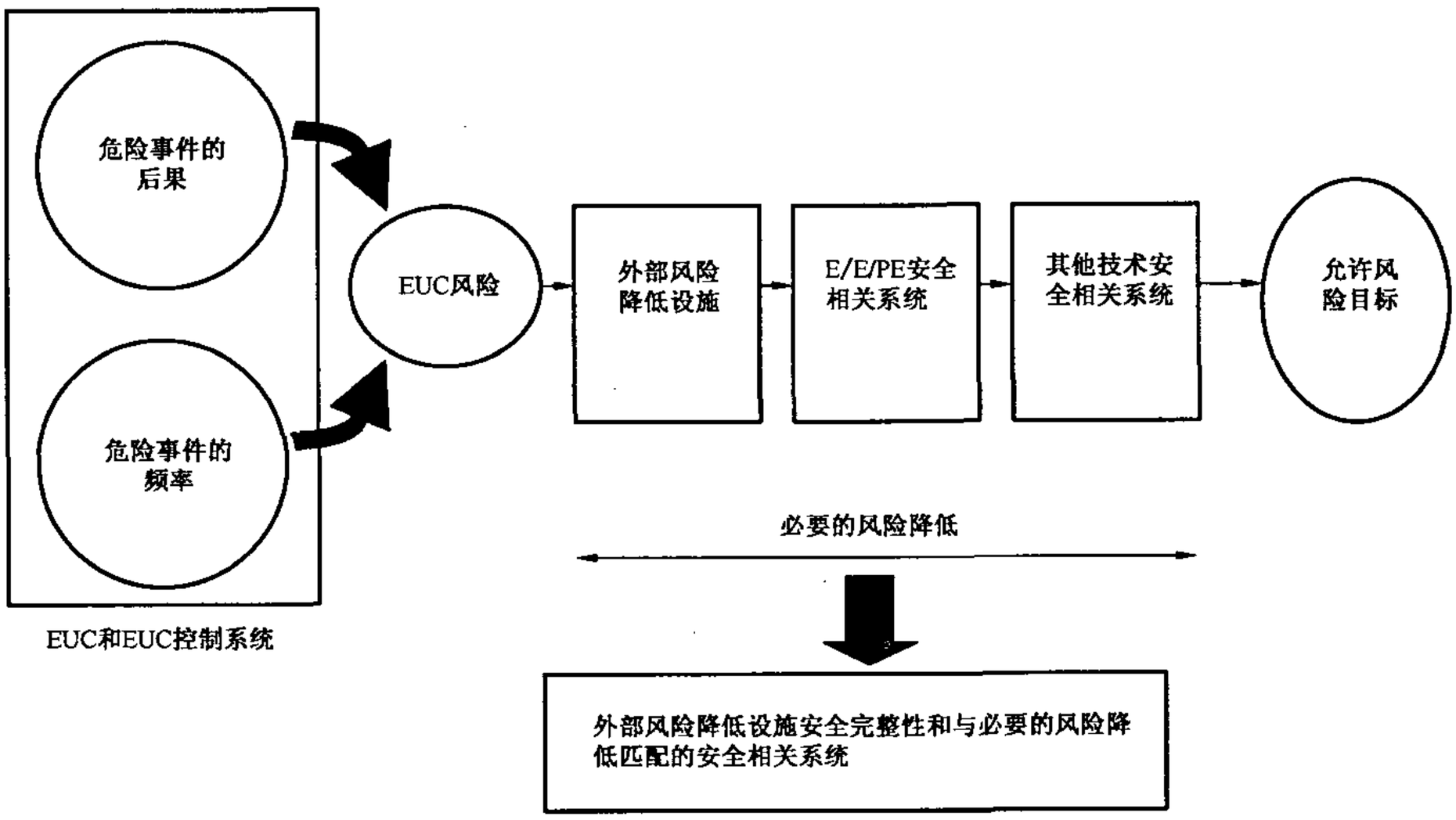


图 A.2 风险和安全完整性概念

A.6 安全完整性等级和软件安全完整性等级

为满足安全相关系统需达到的范围广泛的必要的风险降低,用一系列安全完整性等级来满足分配到安全相关系统的安全功能的安全完整性要求的方法。软件安全完整性等级是规定安全软件执行的安全功能的安全完整性要求的基础。安全完整性要求规范应规定 E/E/PE 安全相关系统的安全完整性等级。

