



中华人民共和国国家标准

GB/T 20438.5—2017/IEC 61508-5:2010
代替 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

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

(IEC 61508-5:2010, 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 发布
中国国家标准化管理委员会

目 次

前言	I
引言	II
1 范围	1
2 规范性引用文件	3
3 定义和缩略语	3
附录 A (资料性附录) 风险和安全完整性—通用概念	4
附录 B (资料性附录) 确定安全完整性等级要求的方法选择	14
附录 C (资料性附录) ALARP 和可容忍风险的概念	16
附录 D (资料性附录) 确定安全完整性等级——一种定量的方法	19
附录 E (资料性附录) 安全完整性等级的确定——风险图方法	21
附录 F (资料性附录) 采用保护层分析的半定量法(LOPA)	27
附录 G (资料性附录) 确定安全完整性等级——一种定性的方法——危险事件严重程度矩阵	31
参考文献	33
图 1 GB/T 20438 的总体框架	2
图 A.1 风险降低:通用概念(低要求运行模式)	7
图 A.2 风险和安全完整性概念	7
图 A.3 高要求应用的风险图	8
图 A.4 连续模式运行的风险图	9
图 A.5 EUC 控制系统元件与 E/E/PE 安全相关系统元件的共因失效(CCF)示例	10
图 A.6 两个 E/E/PE 安全相关系统间的共因失效	11
图 A.7 E/E/PE 安全相关系统和其他风险降低措施的安全要求分配	12
图 C.1 可容忍风险和 ALARP	16
图 D.1 安全完整性分配——安全相关保护系统的示例	20
图 E.1 风险图:通用方案	23
图 E.2 风险图——示例(仅说明一般原则)	24
图 G.1 危险事件严重程度矩阵——示例(只说明一般原则)	32
表 C.1 事故风险分类的示例	17
表 C.2 风险级别的解释	18
表 E.1 与风险图相关的数据示例(图 E.2)	24
表 E.2 通用风险图的校准示例	25
表 F.1 LOPA 报告	28

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5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 20438.5—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》，与 GB/T 20438.5—2006 相比，主要技术变化如下：

- 增加了确定安全完整性等级要求的方法选择；(见附录 B)；
- 增加了风险分析的方法：采用保护层分析的半定量法(LOPA)(见附录 F)。

本部分使用翻译法等同采用 IEC 61508-5:2010《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》。

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、北京市劳动保护科学研究所、风控(北京)工程技术有限公司、北京联合普肯工程科技股份有限公司、上海中沪电子有限公司、西门子(中国)有限公司。

本部分主要起草人：史学玲、熊文泽、靳江红、陈勇、杨柳、肖松青、周有铮、梅豪、黄劲松、鲁毅、冯晓升、罗安、顾峥、李佳、田雨聪、左信、姜雪莲、白焰。

本部分所代替标准的历次版本发布情况为：

- GB/T 20438.5—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。因而不得不考虑各类安全策略,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,建立一个足够健全且广泛满足未来发展需求的框架;
- 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} ;
 - 高要求或连续运行模式下,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5部分:确定安全完整性 等级的方法示例

1 范围

1.1 GB/T 20438 的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(参见附录 A);
- 提供确定 E/E/PE 安全相关系统安全完整性等级的一系列方法(参见附录 C、附录 D、附录 E、附录 F 和附录 G)。

选择的方法应取决于应用领域和所考虑的特定环境。附录 C、附录 D、附录 E、附录 F 和附录 G 列出了定性和定量的方法并为说明基础的原理进行了简化。通过这些附录,说明了一系列方法的通用原理,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:如想获取更多关于附录 B 和附录 E 中说明的方法的有关信息,见参考文献[5]和[8]。对于附加方法的描述见参考文献[6]。

1.2 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,虽然它不适用于低复杂的 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 IEC 60601 涵盖的医疗设备。

1.3 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。在本部分中,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。

1.4 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。

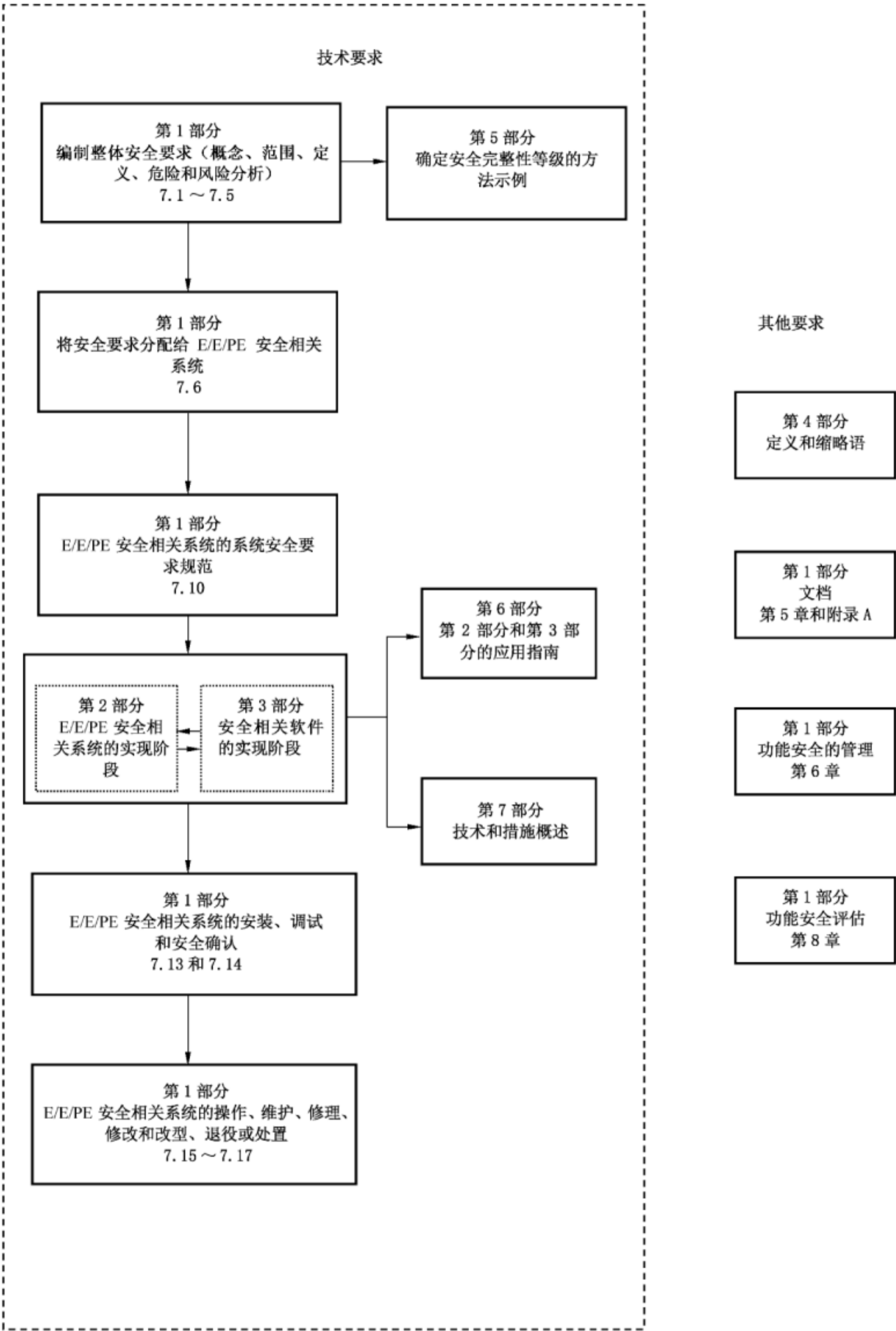


图 1 GB/T 20438 的整体框架

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。

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(IEC 61508-1:2010,IDT)

GB/T 20438.4—2017 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 61508-4:2010,IDT)

3 定义和缩略语

GB/T 20438.4—2017 界定的定义和缩略语适用于本文件。

附录 A

(资料性附录)

风险和安全完整性—通用概念

A.1 概述

本附录提供了关于风险的基本概念和风险与安全完整性之间关系的信息。

A.2 必要的风险降低

必要的风险降低(见 GB/T 20438.4—2017 中的 3.5.18)是保证在特定情况下达到可容忍风险(可以定性¹⁾或定量²⁾说明)的风险降低。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(特别是安全要求规范中的安全完整性部分)非常重要。确定特定危险事件的可容忍风险的目的是为了说明什么样的危险事件发生频率(或概率)及其特定后果是合理的。安全相关系统应设计成用来降低特定危险事件的频率(或概率)和/或减轻该危险事件的后果。

可容忍风险取决于许多因素(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暴露持续时间)。暴露在危险事件中的人的感受和看法是很重要的因素。对于一个特定应用,可容忍风险的构成,需考虑以下一系列决定因素:

- 通用的法律要求,以及与特定应用直接相关的法律要求;
- 相关安全监管机构发布的指南;
- 与应用有关各方的各方争议与一致意见;
- 工业标准和指南;
- 各国争议和国际共识;国家标准和国际标准在确定特定应用的可容忍风险准则中均起到越来越重要的作用;
- 来自咨询机构的领域的、专家的以及科学的最佳独立建议。

在确定 E/E/PE 安全相关系统和其他风险降低措施的安全完整性要求时,为了符合危险事件的可容忍发生频率,需要考虑相关应用的风险特性。可容忍频率取决于相关应用的国家法定要求以及用户机构规定的准则。需考虑的问题以及如何将它们应用于 E/E/PE 安全相关系统将在下面讨论。

A.2.1 个人风险

对于员工和公众,确定的风险目标通常不同。员工的个人风险目标适用于暴露最多的人员,表示为每年来自所有生产活动的总风险。由于该目标用于一个假定的人员,因此需要考虑个人工作时间的百分比。该目标适用于暴露人员的所有风险,而单个安全功能的可容忍风险还需要考虑其他风险。

确保总风险降低到规定目标以下可通过多种方式实现。一种方法是对暴露最多的人员考虑所有风险并求和。这种方式在一个人员暴露于多个风险并需要对系统开发提前决策的情况下可能较为困难。另一种方法是将整体个人风险目标按照一定的百分比分配给需考虑的每个安全功能。分配的百分数通常可通过考虑的同类设备的先前经验确定。

单个安全功能的目标值还需要考虑所用风险分析方法的保守性。所有的定性方法,如风险图,都包

1) 在达到可容忍风险的过程中,需要确定必要的风险降低。本部分的附录 E 和附录 G 给出了定性方法,尽管在实例中提到的必要风险降低是通过 SIL 要求规范隐含表达的,而不是通过要求的风险降低数值明确说明的。

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

含对导致风险的关键参数的评估。导致风险的因素包括危险事件后果及发生频率。要确定这些因素,可能需要考虑大量风险参数,如危险事件的严重程度,可能被危险事件影响的人数,危险事件发生时人员出现的概率(即占有率)及避免危险事件发生的概率。

定性方法通常需要判断某一参数是否在确定的取值范围内。当使用这些方法时,需要考虑如下准则:应有高的置信度表明风险不超过目标。这包含设定所有参数的范围边界,以使参数处于边界值的情况也能满足安全规定的风险准则。设置边界范围的方法是非常保守的,因为所有参数都处于范围最坏情况的应用很少。如果公众面临的是 E/E/PE 安全相关系统失效带来的风险,那么通常使用一个更小的风险目标值。

A.2.2 社会风险

由单一事件引发多个伤亡事故的情形会引起社会风险。这些事件被称为社会事件是因为它们可能会激起社会-政治反应。严重后果事件会引起公众及机构的极大反感,在一些情况下,需要将这一点考虑在内。GB/T 20438 中社会风险通常表达为:特定人数发生致命伤亡的最大累积频率,以 F/N 单曲线或多曲线图表示,其中 F 是危险的累积频率, N 是危险引发的伤亡数,在对数刻度中通常成直线关系。直线斜率取决于机构规避更高风险后果等级的程度。要求是确保特定伤亡数的累积频率低于 F/N 曲线中表示的累积频率。(见参考文献[7])

A.2.3 持续改进

将风险降低到合理可行尽量低的原则将在附录 C 中讨论。

A.2.4 风险概况

为了确定适用于特定危险的风险指标,可能需要考虑贯穿整个资产生命周期的风险概况。残余风险会从刚完成一个周期检验或维修后的最小值变化至进行下一个周期检验前的最大值。规定适用风险指标的机构可能需要加以考虑。如果周期检验间隔很大,应当规定周期检验前可接受的最大危险概率或者超出特定时间比例(如 90%), $PFD(t)$ 或 $PFH(t)$ 低于 SIL 边界上限值的最大危险概率。

A.3 E/E/PE 安全相关系统的作用

E/E/PE 安全相关系统可提供必要的风险降低,以便符合可容忍风险的要求。

安全相关系统:

- 实现所要求的必要的安全功能使受控设备达到或保持安全状态;
- 自身或与其他 E/E/PE 安全相关系统、其他风险降低设施实现所要求的安全功能(见 GB/T 20438.4—2017 的 3.5.1)的必需的安全完整性。

注 1: 定义的第一部分规定了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规定当温度达到 x 时,阀 y 应打开使水流入容器中。

注 2: 定义的第二部分规定了安全功能必须由对应用而言具有适当置信度的安全相关系统来完成,以达到可容忍风险。

人可能会是 E/E/PE 安全相关系统的一个部分。比如,人通过显示屏幕来获取 EUC 状态信息,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运行模式或高要求运行模式或连续运行模式下运行。

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率(见 GB/T 20438.4—2017 中的 3.5.4)。安全完整性关系到安全相关系统执行安全功能的性能(执行

