ICS 25.040
N 10

中华人民共和国国家标准

GB/T 21109.3—2007/IEC 61511-3:2003

过程工业领域安全仪表系统的功能安全 第3部分:确定要求的安全完整性等级的指南

Functional safety—Safety instrumented systems for the process industry sector—Part 3:Guidance for the determination of the required safety integrity levels

(IEC 61511-3:2003,IDT)

2007-10-11 发布　　2007-12-01 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　术语、定义和缩略语 …… 2
3　风险和安全完整性——一般指南 …… 2
3.1　概述 …… 2
3.2　必要的风险降低 …… 2
3.3　安全仪表系统的作用 …… 3
3.4　安全完整性 …… 3
3.5　风险和安全完整性 …… 4
3.6　安全要求的分配 …… 4
3.7　安全完整性等级 …… 4
3.8　选择确定要求的安全完整性等级的方法 …… 5
附录 A(资料性附录)　ALARP 和允许风险的概念 …… 6
附录 B(资料性附录)　半定量方法 …… 9
附录 C(资料性附录)　安全层矩阵法 …… 15
附录 D(资料性附录)　确定要求的安全完整性等级——半定性方法：校正的风险图 …… 19
附录 E(资料性附录)　确定要求的安全完整性等级——定性方法：风险图 …… 26
附录 F(资料性附录)　保护层分析(LOPA) …… 30

图 1　GB/T 21109 的整体框架 …… Ⅴ
图 2　过程工厂中常见的典型风险降低方法(例如保护层模型) …… 2
图 3　风险降低：一般概念 …… 4
图 4　风险和安全完整性的概念 …… 4
图 5　安全仪表系统、非安全仪表系统预防/减轻保护层和其他保护层安全要求的分配 …… 5
图 A.1　允许风险和 ALARP …… 7
图 B.1　具有现有安全系统的压力容器 …… 10
图 B.2　容器超压的故障树 …… 12
图 B.3　具有现有安全系统时的危险事件 …… 12
图 B.4　具有冗余保护层的危险事件 …… 13
图 B.5　具有 SIL2 的 SIS 安全功能的危险事件 …… 14
图 C.1　保护层 …… 15
图 C.2　安全层矩阵示例 …… 18
图 D.1　风险图：通用型式 …… 22
图 D.2　风险图：环境破坏 …… 24
图 E.1　DIN V 19250 风险图——人员保护(见表 E.1) …… 27
图 E.2　GB/T 21109、DIN V 19250 和 VDI/VDE 2180 之间的关系 …… 29
图 F.1　保护层分析(LOPA)报告 …… 31

表 A.1 事故风险等级的示例 …… 7
表 A.2 风险等级的解释 …… 8
表 B.1 HAZOP 研究结果 …… 10
表 C.1 危险事件可能性的频率(不考虑 PL) …… 17
表 C.2 评定危险事件影响严重性等级的准则 …… 17
表 D.1 过程工业风险图参数的描述 …… 19
表 D.2 通用风险图校正示例 …… 22
表 D.3 一般环境后果 …… 24
表 E.1 与风险图有关的数据(见图 E.1) …… 28
表 F.1 从 HAZOP 导出的用于 LOPA 的数据 …… 31
表 F.2 影响事件严重性等级 …… 31
表 F.3 引发可能性 …… 32
表 F.4 保护层(预防和减轻)典型的 PFD_{avg} …… 32

前　言

GB/T 21109《过程工业领域安全仪表系统的功能安全》分为三个部分：

——第1部分：框架、定义、系统、硬件和软件要求；

——第2部分：GB/T 21109.1的应用指南；

——第3部分：确定要求的安全完整性等级的指南。

本部分为GB/T 21109的第3部分，等同采用IEC 61511-3:2003《过程工业领域安全仪表系统的功能安全　第3部分：确定要求的安全完整性等级的指南》(英文版)。为便于使用，对IEC 61511-3:2003做了下列编辑性修改：

——删除国际标准的前言，按GB/T 1.1—2000重新编写了本部分的前言；

——凡是出现“IEC 61511”之处均改为“GB/T 21109”，“IEC 61511-1”均改为“GB/T 21109.1”，“IEC 61511-2”均改为“GB/T 21109.2”，“IEC 61511-3”均改为“GB/T 21109.3”；

——凡是出现“本国际标准”之处均改为“GB/T 21109”；

——用小数点“.”代替作小数点的逗号“,”；

——根据GB/T 1.1—2000进行编辑性修改。

本部分的附录A、附录B、附录C、附录D、附录E、附录F为资料性附录。

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归口。

本部分主要起草单位：机械工业仪器仪表综合技术经济研究所、上海自动化仪表股份有限公司技术中心、北京华控技术有限责任公司、中科院沈阳自动化研究所、浙江中控技术有限公司、上海工业自动化仪表研究所、国营759厂。

本部分主要起草人：王春喜、梅恪、包伟华、王麟琨、刘丹、陈小枫、魏剑嵬、史学玲、谭平、李佳嘉、欧阳劲松、蔡廷安、马光武。

本部分为首次制定。

引　言

在过程工业(process industry sector)中,用来执行仪表安全功能的安全仪表系统已使用了多年。如要使仪表能有效地用于仪表安全功能,最重要的是该仪表应达到某些最低标准和性能水平。

GB/T 21109 阐述了过程工业安全仪表系统的应用。GB/T 21109 还要求执行一次过程危险和风险评估使之能导出安全仪表系统的规范。当考虑安全仪表系统的性能要求时,才考虑其他安全系统,从而把其他安全系统的贡献计算在内。安全仪表系统包括从传感器到最终元件之内的所有部件和子系统,它们都是执行仪表安全功能所必要的。

GB/T 21109 包含了作为应用基础的两个概念:安全生命周期和安全完整性等级。

GB/T 21109 针对基于使用电气(E)/电子(E)/可编程电子(PE)技术安全仪表系统。在逻辑解算器使用其他技术的情况下,宜使用 GB/T 21109 的基本原则。GB/T 21109 还论述了安全仪表系统的传感器和最终元件而不管它们所使用的技术。GB/T 21109 在 GB/T 20438—2006 的框架范围内专用于过程工业(见 GB/T 21109.1—2007 附录 A)。

GB/T 21109 提出了达到这些最低标准的安全生命周期活动的方案。为了使用一个合理和一致的技术策略,此方案已被采纳。

在大多数情况下,固有(inherently)安全过程设计就能很好地达到安全性。必要时,还可结合一个或一些保护系统,以便处理任何已发现的残余风险。保护系统可依靠不同的技术(化学的、机械的、液压的、气动的、电气的、电子的、可编程电子的)。任何安全策略都需要将每个单独的安全仪表系统放在其他保护系统环境下进行考虑。为促成该方案,GB/T 21109 要求:

——执行一次危险和风险评估以便确定整体安全要求;

——给安全仪表系统分配安全要求;

——应在一个适用于所有用仪表实现功能安全的方法的框架内进行工作;

——详述了适用于实现功能安全的所有方法的某些活动(如安全管理)的使用。

关于过程工业的安全仪表系统的 GB/T 21109:

——涉及从初始概念、设计、实现、运行和维护直到停用的所有安全生命周期阶段;

——能使现有的或新的国家专用的过程工业标准同本标准协调一致。

GB/T 21109 致力于在过程工业领域内导致高度一致(如基本原则、术语、信息等)。这将带来安全和经济两方面的好处。

在权限方面,在管理当局(如国家的、省的、自治区的等)已建立过程安全设计、过程安全管理或其他要求的情况下,这些要求应比本标准中定义的要求优先考虑。

本部分涉及到了危险和风险分析(H&RA)中确定要求的 SIL 范围的指南。这当中的信息用来提供一个用于实现 H&RA 的各种各样的全局方法的广泛概览。但提供的信息并未详细到足以实现这些方案中的任何一种。

在继续之前,应回顾一下 GB/T 21109.1 中提供的安全完整性等级(SIL)的概念和确定方法。本部分的附录描述了以下内容:

附录 A　提供允许风险和 ALARP 的概念的概述。

附录 B　提供一种用来确定要求的 SIL 的半定量方法的概述。

附录 C　提供一种用来确定要求的 SIL 的安全矩阵方法的概述。

附录 D　提供一种使用半定性风险图方法来确定要求的 SIL 的方法的概述。

附录 E　提供一种使用定性风险图方法来确定要求的 SIL 的方法的概述。

附录 F　提供一种使用保护层分析(LOPA)方法来选择要求的 SIL 的方法的概述。

GB/T 21109 的整体框架见图 1。

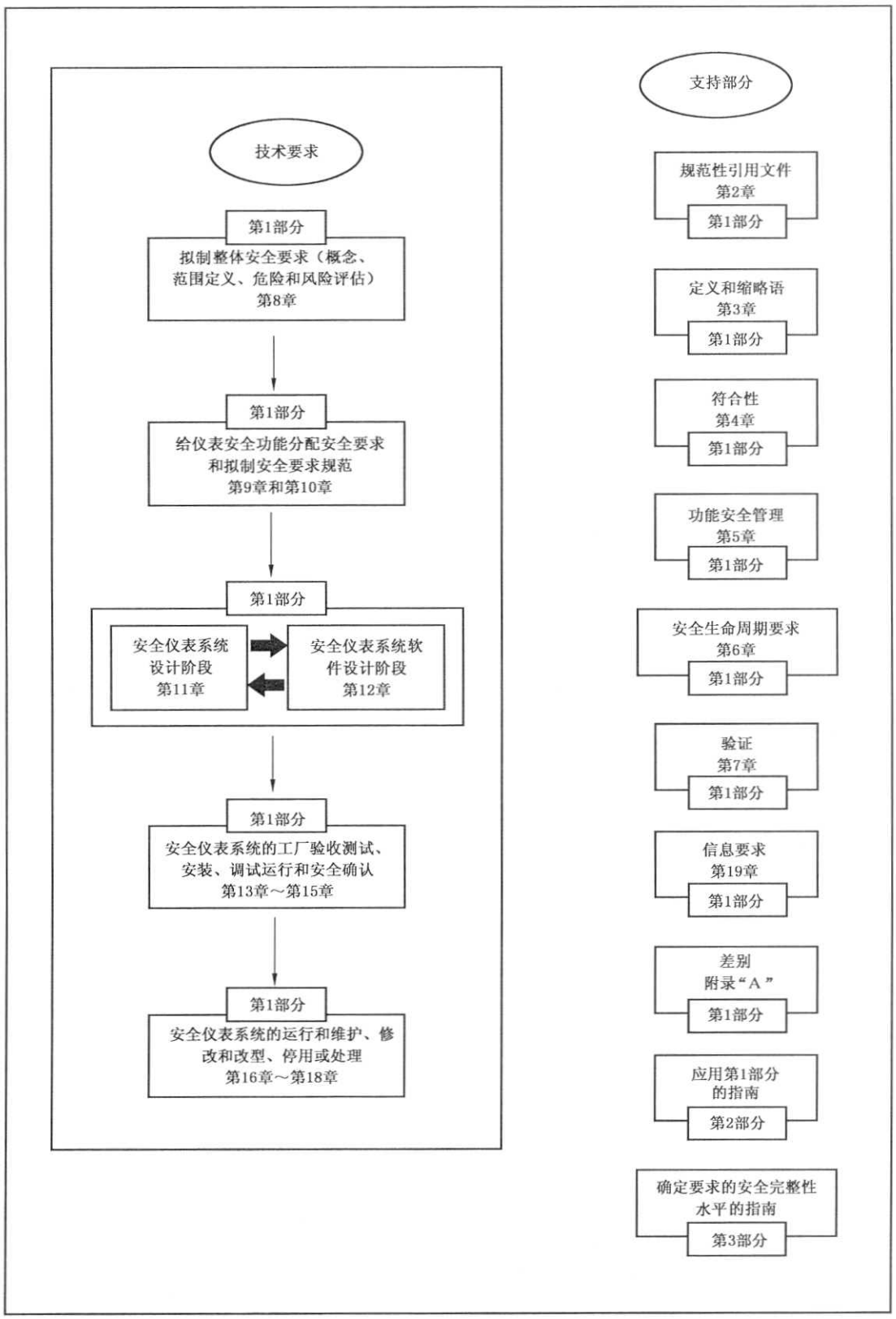


图 1　GB/T 21109 的整体框架

附录 F　提供一种使用保护层分析(LOPA)方法来选择要求的 SIL 的方法的概述。

GB/T 21109 的整体框架见图 1。

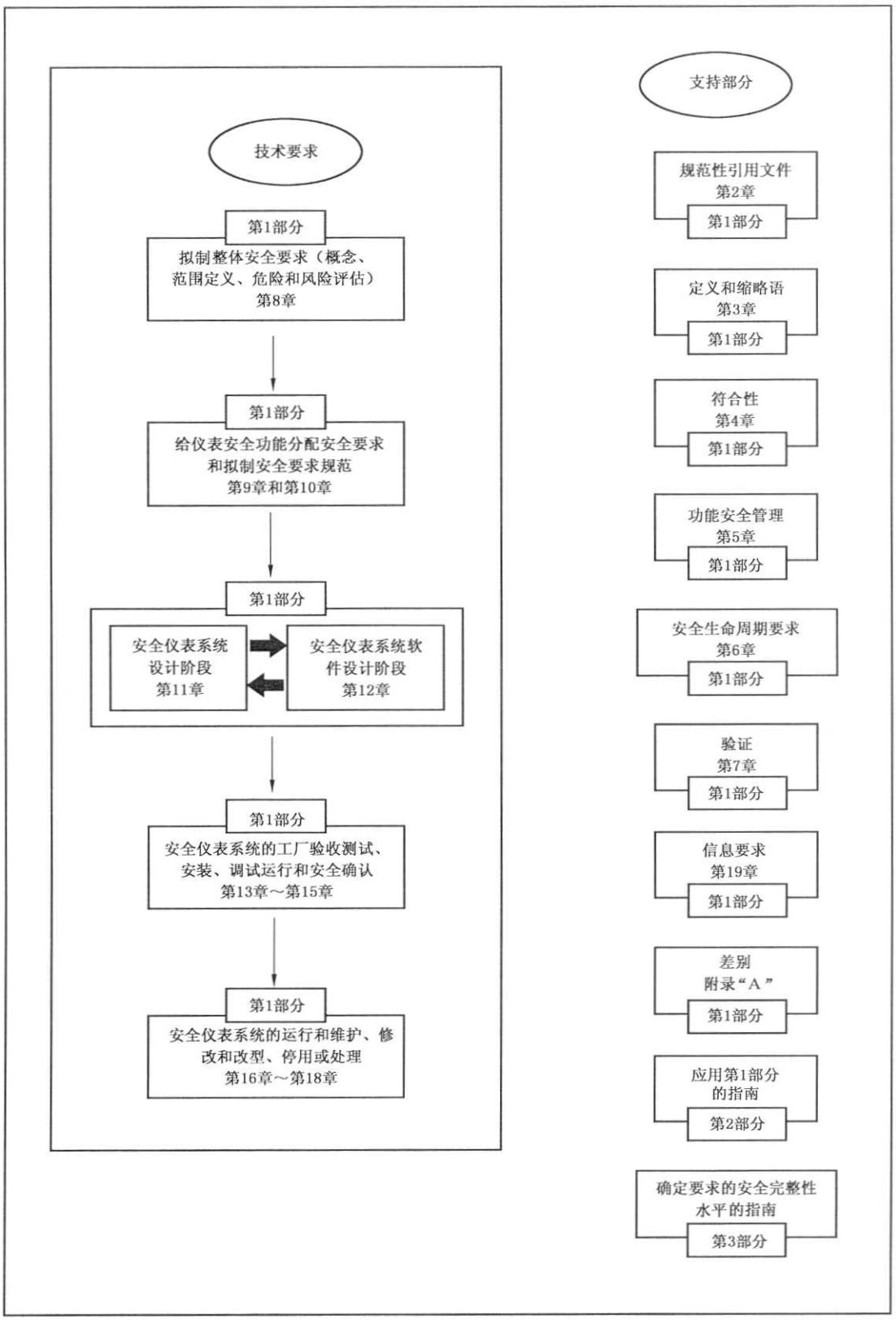


图 1　GB/T 21109 的整体框架

过程工业领域安全仪表系统的功能安全 第3部分：确定要求的安全完整性等级的指南

1 范围

本部分提供了与以下有关的信息：

——风险的基础概念、风险与安全完整性的关系，见第3章；

——允许风险的确定，见附录A；

——确定仪表安全功能的安全完整性等级的各种不同方法，见附录B、附录C、附录D、附录E和附录F。

特别是：

a) 为了保护人员、公共设施或环境，使用一个或多个仪表安全功能来达到功能安全时可使用本部分；

b) 在比如资产保护这类非安全应用中也可使用本部分；

c) 本部分说明了定义安全功能要求和每个仪表安全功能的安全完整性等级需要执行的典型危险和风险评估的方法；

d) 本部分说明了可用来确定要求的安全完整性等级的技术/措施；

e) 本部分为确立安全完整性等级提供了一个框架，但并不规定特殊应用要求的安全完整性等级；

f) 本部分不给出确定其他风险降低方法的要求的例子。

附录B、附录C、附录D、附录E和附录F说明了各种定量和定性方法，并且为了说明基础原理已对这些方法作了简化。本部分包含了这些附录以便说明这些方法的一般原理但并不提供一个权威的计算。