GB/T 20438 中,规定了四种安全完整性等级,安全完整性等级 4 为最高,安全完整性等级 1 为最低。

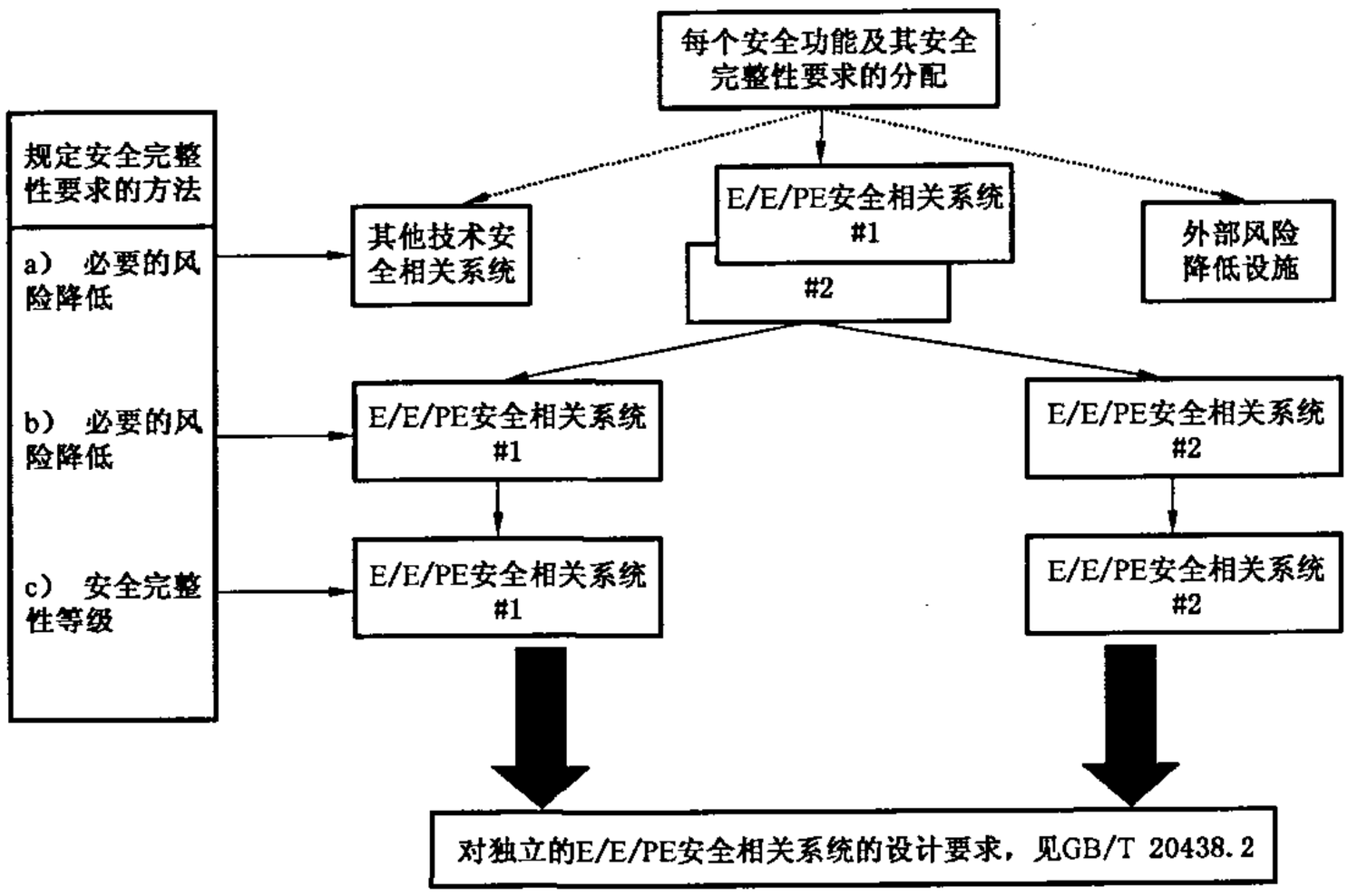
对四种安全完整性等级的安全完整性等级目标失效量的规定见 GB/T 20438.1—2006 中的表 2 和表 3。规定了两种参数,一种用于低要求操作模式的安全相关系统,另一种用于高要求操作模式或连续操作模式的安全相关系统。

注:对于低要求操作模式的安全相关系统,安全完整性量值是根据要求执行其设计功能的失效概率。对于高要求操作模式或连续操作模式的安全相关系统,安全完整性量值是每小时危险失效的平均概率(见 GB/T 20438.4—2006 中的 3.5.12 和 3.5.13)。

A.7 安全要求分配

在 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间的安全要求分配(安全功能和安全完整性要求)见图 A.3(同 GB/T 20438.1—2006 中的图 A.6)。安全要求分配阶段的要求见 GB/T 20438.1—2006 中的 7.6。

在 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间的安全要求分配的方法是对必要的风险降低分别用数字的或定性的方法进行规定。这些方法分别被称为定量或定性方法(见附录 B、附录 C、附录 D 和附录 E)。



注 1:安全完整性要求是与分配之前的各安全功能相联系的(见 7.5.2.6)。

注 2:一个安全功能可能分配于多个的安全相关系统。

图 A.3 等同于 GB/T 20438.1—2006 中的图 6

附 录 B
（资料性附录）
合理可行的低（ALARP）和允许风险概念

B.1 一般要求

本附录考虑了取得允许风险的一个特殊方法，目的不是为了提供明确的方法而是表示基本的原理。应用本附录中所提到的方法需查询原始材料。

B.2 ALARP 模型

B.2.1 简介

A.2 描述了应用在规定工业风险的主要测试，并指出与确定以下内容有关的活动：

a) 风险非常大，必须完全排除；或

b) 将产生或已产生的风险非常小，可以认为无关紧要；或

c) 风险介于上述 a)和 b)之间，并已被降低到可行的最低水平，考虑接受风险带来的利益和任何进一步减小风险所需的成本。

根据 c)，ALARP 原理要求任何风险必须降低到可行的合理水平或与可行的合理水平一样低（即最后 5 个字构成了缩写的 ALARP）。如果风险介于两个极限值之间（即不可行的区域和广泛可接受的区域），并应用了 ALARP 原理，这样产生的风险即这种特定应用的允许风险。图 B.1 表示了三个区域。