的安全功能将在安全功能要求规范中规定)。

安全完整性可认为由下列两个部分组成：

- 硬件安全完整性：这部分安全完整性与在危险失效模式下的随机硬件失效有关（见 GB/T 20438.4—2017 中的 3.5.7）。可以一个合理的精确度水平对安全相关的硬件安全完整性达到的规定等级进行估计，因此，可用组合概率的通用法则在子系统中进行要求分配。可能需要使用冗余架构来达到足够的硬件安全完整性。
- 系统性安全完整性：这部分安全完整性与在危险失效模式下的系统性失效有关（见 GB/T 20438.4—2017 中的 3.5.6）。尽管与系统性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论证以将不确定性最小化。注意减少随机硬件失效概率的措施不会对系统性失效的概率产生相同影响。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，但在减少系统性失效方面（如软件错误）作用非常有限。

A.5 运行模式及 SIL 的确定

运行模式与按要求频率使用安全功能的方式有关，分为：

- 低要求模式：安全功能的运行要求频率低于每年一次；
- 高要求模式：安全功能的运行要求频率高于每年一次；
- 连续模式：安全功能的运行要求是连续的。

GB/T 20438.1—2017 的表 2 和表 3 详细说明了各运行模式下的四个安全完整性等级对应的目标失效量。运行模式会在以下段落中得到进一步说明。

A.5.1 低要求模式应用的安全完整性及风险降低

E/E/PE 安全相关系统和其他风险降低措施所要求的安全完整性应该达到相应等级，以保证：

- 安全相关系统的要求时平均失效概率足够低以防止危险事件频率超过要求，以满足可容忍风险，和/或
 - 安全相关系统修改失效后果达到要求，以满足可容忍风险。
- 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：
 - E/E/PE 安全相关系统；
 - 其他风险降低措施。

注：图 A.1 是说明通用原理的通用风险模型。特定应用的风险模型需考虑 E/E/PE 安全相关系统和/或其他风险降低措施，实际取得的必要风险降低所用的特定方式来开发。因此得到的风险模型可能不同于图 A.1。

图 A.1 和图 A.2 中的各种风险为：

- EUC 风险：EUC、EUC 控制系统和有关人为因素问题在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（见 GB/T 20438.4—2017 中的 3.1.9）；
- 可容忍风险：根据当今社会水平所能接受的风险（见 GB/T 20438.4—2017 中的 3.1.7）；
- 残余风险：标准文本中，残余风险是使用了 E/E/PE 安全相关系统和其他风险降低措施后，残留在 EUC、EUC 控制系统、人为因素的特定危险事件中的风险（见 GB/T 20438.4—2017 中的 3.1.7）。

EUC 风险与 EUC 本身的风险密切相关，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—2017 中的 7.5.2.5)。

必要的风险降低是通过所有安全防护性能共同实现的。图 A.1(关于低要求运行模式下运行的安全功能)表示了从起点 EUC 风险开始到达到规定的可容忍风险的必要的风险降低。

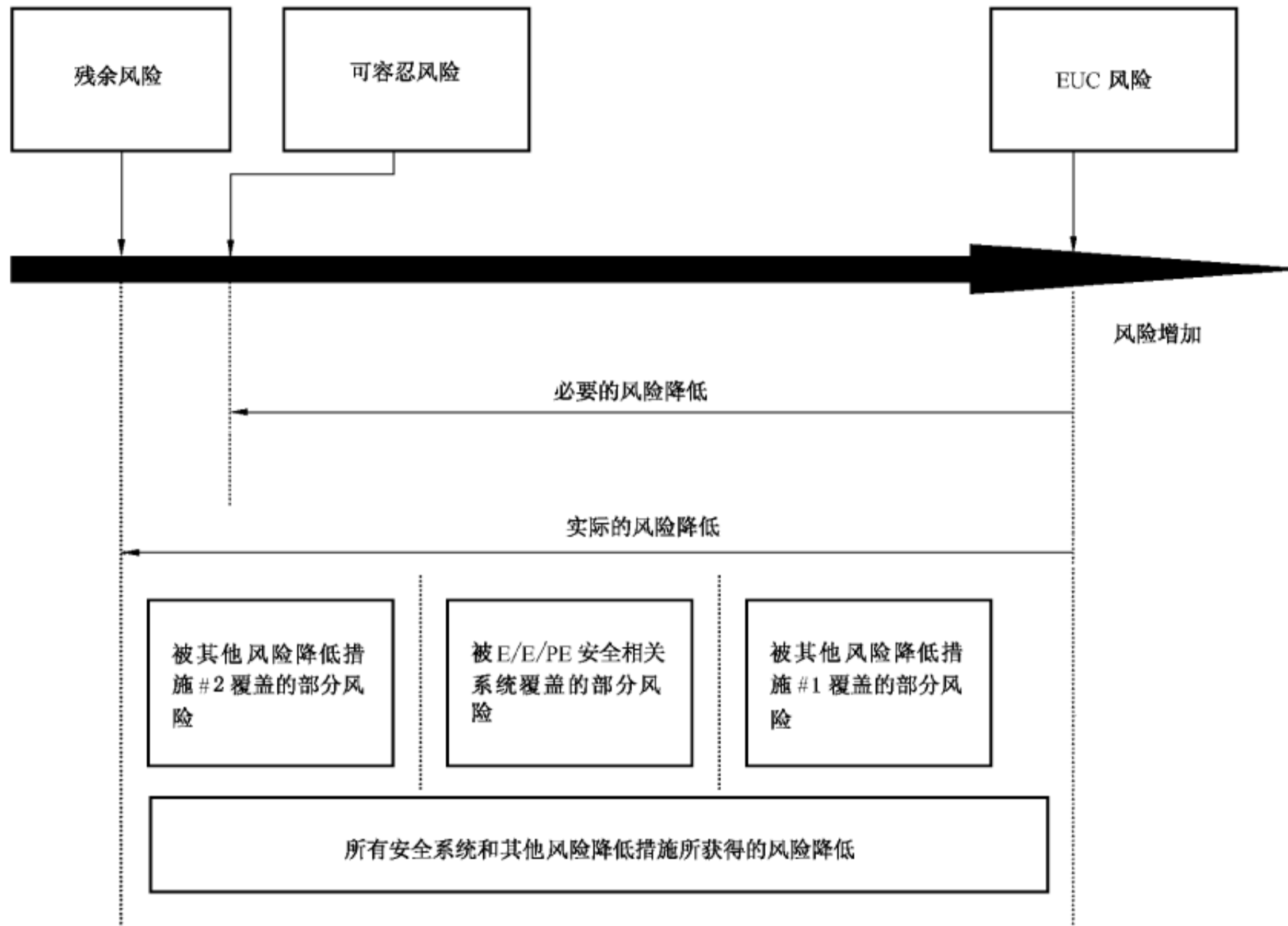


图 A.1 风险降低:通用概念(低要求运行模式)

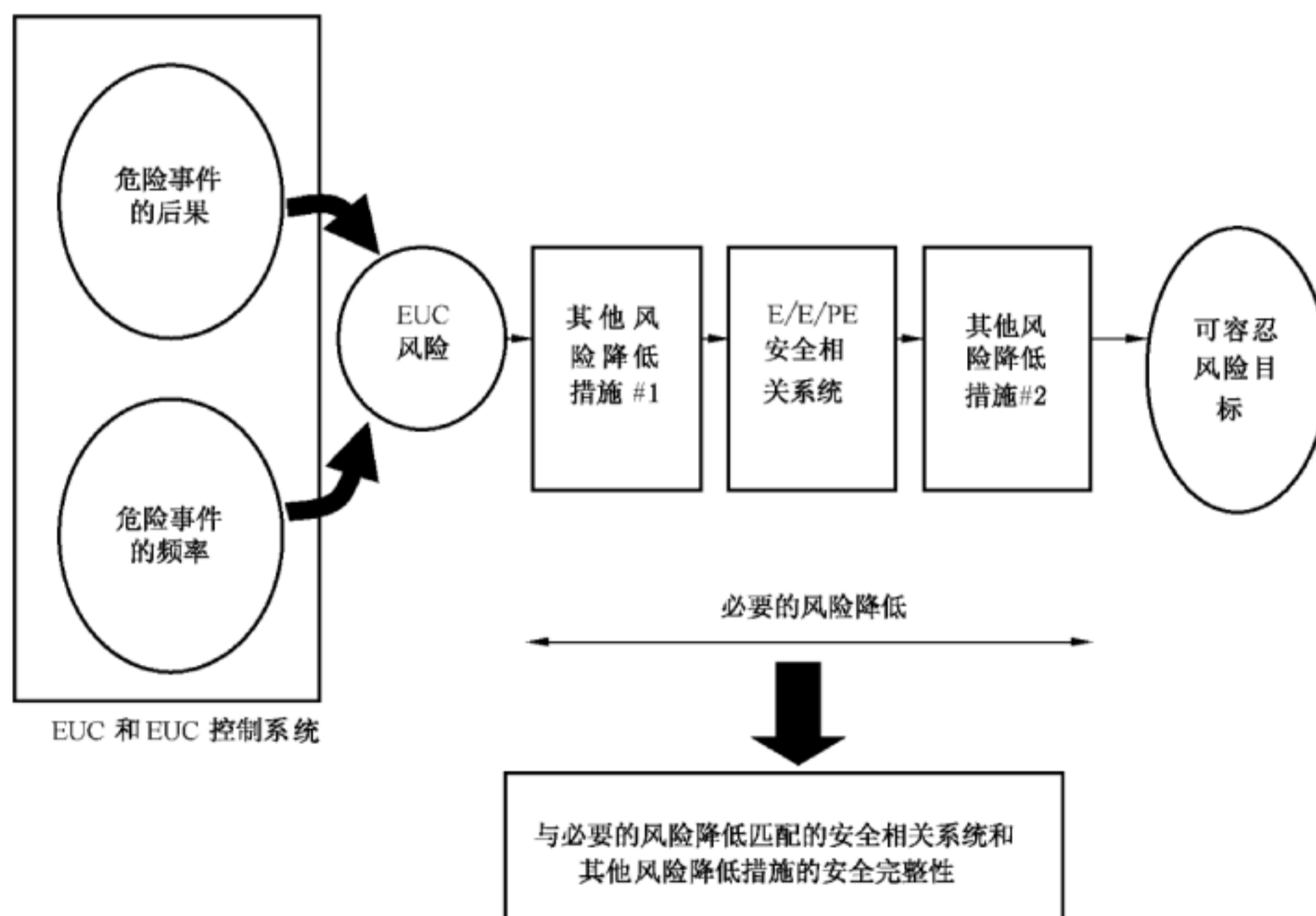


图 A.2 风险和安全完整性概念

A.5.2 高要求模式应用的安全完整性

E/E/PE 安全相关系统和其他风险降低措施所要求的安全完整性应该达到相应等级,以保证:

- 安全相关系统的要求时平均失效概率足够低以防止危险事件频率超过要求,以满足可容忍风险,和/或
- 安全相关系统的每小时平均失效概率足够低以防止危险事件频率超过要求,以满足可容忍风险。

图 A.3 说明高要求应用的通用概念。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:
 - 运行在高要求模式下的 E/E/PE 安全相关系统;
 - 其他风险降低措施。

对 E/E/PE 安全相关系统的要求包括以下几类:

- 来自 EUC 的一般要求;
- EUC 控制系统失效引发的要求;
- 人为失效引发的要求。

若系统所有要求的总要求率超过每年一次,则 E/E/PE 安全相关系统的危险失效率成为关键因素。残余危险频率绝不会超过 E/E/PE 安全相关系统的危险失效率,并在有其他风险降低措施降低伤害概率时会更低。