注：如打算使用这些附录中指出的那些方法，应查阅每个附录中引用的原始资料。

图1表示GB/T 21109的整体框架，并指出本部分在实现安全仪表系统的功能安全中所起的作用。

图2给出了风险降低方法的总览。

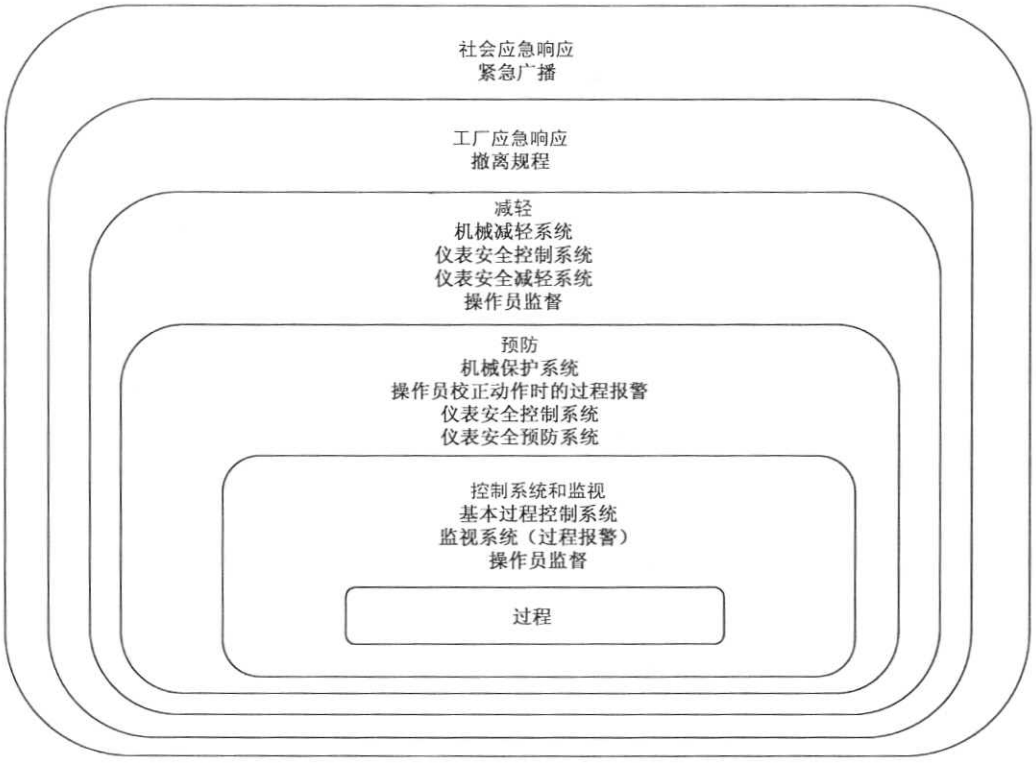


图 2 过程工厂中常见的典型风险降低方法(例如保护层模型)

2 术语、定义和缩略语

本部分使用的术语、定义和缩略语见 GB/T 21109.1—2007 的第 3 章。

3 风险和安全完整性——一般指南

3.1 概述

本章提供了有关风险和风险与安全完整性关系的基础概念的信息。此信息可为本部分中所示的多种危险和风险分析(H&RA)方法所共用。

3.2 必要的风险降低

必要的风险降低(既可以定性地[1)],也可以定量地[2)]被说明)是为满足特定情况的允许风险(过程安全目标水平)而一定要达到的风险的降低。在编写仪表安全功能(SIF)的安全要求规范(尤其是安全要求规范的安全完整性要求)时,必要的风险降低的概念十分重要。确定一个特定危险事件的允许风险(过程安全目标水平)的目的是要说明对于危险事件的频率和它的特定后果,哪些风险被认为是合理的。保护层(见图 3)被设计用来降低危险事件的频率和/或危险事件的后果。

评估允许风险的重要因素包括对暴露在危险事件中的风险的理解和看法。在获得某个特定应用的允许风险的构成时可考虑许多输入,它们包括:

——相关管理当局提供的指南;

——应用相关各方的讨论和协定;

——工业标准和指南;

1) 在确定必要的风险降低时,应确定必要的允许风险。GB/T 20438.5—2006 的附录 D 和附录 E 描述了一些定性方法,不过在必要的风险降低的示例中只是隐含了那些方法,而并未明显地作阐述。

2) 例如,导致某个特定后果的危险事件典型地可表示为每年的最大发生频率。

——工业、专家和科学建议；

——法律和法规要求：一般的和直接与特定应用有关的要求。

3.3 安全仪表系统的作用

安全仪表系统实现仪表安全功能，以达到或保持过程安全状态，即它将对必要的风险降低发挥作用来满足允许风险。例如，安全功能要求规范可说明当温度达到 X 值时，阀 Y 开启使水流入容器。

一个安全仪表系统(SIS)或多个 SIS 的组合或者其他保护层都可实现必要的风险降低。

人员也可以是一个安全功能的组成部分。例如，人员可接收过程状态信息，并根据该信息执行一个安全动作。当人员是一个安全功能的组成部分时，应考虑所有的人为因素。

仪表安全功能可在要求操作模式下或者在连续操作模式下运行。

3.4 安全完整性

安全完整性被认为由以下两个部分组成：

a) 硬件安全完整性，即在危险失效模式下与硬件随机失效有关的安全完整性部分。估算规定的硬件安全完整性等级的实现所达到的一个合理的准确度水平，因此，使用已建立的用于概率组合和考虑共同原因失效的规则，可在子系统当中分配安全要求。也许需要使用冗余结构来达到要求的硬件安全完整性。

b) 系统安全完整性，即在危险失效模式下与系统失效有关的安全完整性部分。虽然也许能估算某些系统失效产生的影响，但从设计缺陷和共同原因失效得到的失效数据意味着这些失效的分布难以预测。在某种特定情况，这增加了失效概率(如一个 SIS 的失效概率)计算的不确定性。因此，为了减小不确定性，必须对最佳技术的选择做出判断。注意，为降低硬件随机失效概率所采取的措施不一定能降低系统失效概率。比如同型硬件的冗余信道这样的技术对控制硬件随机失效十分有效，但很少用来减少系统失效。

仪表安全功能和其他任何保护层所提供的总风险降低必须保证：

——安全功能的失效频率足够低，使之能防止危险事件频率超过满足允许风险所要求的值；和/或

——安全功能把失效的后果减轻到满足允许风险所要求的程度。

图 3 说明了风险降低的一般概念。通用模型假设：

——有一个过程及其相关的一个基本过程控制系统(BPCS)；

——存在相关的人为因素；

——安全保护层特征包括：

1) 机械保护系统；
2) 安全仪表系统；
3) 机械减轻系统。

注：图 3 表示用来说明一般原理的广义风险模型。应考虑安全仪表系统和/或其他保护层实际上实现必要的风险降低所使用的特定方式，来开发特定的应用风险模型，因此得出的风险模型可能与图 3 所示不同。

图 3 和图 4 中所示的各种风险如下：

——**过程风险**：由于过程、基本过程控制系统和相关的人员因素问题而存在的特定的危险事件的风险。在确定此风险时未考虑指定的安全保护特征。

——**允许风险**(过程安全目标水平)：根据当今社会的水准，在给定的环境内能够接受的风险。

——**残余风险**：在本部分的上下文中，残余风险是在增加保护层之后发生危险事件的风险。

过程风险是与过程本身相关的风险函数，但它考虑了过程控制系统带来的风险降低。为了防止对基本过程控制系统的安全完整性的不合理声明，本部分对可做出的此类声明作了一些限制。

必要的风险降低只是为满足允许风险必须要达到的最低风险降低水平。可以用一种或多种风险降低技术的组合来实现它。图 3 表示从一个过程风险的起点达到规定的允许风险所必要的风险降低。

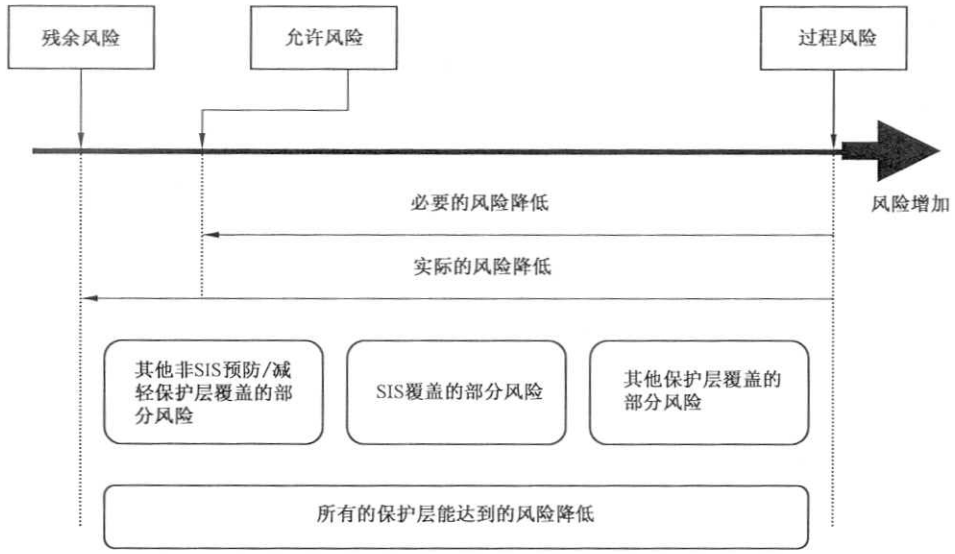


图 3 风险降低:一般概念

3.5 风险和安全完整性

充分理解风险和安全完整性之间的差别是重要的。风险是某个规定的危险事件发生的频率及其后果的一个度量。可对各种情况的风险(过程风险、允许风险、残余风险,见图 3)进行评估。允许风险涉及到社会和政治因素的考虑。安全完整性是 SIF 和其他保护层达到规定安全功能的可能性的一个度量。一旦设定了允许风险并估算了必要的风险降低,就能分配 SIS 的安全完整性要求。

注:为了优化设计以便满足各种要求,可能需要反复进行分配。

图 3 和图 4 说明了安全功能在达到必要的风险降低中所起的作用。

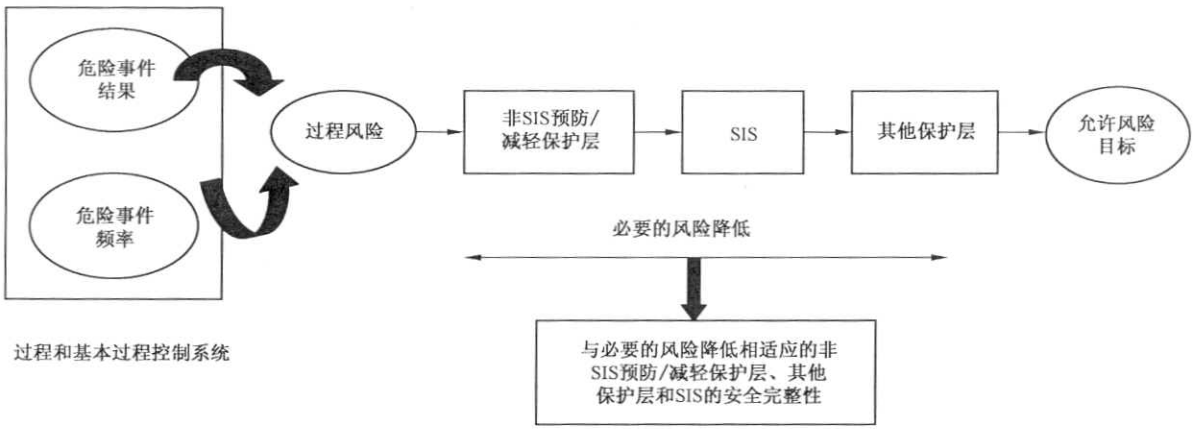


图 4 风险和安全完整性的概念

3.6 安全要求的分配

图 5 表示了安全仪表系统和其他保护层安全要求(安全功能和安全完整性要求)的分配。GB/T 21109.1—2007 第 9 章给出了对安全要求分配阶段的要求。

给安全仪表系统、其他技术安全相关系统和外部风险降低设施分配安全完整性要求所使用的方法主要取决于必要的风险降低是以一种数值方式还是以一种定性方式被清晰地规定。这些方式分别称为半定量、半定性或定性方法(见附录 B、附录 C、附录 D、附录 E 和附录 F)。

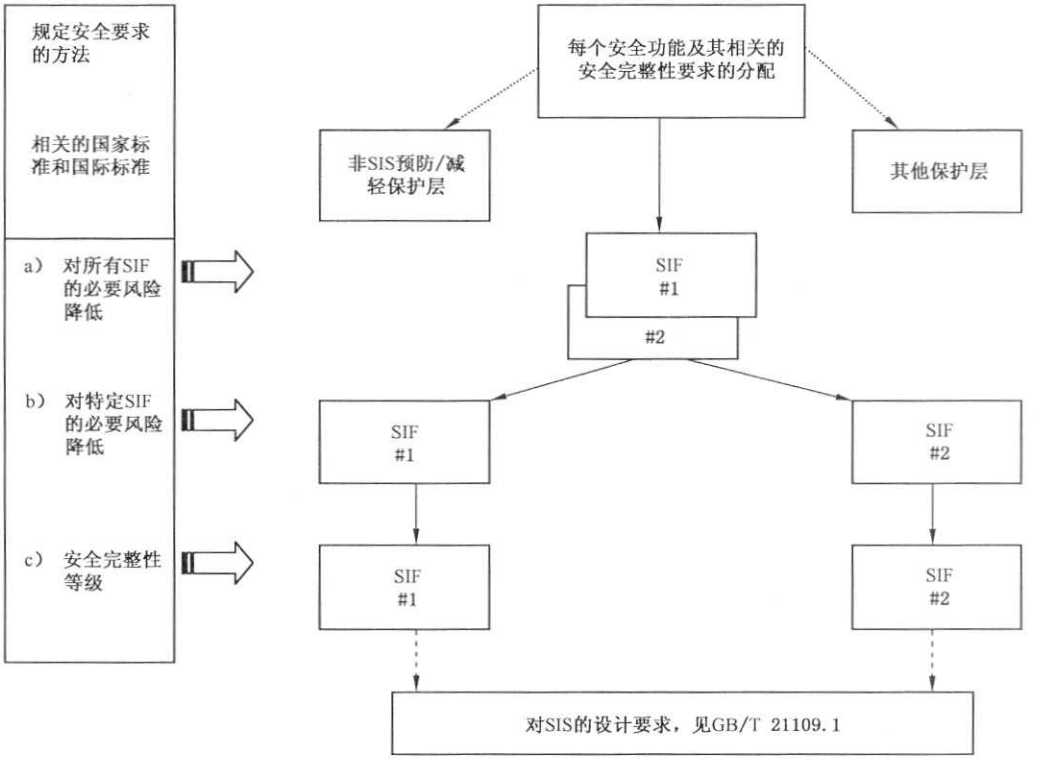
3.7 安全完整性等级

本部分规定了 4 种安全完整性等级,安全完整性等级 4 是最高等级,安全完整性等级 1 是最低

等级。

GB/T 21109.1—2007 的表 3 和表 4 规定了 4 种安全完整性等级的安全完整性等级目标失效量。规定了两个参数，一个用于工作在要求操作模式下的 SIS，另一个用于工作在连续操作模式下的 SIS。