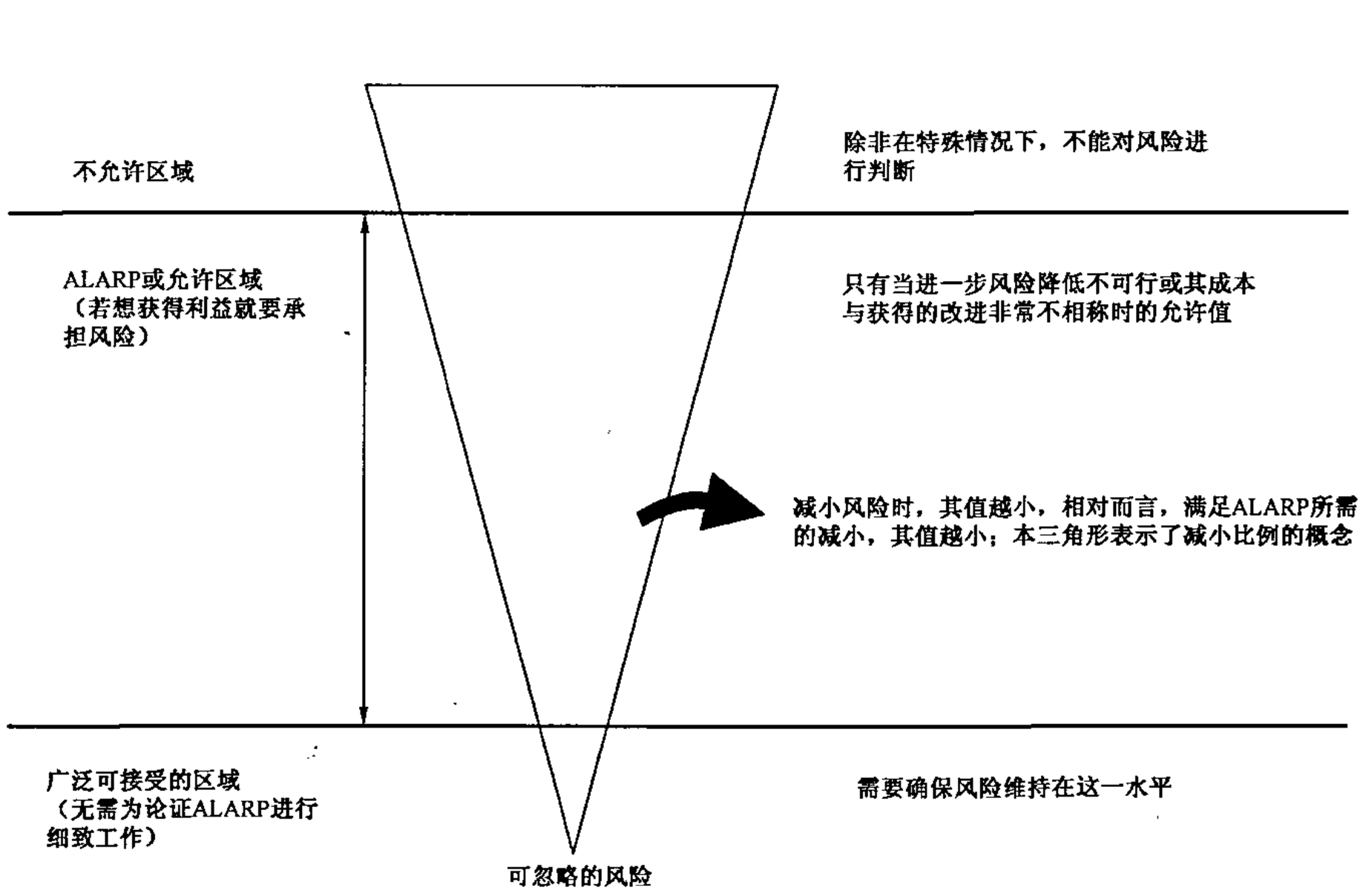


图 B.1 允许风险和 ALARP

在一定的水平之上，风险被认为是不允许的，并且不能在任何正常情况下进行判断。

低于这一水平，存在一个允许区域，在此范围内可采取将有关风险降低到可行的合理水平的措施，在这里允许不同于可接受。其表明这样一种愿望，即允许风险存在以保证一定利益，同时又期望它保持

在可检查并能被减小的范围内。在此要求一个或清楚或含蓄地权衡成本和需要或其他附加安全量的成本——利益评估。风险越高,需用于减少风险的花费会成比例的加大。在可允许的极限,应对获得的利益和不成比例的花费进行判断。此处将实质定义风险,并对相应努力的同等要求进行判断,既使风险只减小了一点。

当风险较不明显时,也只需较小比例花费去减小风险,在允许区域的低值端,会达到成本与利益的平衡。

在低于允许区域,风险的水平被认为是非常不明显,不需要进一步改善。这是一个广泛接受区域,在此区域内风险小于我们每天会实际经历的风险,无需为论证 ALARP 进行细致工作,但需提高警惕以确保风险维持在这一水平。

当采用定性或定量的风险目标时可使用 ALARP 的概念。B.2.2 说明了定量风险目的的方法(附录 C 说明了一种定量方法,附录 D 和附录 E 说明了对一特定危险确定必要的风险降低的定性方法。说明的方法可以结合 ALARP 概念用于做出决定)。

注:参考文献[4]给出了 ALARP 的进一步信息。

B.2.2 允许风险目标

获得允许风险目标的一个方法是对于一系列确定的后果,分配允许频率。后果与允许频率的匹配应在有关机构中讨论并达成一致(如安全管理政府机构、产生风险的机构和承受风险的机构)。

考虑 ALARP 概念,后果与允许频率的匹配可通过风险等级确定。表 B.1 是一系列后果和频率的四种风险等级(1,2,3,4)的示例。表 B.2 使用 ALARP 概念解释了每一风险等级。四种风险等级中的每一种描述都依据图 B.1。这些风险等级定义中的风险是采取风险降低措施后出现的风险。根据图 B.1,风险等级如下:

——风险等级 1 在不允许区域;

——风险等级 2 和风险等级 3 在 ALARP 区域,风险等级 2 正好在 ALARP 区域内;