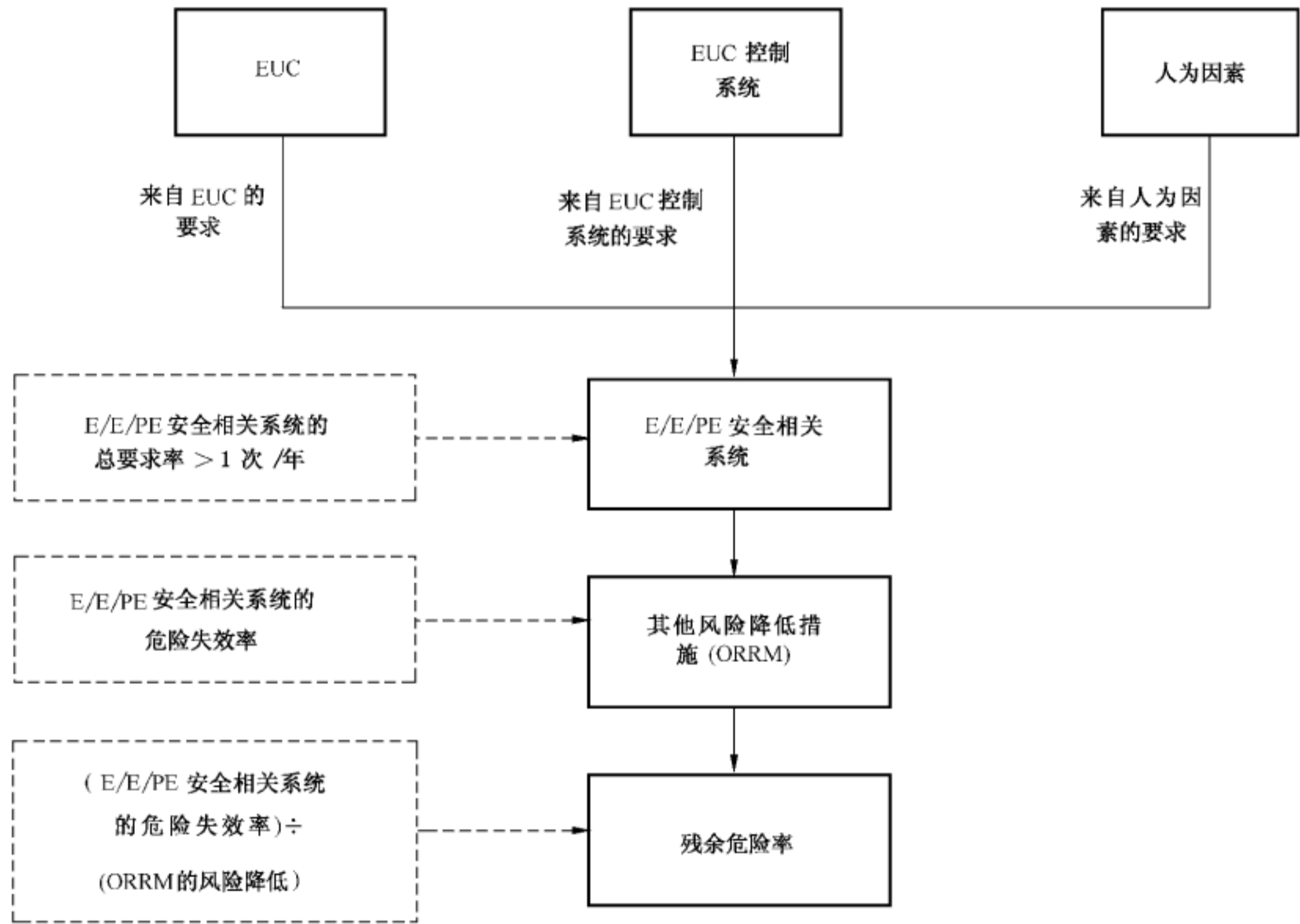


图 A.3 高要求应用的风险图

A.5.3 连续模式应用的安全完整性

E/E/PE 安全相关系统和其他风险降低措施所要求的安全完整性应该达到相应等级,以保证安全相关系统每小时平均危险失效概率足够低,以防止危险事件频率超过满足可容忍风险要求的频率。

E/E/PE 安全相关系统运行在连续模式时,根据提供的风险降低,其他风险降低措施能够降低残余危险频率。该模型如图 A.4 所示。

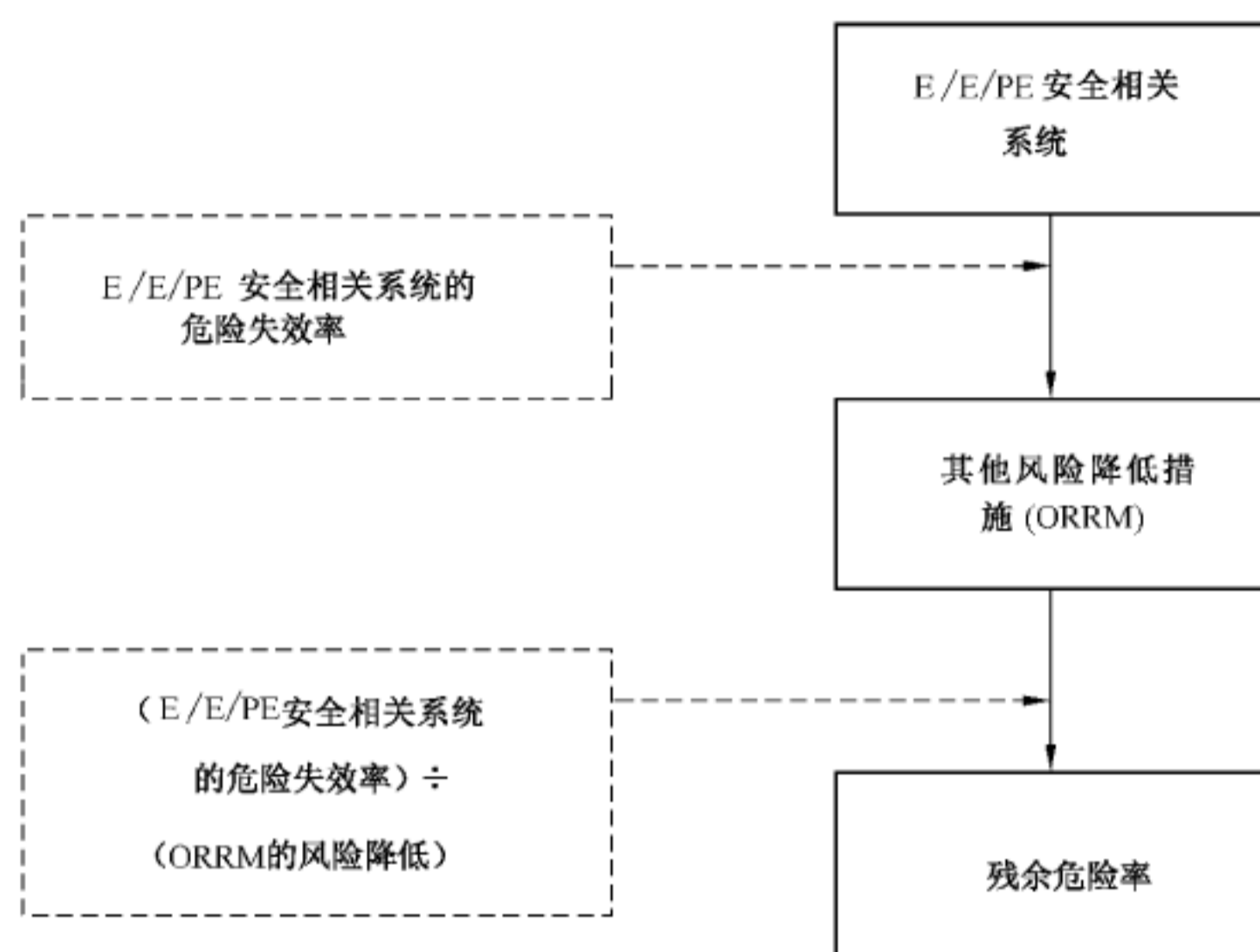


图 A.4 连续模式运行的风险图

A.5.4 共因失效与相关失效

确定安全完整性等级时,考虑共因失效与相关失效是很重要的。图 A.1、图 A.2、图 A.3 和图 A.4 中所示的模型都是基于同一危险相关的各安全系统充分独立而绘制的。不属于这种情况的应用很多,例如:

- 1) EUC 控制系统的一个元件的一个危险失效引发对安全相关系统的一个要求,而安全相关系统使用的一个元件会由于同一原因发生失效。例如,控制系统与保护系统的传感器是不同的,但会由于同一原因导致两者都失效(见图 A.5)。
- 2) 使用一个以上安全相关系统,各安全相关系统中使用一些同种类型的设备,每个设备都会由于相同原因发生失效。例如,两个不同的保护系统使用相同类型的传感器,对同一危险进行风险降低(见图 A.6)。
- 3) 使用一个以上的防护系统,防护系统是不同的,但对各系统执行的周期检验是基于相同基准的。在这种情况下,多个系统组合的实际 PFD_{avg} 要比单个系统 PFD_{avg} 的乘积高的多。
- 4) 使用相同的单一元件作为控制系统与安全相关系统的一部分。
- 5) 使用一个以上的防护系统,且使用相同的单一元件作为一个以上系统的一部分。

在这些情况中,需要考虑共同原因的影响。需要考虑最终解决方法是否能满足必要的系统能力及整体风险降低要求的必要的危险随机硬件失效概率。共因失效影响难以确定,通常需要构造特定用途的模型(如故障树或马尔科夫模型)。

在高安全完整性等级的应用中,共同原因的影响可能更为显著。在一些应用中,有必要引入多样性技术使共因影响最小化。但是,应当注意多样化会引起设计、维护和修改中的一些问题。引入多样化会导致由于对不同设备不了解并缺乏操作经验而发生的错误。