注：对于在要求操作模式下工作的 SIS 来说，关心的安全完整性度量是在要求时执行 SIS 设计的功能的平均失效概率。而对在连续操作模式下工作的 SIS 来说，关心的安全完整性度量是每小时的危险失效频率，见 GB/T 21109.1—2007 的 3.2.43。



注：在分配之前，安全完整性要求与各个安全功能相关联（见 GB/T 21109.1—2007 第 9 章）。

图 5　安全仪表系统、非安全仪表系统预防/减轻保护层和其他保护层安全要求的分配

3.8　选择确定要求的安全完整性等级的方法

建立一个特殊应用所要求的安全完整性等级的方法有很多。附录 B～附录 F 提供了许多有关所使用方法的信息。为特殊应用所选择的方法取决于许多因素，其中包括：

——应用的复杂程度；

——来自管理当局的指南；

——风险特性和要求的风险降低；

——可承担工作人员的经验和技能。

——关于风险的参数的可用信息。

在一些应用中，可以使用不只一种方法。首先，使用定性方法确定所有 SIF 要求的 SIL。然后对于那些用该方法分配了 SIL 3 或 SIL 4 的 SIF，应考虑再使用定量方法进一步细化，以便更精确地理解所要求的安全完整性。

附 录 A
（资料性附录）
ALARP 和允许风险的概念

A.1 概述

本附录考虑可在确定允许风险和安全完整性等级过程中使用的一个特殊原则(ALARP)。ALARP是一个可在确定安全完整性等级过程中使用的概念，而不是一个确定安全完整性等级的方法。如果意图使用本附录中所示原则，应查看以下参考资料：

Reducing Risk, Protecting People, HSE, London, 2001 (ISBN 0 7176 2151 0)

Assessment Principles for offshore safety cases, HSE, London, 1998 (ref. HSG 181) (ISBN 0 7176 1238 4)

Safety assessment principles for nuclear plants, HSE, London, 1992 (ISBN 0 11 882043 5)

Tolerability of risks from nuclear power stations, HMSO, London, 1992 (ISBN 0 11 886368 1)

The use of computers in safety-critical applications, Health and Safety Commission, London, 1998 (ISBN 0 7176 1620 7)。

A.2 ALARP 模型

A.2.1 引言

3.2 条描述了在管理工业风险中使用的主要准则，并指出了确定下列情况所涉及的活动：

a) 风险大到完全不能接受；或者

b) 风险小到或者已经被减小到无关紧要的程度；或者

c) 风险处于上面 a)和 b)所规定的两种状态之间并从接受此风险可得到的利益和任何进一步降低所花费的成本考虑，此风险已被降低到最低可行的水平。

关于 c)项，ALARP 原则推荐应把风险降低到“只要合理可行”或者降低到“ALARP”的某个水平。如果一个风险位于两种极端情况(即不可接受的区域和广泛可接受的区域)之间并已使用了 ALARP 原则，则所得到的风险就是该特殊应用的可允许风险。根据此方法，一个风险被认为应处于被称为“不可接受的”、“允许的”或“广泛可接受的”三个区域中的某一个之中(见图 A.1)。

在某个水平之上的风险被看作是不可接受的。在任何正常情况下，此风险都被认为是不合理的。如果存在这样的风险，则应把它降低到“允许的”或者“广泛可接受的”区域内，或者必须排除相关的危险。

低于上述水平的风险，如果该风险已经降低到当达到进一步风险降低所花费的成本超过所获得的好处，并且已经采用了被普遍接受的用于风险控制的标准时，则被认为是“允许的”。风险越高，为了降低它所花费的(成本)就越多。按照这种方式已被降低的风险可认为它已被降低到一个“ALARP”的水平。

低于允许区的风险水平被认为是无关紧要的，管理者不必请求进一步改进。这个区域是广泛可接受的区域，此区域中的风险同我们每天经历的的风险相比较小。在广泛可接受的区域中不需要细致工作来证明 ALARP，但有必要保持警惕以确保风险维持在这一水平。

当采用定性或定量风险目标时，可使用 ALARP 概念。A.2.2 描述了一种用于定量风险目标的方法。(附录 C 描述了一种确定特定危险的必要风险降低的半定量方法，附录 D 和附录 E 则描述了定性方法。在决策时，所示方法可结合 ALARP 的概念。)

当使用 ALARP 原则时，应注意确保所有的假设都要合理并被文档化。

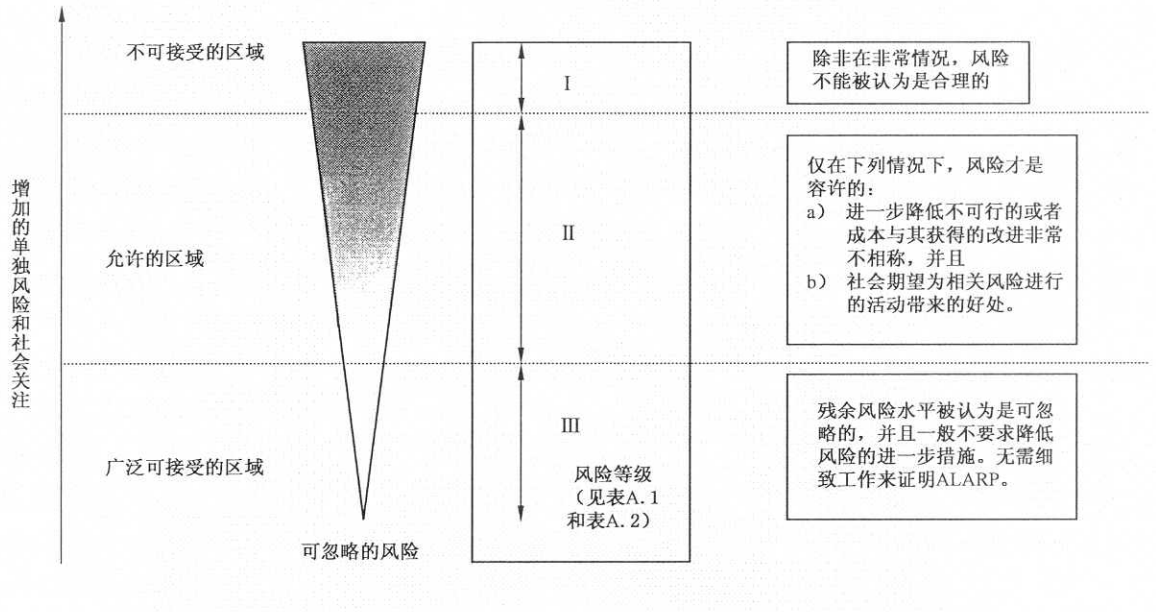


图 A.1 允许风险和 ALARP

A.2.2 允许风险目标

为了应用 ALARP 原则，有必要根据事故发生的概率和后果来定义图 A.1 中的三个区域。这个定义应通过利益相关的各方（如安全管理当局、产生风险和承受风险的那些人）之间的讨论和达成一致意见来进行。

在考虑 ALARP 概念时，通过风险等级可进行后果与允许频率之间的搭配。表 A.1 是显示对应于许多后果和频率的 3 种风险等级（Ⅰ、Ⅱ、Ⅲ）的一个示例。表 A.2 使用 ALARP 概念对每个风险等级进行解释。即基于图 A.1 对 4 个风险等级的每一个等级进行描述。这些风险等级定义中的风险是已经实施风险降低措施后显现的风险。关于图 A.1，风险等级如下：

——风险等级Ⅰ处于不可接受的区域中；

——风险等级Ⅱ处于 ALARP 区域；

——风险等级Ⅲ处于广泛可接受的区域中。

对每个特殊情况或者工业子部门，应考虑广泛的社会、政治和经济因素，编制一个类似于表 A.1 的表。每种后果都应匹配一个概率并且在表中填写风险等级。例如，表 A.1 中可能有一个事件的发生频率大于 10 次/年。其致命后果是导致一人死亡，和/或多人严重伤害或严重职业病。

在确定允许风险目标后，就能够通过使用例如附录 C～附录 F 中描绘的一种方法来确定仪表安全功能的安全完整性等级。

表 A.1 事故风险等级的示例

概率	风险等级			
	灾难性的后果	致命的后果	微小的后果	可忽略的后果
极可能	Ⅰ	Ⅰ	Ⅰ	Ⅱ
很可能	Ⅰ	Ⅰ	Ⅱ	Ⅱ
可能	Ⅰ	Ⅱ	Ⅱ	Ⅱ
极小可能	Ⅱ	Ⅱ	Ⅱ	Ⅲ
不太可能	Ⅱ	Ⅲ	Ⅲ	Ⅲ
难以置信	Ⅱ	Ⅲ	Ⅲ	Ⅲ

表 A.1(续)

概率	风险等级			
	灾难性的后果	致命的后果	微小的后果	可忽略的后果
注 1：风险等级Ⅰ～风险等级Ⅲ的解释见表 A.2。 注 2：用风险等级Ⅰ、风险等级Ⅱ和风险等级Ⅲ进行本表的实际填写与应用有关，并还取决于很可能、可能等的实际概率。因此，应将本表看作是说明此类表如何被填写的一个示例，而不作为对将来应用的规范。				

表 A.2 风险等级的解释

风险等级	解　　释
Ⅰ级	不允许风险
Ⅱ级	不期望的风险，仅当风险降低不可行或成本与取得的改善极不相称时才允许
Ⅲ级	可忽略的风险
注：风险等级和安全完整性等级(SIL)无关。SIL 由与一个特定仪表安全功能相关的风险降低确定，见附录 B～附录 F。	

附 录 B
（资料性附录）
半定量方法

B.1 概述

本附录描述了当采用一种半定量方法时怎样确定安全完整性等级。半定量方法在使用数字方式规定允许风险时有显著的价值（例如一个特定后果的事件发生频率不大于1次/100年）。

本附录并不作为一个权威性计算方法，仅用于说明一般原则。它基于下面参考中更详细描述的方法：

CONTINI，S.，Benchmark Exercise on Major Hazard Analysis，Commission of European Communities，1992。

B.2 与GB/T 21109.1的符合性

本附录的总体目标是通过描述一个规程来确定所要求的仪表安全功能，并确定这些功能的SIL。需要遵循的基本步骤如下：

1） 确立过程的安全目标（允许风险）；

2） 执行一次危险和风险分析以评价现有的风险；

3） 确定所需的安全功能；

4） 将安全功能分配给保护层；

注：各保护层彼此独立。

5） 确定是否要求一个SIF；

6） 确定SIF所需的SIL。

第1步确立过程的安全目标。第2步关注过程的风险分析。第3步则从风险分析推出要求哪些安全功能以及为满足安全目标需要哪些风险降低。当在第4步中把这些安全功能分配给保护层之后，是否要求一个仪表安全功能（第5步）以及需要满足哪一级SIL（第6步）也就变得显而易见了。

本附录建议使用一种半定量的风险评估技术以满足GB/T 21109的目标。通过一个简单的示例来说明该技术。

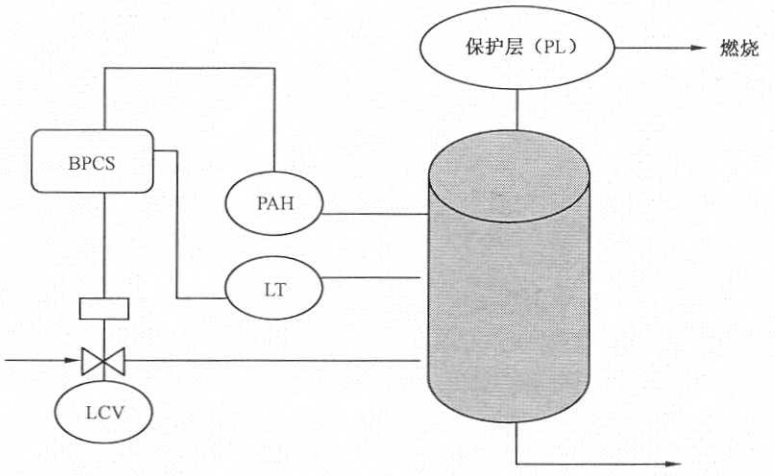
B.3 示例

内装挥发性易燃液体的压力容器的过程及相关仪表一起考虑（见图B.1）。过程控制的处理通过一个基本过程控制系统（BPCS）实现，BPCS监视来自液位变送器的信号并控制阀的操作。可用的工程化系统是a）一个独立压力变送器，用于启动高压报警并警告操作员采取适当动作以停止物质流入；及b）一个非仪器保护层，在操作员未响应的情况下，用于处理与容器高压相关的危险。保护层释放的气体用管道引到一个喷射箱中，喷射箱再把气体泄放到一个燃烧系统。在本例中假设燃烧系统经适当许可并且正确设计、安装及操作，因此本例中不考虑燃烧系统的潜在失效。

注：工程化系统指的是所有可用于响应一个过程要求的系统，包括其他自动保护层和操作人员。

B.3.1 过程安全目标水平

成功管理工业风险的一个基本要求是简明扼要和清楚地定义所期望的过程安全目标水平（允许风险）。它可以通过使用国家和国际标准、法规、公司政策以及有关各方如社团、当地司法部门和有良好的工程实践支持的保险公司的投入进行定义。过程安全目标水平专用于一个过程、一个公司或者一个行业。因此，不应将其一般化，除非现有法规和标准提供这种一般化的支持。在说明示例中，根据释放到环境中的预计后果，假设过程安全目标设定为平均释放率小于每年10^{-4}。



图中：

PL　附加的减轻用保护层(即堤堰、泄压装置、限制区、贮罐)

PAH　压力高报警

LT　液位变送器

LCV　液位控制阀

BPCS　基本过程控制系统

图 B.1　具有现有安全系统的压力容器

B.3.2　危险分析

应对过程进行一次危险分析以确定危险、潜在的过程偏差及其起因、可用的工程化系统、引发事件以及可能发生的潜在危险事件(意外事故)。这可以通过使用以下几种定性技术实现：

——安全复审；

——检验表；

——假设分析；

——HAZOP 研究；

——失效模式和影响分析；

——因果分析。

被广泛应用的一种这样的技术是危险和可操作性(HAZOP 研究)分析。危险和可操作性分析(或研究)可确定并评估过程工厂中的危险，以及可能损害达到设计产量能力的非危险可操作性问题。

第 2 步就是对图 B.1 所示示例执行一次 HAZOP 研究。这种 HAZOP 研究分析的目标是评估把物质释放到环境中的潜在危险事件。表 B.1 展示了一个简化表来说明 HAZOP 的结果。

HAZOP 研究的结果确认了一个超压工况可能导致易燃物质向环境的一次释放。这是一个引发事件，根据可用的工程化系统的响应，它有可能导致一个危险事件。当对过程进行一次全面的 HAZOP 分析时，能导致向环境释放物质的其他引发事件还包括过程设备的泄漏、管道钻孔完全破裂和外部事件如火灾。对于本说明示例，应检查过压工况。