——风险等级 4 在广泛可接受区域。

对每一种规定的情况或可比较的工业领域,将考虑大量的社会、政治和经济因素,并开发类似于表 B.1 的表。每一后果将与频率相匹配,并将风险等级填入表中。例如,表 B.1 中的频率可指明很可能持续出现的事件可能被规定频率大于每年 10 次。一个危险的后果是个体死亡或大量严重伤害或严重职业病。

表 B.1 意外事件的风险等级示例

频率	后果			
	大灾难	严重	不严重	可忽略
频繁发生	1	1	1	2
很可能发生	1	1	2	2
偶而发生	1	2	3	3
极小可能发生	2	3	3	4
不可能发生	3	3	4	4
难以相信会发生	4	4	4	4

注 1:风险等级 1、2、3、4 的实际数与领域有关,并根据实际频率是频繁、可能等,因此应将本表看作是一个说明如何填写此类表的示例,而不是对未来应用的规范。

注 2:从本表中的频率确定安全完整性等级的方法在附录 C 中说明。

表 B.2　风险等级解释

风险等级	解　　释
等级 1	不允许风险
等级 2	不期望风险，当风险降低不可行或成本与取得的改善严重不相称时为允许
等级 3	如果风险降低的成本超过取得的改善时允许的风险
等级 4	可忽略风险

附 录 C
（资料性附录）
安全完整性等级的确定:一种定量方法

C.1 一般要求

本附录描述了如何通过采用一种定量方法来确定安全完整性等级,并说明如何使用表 B.1 中的信息。一种定量方法是一种特定值,当:

——以数据形式规定了允许风险(如一个特定的后果不能以大于 1 次/10^4 年的频率出现);

——对安全相关系统的安全完整性等级的数字目标进行规定,该目标已在 GB/T 20438 中规定(见 GB/T 20438.1—2006 中的表 2 和表 3)。

本附录的目的不是提供明确的方法而是说明一般原理。如果风险模式为图 A.1 和图 A.2 中说明的模式则更适用。

C.2 一般方法

说明一般原理的模式已在图 A.1 中表示。方法中的关键步骤如下,这些步骤需要对由 E/E/PE 安全相关系统实现的每一安全功能来实施:

——从类似表 B.1 的表中确定允许风险;

——确定 EUC 风险;

——确定满足允许风险的必要的风险降低;

——将必要的风险降低分配到 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(见 GB/T 20438.1—2006 中的 7.6)。

表 B.1 应填入风险频率和规定的数字允许风险目标(F_t)。

与 EUC 存在的风险有关的频率,包括 EUC 控制系统和人的因素(EUC 风险),在没有任何防护因素时,可使用定量风险评估方法进行估计。没有防护因素时危险事件可能出现的频率(F_{np})是 EUC 风险两个构成部分之一;另一构成部分是危险事件的后果。F_{np}可由下列确定:

——从可比较的情况分析失效率;

——有关数据库的数据;

——使用适当的预计方法进行计算。

标准对 EUC 控制系统声明的最小失效率提出约束(见 GB/T 20438.1—2006 中的 7.5.2.5)。如果声明的 EUC 控制系统失效率低于最小失效率,则 EUC 控制系统可认为是安全相关系统,并满足 GB/T 20438 中对安全相关系统的要求。

C.3 计算示例

图 C.1 提供了一个如何计算单一安全防护系统的目标安全完整性的示例。对这一情况

$$PFD_{avg} \leqslant F_t / F_{np}$$

式中:

PFD_{avg}——安全防护系统要求的平均失效概率,是在低要求操作模式下操作的安全防护系统的安全完整性失效量(见 GB/T 20438.1—2006 中的表 2 和 GB/T 20438.4—2006 中的 3.5.12);

F_t——允许风险频率;

F_{np}——安全防护系统的要求率。

另外在图 C.1 中：

——C 是危险事件的后果；

——F_p 是具有防护因素的风险频率。

可以看出，因为 F_{np} 与 PFD_{avg} 的关系以及由此引起的与安全防护系统的安全完整性等级的关系，确定 EUC 的 F_{np} 是很重要的。

获得安全完整性等级（当后果 C 保持不变时）的必要步骤通常如下（图 C.1 所示），本内容是针对全部必要的风险降低是通过单一安全防护系统得的情况，该安全防护系统必须将危险率从 F_{np} 至少减小至 F_t：

——确定不附加任何防护因素（F_{np}）的 EUC 风险的频率因素。

——确定不附加任何防护因素的后果 C。

——通过使用表 B.1，确定无论频率还是后果是否达到允许风险等级。然后，通过使用表 B.1 得到风险等级 1，则要求进一步的风险降低。风险等级 4 或风险等级 3 是允许风险。风险等级 2 则需进一步调查。

注：表 B.1 用于检查是否需要进一步的风险降低措施，因为可能不采用附加防护因素也能获得允许风险。

——根据安全防护系统满足必要的风险降低（ΔR）的要求确定失效的概率（PFD_{avg}）。对于描述的特定情况中的固定后果，$PFD_{avg}=(F_t/F_{np})=\Delta R$。

——对于 $PFD_{avg}=(F_t/F_{np})$，可通过 GB/T 20438.1—2006 中的表 2 获得安全完整性等级（如对于 $PFD_{avg}=10^{-2}\sim10^{-3}$，安全完整性等级为 2）。