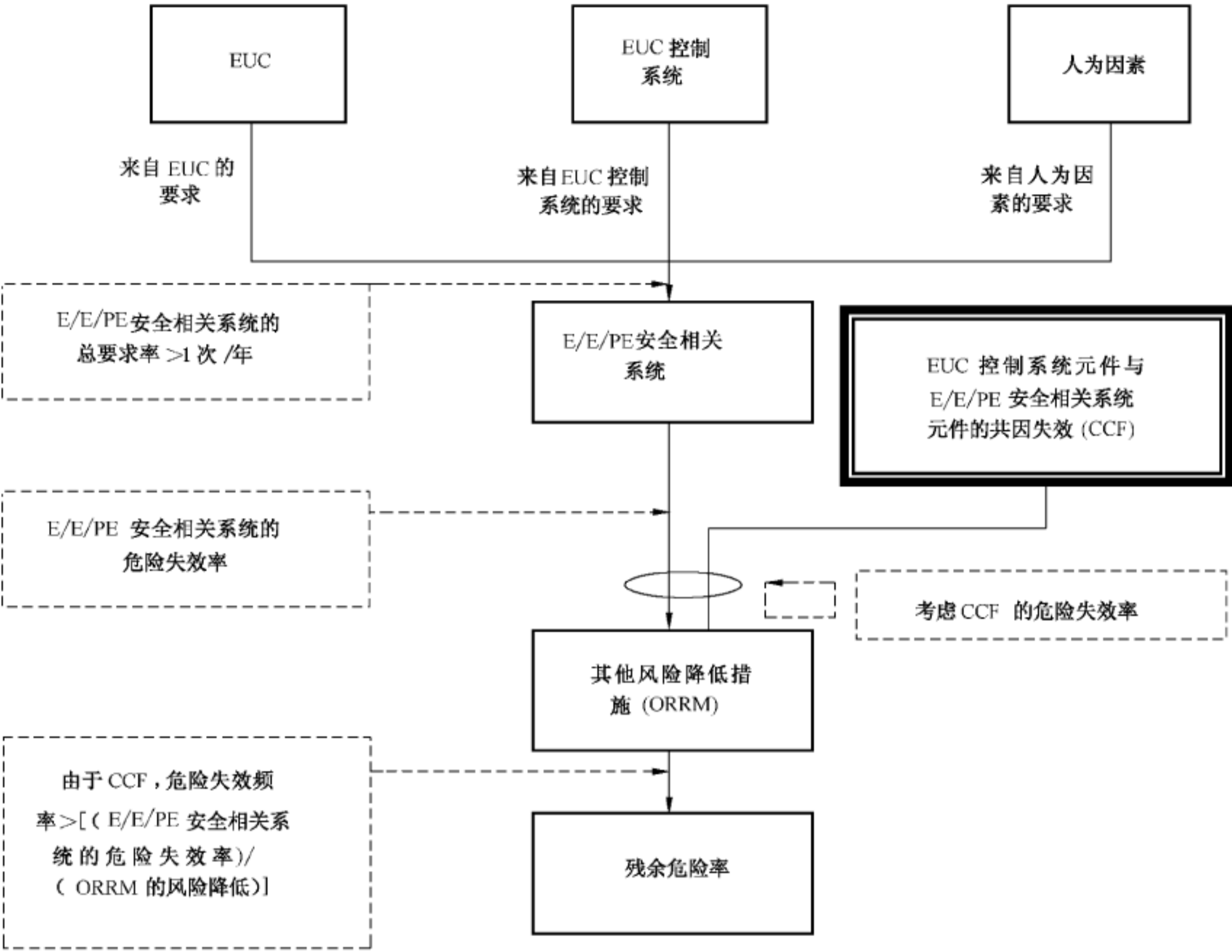


图 A.5 EUC 控制系统元件与 E/E/PE 安全相关系统元件的共因失效(CCF)示例

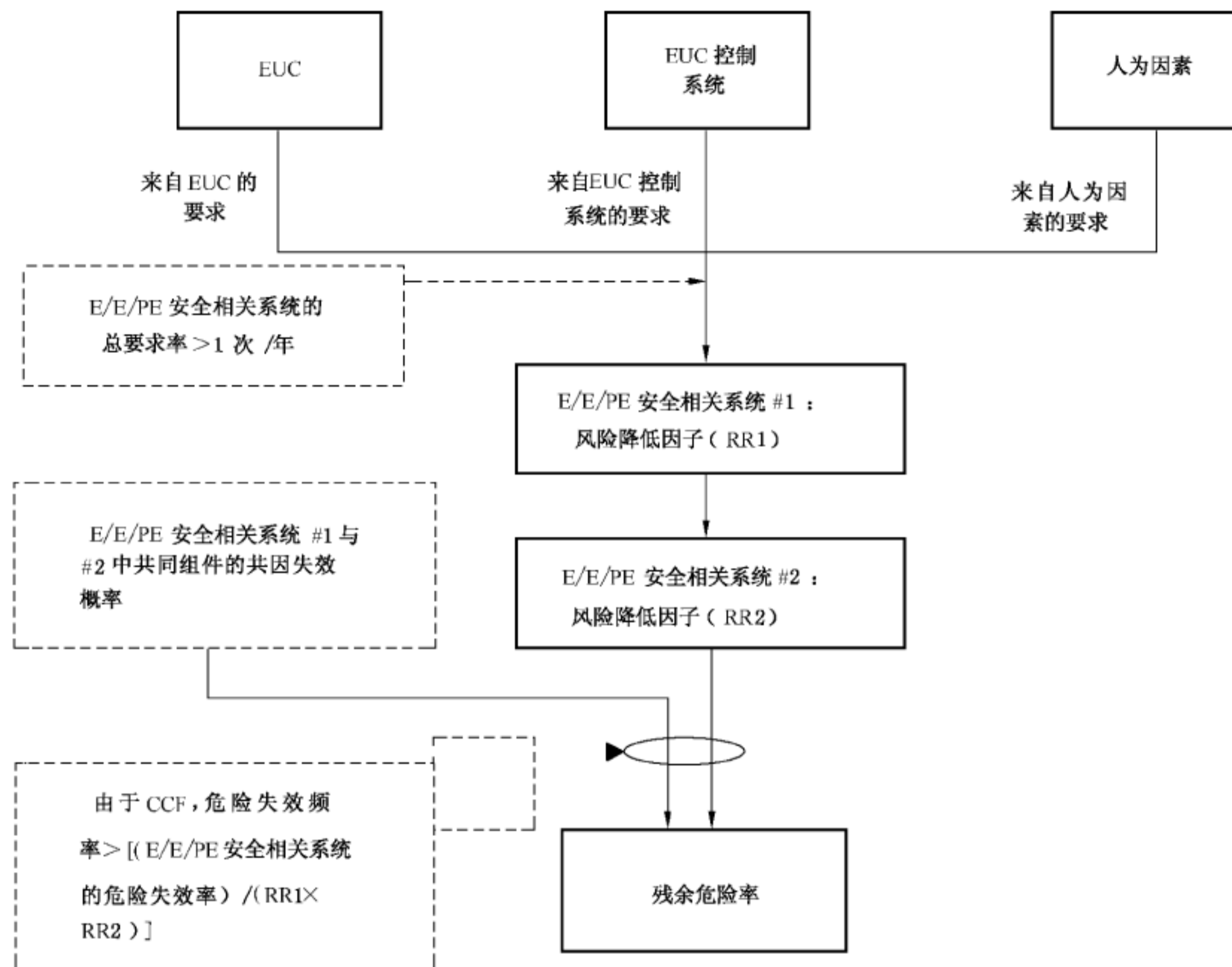


图 A.6 两个 E/E/PE 安全相关系统间的共因失效

A.5.5 使用多个保护层时的安全完整性等级

使用多个保护层达到可容忍风险时,可能会在系统之间、系统与产生要求的起因之间存在相互作用。如 A.5.4 中讨论的,通常要关心测试同步性及共因失效,因为当整体风险降低要求高或当要求频率低时,这些因素会成为重要因素。对安全层之间、安全层与要求起因之间相互作用的评估会很复杂,可能需要开发一个整体模型(如 ISO/IEC 31010 中所述),如基于一个自上到下的方法,顶事件规定为可容忍危险频率。该模型可能包括所有的安全层以计算实际的风险降低,所有的要求起因以计算实际的事故频率。需要识别最小割集(即故障详细说明),揭示系统解决方法中的弱点(即最小割集:单一故障、双重故障等),并通过敏感性分析便于系统改进。

A.6 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发生的概率和后果的估量,可以对不同情况的风险进行评估(EUC 风险、满足可容忍风险需要的风险降低、实际风险[见图 A.1])。可容忍风险需要考虑 A.2 中描述的问题来确定。安全完整性只应用于 E/E/PE 安全相关系统和其他风险降低措施,并作为这些系统/措施在规定的的安全功能方面成功取得必要的风险降低的概率的衡量标准。一旦确定了可容忍风险,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—2017 中的 7.4、7.5 和 7.6)。

注:分配需反复进行以使设计最优化以满足各种要求。

A.7 安全完整性等级和软件系统能力

为满足安全相关系统需达到广泛的必要风险降低,用分配安全功能的安全完整性要求到一系列安全相关系统的方法来满足要求。软件系统能力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。

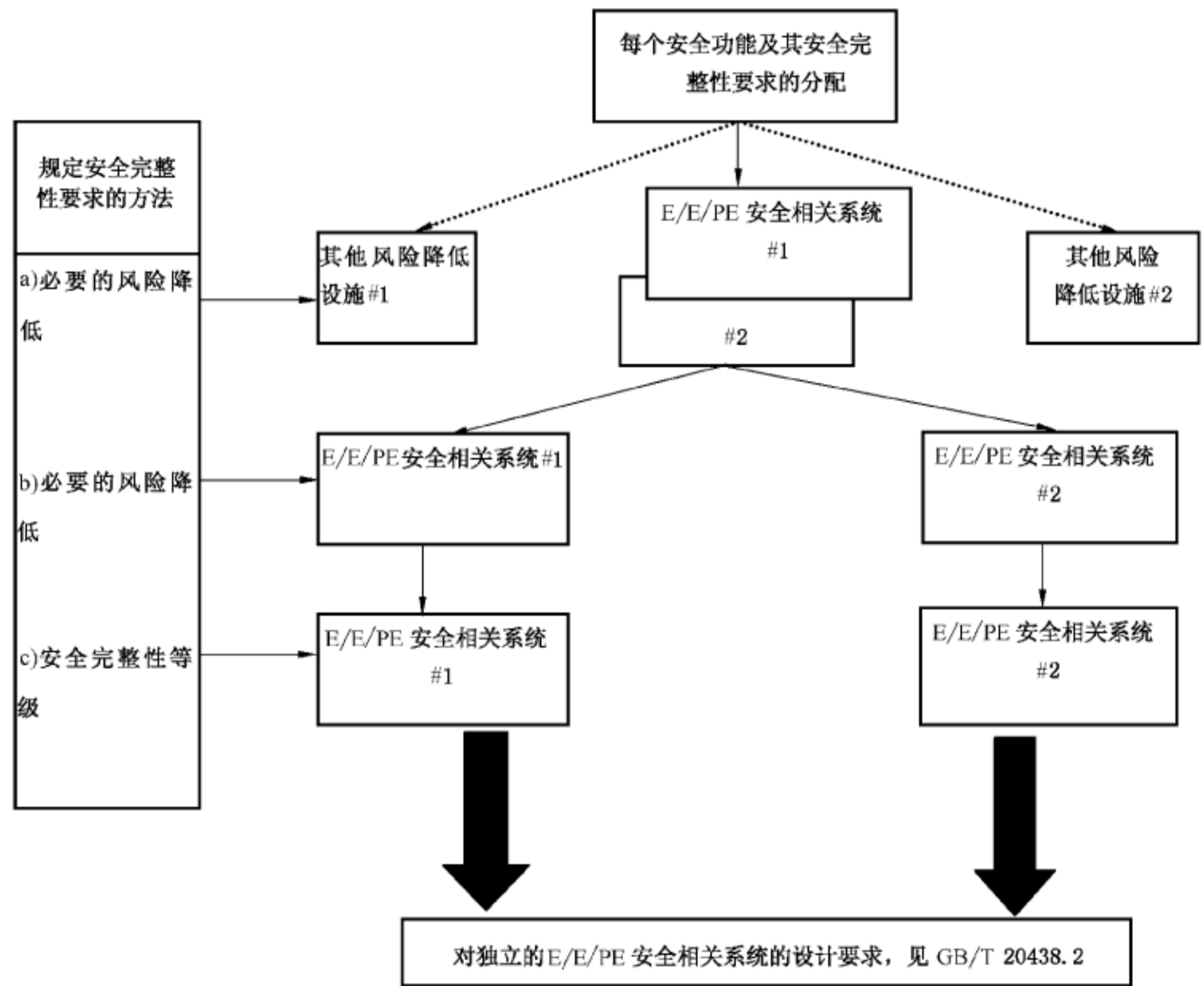
对四种安全完整性等级的安全完整性等级目标失效量的规定见 GB/T 20438.1—2017 中的表 2 和表 3。规定了两种参数,一种用于低要求运行模式的安全相关系统,另一种用于高要求运行模式或连续运行模式的安全相关系统。

注:对于低要求运行模式的安全相关系统,安全完整性量值关注的是在要求时执行其设计功能失效的概率。对于高要求运行模式或连续运行模式的安全相关系统,安全完整性量值关注的是每小时危险失效的平均概率(见 GB/T 20438.4—2017 中的 3.5.16 和 3.5.17)。

A.8 安全要求分配

对 E/E/PE 安全相关系统、其他风险降低措施的安全要求分配(安全功能和安全完整性要求)见图 A.7 (同 GB/T 20438.1—2017 中的图 6)。安全要求分配阶段的要求见 GB/T 20438.1—2017 的 7.6。

对 E/E/PE 安全相关系统、其他风险降低措施的安全要求分配使用的方法主要取决于必要的风险降低是否以定量的或定性的方式进行了明确规定。这些方法分别被称为定量或定性方法(参见附录 C、附录 D、附录 E、附录 F 和附录 G)。



注 1: 分配之前,安全完整性要求是与各安全功能相联系的(见 GB/T 20438.1—2017 的 7.5.2.3 和 7.5.2.4)。

注 2: 一个安全功能可能分配于多于一个的安全相关系统。

图 A.7 E/E/PE 安全相关系统和其他风险降低措施的安全要求分配

A.9 减轻系统

减轻系统在其他安全相关系统(如 E/E/PE 安全系统)发生全部或部分失效的情况下动作。目的是减轻危险事件的后果,而不是降低其发生频率。减轻系统的例子包括火气系统[检测火灾/气体,随后动作将火灾扑灭(例如,通过喷淋)]及汽车的气囊系统。

确定安全完整性要求时,应当注意判断后果严重程度只需考虑后果增量。也就是说,如果功能在其应当操作时未操作,则要确定后果严重程度的增量。首先,若系统失效无法操作,则考虑后果;然后,若减轻功能操作正确,则考虑将有何不同。若系统失效无法操作,在考虑后果时,通常会有许多结果,发生的概率也会不同。事件树(ETA)会是一个有用的工具。

注:对于确定火气系统和紧急停车系统的安全完整性等级的说明见 ISO 10418 的附件 B。

附录 B

(资料性附录)

确定安全完整性等级要求的方法选择

B.1 概述

本附录列出了多种用于确定安全完整性等级的方法。没有一种方法可适用于所有的应用,因此,用户需要选择最合适的方法。选择最恰当的方法时,应考虑以下因素:

- 1) 需要满足的风险可接受准则。如果要求说明风险降低到合理可行的低,那么一些方法将不适用。
- 2) 安全功能的运行模式。一些方法只适用于低要求模式。
- 3) 从事 SIL 确定工作的人员的知识和经验以及在此领域已有的传统方法。
- 4) 确信最终残余风险满足用户机构规定的指标。一些方法能得到定量指标,但一些方法只能是定性的。
- 5) 可以使用多于一种方法。一种方法可能用于筛选,如果筛选方法指明需要高的安全完整性等级,那么接着会有另一种更加严格的方法。
- 6) 后果严重程度。对于包含多个伤亡事故的后果,可能要选择更加严格的方法。
- 7) E/E/PE 安全相关系统之间或 E/E/PE 安全相关系统与要求起因之间是否发生共因失效。

无论使用什么方法,都应记录所有的假设,便于未来的安全管理。应当记录所有的判断结果,从而可进行 SIL 评估的验证,并提供用于独立的功能安全评估。

B.2 ALARP 方法

可以单独使用 ALARP 原理或结合其他方法来确定安全功能的 SIL 要求。可以定性或定量方式使用 ALARP。以定性方式使用时,对于一个特定的安全功能,增加其 SIL 要求,直到发生频率降低到满足第Ⅱ类或第Ⅲ类风险的标准为止。以定量方式使用时,频率与后果都以数值规定,增加 SIL 要求,直至显示与实现更高 SIL 相关的附加资本与运行成本满足第Ⅱ类或第Ⅲ类风险的条件为止(见图 C.1)。

使用 ALARP 方法时,需要考虑不可容忍区域与 ALARP 区域的边界。

B.3 SIL 确定的定量方法

定量方法参见附录 D。可与附录 C 中描述的 ALARP 方法一起使用。

定量方法可用于简单和复杂的应用。对于复杂应用,可以构造故障树来表示危险模型。顶事件通常是一个或多个事故,逻辑构成用于表示导致顶事件的要求起因和 E/E/PE 安全相关系统失效。若控制与防护功能采用了同类设备,可采用软件工具对共因失效建模。在一些复杂应用中,一个单一失效事件可能发生在故障树中的多个位置,这需要执行一次布尔减少。这些工具同样便于敏感性分析,以显示影响顶事件频率的决定性因素。SIL 可以通过确定达到可容忍风险目标的要求风险降低来确定。

该方法适用于运行在连续/高要求模式和低要求模式的安全功能。该方法通常得到低 SIL 值,这是因为风险模型是为各应用专门设计的,用数值来表示各风险因素而不是在校正的风险图中使用数值范围。但是,定量方法需要构造各危险事件的特定模型。建模需要技巧、方法和应用的知识,且需消耗大量时间来开发和验证模型。

该方法便于说明风险降低到合理可行的低。通过选择未来风险降低的方法,将附加措施集成于故障树模型中,然后确定风险的降低并将其与选择方法的成本进行比较来完成。

B.4 风险图方法

定性的风险图方法参见附录 E。该方法通过与 EUC 和 EUC 控制系统相关的风险因素的知识使安全完整性等级得以确定。引入大量参数用于共同描述安全相关系统故障或不可用时危险情形的特性。每四个集合中选择一个参数,然后选择的参数共同确定分配给各安全功能的安全完整性等级。该方法已广泛应用于机械领域,见 ISO 14121-2 及 ISO 13849-1 中的附录 A。

在参数选择是主观的且需要大量判断的情况下,该方法是定性的。残余风险不能由参数值计算出来。如果一个机构需要确保残余风险降低到规定的定量数值,则该方法不适用。

参数描述包括风险图与数值可容忍风险指标校准导出的数值。残余风险可以由各参数的数值计算得出。该方法适用于一个机构需要确保残余风险降低到规定的定量数值的情况。经验表明使用校准的风险图可得到高安全完整性等级。这是因为校准通常采用各参数的最差值。各参数有一个十倍的区间,如应用时对于所有参数范围取均值,SIL 会比可容忍风险要求的 SIL 高。该方法广泛应用于过程与海上领域。