表 B.1　HAZOP 研究结果

项	偏差	原因	后果	安全措施	动作
容器	高液位	BPCS 失效	高压	操作员	—
—	高压	1)　高液位 2)　外部火灾	释放到环境中	1)　报警、操作员、保护层 2)　消防(deluge)系统	评价向环境释放的工况
—	低/无流量	BPCS 失效	没有关心的后果	—	—
—	反向流	—	没有关心的后果	—	—

B.3.3 半定量风险分析技术

过程风险的一个评估是通过对与潜在过程意外事故或危险事件相关的风险进行确定和量化来完成的。其结果可用来确定必要的安全功能及其相关的 SIL，从而把过程风险降低到一个可接受的水平。在下面的主要步骤中可以区别出使用半定量技术的过程风险评估。前 4 个步骤可在 HAZOP 研究过程中执行。

1) 确定过程危险；

2) 确定安全层的组成；

注 1：安全层由可用于保护一个过程的所有安全系统组成，它包括 SIS、其他技术的安全相关系统、外部风险降低设施和操作员响应。

注 2：使用第 2 步是因为它是例子中给出的一个现有过程。

3) 确定引发事件；

4) 为每个引发事件编写危险事件情景；

5) 通过使用历史数据或建模技术(故障树分析、Markov 建模)，确定引发事件的发生频率及现有安全系统的可靠性；

6) 量化重大危险事件的发生频率；

7) 评估所有重大危险事件的后果；

8) 将结果(一个意外事故的后果和频率)集成到与每个危险事件相关的风险。

关心的重大结果是：

——对与过程相关的危险和风险的一个较好和更详细的了解；

——过程风险的了解；

——现有安全系统对整体风险降低的贡献；

——把过程风险降低到一个可接受的水平所需的每个安全功能的识别；

——估计的过程风险同目标风险的比较。

半定量技术是资源密集型方法，它能提供定性方法所不具有的好处。此技术在很大程度上取决于小组识别危险的专业技术，提供一种明确方法来处理其他技术的现有安全系统，使用一个框架来文档化会导致上述产出的所有活动，并提供一个生命周期管理系统。

对于说明示例而言，通过 HAZOP 研究确认的一个引发事件就是超压，它有向环境释放物质的潜在可能。应当注意，本子条中使用的方法是对危险事件发生频率进行定量估算和对后果进行定性评估的联合使用。这种方法被用来说明确定危险事件和仪表安全功能所应遵循的系统规程。

B.3.4 现有过程的风险分析

下一个步骤是识别对引发事件的发展有贡献的因素。图 B.2 中所示的一个简单的故障树表示了在容器中对超压工况的发展有贡献的一些事件。顶端的事件，即容器超压，是由于基本过程控制系统(BPCS)失效或者外部火灾引起的(见表 B.1)。显示故障树是为了突出 BPCS 失效对过程的影响。BPCS 并不执行任何安全功能，但其失效可促使在要求模式下对 SIS 操作的增加。因此，可靠的 BPCS 可产生对 SIS 操作较小的要求。故障树可以被量化，对此例而言，假设一年内超压工况的频率在 10^{-1} 数量级。

一旦确立了引发事件的发生频率，就可使用事件树分析为安全系统对异常工况响应的成功或失效建模。安全系统性能的可靠性数据可从现场数据、公布的数据库或使用可靠性建模技术的预测获得。对本例而言，可靠性数据曾被假设，并且不应被看作代表公布的和/或预测的系统性能。图 B.2 显示了在过压工况下可能发展成潜在的释放场景。事故建模的结果是：a)每个事故序列的发生频率；和 b)关于易燃物质释放的定性后果。在图 B.3 中，确认了 5 种危险事件，每种事件有其发生频率和潜在发生的后果。事故情景 1 不发生释放，是所设计的过程条件。此外，危险事件 2 和 4 要释放易燃物质到燃烧系统，也被认为是所设计的过程条件。其余的情景即 3 和 5，其发生频率在每年 $9\times10^{-4}\sim1\times10^{-3}$ 数量

级范围之间，并将向环境释放物质。

注：假设图 B.3 中的每个事件是独立的。此外，所示数据只是近似值；因此，所有事故的频率之和接近引发事件的频率(0.1/年)。

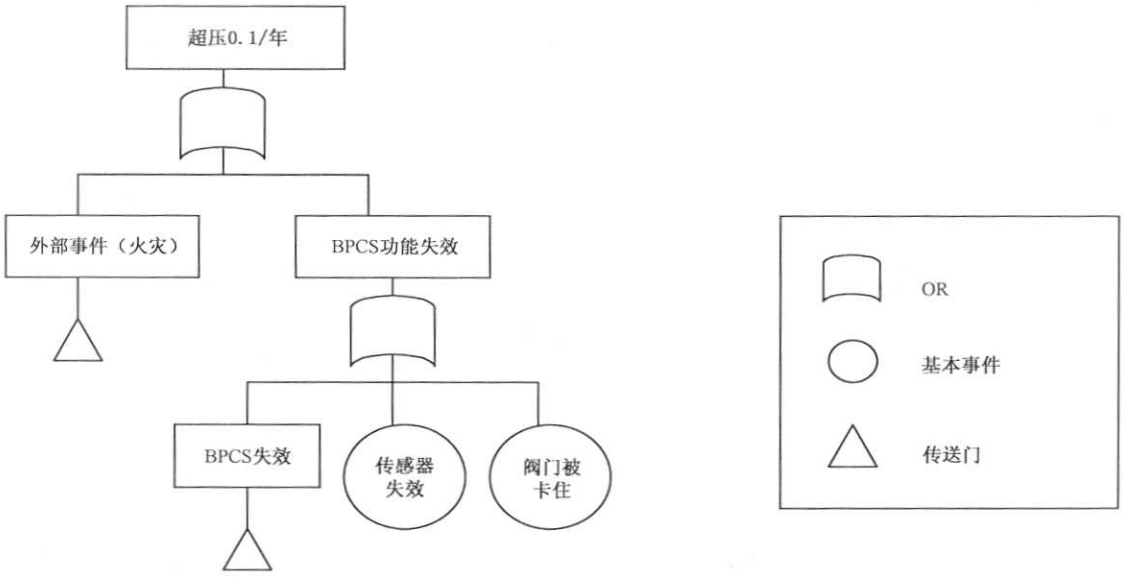


图 B.2　容器超压的故障树

应注意，此分析并未考虑高压报警和 BPCS 液位传感器失效的共同原因失效的可能性。这种共同原因失效可能导致报警系统在要求时失效概率的显著增大并因此造成整体风险。进一步信息参见“A process industry view of IEC 61508”，Dr A. G. King，IEE Computing and Control Engineering Journal，February 2000，Institution of Electrical Engineers，London，2000。

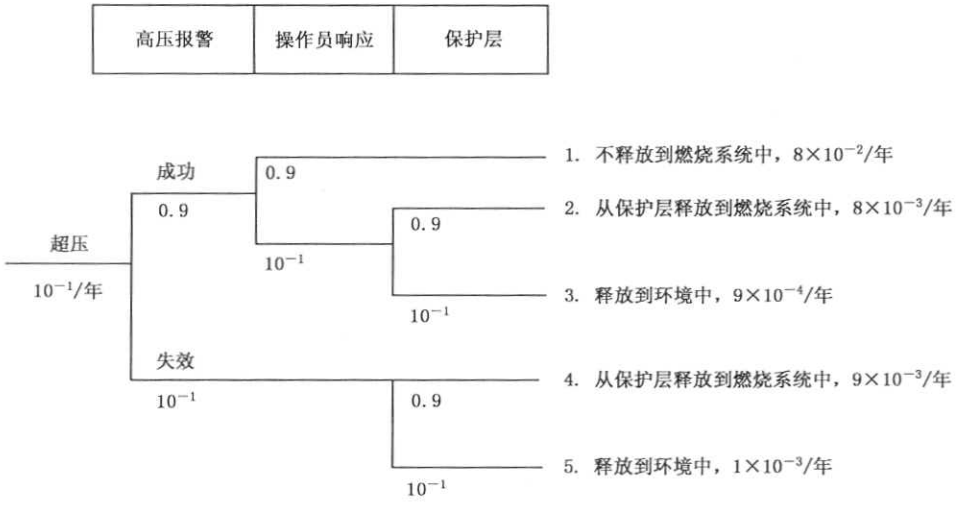


图 B.3　具有现有安全系统时的危险事件

B.3.5　不满足安全目标水平的事件

如前所述，工厂特定指南确立的安全目标水平为：向环境释放物质的事故发生频率不应大于每年 10^{-4}。假设在图 B.3 中给出的危险事件发生频率和后果数据，有必要把事故 3 和 5 的风险降低到安全目标水平以下。

B.3.6　使用其他保护层降低风险

在确立在一个 SIS 中实现一个仪表安全功能的需要之前，应考虑其他技术的保护层。为了说明此

规程，假设引入一个附加的完全独立的保护层以扩大现有的安全系统。图 B.4 示出了具有新保护层的过程。应用事件树分析来导出所有潜在的危险事件。从图 B.4 可看到，在给定的相同超压条件下，可能发生 7 种释放事故。

检查图 B.4 中被建模的危险事件的发生频率表明，因为危险事件 4 和 7 将向环境释放物质并且仍然不低于安全目标水平，所以容器的安全目标水平未被满足。事实上，向环境释放物质的总频率为每年 1.9×10^{-4}。此时应对使用外部风险降低设施的可行性进行评估。如果安全目标是把由于向环境释放物质而产生的风险降到最小，那么可以设想，像堰(堤)这样的外部风险降低设施并不是一种降低风险的可行替代方案。既然没有其他非 SIS 保护能满足安全目标水平，因此，就要求在 SIS 中实现一个仪表安全功能来防止超压和易燃物质的释放。

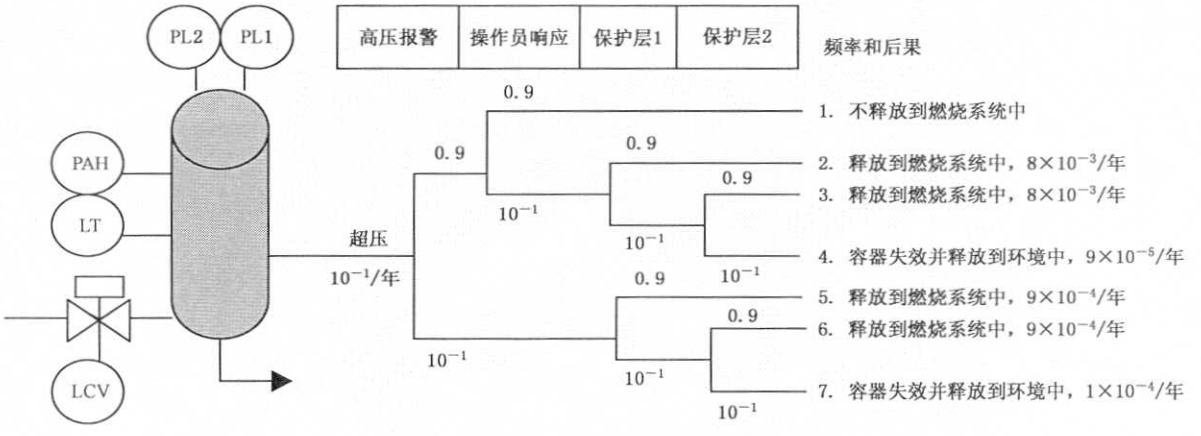


图 B.4　具有冗余保护层的危险事件

B.3.7　使用仪表安全功能降低风险

使用其他技术的保护层或外部风险降低设施不能达到安全目标。释放情景 7 仍然在安全目标内。事实上，从图 B.4 可看出向环境释放物质的总频率为每年 1.9×10^{-4}(情景 4 和情景 7 的频率之和)。为了降低释放到大气的总频率，要求在 SIS 中实现一个新的 SIL 2 仪表安全功能以满足安全目标水平。新的仪表安全功能见图 B.5。此时没有必要对仪表安全功能进行详细设计。一般的 SIF 设计构思就足够了。这一步的目的是确定一个 SIL 2 的 SIF 能否提供所要求的风险降低并使之能达到安全目标水平。在达到安全目标水平之后才进行 SIF 的详细设计。例如，新的仪表安全功能可在 1oo2 组态中使用双重的、安全专用的压力传感器，把信号发送给一个逻辑解算器。逻辑解算器的输出可控制一个附加的停机阀。

注：1oo2 意味着无论哪个压力传感器都能发送一个信号来停止过程。

新的 SIL 2 仪表安全功能被用来将因超压导致压力容器释放的频率降到最小。图 B.5 表示了新的安全层并提供所有潜在的事故情景。正如此图所示，如果对仪表安全功能的评估可同 SIL 2 要求一致，该容器的任何释放频率都能降低到不大于每年 10^{-4}，并能满足安全目标水平。向环境释放的总频率(情景 4 和 7 的频率之和)已降低到每年 1.9×10^{-5}，低于每年 10^{-4} 的安全目标。

应注意，此事件树分析未考虑高压报警和 SIL 仪表安全功能的共同原因失效的可能性。并且，两个保护布置之间以及同 BPCS 液位传感器失效之间也存在潜在的共同原因失效。

这些共同原因失效可导致保护功能在要求时的失效概率显著增加，并因此使整体风险明显增大。进一步信息可参考“A process industry view of IEC 61508”，Dr A. G. King，IEE Computing and Control Engineering Journal，February 2000，Institution of Electrical Engineers，London，2000。

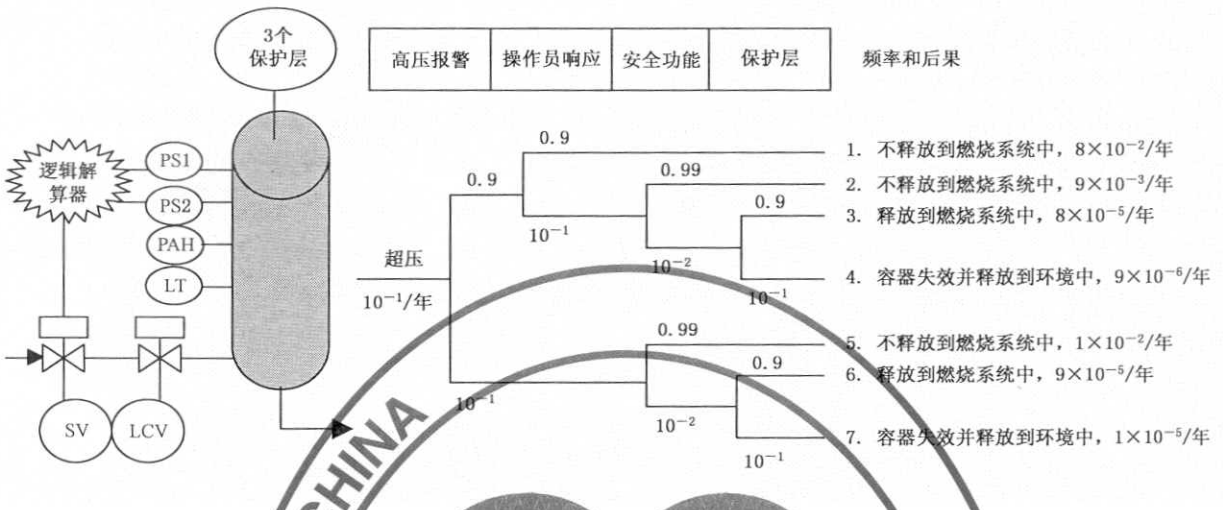


图 B.5 具有 SIL 2 的 SIS 安全功能的危险事件

附 录 C
（资料性附录）
安全层矩阵法

C.1 引言

在每个过程中，风险降低应从过程设计的最基本元素开始：过程本身的选择、现场选址、有关危险品库存量和工厂布局的决策。降低运行风险的过程设计决策有：库存危险化学品数量尽可能少；管道和热交换系统的安装，物理上应能防止可发生反应的化学物品无意或疏忽导致的混合；选择能耐最高可能的过程压力的厚壁压力容器；选择最高工作温度低于过程化学物的分解温度的加热介质。上述通过仔细选择过程设计和运行参数来降低风险是安全过程设计中的一个关键步骤。建议进一步寻求在过程开发活动中消除危险和实施固有的安全设计习惯作法的方法。遗憾的是，即使把这种设计原理发挥到了最完美的程度，依然存在潜在的危险并且仍需使用附加的保护措施。