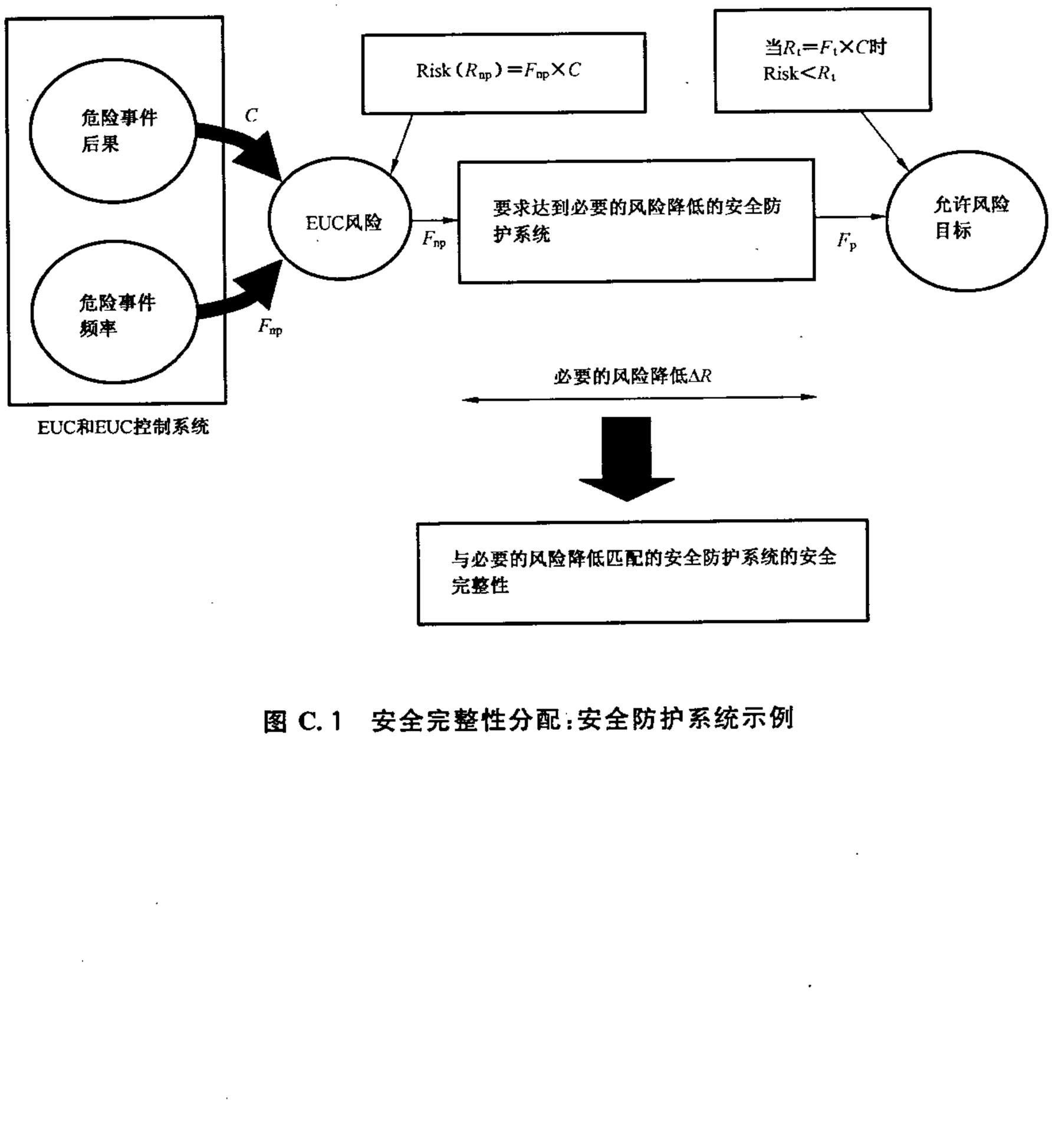


图 C.1　安全完整性分配：安全防护系统示例

附 录 D
（资料性附录）
确定安全完整性等级——一种定性方法：风险图

D.1 一般要求

本附录描述了一种风险图方法，这种定性方法可以通过对与 EUC 和 EUC 控制系统有关的风险因素的了解来确定安全相关系统的安全完整性等级。当风险模型为图 A.1 和图 A.2 中说明的模型时，这种方法特别有用。

当采用定性方法时，为了简化问题，引用一些参数来共同描述当安全相关系统失效或不可用时危险情况的性质。从每四套中选择一个参数，选择的参数结合起来描述分配到安全相关系统的安全完整性等级。这些参数：

——允许对产生的风险进行合理的分级；并

——包括关键风险评估因素。

本附录的目的并非提供明确的方法而是说明一般原理。应用本附录中所提到的方法需查询原始材料。

D.2 风险图合成

下列简化的程序根据以下公式：

$$R=f\times C$$

式中：

R——没有安全相关系统时的风险；

f——没有安全相关系统时的危险事件的频率；

C——危险事件的后果（后果可能与健康和安全有关的危害或环境破坏带来的危害有关）。

在这种情况下，危险事件的频率 f 认为是由三种有关因素组成：

a) 频率、暴露时间、危险区域；

b) 避开危险事件的概率；

c) 没有任何附加安全相关系统时危险事件发生的概率（但有外部风险降低设施）——这意味着不期望事件的发生概率。

产生下列四种风险参数：

a) 危险事件的后果（C）；

b) 频率、暴露时间、危险区域（F）；

c) 未能避开危险事件的概率（P）；

d) 不期望事件的发生概率（W）。

D.3 其他可能风险参数

以上规定的风险参数被认为一般已足够处理广泛应用情况。但可能还有要求在某方面引入附加风险参数的应用。例如，EUC 或 EUC 控制系统中新技术的使用。附加参数的目的是更加精确地估计必要的风险降低（见图 A.1）。