风险图方法未考虑要求起因与 E/E/PE 安全相关系统失效起因的共因失效或其他保护层的共因问题。

B.5 保护层分析(LOPA)

基本方法已经在大量书本中描述,这种技术可以多种形式使用。一种用于确定 SIL 的方法参见附录 F。

该方法是定量的,且用户需要确定各后果严重性等级的可容忍频率。用于降低单一要求起因频率的保护层都给出数值置信度。不是所有的保护层都与所有的要求起因有关,因此,该方法可用于更复杂的应用。分配给保护层的数值可四舍五入到下一个较大的数字或十倍区间。如果保护层数值四舍五入到下一个较大的数字,相比校准的风险图,该方法会给出较低的风险降低要求及较低的 SIL 值。

由于将数值目标分配给特定的后果严重性等级,用户可相信残余风险满足机构指标。

上述方法不适用于运行于连续模式的功能,且未考虑要求起因和 E/E/PE 安全相关系统之间的共因失效。但是,可以调整使该方法适用于这些情况。

B.6 危险事件严重性矩阵

危险事件严重性方法参见附件 G。一个基本假设是加入一个保护层时,就实现一个显著的风险降低。更进一步的假设是保护层与要求起因之间、各保护层之间是独立的。上述方法不适用于运行于连续模式的功能。在选择风险因子是主观的及需要大量判断的情况下,该方法是定性的。残余风险不能从选择的危险因子计算得出。如果一个机构需要确信残余风险降低到规定的定量数值,该方法也不适用。

附录 C
(资料性附录)

ALARP 和可容忍风险的概念

C.1 概述

本附录考虑一个特定的方法来实现一个可容忍风险,其目的不是提供一个明确的统计方法,而是一个一般原则性的方法。该方法包括一个不断完善的过程,进一步降低风险的所有选项需要考虑效益和成本。如想采用附录中的方法应查阅引用的原始资料(参见参考文献[7])。

C.2 ALARP 模型

C.2.1 介绍

C.2 概述了用于调节工业风险的主要考核后果,并指出该活动涉及确定是否:

- a) 风险如此大,将被拒绝;或
- b) 风险或已经产生,很小可以忽略;或
- c) 风险已经降低到上文规定的情况 a)和 b)之间,且已经降低到了最低可行水平,牢记可接受的效益和考虑进一步减少的成本。

至于 c),ALARP 原理要求任何风险应降低到合理可行的范围,或低到合理可行的水平(ALARP 来自最后 5 个单词的缩写)。如果风险降低到两个极端(即不可接受范围和明显可接受范围)之间且 ALARP 原理已经被应用,那么对于特定应用,由此产生的风险是容许风险。这三个区域的方法如图 C.1 所示。

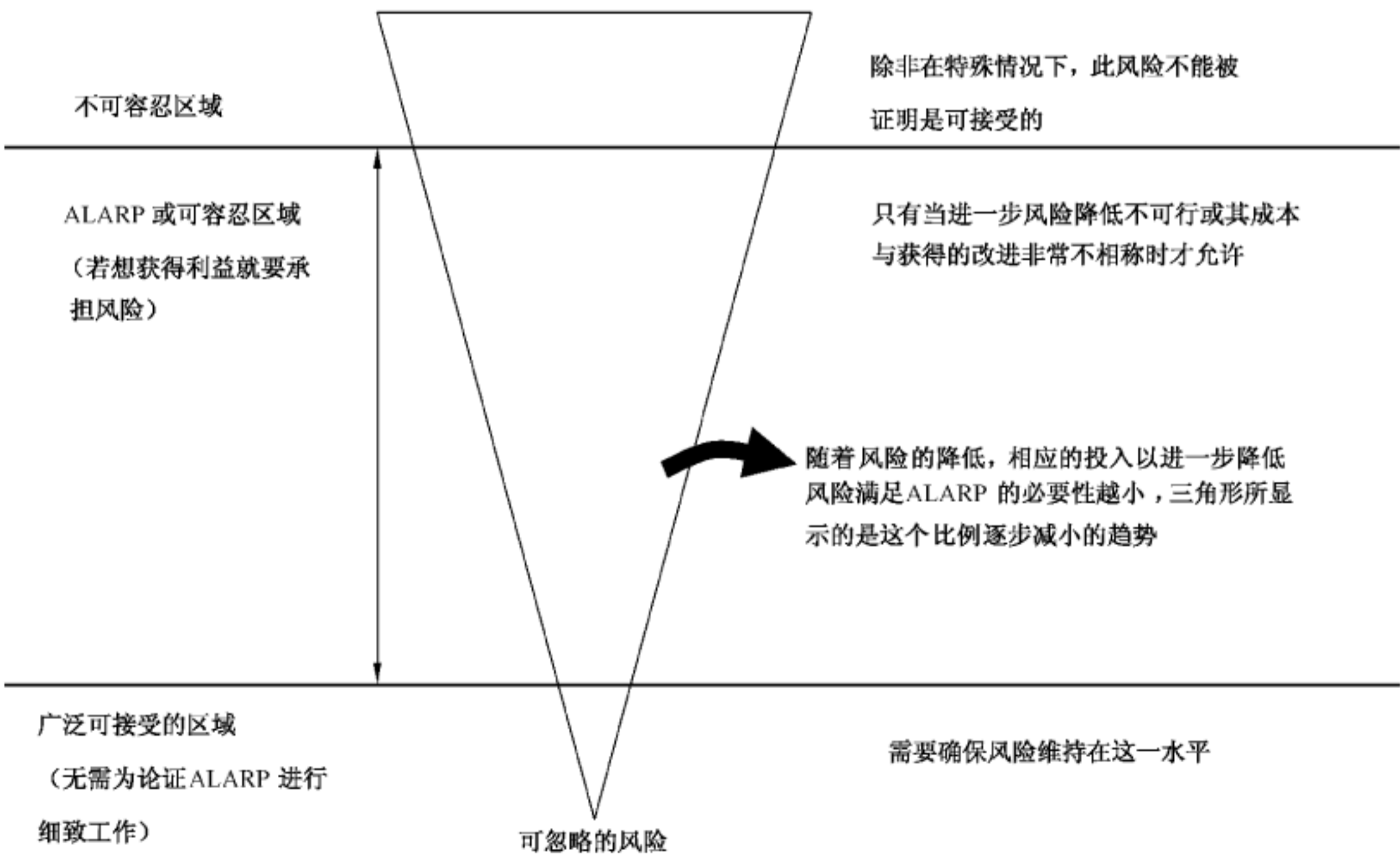


图 C.1 可容忍风险和 ALARP

超过一定水平,一个风险被视为无法容忍且在任何一般情况下是不合理的。

低于那个水平,假如相关风险已经低到合理可行,容忍度范围内的一个活动被允许发生。在这里可容许的不同于可接受的:它表明乐意忍受风险以确保某些利益,当能够这么做的同时期望它不断进行审查和消减。这里的成本效益评估被要求要么明确地要么含蓄地权衡成本和需要或对应的额外的安全措施。风险越高,相对应地期望更多的花费去降低风险。在有限的容忍度,与效益不成比例的支出将被调整。这里对风险的定义将是实质性的,一个甚至达到了降低边缘的相当大的努力是合乎情理的权益要求。

风险不那么重要的地方,相对应地为了减少风险需要更少的花费,并且在容忍度范围的下端,成本和效益之间平衡就足够了。

在容忍度范围以下的是相对于每天需要面对的微不足道的风险的明显可接受范围。在普遍可接受范围内,不需要一个详细的工作去论证 ALARP,然而,应该保持警惕,确保风险维持在这个水平。

ALARP 的概念可用于定性或定量风险目标被采用时。C.2.2 概述了用于定量风险目标的一个方法。(附录 D 和附录 F 概述了定量方法,附录 E 和附录 G 概述了针对特定危险确定必要的风险降低的定性方法。该方法表明在决策时可以体现 ALARP 的概念。)

注: ALARP 的更多信息已在文献目录的参考文献[7]中给出。

C.2.2 可容许风险目标

对一些结果加以确定和分配给他们的可容许频率获得一个可容许风险目标的一种方法。这个与可容许频率相匹配的结果将通过有关各方的讨论和同意(例如安全管理部门,那些生产风险和那些暴露于风险的)。

考虑到 ALARP 概念,与可容许频率匹配的结果可以通过风险类别来实现。表 C.1 是一个显示了用于一系列结果和频率的 4 个风险类别的示例(I, II, III, IV)。表 C.2 解释了每一个运用 ALARP 概念的风险类别。即,4 个风险类别中每一个的描述基于图 C.1。这些风险类别定义的风险是当风险降低措施已经落实到位时出现的。对于图 C.1,风险类别如下:

- 风险类别 I 是在无法容忍的范围内;
- 风险类别 II 和 III 是在 ALARP 范围内,风险类别 II 仅仅是在 ALARP 范围内;
- 风险类别 II 和 III 是在 ALARP 范围内,风险类别 II 仅仅是在 ALARP 范围内;

对于每一个具体情况或类似的行业,一个类似于表 C.1 的表格的制定将考虑到广泛的社会、政治和经济因素。每一个结果将匹配一个频率和依据风险类别填写的表。例如,经常在表 C.1 出现的可以表示一个事件经常发生,这可以规定为频率高于每年 10 次。一个关键的结果可能是一个个体死亡和/或多个严重伤害或严重的职业疾病。

表 C.1 事故风险分类的示例

频 率	结 果			
	灾难性的	危险的	微小的	可以忽略不计的
频繁的	I	I	I	II
很可能的	I	I	II	III
偶然的	I	II	III	III
微少的	II	III	III	IV
不大可能的	III	III	IV	IV
未必可能的	IV	IV	IV	IV
注 1: 风险类别 I、II、III 和 IV 的实际的总体取决于分布,也将取决于实际的频率是频繁的、很可能的,等等。因此本表宜是一个如何填写的示例,而不是作为一个将来使用的规范。				
注 2: 根据表中的频率,安全完整性等级的确定在附录 D 中做了概述。				

表 C.2 风险级别的解释

风险级别	解 释
级别 I	无法容忍的风险
级别 II	不良的风险,可容许的,只有降低风险不切实际或如果成本与获得的改善极不相称
级别 III	可容许风险,如果风险降低的成本将超过获得的改善
级别 IV	可以忽略不计的风险

附录 D

(资料性附录)

确定安全完整性等级——一种定量的方法

D.1 概述

本附录给出了一个确定安全完整性的定量方法,并说明了如何运用表 C.1 中包含的信息。在下列情况时,定量方法是一个特定值:

- 以数值的方式规定可容忍的风险(例如一个特定后果的发生频率应不大于 10^4 年一次)。
- 为安全相关系统的安全完整性等级规定数值目标。该目标已在 GB/T 20438 里被规定了(见 GB/T 20438.1—2017 的表 2 和表 3)

本附录并不打算确定一个最终方法,旨在说明一般原则。尤其适用于图 A.1 和图 A.2 所示的风险模型。

D.2 一般方法

用来说明一般原则的模型见图 A.1。且需要 E/E/PE 安全相关系统实施每一个安全功能,该方法的关键步骤如下:

- 确定如表 C.1 所示的可容忍风险;
- 确定 EUC 风险;
- 确定必要的风险降低,以满足可容忍风险;
- 将必要的风险降低分配给 E/E/PE 安全相关系统,其他风险降低措施(见 GB/T 20438.1—2017 的 7.6)。

表 C.1 中填写了风险频率并允许指定一个可容忍风险目标数值(F_t)。

可以使用定量风险评估方法预计在没有保护时,存在于 EUC 的、与风险相关的频率,包括 EUC 控制系统和人为因素问题(EUC 风险)。危险事件在没有保护时发生的频率(F_{np})是 EUC 风险的两个组成部分之一;另一个部分是危险事件的后果。 F_{np} 可能由以下决定:

- 来自于类似情况的失效率分析;
- 来自于相关数据库的数据;
- 用适当预测方法得出的计算结果。

GB/T 20438 为 EUC 控制系统限制了可声明的最低失效率(见 GB/T 20438.1—2017 的 7.5.2.5)。如果 EUC 控制系统声明的失效率小于此最低失效率,那么 EUC 控制系统将被视为一个安全相关系统,并且应满足 GB/T 20438 中对于安全相关系统的所有要求。

D.3 示例计算

图 D.1 提供了如何计算单个安全相关防护系统的目标安全完整性的示例。

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

式中

PFD_{avg} ——安全相关防护系统在要求时的平均危险失效概率,是在一个低要求运行模式下运行的安全相关防护系统的目标失效量(见 GB/T 20438.1—2017 的表 2 和 GB/T 20438.4—2017

的 3.5.16)。

F_t ——一个可容忍危险频率；

F_{np} ——安全相关防护系统的要求率。

在图 D.1 中还有：

—— C 是危险事件的后果；

—— F_p 是采用防护措施后的风险频率。

由此可见,EUC 的 F_{np} 的确定是重要的,因为它关系到 PFD_{avg} 和此后的安全相关防护系统的安全完整性等级。

下面给出了获得安全完整性等级的必要步骤(当后果 C 保持不变)(如图 1),对于这种情况,全部必要的风险降低是通过一个单独的安全相关防护系统达到的,(这个系统)必须将危险率降低到最低,从 $F_{np} \sim F_t$:

——在没有额外的任何防护措施(F_{np})时,确定 EUC 风险的频率；

——在没有额外的任何防护措施时,确定后果 C ；

——用表 C.1 来确定,频率 F_{np} 和后果 C 是否已实现了可容忍风险等级。如果通过采用表 C.1 导致了风险等级 I ,那么还需要进一步降低风险。风险等级 IV 或 III 将是可容忍的风险。风险等级 II 将需要做进一步的调研；

注：表 C.1 用于检查是否进一步的风险降低措施是必要的,因为,在没有额外的任何防护措施时,可能已经达到了可容忍风险。

——确定安全相关防护系统在要求时的失效概率(PFD_{avg})以满足必要的风险降低(ΔR)。对于一个后果是常量的具体情况, $PFD_{avg} = (F_p / F_{np}) = \Delta R$ ；

——对于 $PFD_{avg} = (F_p / F_{np})$,安全完整性等级可以从 GB/T 20438.1—2017 的表 2 中获得(例如,对于 $PFD_{avg} = 10^{-2} \sim 10^{-3}$,安全完整性等级=2)

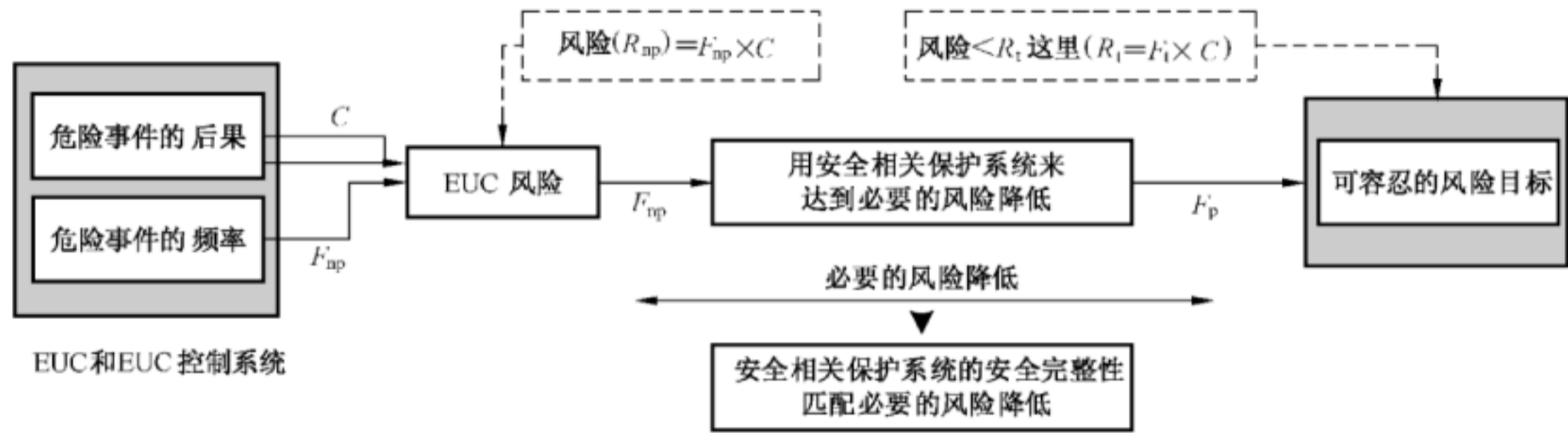


图 D.1 安全完整性分配—安全相关保护系统的示例

附录 E

(资料性附录)

安全完整性等级的确定—风险图方法

E.1 概述

本附录描述了风险图方法,这是一种根据与 EUC 和 EUC 控制系统相关的风险因素方面的知识,确定安全相关系统的安全完整性等级的方法。当风险模型如图 A.1 和图 A.2 所示时,特别适用。这种方法可用于定性或定量。

当采用这种方法时,为了简化,用一组参数,一起描述危险情况的性质。该组参数是当没有安全相关系统或其失效时的参数。从四个参数的每个参数组中选择一个参数,然后组合起选定的参数,用以确定分配到安全功能的安全完整性等级。这些参数

——为风险给予有意义的分级;和

——包含关键的风险评价因素。

本附录并不打算确定一个最终方法,旨在说明一般原则。

E.2 风险图构成

下面的简化过程是基于以下方程:

$$\text{确定了}(C)\text{之后}, R = (f)$$

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频率;

C ——危险事件的后果(其后果可能是健康和安全相关的伤害或环境破坏导致的伤害)。

在这种情况下,危险事件的频率 f 被认为由三个影响因素组成:

——暴露于危险区域的频率、时间;

——避免危险事件的可能性;

——没有增加任何安全相关系统时危险事件发生的可能性(但有其他风险降低措施),这被称为不期望事件的发生概率。

这里引出下面的 4 个风险参数:

——危险事件的后果(C);

——暴露于危险区域的频率、时间(F);

——无法避免危险事件的可能性(P);

——不期望事件发生的概率(W)。

风险参数可能是定性的,如表 E.1 所描述的,或定量的,如表 E.2 所描述的。确定表 E.2 中的每个参数的数值时,要求一个校准的过程。

E.3 校准

校准过程的目的如下:

——以一种方式描述所有的参数,使 SIL 评估团队基于应用特征能做出客观的判断;

- 确保为应用选择的 SIL,是依据企业风险准则的,并考虑了来自其他来源的风险;
- 使参数的选择过程能够被验证。

校准风险图是给风险图参数设定数值的过程。这是评估现有的过程风险的基础,也是确定考虑中的安全功能所需完整性的基础。在没有设置特定安全功能时,结合应用风险的一个分级评价,给每个参数分配一个范围值。这样,就确定了对安全功能的依赖程度。风险图将特定组合的风险参数与安全完整性等级结合起来。通过考虑与特定危险相关的可容忍风险,建立了组合的风险参数和安全完整性等级之间的关系。

当考虑风险图校准时,重要的是考虑由业主的期望和监管机构的要求而产生的对风险的要求。可用许多方法描述对生命的风险,如 A.2 和附录 C 的描述。

如果应该将单一原因死亡事故的频率降低,且规定的降低量很大,则不能假设将所有风险降低分配给单独的 E/E/PE 安全相关系统。暴露在危险中的人员可能会遭受来自于其他来源(例如跌落、火灾和爆炸风险)的许多各种不同的风险。在校准时,要考虑各类危险、和处于风险中的总时间。

当考虑风险降低要求的程度时,一些组织机构可能有关于避免人身伤害增加成本的准则。可通过为实现更高的完整性等级而增加的硬件和工程的年度成本,与风险降低幅度相除进行计算。如果为避免死亡而增加的成本少于预定值,则完整性等级的增加是合理的。

在确定每个参数值之前,需要考虑上述问题。大多数参数被指定了一个范围(例如,如果一个特定过程的预期要求率在规定的每年 1~10 的范围内,那么 W_3 可能被采用)。同样,对于更低的数量级范围内的需求, W_2 将适用,至于下一个更低的数量级范围内的需求,适用 W_1 。给每个参数一个规定的范围,帮助团队针对一个特定的应用决定选择哪个参数值。为了校准风险图,给每个参数指定值或值的范围。然后确定每个参数组合与风险的联系以满足已定义的风险标准。修正所有参数组合中的参数的描述,达到已定义的风险标准。如表 E.2 的校准示例中,引入一个“D”因素使得与 W 因素相关联的要求范围能够得到修正以实现可容忍风险。在某些情况下,与其他风险因素相关的范围可能需要修改,以反映参数值在被考虑的应用范围内。校准是一个迭代过程且过程一直持续到所有参数值组合满足了规定可接受的风险准则。

确定一个特定应用的 SIL,不需要每次都执行校准活动。对于类似的危险,通常只需要有关机构去承担这项工作。如果,针对具体项目,发现在校准期间的原始假设是无效的,则可能需要调整。

当完成指定参数后,如何得到数值的信息应该是可知的。

重要的是,校准的过程要得到组织机构内负责安全的高层的同意。所采取的决策决定了可达到的整体安全。

通常,用风险图法,难以考虑要求源和 E/E/PE 安全相关系统所使用设备之间相关失效的可能性。因此可能导致对 E/E/PE 安全相关系统有效性的高估。对风险图的校准时如果包括高于每年一次的要求率,则采用风险图导出的 SIL 要求可能高于需求,此时推荐采用其他技术。

E.4 其他可能的风险参数

以上规定的风险参数足够适用于广泛的应用。但是,有可能在应用方面需要引进额外的风险参数,例如在 EUC 和 EUC 控制系统中采用新的技术。额外参数的用途将更加精确地估算必要的风险降低(见图 A.1)。

E.5 风险图实施—通用方案

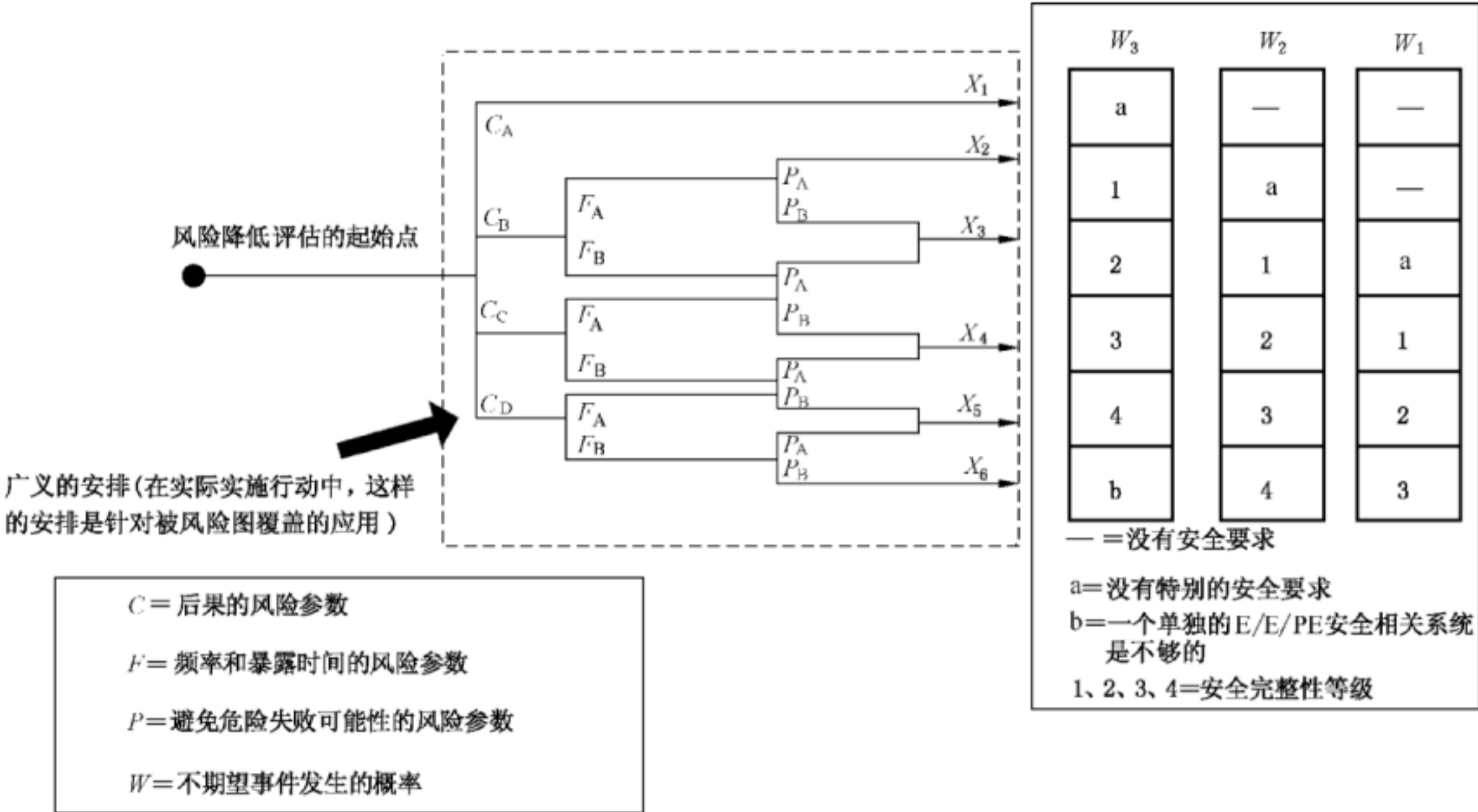
用上述的风险参数组合开发一个风险图,如图 E.1 所示。关于图 E.1:

$$C_A < C_B < C_C < C_D; F_A < F_B; P_A < P_B; W_1 < W_2 < W_3$$

- 该风险图的解释如下：
- 采用风险参数 C 、 F 和 P 导出了许多输出 X_1 、 X_2 、 X_3 …… X_n （确切数字依赖于风险图覆盖的特定应用领域）。图 E.1 是没有为更为严重的后果额外加权时的情况。这些输出的每一个映射到三个标尺中的一个（ W_1 、 W_2 和 W_3 ）。这些标尺上的每一个点，就是考虑中的 E/E/PE 安全相关系统应达到的安全完整性。实际上，对于规定的后果，可能会有一个单独的 E/E/PE 安全相关系统不足以提供必要风险降低的情况。
 - 映射 W_1 、 W_2 或 W_3 允许采取其他风险降低措施。标尺 W_1 、 W_2 和 W_3 的补偿特点允许来自其他措施的三个不同等级的风险降低。此处，标尺 W_3 对应其他措施提供最小风险降低的情况（也就是意外事故发生的概率最大），标尺 W_2 对应其他措施提供中等风险降低的情况，标尺 W_1 对应其他措施提供最大风险降低的情况。对应于风险图中特定的中间输出（即： X_1 、 X_2 ……或 X_6 ）以及特定的 W 标尺（即： W_1 、 W_2 或 W_3 ），风险图的最终输出给出了 E/E/PE 安全相关系统的安全完整性等级（即：1、2、3 或 4），这也是系统必要的风险降低量。这个风险降低与通过其他已被考虑进 W 标尺机制的措施达到的风险降低（例如通过其他技术的安全相关系统和其他风险降低措施）一起，对具体情况给出了必要的风险降低。
 - 对于每个具体情况或可类比的行业，图 E.1 中的参数（ C_A 、 C_B 、 C_C 、 C_D 、 F_A 、 F_B 、 P_A 、 P_B 、 W_1 、 W_2 、 W_3 ）及其权重需要精确定义，并需要在应用领域的标准中规定。