在过程工业中，为了保护一个过程需使用多个保护层，如图 C.1 所示。图中每个保护层都由设备和/或管理措施组成，与其他保护层协同行使控制和/或降低过程风险的功能。

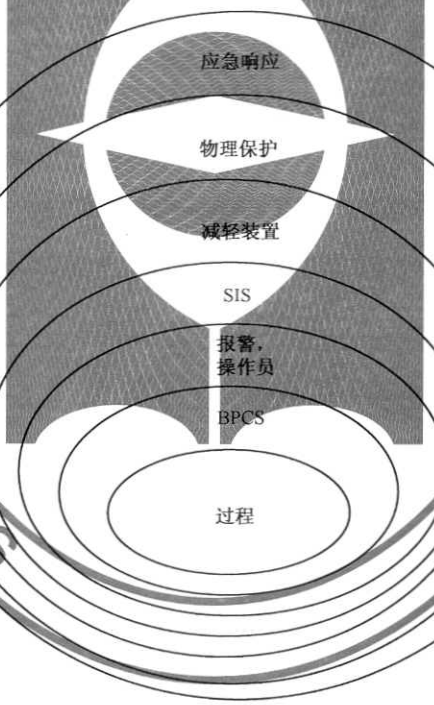


图 C.1 保护层

保护层的概念基于 3 个基本概念：

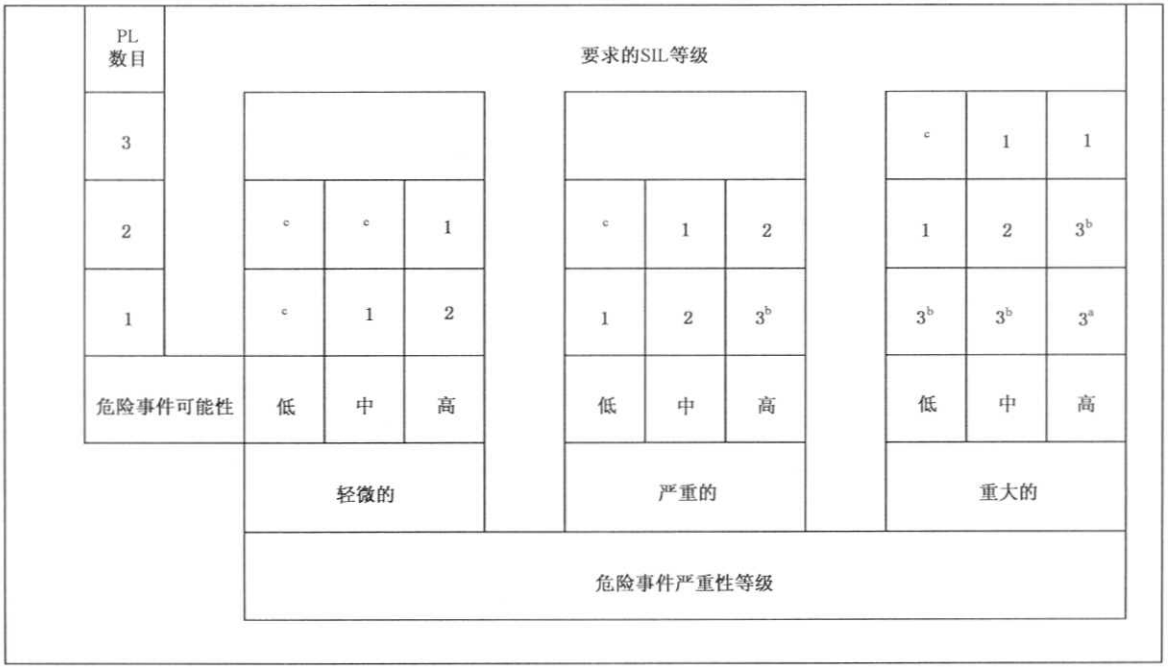
1) 一个保护层由一组设备和/或管理措施组成，它同其他保护层协同行使控制或减轻过程风险的功能；

2) 一个保护层(PL)满足下列准则：

——至少可把已确定的风险降低 10 倍；

——应具有以下重要特性：

- 专一性——PL 被设计用来防止或减轻一个潜在的危险事件的后果。由于多种原因都可能导致同一危险事件，因此多个事件情景都可由一个 PL 来启动动作。



图中：

a 一个3级的仪表安全功能并不能给该风险等级提供足够的风险降低。为了降低风险，需要附加修改(见d)。

b 一个3级的仪表安全功能并不能给该风险等级提供足够的风险降低。需要附加复审(见d)。

c 有可能不需要独立的SIS保护层。

d 此方法不适合SIL 4的情况。

图 C.2 安全层矩阵示例

PL的总数：包括用于保护过程的所有PL，其中包括被归类为SIS的PL。

危险事件的可能性：不使用任何PL时发生危险事件的可能性。见本附录的表C.1。

危险事件的严重性：与危险事件相关的影响。见本附录的表C.2。

C.5 一般规程

1) 确立过程安全目标等级；
2) 实施一次危险识别(例如HAZOP研究)以识别所有关心的危险事件；
3) 根据公司特定的方针和数据，确立危险事件模式并估计危险事件的可能性；
4) 根据公司特定的方针确立危险事件的严重性等级；
5) 识别现有的PL。对每个PL估计危险事件的可能性的降低应为10倍；
6) 通过残余风险同安全目标等级的比较，识别是否需要一个附加的SIS保护层；
7) 从图C.2确定SIL。

注：用户应评估保护层之间的相关性的可能等级，并使危险事件的发生降到最小。

附 录 D
（资料性附录）
确定要求的安全完整性等级——半定性方法：校正的风险图

D.1 引言

本附录以 GB/T 20438.5—2006 的 D.4 中描述的风险图实现的通用模式为基础。本附录做了调整以更适合于过程工业的需要。

本附录描述了用于确定仪表安全功能的安全完整性等级的校正的风险图方法。它是一种半定性方法，这种方法可通过与过程和基本过程控制系统有关的风险因素的知识，来确定一个仪表安全功能的安全完整性等级。

此方法使用了许多参数，这些参数共同描述了安全仪表系统失效或不可用时的危险状况的性质。从每 4 个一组中选择一个参数，然后把选择的这些参数组合起来决定分配给仪表安全功能的安全完整性等级。这些参数：

——允许对风险进行分级评估；和

——表示关键的风险评估因素。

在后果包括严重的环境破坏或者资产损失的场合，风险图方法还能确定风险降低的要求。本附录的目的是提供上述问题的指南。

本附录从保护人员免于危险开始。它提出了把 GB/T 20438.5—2006 的图 D.1 的通用风险图应用到过程工业的一种可能性。最后，给出了风险图在环境保护和资产保护中的应用。

D.2 风险图综合法

风险被定义成发生伤害的概率和该伤害的严重程度的组合（见 GB/T 21109.1—2007 的第 3 章）。典型地，在过程领域中，风险是以下 4 个参数的函数：

——危险状况的后果（C）；

——占用率（暴露区域被占用的概率）（F）；

——避免风险状况的概率（P）；

——要求率（在所考虑的仪表安全功能不存在的情况下，每年发生危险状况的次数）（W）。

当风险图用于确定在连续模式下起作用的一个安全功能的安全完整性等级时，则需考虑改变风险图中使用的那些参数。这些参数应表示与所涉及的应用特点最密切相关的那些风险因素。当为了保证把风险降低到允许等级而需要作某些调整时，还需要考虑给出安全完整性等级到参数判定结果的映射。作为一个例子，参数 W 被重新定义成系统处于运行期间系统寿命的百分数。在危险并不是连续出现，并且一年中失效导致危险的时段很短的情况下，应选择 W_1。在此例中，为了确保允许风险所涉及的判定准则和被复审的完整性等级结果，还需考虑其他的一些参数。详见表 D.1。

表 D.1 过程工业风险图参数的描述

参数		描 述
后果	C	发生危险事件很可能导致的死亡和/或严重伤害的人数。此人数可在考虑危险事件的致命性的情况下，通过计算当区域被占用时暴露区中的人数来确定。
占用率	F	在发生危险事件的时段内暴露区被占用的概率。可以通过在发生危险事件的时段内区域被占用的时间分数来确定此概率。还应考虑在发展成危险事件的过程中，为了调查可能存在的异常情况，而使处于暴露区的人员可能增多的可能性（还要考虑这是否会改变 C 参数）。

表 D.1(续)

参数		描　述
避免风险的概率	P	如果要求时仪表安全功能失效,暴露的人员能够避免存在的危险状况的概率。它取决于在发生危险以前向暴露的人员发警报的独立方法以及逃脱的方法。
要求率	W	在所考虑的仪表安全功能不存在的情况下,每年发生危险事件的次数。可通过考虑可能导致危险事件的所有失效并估算总的发生率来确定它。在考虑时还应包含其他保护层。

D.3 校正

校正过程的目的如下:

a) 为了用这样一种方法描述所有的参数,从而使 SIL 评估组能根据应用特点进行客观的判断;

b) 为了确保为某个应用选择的 SIL 符合公司的风险准则,并考虑到了其他来源的风险;

c) 为了使参数选择过程能被验证。

风险图的校正是给风险图参数赋值的过程。它构成了评估存在的过程风险,并允许确定考虑中的仪表安全功能的要求的完整性的基础。每个参数都分配了一个值的范围,这样当在组合中使用它们时,就可产生在没有某个特定的安全功能时所存在的风险的一个等级评估。于是就确定了对 SIF 的信任程度的一个度量。风险图把风险参数的特定组合同安全完整性等级关联起来。通过考虑与特定危险相关的允许风险,可确立风险参数组合和安全完整性等级之间的关联。

在考虑风险图的校正时,重要的是要考虑到与来自业主期望和管理当局要求的风险有关的要求。能从以下两个角度考虑生命的风险:

——个体风险:定义为暴露最多的个体每年的风险。通常有一个可允许的最大值。此最大值一般来自所有的危险源。

——社会风险:定义为暴露个体的一个群体每年经受的风险。一般要求把社会风险降低到至少社会能允许的一个最大值,并且直到进一步降低风险所花成本与降低的风险不成比例时为止。

如果有必要把个体风险降低到某个规定的最大值,则不能假设可以把全部的这种风险降低都分配给单独一个 SIS。暴露人员所受风险范围很宽,这些风险可由其他原因产生(例如坠落、火灾和爆炸风险)。

当考虑所需风险降低的程度时,一个组织应具有关于防止一次死亡事故所增加的成本的准则。通过分摊由于提高风险降低,而追加较高完整性等级相关的附加硬件和工程的年度成本就可计算出来。当防止一次死亡事故所增加的成本小于预定的数量时,就可认为追加的完整性等级是合理的。

一个广泛使用的社会风险准则是以 N 次致命事故的可能性 F 为基础的。允许的社会风险在一幅死亡人数与事故频率关系的对数——对数曲线图上用一条曲线或者一组曲线的形式表示。为所有事故描绘累积频率与事故后果的关系曲线(即 F-N 曲线),并确保 F-N 曲线不超过允许风险曲线,就可完成没有违背社会风险指南的确认。

在规定每个参数值之前就需考虑上述问题。大多数参数只能指定一个范围(例如,在一个特定过程的预期要求率位于所规定的一个每年要求次数的十进制数量级组成的范围之间,则可使用 W_3)。类似地,对于低一个数量级的要求范围,可使用 W_2,对于低二个数量级的要求范围则使用 W_1。给每个参数一个规定的范围有助于小组判定对一个特定的应用应选择多大的参数值。为了校正风险图,应给每个参数赋与一个值或值范围。与每个参数组相关的风险则以个体风险和社会风险的方式进行评估。然后就可确定满足所确立的风险准则(允许风险或更低)所需的风险降低。不需要在确定一个特定应用的 SIL 时每次都要执行这样的校正活动。对于类似的危险而言,对于组织一般仅需要进行一次这样的工作。在校正过程中,当发现最初所作的假设对任何特定的工程项目都无效时,则有必要对特定的项目进行调整。

表 D.1(续)

参数		描　述
避免风险的概率	P	如果要求时仪表安全功能失效,暴露的人员能够避免存在的危险状况的概率。它取决于在发生危险以前向暴露的人员发警报的独立方法以及逃脱的方法。
要求率	W	在所考虑的仪表安全功能不存在的情况下,每年发生危险事件的次数。可通过考虑可能导致危险事件的所有失效并估算总的发生率来确定它。在考虑时还应包含其他保护层。

D.3　校正

校正过程的目的如下:

a)　为了用这样一种方法描述所有的参数,从而使 SIL 评估组能根据应用特点进行客观的判断;

b)　为了确保为某个应用选择的 SIL 符合公司的风险准则,并考虑到了其他来源的风险;

c)　为了使参数选择过程能被验证。

风险图的校正是给风险图参数赋值的过程。它构成了评估存在的过程风险,并允许确定考虑中的仪表安全功能的要求的完整性的基础。每个参数都分配了一个值的范围,这样当在组合中使用它们时,就可产生在没有某个特定的安全功能时所存在的风险的一个等级评估。于是就确定了对 SIF 的信任程度的一个度量。风险图把风险参数的特定组合同安全完整性等级关联起来。通过考虑与特定危险相关的允许风险,可确立风险参数组合和安全完整性等级之间的关联。

在考虑风险图的校正时,重要的是要考虑到与来自业主期望和管理当局要求的风险有关的要求。能从以下两个角度考虑生命的风险:

——个体风险:定义为暴露最多的个体每年的风险。通常有一个可允许的最大值。此最大值一般来自所有的危险源。

——社会风险:定义为暴露个体的一个群体每年经受的风险。一般要求把社会风险降低到至少社会能允许的一个最大值,并且直到进一步降低风险所花成本与降低的风险不成比例时为止。

如果有必要把个体风险降低到某个规定的最大值,则不能假设可以把全部的这种风险降低都分配给单独一个 SIS。暴露人员所受风险范围很宽,这些风险可由其他原因产生(例如坠落、火灾和爆炸风险)。

当考虑所需风险降低的程度时,一个组织应具有关于防止一次死亡事故所增加的成本的准则。通过分摊由于提高风险降低,而追加较高完整性等级相关的附加硬件和工程的年度成本就可计算出来。当防止一次死亡事故所增加的成本小于预定的数量时,就可认为追加的完整性等级是合理的。

一个广泛使用的社会风险准则是以 N 次致命事故的可能性 F 为基础的。允许的社会风险在一幅死亡人数与事故频率关系的对数——对数曲线图上用一条曲线或者一组曲线的形式表示。为所有事故描绘累积频率与事故后果的关系曲线(即 F-N 曲线),并确保 F-N 曲线不超过允许风险曲线,就可完成没有违背社会风险指南的确认。

在规定每个参数值之前就需考虑上述问题。大多数参数只能指定一个范围(例如,在一个特定过程的预期要求率位于所规定的一个每年要求次数的十进制数量级组成的范围之间,则可使用 W_3)。类似地,对于低一个数量级的要求范围,可使用 W_2,对于低二个数量级的要求范围则使用 W_1。给每个参数一个规定的范围有助于小组判定对一个特定的应用应选择多大的参数值。为了校正风险图,应给每个参数赋与一个值或值范围。与每个参数组相关的风险则以个体风险和社会风险的方式进行评估。然后就可确定满足所确立的风险准则(允许风险或更低)所需的风险降低。不需要在确定一个特定应用的 SIL 时每次都要执行这样的校正活动。对于类似的危险而言,对于组织一般仅需要进行一次这样的工作。在校正过程中,当发现最初所作的假设对任何特定的工程项目都无效时,则有必要对特定的项目进行调整。