D.4 风险图实现：总框图

以上描述的风险参数的组合使得可以开发如图 D.1 中所示的风险图。图 D.1 中，$C_A<C_B<C_C<$

C_D;F_A<F_B;P_A<P_B;W_1<W_2<W_3<W_4。一个风险图的示例如下：

——风险参数 C、F 和 P 的使用引出一系列输出 X_1 X_2 X_3…X_n(准确的数据依据风险图覆盖的特定应用领域)。图 D.1 指出了对更加严重后果的无加权考虑的情况。这些输出中的每一个映射为三种尺度之一(W_1、W_2 和 W_3)。这些尺度上的每一点都是由考虑情况下的 E/E/PE 安全相关系统满足的必要的风险降低的指示。实际中，对特定后果，会出现单一 E/E/PE 安全相关系统不足以给出必要的风险降低的情况。

——W_1、W_2 和 W_3 上的映射可以包含其他风险降低措施产生的作用。在 W_1、W_2 和 W_3 的尺度的偏移特性可以包含来自其他措施的三种不同等级的风险降低。W_3 由其他措施提供的最小风险降低(即不期望发生情况的最高概率)，W_2 由其他措施提供的中等风险降低，W_1 由其他措施提供的最大风险降低。根据风险图的特定中间输出量(即 X_1 X_2…或 X_6)和规定的 W 尺度(即 W_1、W_2 或 W_3)，风险图的最终输出为 E/E/PE 安全相关系统的安全完整性等级(即 1，2，3 或 4)，并作为这一系统要求风险降低的量值。这一风险降低和其他考虑进 W 尺度机制的措施所取得的风险降低(如其他技术安全相关系统和外部风险降低设施)给出特定情况下的必要的风险降低。

图 D.1 中所示的参数(C_A，C_B，C_C，C_D，F_A，F_B；P_A，P_B；W_1，W_2，W_3)和其加权，需要在每种特定情况下或类似工业领域中被准确定义，还需要在应用领域的标准中被定义。

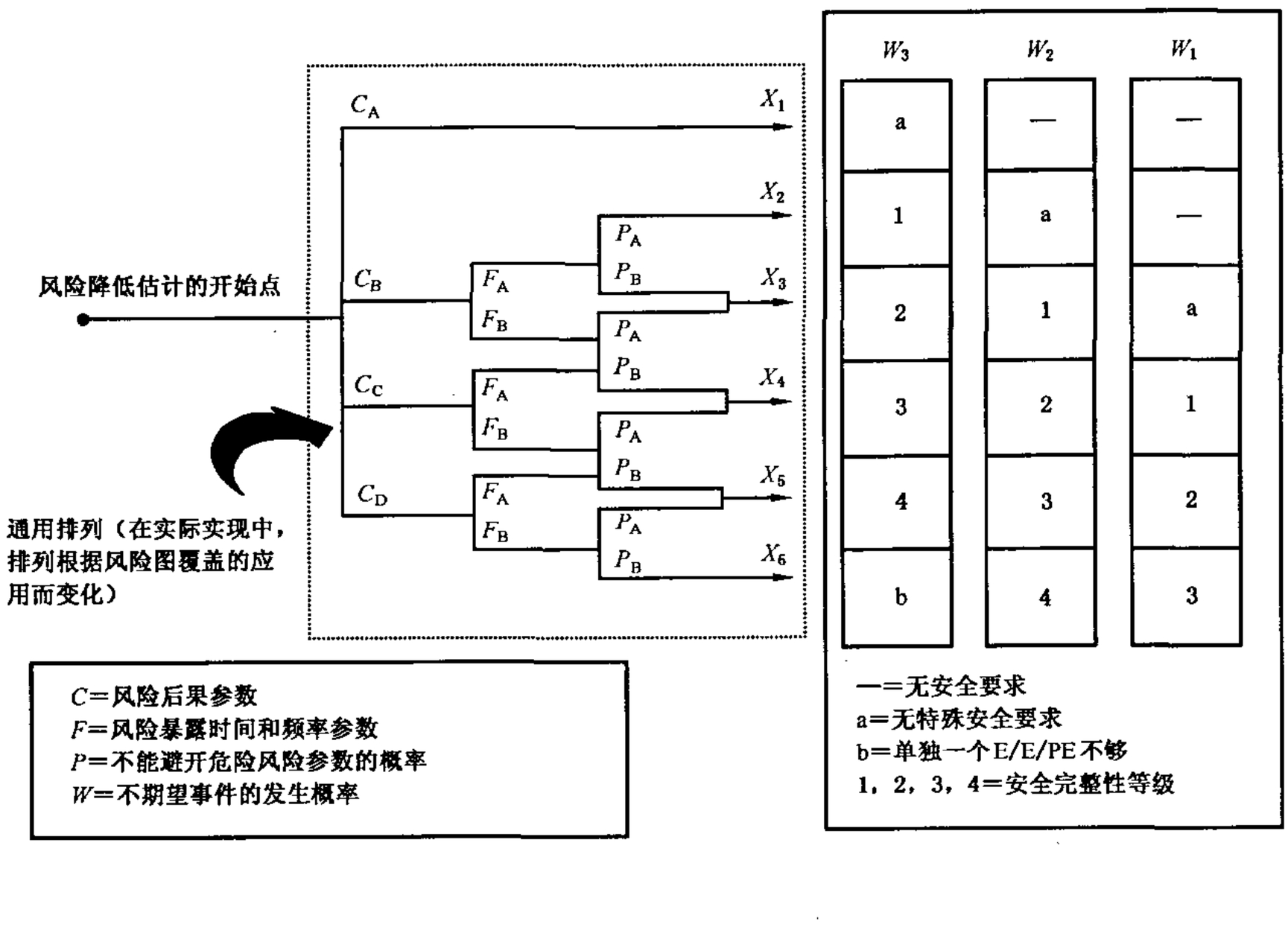
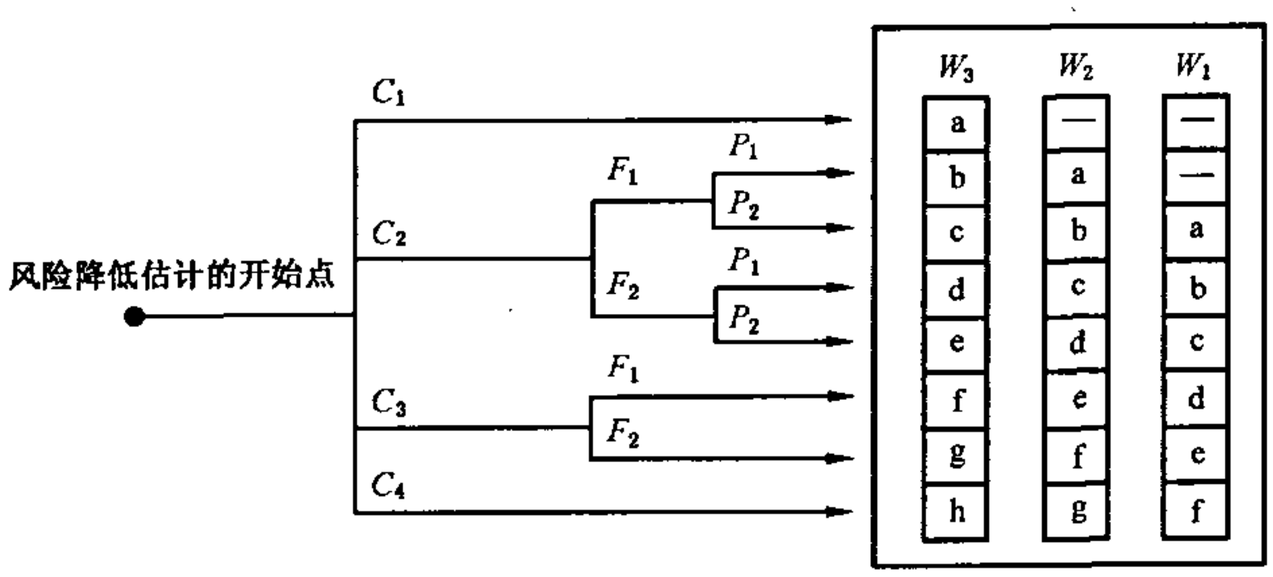