E.6 风险图示例

基于表 E.1 中的数据，实现风险图的示例见下面的图 E.2。采用了风险参数 C 、 F 和 P 导出了 8 个输出中的一个。这些输出的每一个，映射到三个标尺中的一个标尺（ W_1 、 W_2 和 W_3 ）上。这些标尺中的每一个点（a、b、c、d、e、f、g 和 h）指示出通过安全相关系统应该满足的安全完整性。



IEC 1666/98

图 E.1 风险图：通用方案

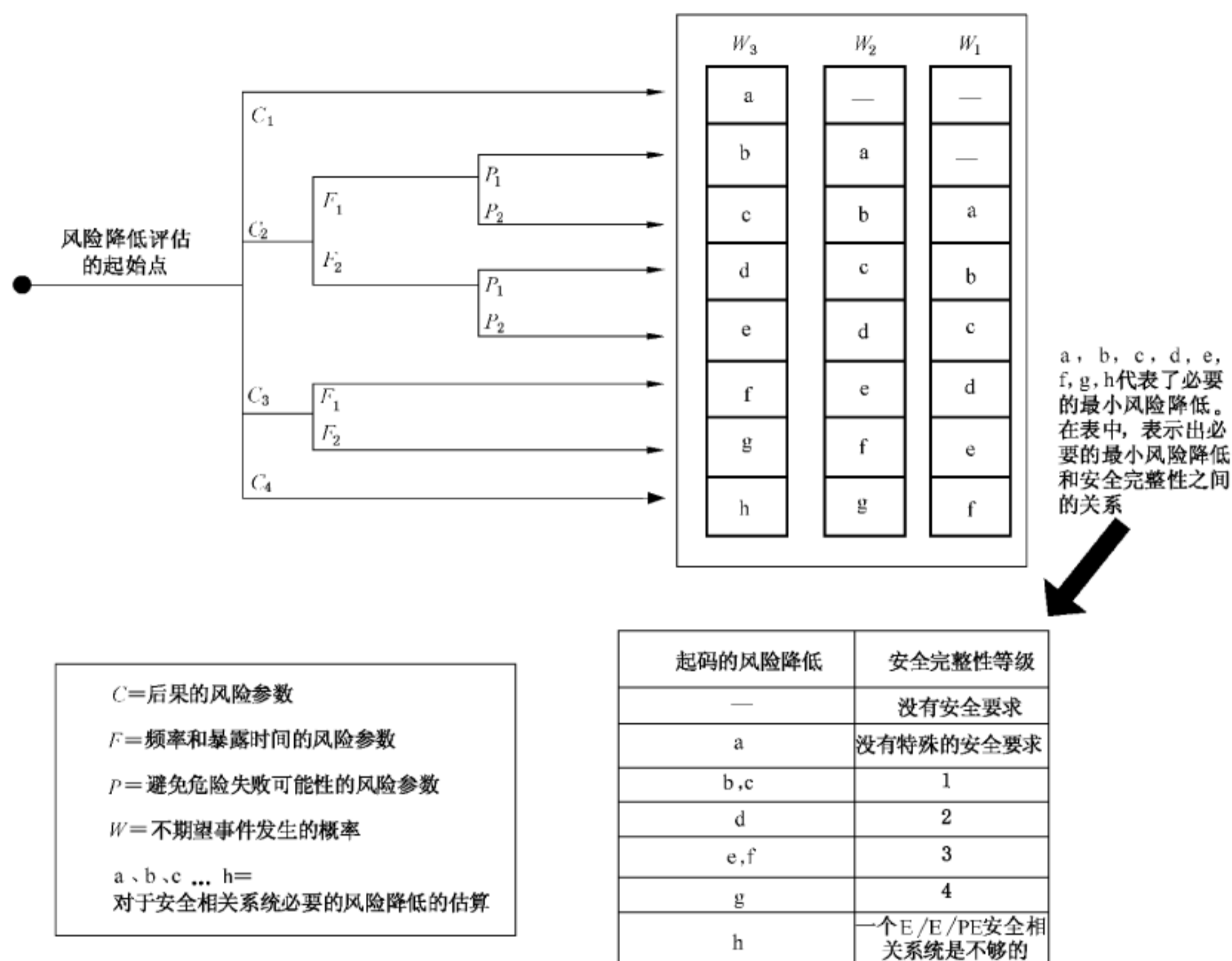


图 E.2 风险图一示例(仅说明一般原则)

表 E.1 与风险图相关的数据示例(图 E.2)

风 险 参 数		类 别	注 释
后果(C)	C_1	轻伤	1. 本分类系统的制定针对人的伤害和死亡。 对于环境破坏或财产损失需要制定其他的分类法 2. 对于 C_1 、 C_2 、 C_3 和 C_4 的解释,要考虑事故的后果和正常的康复
	C_2	对于 1 人或多人的严重的永久性损伤;1 人死亡	
	C_3	多人死亡	
	C_4	非常多的人死亡	
危险区中的频率和暴露时间(F)	F_1	极少到经常暴露在危险区中	3. 参见上面的注释 1
	F_2	频繁到持续暴露在危险区中	

表 E.1 (续)

风 险 参 数		类 别	注 释
避免危险事件的可能性(P)	P_1	某些条件下可能	4. 这个参数考虑了 ——过程的操作[有管理的(也就是被熟练的或不熟练的人操作)或无管理的]; ——危险事件的发展速度(例如突然地、迅速地或缓慢地); ——识别危险的难易(例如立即看到,通过技术措施的检测可发现或没有技术措施的检测可发现); ——避免危险事件(例如可能的逃生路线,不可能或在一定条件下可能); ——实际的安全经验(这样的经验可能和一个完全相同的 EUC 一起存在或和一个类似的 EUC 一起存在或可能不存在)
	P_2	几乎不可能	
不期望事件发生的概率(W)	W_1	一个非常小的概率,即:几乎没有不期望事件发生	5. W 因素的目的是预估在没有额外的任何安全相关系统(E/E/PE 或其他技术),不期望事件出现的频率,但包括任何其他的风险降低措施 6. 如果很少或没有 EUC,或 EUC 控制系统,或一个类似的 EUC 和 EUC 控制系统的经验存在, W 因素可能通过计算得出。在这种情况下,应做出最坏的预测
	W_2	一个小概率,即:只有很少的不期望事件发生	
	W_3	一个相当高的概率,即:不期望事件可能频繁发生	

表 E.2 通用风险图的校准示例

风 险 参 数		类 别	注 释
后果(C)	C_A	轻伤	1. 针对人员的伤害和死亡,已开发了分类系统。 2. 对于 C_A 、 C_B 、 C_C 和 C_D 的解释,应考虑事故的后果和正常的康复
死亡人数	C_B	范围:0.01~0.1	
通过确认暴露在危险区域的人数,并乘以已识别危险的致命性来计算	C_C	范围>0.1~1.0	
致命性由危险的可防护性质所决定。可采用如下因子: $V=0.01$ 易燃物或有毒物质的少量释放	C_D	范围>1.0	
$V=0.1$ 易燃物或有毒物质的大量释放			
$V=0.5$ 同上,且伴有高的着火的可能性或剧毒物质			
$V=1$ 破裂或爆炸			

表 E.2 (续)

风 险 参 数		类 别	注 释
占有率(F) 通过确定正常工作期间危险区域被占有的时间比来计算 注 1: 如果不同的班组,处在危险区域的时间是不同的,那么宜选择最大值 注 2: 只有当要求率是随机的,并且当要求率与占有率的升高无关时,则适合采用 F_A 。通常在设备启动或在发生异常调查期间,占有率会升高	F_A	极少到经常暴露在危险区域中 占有率少于 0.1	3. 参见上面的注释 1
	F_B	频繁到持续暴露在危险区中	
如果保护系统不能运行,避免危险事件的可能性(P)	P_A	如果列 4 的所有条件都满足时采用	4. 如果以下所有条件都满足,选择 P_A : ——设施提供警报给操作人员,SIS 已经失效了; ——单独的设施用于停机,使得危险可以避免或使所有的人员逃到安全区; ——操作人员接到报警到一个危险事件出现的时间超过 1 h,或肯定足够采取必要的行动
	P_B	如果不满足所有的条件时采用	
要求率(W) 在没有 E/E/PE 安全相关系统时,危险事件每年将出现的次数 确定要求率,有必要考虑导致一个危险事件的所有的失效源。确定要求率时,要对控制系统的性能和介入给予置信度的限制。如果控制系统没有按 GB/T 20438 设计且维护,可以声明的性能应低于 SIL 1	W_1	要求率少于 0.1 D /年	5. W 因素的用途是预估没有额外的 E/E/PE 安全相关系统时,危险发生的频率 如果要求率非常高,SIL 应该通过另外的方法或已重新校准的风险图去确认。值得注意的是,对于连续模式(见 GB/T 20438.4—2017 的 3.5.16)下的应用操作,风险图方法可能不是最好的方法。
	W_2	要求率在 0.1 $D \sim D$ /年之间	
	W_3	要求率在 $D \sim 10D$ /年 对于要求率高于 10 D /年,应当需要较高的完整性	6. 通过企业准则中的可容忍风险,考虑对暴露人群的其他风险,来确定 D 值
注: 这是一个说明风险图设计原理的应用示例。针对特殊应用和特殊危险的风险图,要考虑到可容忍风险,并与其相一致,参见 E.1~E.6。			

附录 F

(资料性附录)

采用保护层分析的半定量法(LOPA)

F.1 通用

F.1.1 描述

本附录描述了一个叫做保护层分析(LOPA)的方法。并不打算确定一个明确的统计方法,而是打算说明一般原则。

F.1.2 附录引用

本附录基于一个方法,更详细的描述见 AIChE(美国化学工程师学会, American Institute of Chemical Engineers)的出版物(见参考文献[8])。本参考细节很多方法采用了 LOPA 技术。

在一个方法中,所有相关参数取整到更高的十进制范围(例如, 5×10^{-2} 的一个可能性是四舍五入到 10^{-1})。这是一个非常保守的方法,能够显著地导向更高的 SIL 等级。通过对所有参数值四舍五入到下一个最高的有效数字,无论如何数据的不确定性将被辨识(例如, 5.4×10^{-2} 取整到 6×10^{-2})。

F.1.3 方法描述

LOPA 分析危险并确定所需的安全功能,及所需安全功能的 SIL。应对 LOPA 方法进行调整以满足风险可接受准则。该方法从危险识别中获得的数据作为出发点,对每个辨识出的危险通过记录初始原因和阻止或减轻危险的防护层来进行分析。以此来确定风险降低的总量以及分析是否需要更多的风险降低。如果额外的风险降低是必需的,而且如果是以 E/E/PE 安全相关系统的形式被提供,LOPA 方法能用来确定适当的 SIL。针对每一个危险,确定一个适当的 SIL 来将降低风险到可容忍的等级。下文中的表 F.1 显示了一个典型的 LOPA 形式。

F.2 影响事件

利用表 F.1,在表 F.1 的第 1 列输入在风险识别中确定的每个影响事件的描述(后果)。

F.3 严重等级

在表 F.1 的第 2 列中输入事件的严重等级。严重程度将从一个表格中获得,在表格中对次要的、严重的、灾难性的结果等级做一般性的描述,并且对每个严重等级规定了后果范围和最大频率。实际上这张表设置了用户的容忍度条件。对于能引起安全和环境后果的事件,需要收集信息以确定其严重等级和最大频率。

F.4 初始原因

影响事件的所有初始原因被列在了表 F.1 的第 3 列。影响事件可能有很多的初始原因,都应该被列出。

表 F.1 LOPA 报告

a	1	2	3	4	5				7	8	9	10	11
					保护层(PLs)								
	影响事件的描述 F.2	严重程度等级 F.3	初始原因 F.4	初始可能性 F.5	总体设计 F.6.1	控制系统 F.6.2	报警,等 F.7	额外的减缓,访问受限 F.7	额外的减缓 F.8	中间事件的可能性 F.9	对 E/E/PE 要求的 PFD_{avg} 和 SIL F.10	可容忍减缓的事件的可能性 F.11	注释
1	电机超速导致的套管的断裂	临近套管的人员生命的丧失,死亡人数不会超过2个人	速度控制系统故障	0.1	1	1	1	0.1	0.1	10^{-3}	5×10^{-3} (SIL2, 对应 5×10^{-3} 的一个最小的一个最小 PFD_{avg})	10^{-5}	可容许频率,如果死亡率,如果死亡人数没有超过 5 个人
			过载	1	0.1	1	1	0.1	0.1	10^{-3}			
			离合器故障	0.1	0.1	1	1	0.1	10^{-4}				
				0.1, 给控制系统信任度	占用有限, 90%的时间没有人出现	死亡只发生在如果碎片碰到了人	2.1×10^{-3}						
2	对环境风险分析重复上述过程												
3					按求续								
...													
...													
N													
注 1: 严重程度等级可能被归类为 C(灾难性的)、E(大量的)、S(紧急的)或 M(较小的)。可容忍减缓事件的可能性取决于严重程度等级。													
注 2: 列 4、8、10 的单元是每年的事件。													
注 3: 列 5~7、9 的单元是无量纲的。0 和 1 之间的数是一个因子,通过与事件可能性相乘来表示相应防护层的减缓效果。因此 1 表示没有减缓效果,0.1 表示 10 倍的风险降低因子。													
a. 对给出的行和列的数更加详细的描述包含在附录 F 中。													