表 D.1(续)

参数		描　述
避免风险的概率	P	如果要求时仪表安全功能失效,暴露的人员能够避免存在的危险状况的概率。它取决于在发生危险以前向暴露的人员发警报的独立方法以及逃脱的方法。
要求率	W	在所考虑的仪表安全功能不存在的情况下,每年发生危险事件的次数。可通过考虑可能导致危险事件的所有失效并估算总的发生率来确定它。在考虑时还应包含其他保护层。

D.3　校正

校正过程的目的如下:

a)　为了用这样一种方法描述所有的参数,从而使 SIL 评估组能根据应用特点进行客观的判断;

b)　为了确保为某个应用选择的 SIL 符合公司的风险准则,并考虑到了其他来源的风险;

c)　为了使参数选择过程能被验证。

风险图的校正是给风险图参数赋值的过程。它构成了评估存在的过程风险,并允许确定考虑中的仪表安全功能的要求的完整性的基础。每个参数都分配了一个值的范围,这样当在组合中使用它们时,就可产生在没有某个特定的安全功能时所存在的风险的一个等级评估。于是就确定了对 SIF 的信任程度的一个度量。风险图把风险参数的特定组合同安全完整性等级关联起来。通过考虑与特定危险相关的允许风险,可确立风险参数组合和安全完整性等级之间的关联。

在考虑风险图的校正时,重要的是要考虑到与来自业主期望和管理当局要求的风险有关的要求。能从以下两个角度考虑生命的风险:

——个体风险:定义为暴露最多的个体每年的风险。通常有一个可允许的最大值。此最大值一般来自所有的危险源。

——社会风险:定义为暴露个体的一个群体每年经受的风险。一般要求把社会风险降低到至少社会能允许的一个最大值,并且直到进一步降低风险所花成本与降低的风险不成比例时为止。

如果有必要把个体风险降低到某个规定的最大值,则不能假设可以把全部的这种风险降低都分配给单独一个 SIS。暴露人员所受风险范围很宽,这些风险可由其他原因产生(例如坠落、火灾和爆炸风险)。

当考虑所需风险降低的程度时,一个组织应具有关于防止一次死亡事故所增加的成本的准则。通过分摊由于提高风险降低,而追加较高完整性等级相关的附加硬件和工程的年度成本就可计算出来。当防止一次死亡事故所增加的成本小于预定的数量时,就可认为追加的完整性等级是合理的。

一个广泛使用的社会风险准则是以 N 次致命事故的可能性 F 为基础的。允许的社会风险在一幅死亡人数与事故频率关系的对数——对数曲线图上用一条曲线或者一组曲线的形式表示。为所有事故描绘累积频率与事故后果的关系曲线(即 F-N 曲线),并确保 F-N 曲线不超过允许风险曲线,就可完成没有违背社会风险指南的确认。

在规定每个参数值之前就需考虑上述问题。大多数参数只能指定一个范围(例如,在一个特定过程的预期要求率位于所规定的一个每年要求次数的十进制数量级组成的范围之间,则可使用 W_3)。类似地,对于低一个数量级的要求范围,可使用 W_2,对于低二个数量级的要求范围则使用 W_1。给每个参数一个规定的范围有助于小组判定对一个特定的应用应选择多大的参数值。为了校正风险图,应给每个参数赋与一个值或值范围。与每个参数组相关的风险则以个体风险和社会风险的方式进行评估。然后就可确定满足所确立的风险准则(允许风险或更低)所需的风险降低。不需要在确定一个特定应用的 SIL 时每次都要执行这样的校正活动。对于类似的危险而言,对于组织一般仅需要进行一次这样的工作。在校正过程中,当发现最初所作的假设对任何特定的工程项目都无效时,则有必要对特定的项目进行调整。

在对参数赋值时，应提供这些值是如何得出的信息。

这样的校正过程在承担安全责任的组织内得到高度一致的同意是非常重要的。达成的决议决定了可达到的整体安全。

一般来说，用一个风险图来考虑要求的来源和 SIS 之间相关失效的可能性是困难的，会因此而导致 SIS 有效性的过高估计。

D.4 承担 SIL 评估的小组成员和组织

单独一个人要具备判定所有相关参数所必要的全部技能和经验是不可能的。为了确定安全完整性等级，通常采用专门组建一个小组的方法。小组成员一般包括：

——过程专家；

——过程控制工程师；

——运行管理人员；

——安全专家；

——具有操作所考虑的过程的实践经验的人员。

小组一般依次考虑每个仪表安全功能。小组需要关于该过程以及面临风险的可能人数的完整信息。

D.5 SIL 确定的结果的文档编制

很重要一点是，在确定 SIL 的过程中采取的任何决定都应记录在受控于配置管理的文档中。文档应清晰地描述小组为什么选择那些与某个安全功能相关的特定的参数。记录每个安全功能 SIL 的决定的结果及其作为后盾的假设的表格都应编入档案。在由单一操作小组所服务的一个区域内，如果可以确定有大量的执行一些安全功能的系统，则有必要复审校正假设的有效性。档案还应包括如下附加信息：

——使用的风险图，连同所有参数范围的描述；

——图及使用的所有文档的版本号；

——涉及到的人员配置假设和用于评价参数的所有的后果研究；

——涉及到的引起要求的失效以及用于确定要求率的所有的故障传播模型；

——涉及到的用于确定要求率的数据源。

D.6 基于典型准则的校正示例

在表 D.2 中，给出了上述参数描述和每个参数的范围，用于满足化工过程所规定的典型准则。在任意一个项目的范围内，使用此表之前，证实它能够满足承担安全责任的那些人的需要是非常重要的。

为了修改后果参数，引入了致命性的概念。这是因为在许多场合下，一次失效并不会直接造成死亡事故。在风险分析中，受体的致命性是一个重要的考虑内容，因为有时受体所受到的剂量还不足以引起死亡事故。一个受体的致命性作为一个结果，是受体暴露在危险下的频度和暴露持续时间的一个函数。例如，一次失效可能引起设备的一个部件的压力超过设计压力，但没有升高到超过设备测试压力，通常的结果很可能仅限于法兰密封垫圈的泄漏。在这种情况下，逐步升级的速率很可能较慢，操作人员一般都能避免后果。即使在液体漏泄量较大的情况下，由于逐步升级的速率够慢，操作人员避免危险的概率仍然较高。当然，失效导致管道或者压力容器破裂的情况下，操作人员的致命性就可能很高。

应考虑到由于要对事件形成的迹象进行调查，造成危险事件附近区域的人数的增加。必须考虑到最坏的情况。

辨别出“致命性”(V)和“避免危险事件的概率”(P)之间的差别是非常重要的，这样才不至于对同一因素给出两个置信度。致命性是有关危险发生后逐步升级的速度的一个量度，而 P 参数则是有关阻止

危险的一个量度。只有在操作员查觉到 SIS 丧失功能之后，他采取的动作能够阻止危险的情况下，才应使用 P_A。

对于如何选择占用率参数已设置了一些限制。选择占用率的要求是必须根据暴露最多的人员而不是所有人员的平均。理由是为了确保暴露最多的个体不会遭受高风险，然而这个风险已被平均到暴露于风险下的所有人员。

当参数并不落在任何规定的范围内时，有必要使用别的方法来确定风险降低要求，或者使用上面描述的方法重新校正风险图 D.1。

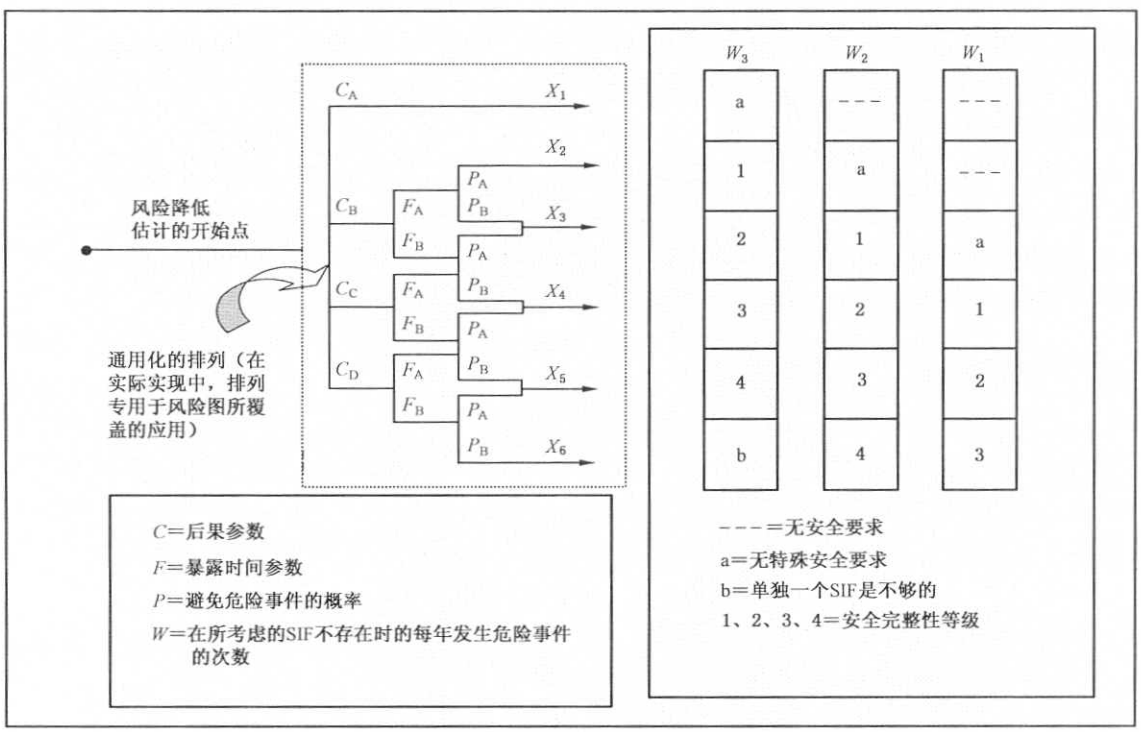


图 D.1　风险图：通用型式

表 D.2　通用风险图校正示例

风险参数		分级	备　注
后果(C) 死亡人数 通过确定当暴露在危险下的区域被占用时在场的人数并乘以查明的危险的致命性可计算死亡人数。 可由要防止的危险的固有特性确定致命性。可使用以下系数： $V=0.01$ 易燃或有毒物质少量释放 $V=0.1$ 易燃或有毒物质大量释放 $V=0.5$ 如上述，而且着火或者中毒概率很高 $V=1$ 管道、压力容器破裂或者爆炸	C_A C_B C_C C_D	轻微伤害 范围 0.01～0.1 范围＞0.1～1.0 范围＞1.0	1. 已经拟定了用于处理人员伤害或死亡的等级系统。 2. 在说明 C_A、C_B、C_C 和 C_D 时应考虑意外事故的后果和正常康复。

表 D.2(续)

风险参数		分级	备 注
占用率(F) 通过确定在正常工作期间，暴露在危险下的区域被占用的时间长度的比值可计算 F。 注 1：如果根据值班情况不同而导致处在危险区的时间有所不同时，应选择最大值。 注 2：当占用率高于标准值时，在能表明要求率是随机的且与占用率无关的情况下，才适合使用 P_A，高于标准的情况通常是在设备起动时或调查异常期间发生要求的情况。	F_A F_B	很少到经常暴露在危险区域 占用率小于 0.1 经常到永久暴露在危险区域	3. 见备注 1。
当保护系统不工作时避免危险事件的概率(P)	P_A P_B	在满足备注 4 的条件时采用 在不能满足所有的条件时采用	4. 只有下列情况都是真实的时候才选择 P_A： ——提供能警告操作员 SIS 已失效的设施； ——提供能关闭过程的独立设施，从而可避免危险或使所有人员能逃避到安全区； ——从操作员接收到警告到发生危险事件之间的时间应超过 1 h，或确实足以采取必要动作。
要求率(W) 在所考虑的 SIF 不存在时，每年发生危险事件的次数。 为了确定要求率，有必要考虑能导致危险事件的所有失效源。在确定要求率时，允许对控制系统的性能和干预持有一定的信任。如果不按 GB/T 21109 设计和维护控制系统，则能声明的性能将局限于与 SIL 1 相关的低性能范围内。	W_1 W_2 W_3	要求率小于每年 0.1D 要求率在每年 0.1D～1D 要求率在每年 1D～10D 之间 要求率高于每年 10D 时，则需要更高的安全完整性	5. W 因数的用途是估计在没有增加 SIS 时发生危险的频率。 如果要求率很高，只好用其他的方法或者重新校正的风险图来确定 SIL。应注意，在应用是连续模式操作的情况下，风险图不一定是最好的方法，见 GB/T 21109.1—2007 的 3.2.43.2。 6. D 是校正因子，其值的确定应使得在考虑到暴露人员的其他风险和公司准则的情况下，风险图得出允许的残余风险等级。
注：此例说明了风险图设计原理的应用。特定应用和特定危险的风险图，应在考虑到允许风险的情况下，由所涉及到的那些人来商定。见 D.1～D.6。			

D.7 在后果是破坏环境的情况下使用风险图

在失效后果包括严重的环境破坏的场合，也可使用风险图方法确定完整性等级要求。所需的完整性等级取决于被释放物质的特性及环境的敏感度。表 D.3 给出了环境方面的后果。上述特定物质规定的释放量与各个过程工厂的位置有关，并且需要报告给当地管理当局。工程项目需要确定在一个特定的位置什么是能被接受的。

表 D.3 一般环境后果

风险参数		等级	备 注
后果(C)	C_A	会造成轻微破坏的释放，破坏不很严重，但却大到足以达到必须报告给工厂管理部门的要求	一个法兰或阀门的中等程度的泄漏 小规模的液体溢出 不影响地下水的小规模土质污染
	C_B	在围墙范围内可造成重大破坏的释放	随着法兰密封垫圈漏气或者压缩容器密封失效，在单元上面形成有害气团
	C_C	可造成大破坏但能很快清除不会产生重大持久后果的超出围墙的释放	可对动植物造成暂时性损伤的气团或烟雾释放，并可能伴随液体滴落
	C_D	可造成大破坏且不能很快清除而会产生重大持久后果的超出围墙的释放	液体溢入河流或海洋中 可对动植物造成持久伤害的气团或烟雾释放，并可能伴随液体滴落 固体沉降(粉尘、催化剂、灰烬、煤灰) 影响地下水的液体释放

以上后果可连同下面所示的图 D.2 风险图的特殊版本一起使用。注意，由于占用率的概念不适用，故此风险图中不使用 F 参数。但还使用了参数 P 和 W，它们的定义同前面对安全后果所使用的那些定义是一样的。