图 D.1　风险图：总框图

D.5　风险图示例

图 D.2 表示了基于表 D.1 中数据实现的风险图示例。使用风险参数 C、F 和 P 导出 8 个输出之一。每一输出映射为三个尺度(W_1，W_2，W_3)之一。这些尺度上的每个点(a，b，c，d，e，f，g，h)都是安全相关系统需满足的必要的风险降低的指示。

注：实现风险图的进一步信息见参考文献[2]。



a，b，c，d，e，f，g，h 表示了必要的最小风险降低；必要的最小风险降低与安全完整性等级的关系在表D.1中表示

C=风险后果参数
F=风险暴露时间和频率参数
P=不能避开危险风险参数的概率
W=不期望事件的发生概率
a，b，c...h=对SRSs的要求风险降低的估计

必要的最小风险降低	安全完整性等级
—	没有安全要求
a	没有特殊安全要求
b，c	1
d	2
e，f	3
g	4
h	一个E/E/PE SRS不够

图 D.2　风险图:示例(只说明一般原理)

表 D.1　风险图示例中的有关数据示例(图 D.2)

风险参数		分　类	备　注
后果(C)	C_1 C_2 C_3 C_4	微小伤害 对一人或多人的严重永久伤害;一人死亡 几人死亡 多人死亡	1. 开发分类系统用于处理对人的伤害或死亡。需开发其他分类系统处理对环境的破坏或物质破坏 2. 对于 C_1、C_2、C_3、C_4 的解释,应考虑意外的后果和正常康复
在危险区域中的频率和暴露时间(F)	F_1 F_2	很少至较多暴露在危险区域 经常至永久暴露在危险区域	3. 见上栏 1
避开危险事件的概率(P)	P_1 P_2	在一定条件下可能 几乎不可能	4. 参数考虑 ——过程操作(被监督,即由熟练或不熟练人员操作,或未被监督) ——危险事件的发生速率(如突然、快速或缓慢) ——识别危险的难易(如立即看到,通过技术措施探测或不通过技术措施探测) ——危险事件的避免(如在特定条件下可能或不可能的逃生路线) ——实际安全经验(有无相同的 EUC 或类似的 EUC 使用经验)
不期望事件的发生概率(W)	W_1 W_2 W_3	出现不期望事件的发生概率非常小并且只有很少不期望事件有可能出现 出现不期望事件的发生概率小并且只有少量不期望事件有可能出现 不期望事件的发生概率相对高并且不期望事件有可能频繁出现	5. W 因素的目的是估计不期望事件在没有任何附加安全相关系统(E/E/PE 或其他技术系统)的情况下发生的频率,但包括任何外部风险降低设施 6. 如果只有很少或没有使用 EUC 或 EUC 控制系统,或类似系统的经验,W 因素的估计可以通过计算得出。在这种情况下应做出最坏的预测

附 录 E
（资料性附录）
安全完整性等级的确定——一种定性方法：危险事件严重性矩阵

E.1 总则

当风险(或风险的频率)不能定量时，附录 C 中描述的数学方法则不适用。本附录描述一种危险事件严重性矩阵方法，这是一种定性方法，使得根据对 EUC 或 EUC 控制系统有关的风险因数的了解就能确定 E/E/PE 安全相关系统的安全完整性等级。当风险模型为图 A.1 和图 A.2 所示时，这种方法特别适用。