F.5 初始可能性

在表 F.1 第 3 列中的初始原因的每个可能性数值以年为单位列于表 F.1 的第 4 列。

初始可能性能够从设备失效率的通用数据和已知的检验测试间隔进行计算或从设备记录来计算。仅当有足够的统计数据作为基础时,才能使用低的初始可能性。

F.6 保护层(PL)

F.6.1 通用

每一个 PL 包含了一组功能独立于其他保护层的设备和/或行政控制。

在表 F.1 的第 5 列中首先给出了设计特点,当初始事件发生时它可以减少影响事件发生的可能性。PL 应该有以下重要的特征:

- 专门性:一个 PL 被设计为单独地预防或减轻一个潜在危险事件的结果(例如,一个失控反应,释放有毒物质,一个限制失效,或一次火灾)。多重原因可能导致相同危险事件,因此多重事件场景可能启动一个 PL 的动作。
- 有效性:当所有其他措施完全失效时,一个 PL 必须能够独立防止不利后果。
- 独立性:一个 PL 独立于与已识别的危险事件相关联的其他 PL。
- 可信性:一个 PL 能够按照设计去实现功能。在设计中已考虑了随机和系统性失效模式。
- 可审核性:将 PL 设计为能进行防护功能的定期验证。对安全系统的检验试验和维护是必要的。

F.6.2 基本控制系统

表 F.1 中第 5 列的下一项是 EUC 控制系统。当初始原因发生时,如果一个控制功能预防影响事件的发生,则对其声明一个基于 PFD_{avg} 的信任度。如果功能失效时引起对 E/E/PE 安全相关系统的要求,则不考虑此控制功能的作用。还应该指出,如果控制功能不是做为一个安全系统来设计和运行,控制功能的 PFD_{avg} 应该限制到最小 0.1。

F.6.3 报警

表 F.1 中第 5 列的最后一项是考虑报警来提醒操作人员和利用操作人员介入的信任度。只有在如下情况下考虑报警的信任度:

- 使用的硬件和软件是分开的且独立于采用的控制系统(例如,不应共享输入卡和处理器)。
- 具有高优先等级的报警显示在一个永久有人的地方(操控室/主控室)。在考虑报警的信任度时应考虑如下:
 - 一个报警的有效性将取决于需要在报警的事件中执行任务的复杂性及同时需要执行的其他任务。
 - 信任度应该限制到一个最小为 0.1 的 PFD_{avg} 。
 - 操作人员需要充分的时间和独立的设施以终止危险。通常,只有报警和危险出现之间的时间超过 20 min,报警才是有效的。

F.7 和 F.8 额外的缓解

缓解层通常是机械、结构或规程上的。示例包括:

- 限制接近；
- 着火概率的减少；
- 减少暴露于危险中人的脆弱性的任何其他因素。

缓解层可减少影响事件的严重程度,但不能预防事件的发生。示例包括:

- 对于火灾发生时的喷淋系统；
- 气体报警器；
- 减少人员暴露于一个逐步升级的事件中的可能性的疏散规程。

缓解考虑了人员受影响最大的危险区域的占有率。每年在危险区域的小时数除以每年 8 760 小时来决定此百分比。

在表 F.1 的第 6 列和第 7 列确定和列出所有缓解层的适当的 PFD_{avg} 或相应参数。

F.9 中间事件的可能性

对于每一个原因,中间事件的可能性通过如下因子的相乘进行计算,并将结果以每年发生频率的形式列于表 F.1 的第 8 列:

- 大多数暴露人员的脆弱性；
- 初始可能性(第 4 列)；
- 防护层和缓解层的 PFD_{avg} (第 5 列、第 6 列和第 7 列)。

总中间事件的频率应该通过将每个原因的中间事件的频率累加来计算。

总中间事件的频率应该与相关严重程度等级的可容忍风险的频率相比较。如果总中间频率超过可容忍频率,则需要降低风险。在应用 E/E/PE 安全相关系统形式的额外的 PL 之前,应该考虑本质上更安全的方法和解决方案。

如果中间事件可能性的数据不能降低到低于最大的频率准则,那么需要一个 E/E/PE 安全相关系统。

F.10 安全完整性等级(SIL)

如果需要一个安全功能,所需的 SIL 能够确定如下:

- 将严重程度等级相关的最大频率除以全部中间事件的可能性,来计算所要求的 PFD_{avg} ;
- PFD_{avg} 的数字目标值能够与 SIL 一起用于安全要求规范。相关 SIL 能够通过 GB/T 20438.1—2017 的表 2 获得；
- 如果在过程要求规范中没有 PFD_{avg} 的数字目标值,且只标明了有所需的 SIL,实际的 SIL 应该比要求的 SIL 高一个等级,这样与特定 SIL 相关的 PFD_{avg} 所有风险数值都降低。

如果所需的 PFD_{avg} 大于或等于 0.1,功能分配到类别“无特殊安全完整性要求”。

F.11 可容许的缓解事件的可能性

可容忍的缓解事件的可能性取决于后果的严重程度等级。这将取决于采用的可容忍风险准则(可容忍风险准则参见 A.2)。

附录 G

(资料性附录)

确定安全完整性等级——一种定性的方法——危险事件严重程度矩阵

G.1 概述

附录 D 中描述的数值方法不适用于风险(或其频率部分)不能量化的地方。本附件描述了危险事件严重程度的矩阵方法,以确定一个 E/E/PE 安全相关系统的安全完整性等级,这是一种定性的方法,它取决于对 EUC 和 EUC 控制系统相关联的风险因素的认知。它特别适用于图 A.1 和图 A.2 中被指明的风险模型。

本附录中概述的方案假定每个安全相关系统和其他风险降低措施是独立的。

本附录并不打算成为一个最终方法的记述,而是试图说明这样的一个矩阵如何由那些对实质性的特定构成参数的详尽了解进行开发的一般原则。那些打算采用的本附录中所示的方法的人员可查阅原始资料参考。

注:危险事件矩阵的更多信息已在参考文献[4]中给出。

G.2 危险事件严重程度矩阵

以下的要求支撑着矩阵,并且每一个要求对于方法的有效性都是必要的:

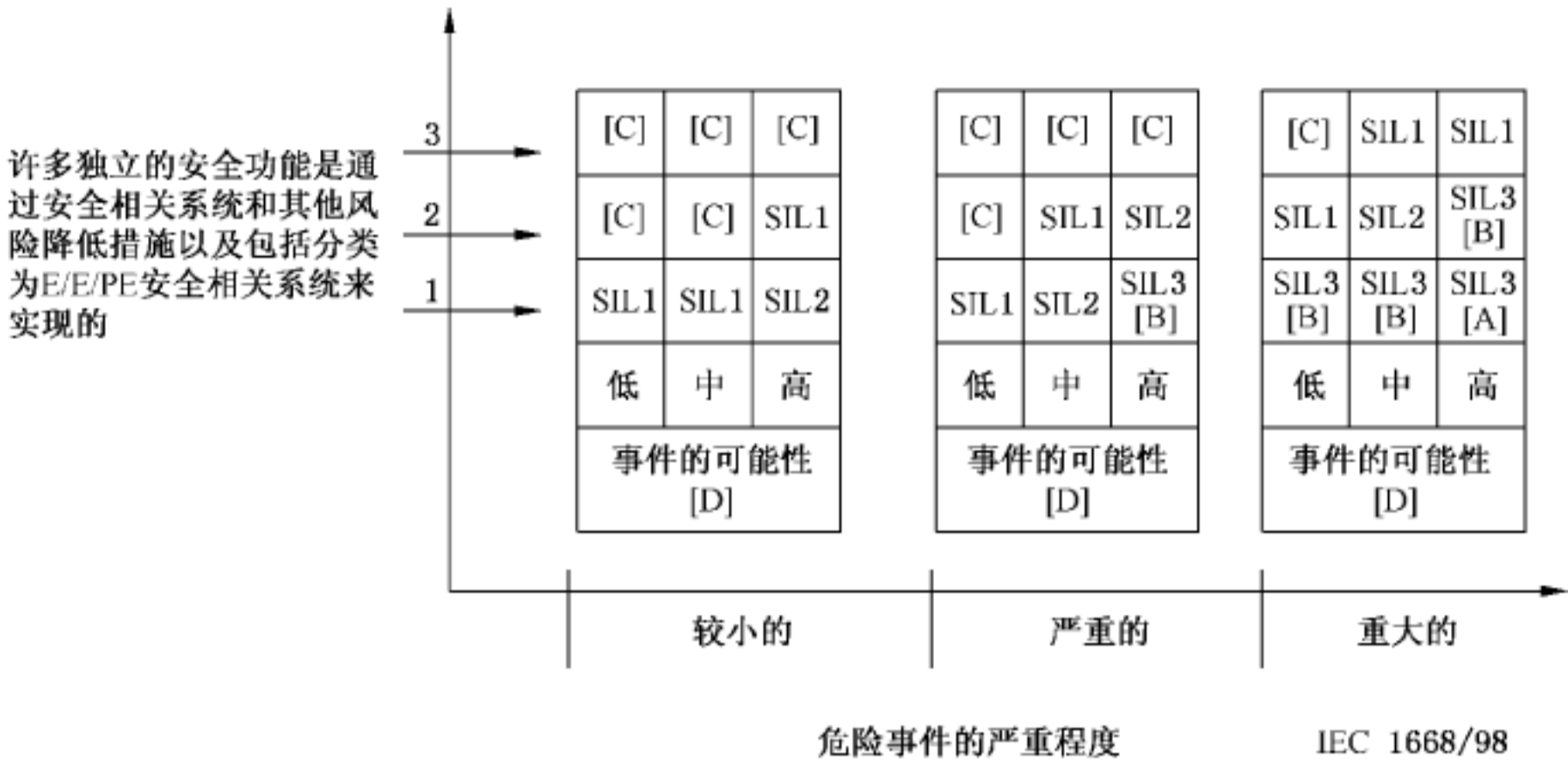
- a) E/E/PE 安全相关系统和其他风险降低措施都是独立的;
- b) 每个安全相关系统(E/E/PE 和其他技术)和其他风险降低措施都被视为保护层,它们提供归于自身的部分风险降低,如图 A.1 所示;

注 1: 只有对保护层执行定期的检验测试,此假设才是有效的。

- c) 当增加了一个保护层[见上述 b)],那么安全完整性可以实现一个数量级的改进;

注 2: 只有安全相关系统和其他风险降低措施实现了充分的独立,此假设才是有效的。

- d) 对于建立必要的安全完整性等级的方法,只使用一个 E/E/PE 安全相关系统(但这可能是结合了一个其他技术的安全相关系统和/或其他风险降低措施);
- e) 由上述考虑导出的危险事件严重程度矩阵如图 G.1 所示。应该指出的是,矩阵已被填充了示例数据来说明一般原则。对于每一个具体情况,或可类比的行业,需要开发一个类似于图 G.1 的矩阵并校准以适用于这个情况的可容忍风险准则。



- [A] 在这个风险等级,一个 SIL 3 的 E/E/PE 安全功能不能提供足够的风险降低。需要额外的风险降低措施。
- [B] 在这个风险等级,一个 SIL 3 的 E/E/PE 安全功能可能无法提供足够的风险降低。需要危险和风险分析以确定额外的风险降低措施是否必要。
- [C] 可能不需要一个独立的 E/E/PE 安全功能。
- [D] 事件的可能性是指在没有任何安全功能或其他风险降低措施时发生危险事件的可能性。
- [E] 事件可能性和独立保护层总数的定义与具体应用有关。

图 G.1 危险事件严重程度矩阵—示例(只说明一般原则)

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 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] ANSI/ISA S84:1996 Application of safety Instrumented Systems for the Process Industries
 - [5] Health and Safety Executive(UK)publication, ISBN 011 886368 1, Tolerability of risk from nuclear power stations, <www.hse.gov.uk/nuclear/tolerability.pdf>
 - [6] The Motor Industry Research Association, 1994, ISBN 09524156 0 7, Development guidelines for vehicle based software
 - [7] Health and Safety Executive(UK)publication, ISBN 0 7176 2151 0, Reducing Risks, Protecting People, <www.hse.gov.uk/risk/theory/r2p2.pdf>
 - [8] CCPS ISBN 0-8169-0811-7, Layer of Protection Analysis—Simplified Process Risk Assessment
 - [9] ISO/IEC 31010 Risk management—Risk assessment techniques
 - [10] ISO 10418:2003 Petroleum and natural gas industries—Offshore production installations—Basic surface process safety systems
 - [11] ISO/TR 14121-2 Safety of machinery—Risk assessment—Part 2: Practical guidance and examples of methods
 - [12] GB/T 16855.1—2008 机械安全 控制系统有关安全部件 第 1 部分:设计通则
 - [13] IEC 60601(all parts) Medical electrical equipment
 - [14] GB/T 20438.2 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
 - [15] GB/T 20438.3 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
 - [16] GB/T 20438.6 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
 - [17] GB/T 20438.7 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
 - [18] GB/T 21109.1 过程工业领域安全仪表系统的功能安全 第 1 部分:框架、定义、系统、硬件和软件要求
-

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—2017/IEC 61508-5:2010

*

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12月第一版

*

书号:155066·1-57737

版权专有 侵权必究



GB/T 20438.5-2017