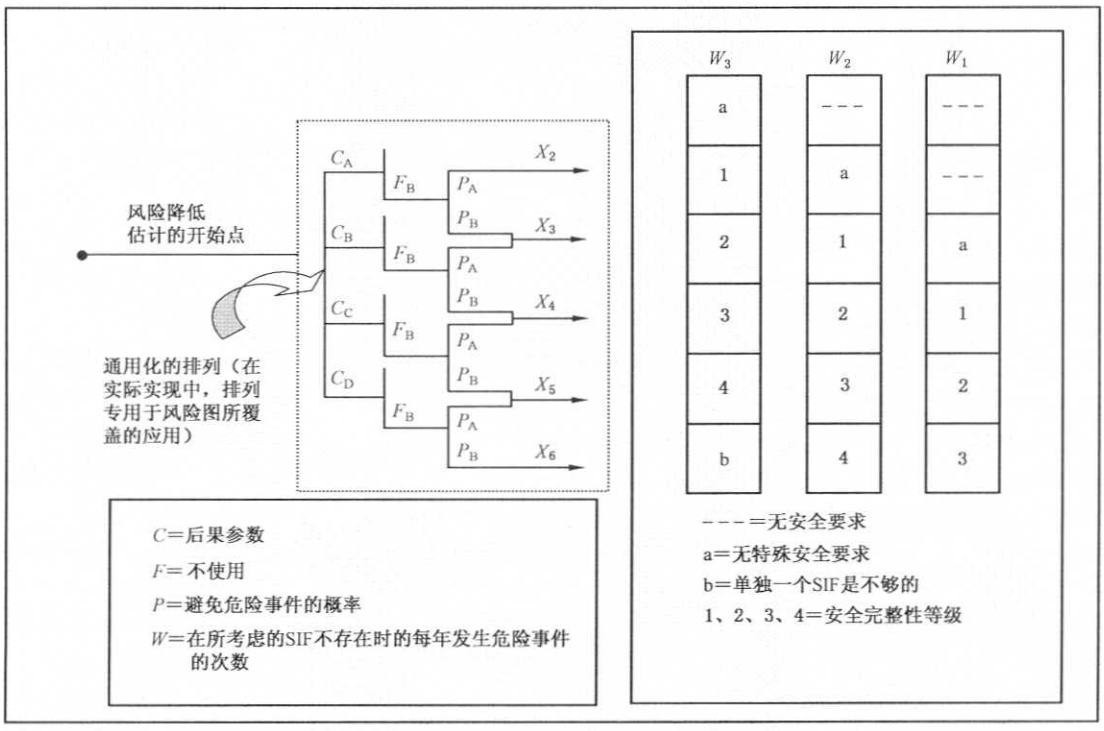


图 D.2 风险图：环境破坏

D.8 在后果是贵重财物损失的情况下使用风险图

对于失效后果包括资产损失的情况，也可使用风险图方法确定完整性等级要求。资产损失是与要求时功能失效相关的总的经济损失。它包括遭受到任何破坏时的重建成本和浪费或耽搁生产的成本。使用一般的成本效益分析可以计算任何损失后果的合理完整性等级。当使用风险图方法确定与安全和环境后果相关的完整性等级时，使用资产损失的风险图是有好处的。当被用来确定与资产损失有关的

完整性等级时，一定要定义后果参数 C_A～C_D。这些参数在不同的公司可能有不同的范围。

用于环境保护的一个风险图可导出一个类似的用于资产损失的风险图。注意，由于不适用占用率的概念，故不应使用 F 参数。但继续使用了参数 P 和 W，它们的定义同前面对安全后果所使用的那些定义是一样的。

D.9 在失效后果涉及一种或多种损害类型的情况下，确定仪表保护功能的完整性等级

在许多情况中，对要求时动作失效的后果涉及多种损害类型。分别确定与每类损害相关的完整性等级要求的情况就是这样。对于已查明的每个单独的风险，可使用不同的方法。为某个功能所规定的完整性等级，应考虑如果在要求时功能失效所涉及到的所有风险的累加总和。

附 录 E
（资料性附录）
确定要求的安全完整性等级——定性方法：风险图

E.1 概述

本附录基于下面的参考中更加详细描述的方法：

DIN V 19250，1994：Control technology：Fundamental safety aspects to be considered for measurement and control equipment

本附录描述了一种确定仪表安全功能的安全完整性等级的风险图方法。它是一种定性方法，利用此方法可通过对与过程和基本过程控制系统相关的风险因素的知识，确定一个仪表安全功能的安全完整性等级。

此方法使用了许多参数，这些参数共同描述了当安全仪表系统失效或不可用时危险情况的种类。从每4个一组中选择一个参数，然后把选择的这些参数组合起来，从而决定分配给仪表安全功能的安全完整性等级。这些参数：

——允许对风险进行分级评估，和

——表示关键的风险评估因素。

风险图方法还可用在确定需要风险降低需求的地方，就是后果包括严重的环境破坏或资产损失的地方。

本附录表示了上述方法（在DIN V 19250和VDI/VDE 2180中做了描述）在过程工业和机械领域中的应用，该方法已使用多年并已被德国过程工业和机械部门所接受。此方法已被TUV（德国鉴定测试实验室）和负责工业部分的德国管理当局接受。此图用于确定一个安全系统的安全完整性等级；图E.1和图E.2表示了此图和安全完整性等级之间的联系。

E.2 仪表功能典型的实现

在使用过程控制方法防护过程工厂中应清楚区别安全任务和操作要求。因此，过程控制系统可分为以下几类：

——基本过程控制系统；

——过程监视系统；

——安全仪表系统。

分类的目的是对每类系统都有足够要求的条件使之能在成本上经济合理的条件下满足工厂的整体要求。分类使之能对计划编制、安装和运行以及其后对过程控制系统的修改过程进行清楚的描绘。

基本过程控制系统被用于在工厂正常运行的范围内校正工厂的运行。它包括相关过程变量的测量、控制和/或记录。在必不可少的安全仪表系统反应之前，基本过程控制系统处于连续操作之中或者被频繁地请求动作。（一般不需按本部分的要求实现BPCS。）

在规定的一个过程工厂运行期间，只要一个或多个过程变量偏离正常操作范围，过程监视系统就会动作。过程监视系统将报告过程工厂的一个允许故障状况从而警告操作人员或者引发手动干预（通常不需按本部分要求来实现过程监视系统）。

安全仪表系统既可预防过程工厂的一个危险故障状态（“保护系统”）也可降低一个危险事件的后果。

如果不存在安全仪表系统，就有可能发生导致人员伤亡的一个危险事件。

与基本过程控制系统相比，通常对安全仪表系统的要求率是低的，这主要是因为发生危险事件的概率低。此外，处于连续操作状态下的BPCS和监视系统通常可使得安全仪表系统的要求率降低。

E.3 风险图的综合法

风险图基于风险与危险事件的后果及频率成正比的原理。它从假设不存在安全仪表系统开始。当然像 BPCS 和监视系统这样的典型的非安全仪表系统还是安装到位的。

后果与对健康或者安全的伤害或者来自环境破坏的伤害有关。

频率则是下列各项的组合：

——出现在危险区域的频率和潜在的暴露时间；

——避免危险事件的可能性；以及

——在安全仪表系统不到位(但所有的其他外部风险降低设施是在工作的)的情况下发生危险事件的概率——它被称为不期望发生的概率。

这就产生了以下 4 个风险参数：

——危险事件的后果(C)；

——出现在危险区域的频率与暴露时间的乘积(F)；

——避免危险事件后果的可能性(P)；

——不期望发生的概率(W)。

当使用风险图确定在连续模式下起作用的一个安全功能的安全完整性等级时，需考虑改变风险图中所使用的那些参数。这些参数应代表与所涉及的应用特点最密切相关的那些风险因素。当为了保证把风险降低到允许水平而需要作某些调整时，则需考虑安全完整性等级与参数判定结果的映射。作为一个例子，参数 W 被重新定义成系统处于运行状态下的寿命的百分数。在危险并不一直存在并且一年中一次失效导致危险的时段很短的情况下，应选择 W_1。在此例中，对于所涉及的判定准则和被复审的完整性等级结果来说，要保证允许风险还需考虑其他参数。

E.4 风险图的实现：人员保护

上述描述的风险参数的组合使风险图如图 E.1 所示。参数指标越高指示风险越大($C_1<C_2<C_3<C_4$；$F_1<F_2$；$P_1<P_2$；$W_1<W_2<W_3$)。图 E.1 中参数的相应分级见表 E.1。每个安全功能各自的风险图被用来确定该功能要求的安全完整性等级。

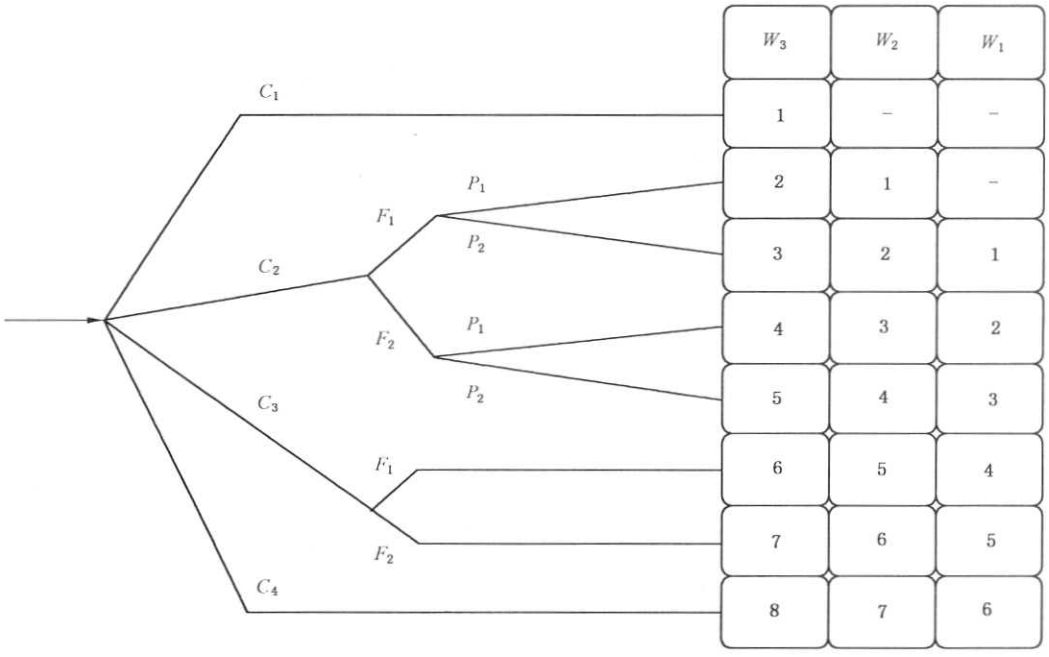


图 E.1 DIN V 19250 风险图——人员保护(见表 E.1)

当确定安全仪表系统所预防的风险时，一定要假定它是不存在所考虑的安全仪表系统时的风险。在此复审中的重点是影响的类型和范围以及过程工厂处于危险状态的预期频率。

使用 DIN V 19250 中详述的方法可以系统性地和可验证地确定风险，该方法可根据确立的参数确定要求等级。作为一条规则，要求等级的序号越高，安全仪表系统所覆盖的部分风险就越大，因此一般来说，要求及相应的措施也更加严厉。

对过程工业而言，单独的安全仪表系统不能覆盖要求等级 AK 7 和 AK 8。要把风险至少降低到 AK 6 需要非过程控制措施。

对这些要求等级来说，由于不可能用适当的几组公式量化各个要求，根据 VDI/VDE 2180，可把风险分成两个区域：

风险区域 1：可覆盖的较低风险(SIL 1 和 SIL 2)

风险区域 2：可覆盖的较高风险(SIL 3)

图 E.1 表示了符合 DIN V 19250 的要求等级和风险区域之间的关系。

表 E.1 与风险图有关的数据(见图 E.1)

风险参数		分级	备注
后果(C)	C_1	对人员轻微的伤害	1. 已拟定了用于处理人员伤亡的等级系统。还需拟定用于环境或资产损害的其他分级模式。
	C_2	对一人或多人严重的永久性伤害；一人死亡	
	C_3	几人死亡	
	C_4	灾难性影响，很多人死亡	
出现在危险区域中的频率与暴露时间的乘积(F)	F_1	很少到经常暴露在危险区域中	2. 见上述的备注 1。
	F_2	经常到永久长时间暴露在危险区域中	
避免危险事件后果的可能性(P)	P_1	在一定条件下有可能	3. 此参数应考虑： ——一个过程的运行(被监控(即由熟练的或不熟练的人员操作)或不被监控)； ——危险事件发展的速率(例如突然地、快速地或缓慢地)； ——识别危险的难易程度(例如直接就可发现，用技术手段才能检测到或者不用技术手段就能检测到)； ——危险事件的避免(例如可能、不可能或在一定条件下可能的逃生通道)； ——实际安全经验(这种经验可以通过相同过程或者类似过程获得，也可能不存在这种经验)。
	P_2	几乎不可能	
不期望发生的概率(W)	W_1	出现不期望发生的事故的概率很小，并且这种事故很可能没有几次	4. W 因素的用途是估计在没有附加任何安全仪表系统(E/E/PE 或其他技术)但包含任何外部风险降低设施的情况下不期望发生的事故的频率。
	W_2	出现不期望发生的事故的概率不大，并且这种事故很可能只有几次	
	W_3	出现不期望发生的事故的概率比较大，并且很可能经常发生	

GB/T 21109、DIN V 19250 和 VDI/VDE 2180 之间的关系见图 E.2。

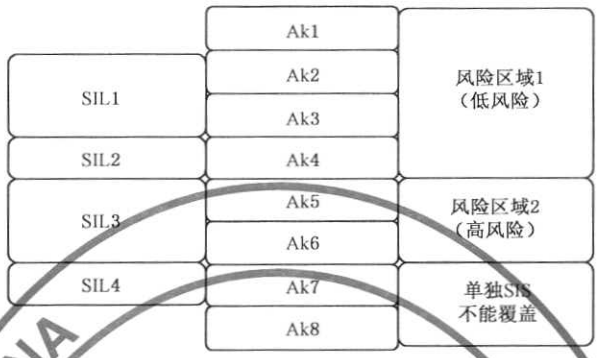


图 E.2 GB/T 21109、DIN V 19250 和 VDI/VDE 2180 之间的关系

E.5 在应用风险图过程中应考虑的相关问题

当应用风险图方法时，考虑来自业主和以及任何应用管理当局的风险要求是重要的。

应以清楚且易理解的措词来描述风险图的每个分支的解释和评价，以确保方法应用时的一致性。

值得注意的是风险图应由负责安全的组织的一些高层人员共同商定。

GB/T 21109、DIN V 19250 和 VDI/VDE 2180 之间的关系见图 E.2。

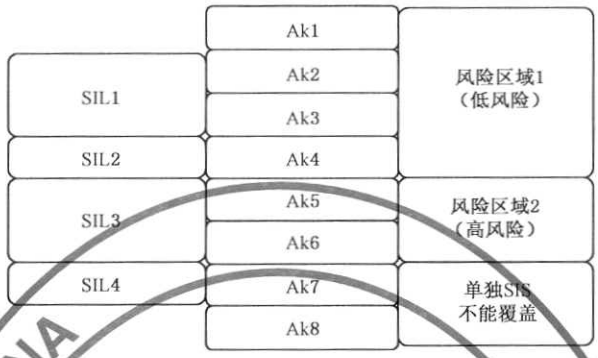


图 E.2 GB/T 21109、DIN V 19250 和 VDI/VDE 2180 之间的关系

E.5 在应用风险图过程中应考虑的相关问题

当应用风险图方法时，考虑来自业主和以及任何应用管理当局的风险要求是重要的。

应以清楚且易理解的措词来描述风险图的每个分支的解释和评价，以确保方法应用时的一致性。

值得注意的是风险图应由负责安全的组织的一些高层人员共同商定。

附 录 F
（资料性附录）
保护层分析（LOPA）

F.1 概述

本附录描述了一种被称为保护层分析（LOPA）的过程危险分析工具。该方法从危险和可操作性分析（HAZOP 研究）导出的数据着手，通过文档化引发原因和预防或减轻危险的保护层计算每个识别的危险。于是就能确定风险降低的总量以及是否需要进一步降低所分析的风险。如需附加的风险降低并且如果是以一个仪表安全功能（SIF）的形式提供这种降低，LOPA 方法允许确定合适的 SIF 的安全完整性等级（SIL）。

本附录不打算提供一种权威的计算方法，但说明了方法的一般原理。此方法基于下面的参考中更加详细描述的一种方法：

Guidelines for Safe Automation of Chemical Processes, American Institute of Chemical Engineers, CCPS, 345 East 47th Street, New York, NY 10017, 1993, ISBN 0-8169-0554-1。

F.2 保护层分析

GB/T 21109.1 中定义的安全生命周期需要确定设计一个仪表安全功能的安全完整性等级。这里描述的 LOPA 是适用于一个现有工厂的一种方法，一个多学科小组中用此方法来确定一个仪表安全功能的 SIL。此小组应包括：