本附录规定的框架假定每一安全相关系统和外部风险降低设施都是独立的。

本附录的目的并非作为方法的定义说明而是说明那些深入了解与其结构有关的特定参数的人们如何开发这样一种矩阵的一般原理。应用本附录中所提到的方法需查询原始材料。

注：有关危险事件严重性矩阵的进一步的信息参见参考文献[3]。

E.2 危险事件严重性矩阵

以下要求作为矩阵的基础，并且每一个对方法的有效性来说都是必要的：

a) 安全相关系统(E/E/PE 和其他技术系统)与外部风险降低设施是独立的；

b) 每一安全相关系统(E/E/PE 和其他技术系统)和外部风险降低设施都认为是提供图 A.1 中所示的部分风险降低的保护层；

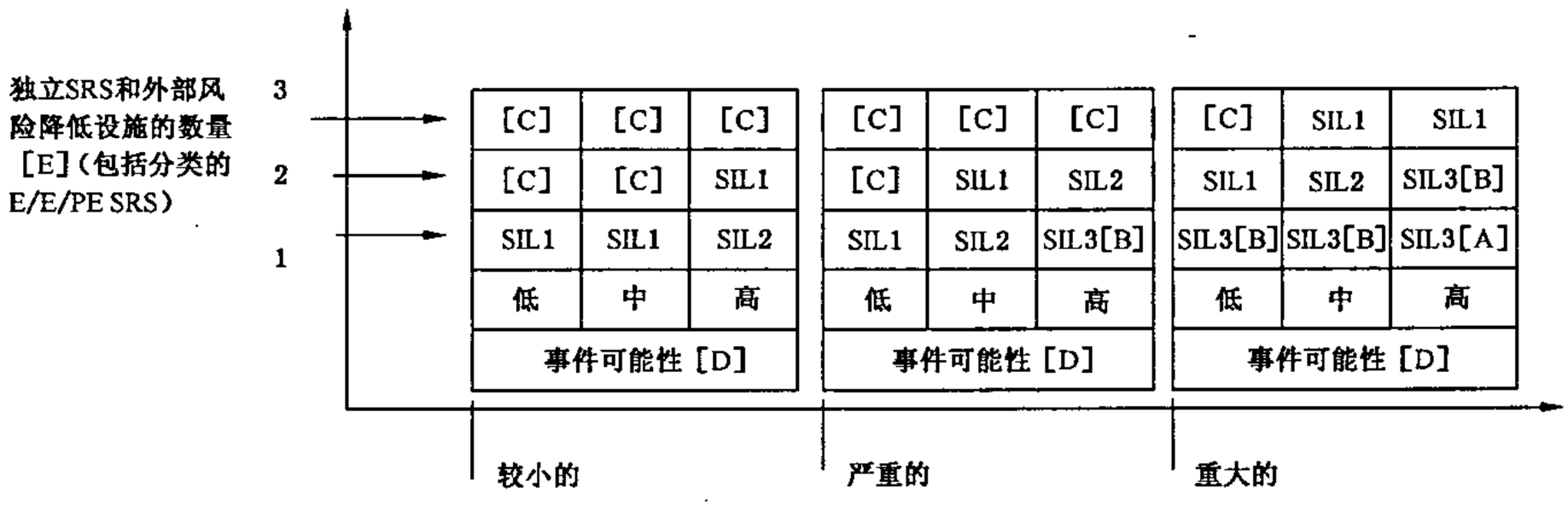
注 1：仅当执行保护层的定期检验时，这一假定才有效。

c) 当增加一个保护层时(见 b))，安全完整性则获得一个数量级的提高；

注 2：仅当安全相关系统和外部风险降低设施具有足够的独立水平时，这一假定才有效。

d) 这一方法建立必要风险完整性等级，且只使用一个 E/E/PE 安全相关系统(但也可以与另一技术安全相关系统和/或外部风险降低设施结合)。

上述考虑导出图 E.1 所示危险事件严重性矩阵。应注意矩阵已通过对示例数据计算来说明一般原理。对每一特定情况，或类似工业领域，应开发类似于图 E.1 的矩阵。



[A] 一个 SIL3 E/E/PE 安全相关系统不能在这一等级上提供足够的风险降低，需要附加风险降低措施。

[B] 一个 SIL3 E/E/PE 安全相关系统不能在这一等级上提供足够的风险降低，要求进行危险和风险分析以确定是否需要附加的风险降低措施。

[C] 可能不需要一个独立的 E/E/PE 安全相关系统。

[D] 事件的概率是在没有任何安全相关系统或外部风险降低设施下危险事件出现的概率。

[E] SRS=安全相关系统，事件的概率和独立保护层的数量是由与特定应用的关系来定义的。

图 E.1 危险事件严重性矩阵示例(只说明一般原理)

参 考 文 献

[1] ANSI/ISA S84:1996 过程工业领域安全仪表系统的应用.

[2] Grundlegende Sicherheitberatungunge für MSR-schutzeinrichtungen DIN V 19250, Bouth varlag, Berlin, FRG, 1994.

[3] 化工过程安全自动化指南,美国化工工程研究所化工过程安全中心出版.

[4] 核电站可允许的风险,健康和安全执委会.

[5] 车用软件开发指南,发动机工业可靠性协会.

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5部分:确定安全完整性
等级的方法示例
GB/T 20438.5—2006/IEC 61508-5:1998
*
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 36 千字
2007年1月第一版 2007年1月第一次印刷
*

GB/T 20438.5-2006