——对所考虑的过程有操作经验的操作员；

——有过程专业知识的工程师；

——制造厂管理人员；

——过程控制工程师；

——对所考虑的过程有经验的仪表/电气维护人员；

——风险分析专家。

在小组供职的某个人应接受过 LOPA 方法的培训。

LOPA 所需要的信息被包含在危险和可操作性分析（HAZOP 研究）收集和导出的数据中。表 F.1 表示了保护层分析（LOPA）所需数据和在 HAZOP 研究过程中所导出的数据之间的关系。图 F.1 表示了可用于 LOPA 的一个典型详细记录表。

LOPA 分析了危险，从而可确定是否需要 SIF 以及需要时每个 SIF 所需的安全完整性等级。

F.3 影响事件

使用图 F.1 时，从 HAZOP 研究所确定的每个影响事件描述（后果）被填在第 1 列中。

F.4 严重性等级

根据表 F.2，对于影响事件而言，下一步要选择的就是严重性等级：轻微（M）、严重（S）或者大范围（E），它们被填在图 F.1 的第 2 列中。

表 F.1 从 HAZOP 导出的用于 LOPA 的数据

LOPA 要求的信息	HAZOP 所导出的信息
影响事件	后果
严重性等级	后果严重性
引发原因	原因
引发可能性	原因频率
保护层	现有保护装置
要求的附加减轻	推荐的新保护装置

#	1	2	3	4		5		6	7	8	9	10	11
					保护层								
	影响事件描述 F.3 F.14.1	严重性等级 F.4 F.14.1	引发原因 F.5 F.14.2	引发可能性 F.6 F.14.3	一般过程设计 F.14.4	BPCS F.14.5	报警等 F.14.6	附加减轻，限制进入 F.8 F.14.7	IPL 附加减轻堤堰，泄压 F.9 F.14.8	中间的事件可能性 F.10 F.14.9	SIF 完整性等级 F.11 F.14.10	已减轻的事件的可能性 F.12 F.14.10	注
1	蒸馏塔破裂引起火灾	S	冷却水流失	0.1	0.1	0.1	0.1	0.1	PRV 01	10^{-7}	10^{-2}	10^{-9}	高压引起塔破裂
2	蒸馏塔破裂引起火灾	S	蒸汽控制回路失效	0.1	0.1		0.1	0.1	PRV 01	10^{-7}	10^{-2}	10^{-8}	高压引起塔破裂
N													

注：严重性等级 E=大范围的，S=严重的；M=轻微的。

可能的值是每年的事件次数，另外的数值是要求时的平均失效概率。

图 F.1 保护层分析(LOPA)报告

表 F.2 影响事件严重性等级

严重性等级	后 果
轻微的(M)	如果采取的动作正确，影响最初只限于事件的局部区域，但具有较大范围后果的潜在可能。
严重的(S)	在现场或现场外，影响事件可能引起严重的人员伤亡。
大范围的(E)	严重程度不小于严重事件后果 5 倍的影响事件。

F.5 引发原因

图 F.1 第 3 列引出了影响事件的所有引发原因。影响事件有许多引发原因，把它们全都罗列出来是重要的。

F.6 引发可能性

图 F.1 第 4 列填入了发生引发原因的可能性值，单位为事件/年。表 F.3 表示了典型引发原因可能性。在确定引发原因可能性时，小组的经验是非常重要的。

表 F.3 引发可能性

低	在工厂预期寿命内具有很低发生概率的一次失效或一系列失效。 示例：——3 个或多个仪表同时失效或人为失效； ——仅一个或多个过程压力容器自然发生的失效。	$f<10^{-4}$，/年
中	在工厂预期寿命内具有低发生概率的一次或一系列失效。 示例：——仪表或阀门双重失效； ——仪表组合失效和操作员错误； ——小的过程管线或接头的单独失效。	$10^{-4}<f<10^{-2}$，/年
高	能够合理的预期在工厂预期寿命内发生的一次失效。 示例：——过程泄漏； ——一个仪表或阀门单独失效； ——可能导致物质释放的人为误差。	$10^{-2}<f$，/年

F.7 保护层

图 2 表示了过程工业中通常配备的多个保护层(PL)。每个保护层都由一组设备和/或其功能与其他一些保护层有关的管理级控制设备组成。能以高可靠性执行其功能的保护层可看作独立保护层(IPL)(见 F.9)

图 F.1 的第 5 列列出了用于在发生一个引发原因时降低发生一个影响事件的可能性的过程设计。这种设计的一个例子就是带套的管道或压力容器。当主管道或压力容器的完整性受到损害时，外套可防止过程物质的释放。

图 F.1 第 5 列的下一项是基本过程控制系统(BPCS)。如果当引发原因发生时，BPCS 中的一个控制回路可防止影响事件发生，则声明基于 PFD_{avg} 的置信度。

图 F.1 第 5 列的最后一项是从警告操作员的报警和利用操作员干预得到的好处。表 F.4 列出了保护层典型的 PFD_{avg} 值。

表 F.4 保护层(预防和减轻)典型的 PFD_{avg}

保护层	PFD_{avg}
控制回路	1.0×10^{-1}
人的执行能力(经培训的、不紧张)	$1.0\times10^{-2}\sim1.0\times10^{-4}$
人的执行能力(处于紧张状态下)	0.5～1.0
操作员对报警的响应	1.0×10^{-1}
容器压力额定值超过来自内部和外部压力源的最大极限值	10^{-4}或更好，在保持容器完整性(即了解腐蚀、按日程表执行检查、维护时)

F.8 附加减轻

减轻层通常有机械的、建筑上的或规程的。其例子有：

——泄压装置；

——堤(堰)；和

——限制接近。

减轻层可以降低影响事件的严重性，但不能防止影响事件的发生。其例子有：

——防火或防烟雾释放用的喷水系统；

——烟雾报警器；和

——撤离规程。

LOPA 小组应确定所有减轻层的恰当的 PFD 并把它们列入图 F.1 的第 6 列中。

F.9 独立保护层(IPL)

图 F.1 第 7 列中列出了满足 IPL 准则的保护层。

把一个保护层(PL)看作一个 IPL 的准则是：

——提供的保护大量降低已识别的风险，即最小降低 100 倍；

——提供可用性程度很高(0.9 或更高)的保护功能；

——它具有以下重要特点：

a) 专一性：IPL 只被设计用来防止或减轻一个潜在的危险事件(例如失控反应、有毒物质的释放、安全壳损坏或者火灾)的后果。由于多种原因都可能导致同一危险事件，因此多个事件情景都可由一个 IPL 来启动动作。

b) 独立性：IPL 是与已验明的危险相关的其他保护层相独立的。

c) 可信性：可信任 IPL 能执行所设计的那些功能。在设计中处理了随机失效和系统失效两种失效模式。

d) 可审核性：它被设计成能有助于定期确认保护功能。安全系统的检验测试和维护是必要的。

只有满足可用性、专一性、独立性、可信性和可审核性测试的那些保护层才可被归类为独立保护层类。

F.10 中间的事件可能性

引发可能性(图 F.1 第 4 列)乘以保护层和减轻层的 PFD(图 F.1 第 5 列～第 7 列)即可得出中间的事件可能性。算出的数的单位为事件/年，并被填入图 F.1 的第 8 列中。

如果中间的事件可能性小于你公司的该严重性等级的事件的准则，则可不用附加的 PL。但是如经济上合适的话，还应进一步降低风险。

如果中间的事件可能性大于你公司的该严重性等级的事件的准则，则需要附加的减轻。在使用安全仪表系统(SIS)型式的附加保护层之前，应考虑固有的较安全的方法和解决办法。如果能进行固有安全设计的改变，则应更新图 F.1 并重新计算中间的事件可能性，以确定它是否低于公司准则。如果不能通过上述方法降低中间的事件可能性至公司准则之下，则要求一个 SIS。

F.11 SIF 完整性等级

如果需要一个新的 SIF，则可由该事件的严重性等级的公司准则除以中间的事件可能性来计算所需的完整性等级。低于此数的 SIF 的一个 PFD_{avg} 被选作 SIS 的最大值并填入第 9 列中。

F.12 已减轻事件的可能性

把第 8 列和第 9 列的数值相乘就可计算出已减轻事件的可能性，结果填入第 10 列中。这种计算一直进行到小组算出每个已识别能查明的影响事件的已减轻事件的可能性为止。

F.13 总风险

最后一步是把显现相同危险的所有严重和大范围事件的已减轻的事件可能性加起来。例如，所有

引起火灾的严重和大范围事件的已减轻事件的可能性相加，并用于类似下面的公式中：

——火灾造成的致命风险＝(所有易燃物质释放的已减轻的事件可能性)×(引燃的概率)×(一个人在区域内的概率)×(在火灾中造成致命伤害的概率)。

将引起有毒物质释放的严重和大范围影响事件应被加上，并用于类似下面的公式中：

——有毒物质释放造成的致命性风险＝(所有有毒物质释放的已减轻的事件可能性)×(一个人在区域中的概率)×(在释放中造成致命伤害的概率)。

风险分析专家的专业知识和小组的知识，对把公式中的因素调节到工厂和受影响的社团所要求的条件来说是重要的。

把应用这些公式所得到的结果加起来就可确定该过程对公司的总风险。

如果它满足或者小于公司受影响的人口数的准则，LOPA 也就完成了。然而，因为受影响的人口有可能经受来自其他现有单元或新项目的风险，如果在经济上能实现的话，提供附加的减轻和风险降低是明智的。

F.14 示例

下面是用来描述在 HAZOP 研究中识别的一个影响事件的 LOPA 方法的一个示例。

F.14.1 影响事件和严重性等级

HAZOP 研究把一个间歇聚合反应器中的高压识别为一个偏差。不锈钢反应器被串联到一个填充钢纤维的增强型塑料塔和一个不锈钢冷凝器。纤维增强型塑料塔破裂将释放易燃蒸汽，如果存在一个点火源就有发生火灾的可能性。因为影响事件将导致在场人员的严重伤亡，LOPA 小组使用表 F.2 选择严重性等级时选择为严重的。影响事件及其严重性分别填入图 F.1 的第 1 列和第 2 列。

F.14.2 引发原因

HAZOP 研究列出了高压的两个引发原因，即至冷凝器的冷却水中断和反应器蒸汽控制回路失效。这两个引发原因被填入图 F.1 的第 3 列。

F.14.3 引发可能性

工厂已有在此区域中每 15 年会发生一次冷却水中断事件的经验。作为一种保守的估计，小组选择每 10 年发生一次冷却水中断事件。在图 F.1 第 4 列中填入 0.1 事件/年。在处理其他引发原因(反应器蒸汽控制回路失效)前，从头到尾直到得出结论都支持这个引发原因是合理的。

F.14.4 保护层设计

过程区域设计具有一个防爆电气等级，并且该区域有一个有效的过程安全管理计划。计划的一个要素是在区域内更换电气设备的更换规程管理。由于更换规程管理，LOPA 小组估计存在点火源的风险将降低 10 倍。因此根据过程设计，图 F.1 第 5 列应填入 0.1 的一个值。

F.14.5 BPCS

在反应器中，高压还伴随高温。BPCS 有一个控制回路，它可根据反应器中的温度调节输入到反应器夹套中的蒸汽。当反应器温度超过设定值时，BPCS 将关断到反应器夹套的蒸汽。因为关断蒸汽足以防止高压，BPCS 是一个保护层。BPCS 是一个很可靠的 DCS(分散型控制系统)并且生产人员从未有过温度控制回路不能使用的失效经历。因此 LOPA 小组决定 0.1 的一个 PFD_{avg} 是恰当的并在图 F.1 第 5 列的 BPCS 下面填入 0.1(对 BPCS 来说，0.1 是最低允许值)。

F.14.6 报警

在流到冷凝器的冷却水上装有一个变送器，它被连接到 BPCS 的另一不同的输入和一个不同于温度控制回路的控制器上。流到冷凝器的冷却水流量低将被报警，并要求操作员干预关断蒸汽。因为报警装置装在与温度控制回路不同的一个 BPCS 控制器中，所以它也被看作是一个保护层。由于操作员一直呆在控制室中，LOPA 小组商定 PFD_{avg} 为 0.1 是恰当的，并把此值填入图 F.1 第 5 列的报警装置下面。

F.14.7 附加减轻

在过程运行期间进入操作区是受限制的。只是在设备停机并被锁定期间才执行维护。过程安全管理计划要求所有非操作人员进入区域时要登记并通知过程操作员。因为强制受限访问规程，LOPA 小组估计在区域中的人员的风险降低 10 倍。因此，在图 F.1 第 6 列的附加减轻和风险降低一栏下填入 0.1。

F.14.8 独立保护层(IPL)

反应器配备有合适规格的一只安全阀，用来处理因冷却水中断在高温和过压期间产生的气体容积。在考虑材料评估和成分之后，从风险降低的角度评估安全阀的贡献。因为安全阀被设定在玻璃纤维塔的设计压力之下，并且在运行时段内不可能发生把塔和安全阀切断的人为失效，所以安全阀也被看作是一个保护层。每年拆除和测试一次安全阀，15 年的运行时间内从未观察到安全阀或者连接管道被堵塞。因为安全阀满足一个 IPL 的准则，它被列在图 F.1 第 7 列中，并给 PFD_{avg} 赋与值 0.01。

F.14.9 中间的事件可能性

把图 F.1 各列的第一排一齐乘起来并把积填入图 F.1 第 8 列中间的事件可能性下面。本例所得到的积为 10^{-7}。

F.14.10 SIS

保护层所取得的减轻和风险降低足以满足公司准则，但因为在 BPCS 的压力容器上装有一个压力发送器并可报警，所以还能从最低的成本获得附加的减轻。LOPA 小组决定增加一个由一个电流开关和一个用来断开连接反应器夹套蒸汽供应管线的一个电磁阀电源的继电器构成的 SIF。设计的 SIF 适合于 SIL 1 的较低范围，具有的 PFD_{avg} 为 0.01。把 0.01 填入 F.1 第 9 列的 SIF 完整性等级下面。

把第 8 列同第 9 列相乘就可计算出已减轻的事件可能性，将结果(1×10^{-9})填入图 F.1 的第 10 列。

F.14.11 下一个 SIF

现在 LOPA 小组考虑第 2 个引发可能性(反应器蒸汽控制回路失效)。使用表 F.3 来确定控制阀失效的可能性，并在图 F.1 第 4 列中填入 0.1。

当蒸汽控制回路发生失效时，从过程设计得出的保护层、报警、附加减轻和 SIS 依然存在。损失的保护层只是 BPCS。LOPA 小组计算出的中间的可能性应为 1×10^{-6}，而已减轻事件的可能性为 1×10^{-8}。这些值被分别填入图 F.1 第 8 列和第 10 列。

LOPA 小组将继续进行这种分析直到 HAZOP 研究中所有查出的偏差都被处理完为止。

最后一步是把表示相同危险的严重事件和大范围事件的已减轻的事件可能性加起来。

在本例中，如果对全部过程只查明一个影响事件，则该值为 1.1×10^{-8}。因为根据过程设计估算出的点火概率为 0.1，在附加减轻条件下，一个人处于区域中的概率也是 0.1，由火灾导致的致命性风险的方法降低到：

火灾产生的致命性风险=(所有易燃物质释放的已减轻的事件可能性)×(火灾产生死伤的概率)

或者

火灾产生的致命性风险=$(1.1\times10^{-8})\times0.5=5.5\times10^{-9}$

此值低于这种危险的公司准则，并且不考虑进一步降低风险在经济上被证明是合理的，因此 LOPA 小组的工作已完成。

中 华 人 民 共 和 国
国 家 标 准
过程工业领域安全仪表系统的功能安全
第3部分:确定要求的安全完整性
等级的指南
GB/T 21109.3—2007/IEC 61511-3:2003
*
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 2.75 字数 72 千字
2008年1月第一版 2008年1月第一次印刷
*
书号:155066·1-30413 定价 30.00 元

GB/T 21109.3-2007