ICS 25.040
N 10

中华人民共和国国家标准

GB/T 32857—2016

保护层分析(LOPA)应用指南

Application guide for layer of protection analysis(LOPA)

2016-08-29 发布　　2017-03-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中国机械工业联合会提出。

本标准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。

本标准起草单位:机械工业仪器仪表综合技术经济研究所、北京联合普肯工程技术有限公司、中国安全生产科学研究院、风控(北京)工程技术有限公司、中国石油天然气管道工程有限公司、中国石油天然气股份有限公司管道分公司、天津市居安企业管理咨询有限公司、中海油安全技术服务有限公司、上海撷果商务咨询有限公司。

本标准主要起草人:孟邹清、肖松青、俞文光、赵劲松、唐彬、袁小军、方来华、帅冰、聂中文、刘瑞、左信、张宝利、赵建民、刘瑶、程德发、游泽彬、许琛琛、史威、李秋娟、顾峥、周有铮、孙舒、靳江红。

引　言

本标准的目的是描述保护层分析(LOPA)的原理和分析过程，为应用 LOPA 分析方法开展风险分析提供适当的指南和参考。保护层分析方法是一种半定量的风险评价方法，它通过评价保护层的要求时危险失效概率来判断现有保护层是否可以将特定场景下的风险降低到风险标准所要求的水平，它的优点是：

- 与定性分析相比较，LOPA 分析可以提供相对量化的风险决策依据。避免主观因素对风险控制决策的影响。
- 虽然没有定量风险分析那么精确，但其过程简便。在定量分析工作之前，可以应用 LOPA 分析方法对风险相对较高的场景进行筛选，从而提高整个风险分析的工作的效率，节约分析工作的成本。
- LOPA 分析是安全完整性等级(SIL)的重要评估工具，与图表法相比较，LOPA 分析可以提供更加准确的结果。
- 通过 LOPA 分析，可以了解不同独立保护层在降低风险过程中的贡献，在此基础上，可以选择更加经济合理的保护措施来降低风险。
- LOPA 分析通常采用表格的形式记录评估的过程，记录过程符合通常的思维习惯，文件易读易用。

通过保护层分析，可以发现可行方案，如增设其他保护层、改变工艺等，从而选择最经济有效的降低危险性的措施。

LOPA 分析方法，作为一种简化的半定量的风险评价方法，使得对场景的分析和评价比其他定量风险评价方法更省时间和精力，更重要的是，它提供了识别场景风险的方法，并且将其与可容许风险比较，以确定现有的安全措施是否合适，是否需要增加新的安全措施。LOPA 分析通过展开分析场景的全过程，能很好地识别中间事件、安全措施和事故后果，帮助分析人员全面了解、认识特定的场景。

LOPA 分析也存在其不足之处。与定性分析方法相比较，它每次只是针对一起特定的场景进行分析，不能反映各种场景之间相互影响。此外，初始事件的发生频率及独立保护层的要求时危险失效概率等数据对 LOPA 分析的结果有很大的影响，需要付出很多努力和积累才能获取这些数据。

这种半定量的风险评价方法可以减少定性评价方法的主观性，且较完全的定量评价方法容易实行，在风险评估中被越来越广泛地应用。

保护层分析(LOPA)应用指南

1 范围

本标准规定了LOPA分析的相关策略和细则,包括LOPA分析方法的技术性说明及开展LOPA分析时的组织工作的要求,如准备工作、分析会议、分析报告及建议项跟踪等环节的要求,并给出在过程工业中不同应用的示例。

本标准适用于过程工业开展的保护层分析,其他行业也可参照使用。

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 20002.4—2015 标准中特定内容的起草 第4部分:标准中涉及安全的内容

GB/T 21109.1—2007 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

IEC 61508-4:2010 电气/电子/可编程电子安全相关系统的功能安全 第4部分:定义和缩略语(Functional safety of electrical/electronic/programmable electronic safety-realted systems—Part 4: Definitions and abbreviations)

3 术语和定义、缩略语

3.1 术语和定义

GB/T 20002.4、GB/T 21109.1和IEC 61508-4界定的以及下列术语和定义适用于本文件。

3.1.1

保护层分析 layer of protection analysis;LOPA

对降低不期望事件频率或后果严重性的独立保护层的有效性进行评估的一种过程方法或系统。

3.1.2

基本过程控制系统 basic process control system;BPCS

对来自过程的、系统相关设备的、其他可编程系统的和/或某个操作员的输入信号进行响应,并产生使过程和系统相关设备按要求方式运行的系统,但它并不执行任何具有被声明的SIL≥1的仪表安全功能。

注:对于过程领域而言,基本过程控制系统是一个全局性的术语。

3.1.3

保护层 layer of protect

用来防止不期望事件的发生或降低不期望事件后果严重性从而降低过程风险的设备、设施或方案。

3.1.4

事件 event

过程中发生的、可能由于设备能力或人员行动或影响风险控制系统的外部因素引起的过程事件。

3.1.5

初始事件　initial event

产生导致不期望后果场景的事件。

3.1.6

频率　frequency

一个事件单位时间内发生的次数。

3.1.7

独立保护层　Independent protection layer;IPL

一种设备、系统或行动，有效地防止场景向不期望的后果发展，它与场景的初始事件或其他保护层的行动无关。独立性表示保护层的执行能力不会受到初始事件或其他保护层失效的影响。独立保护层的有效性和独立性可以被审查。

3.1.8

后果　consequence

某一特定事件的结果。通常包括人员伤亡、财产损失、环境污染、声誉影响等。

3.1.9

场景　scenario

可能导致不期望后果的一种事件或事件序列。

3.1.10

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

当受保护设备或受保护设备控制系统发出要求时，执行规定安全功能的独立保护层的安全不可用性。

3.1.11

安全完整性等级　safety integrity level;SIL

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

[IEC 61508-4:2010，定义 3.5.8]

3.1.12

使能事件或使能条件　enable event/enable condition

导致场景发生的必要条件或事件，但不会直接导致场景发生。

3.1.13

安全仪表系统　safety instrumented system;SIS

用来实现一个或几个仪表安全功能的仪表系统。SIS 可以由传感器、逻辑解算器和最终元件的任何组合组成。

[GB/T 21109.1—2007，定义 3.2.72]

3.1.14

共因失效　common cause failure;CCF

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

3.1.15

低要求模式　low demand mode

将受保护设备或受保护设备控制系统导入规定安全状态的安全功能仅当要求时才执行，并且要求的频率不大于每年一次。

3.1.16

高要求模式　high demand mode

将受保护设备或受保护设备控制系统导入规定安全状态的安全功能仅当要求时才执行，并且要求的频率大于每年一次。

3.1.17

连续模式　continuous mode

安全功能将受保护设备或受保护设备控制系统保持在安全状态是正常运行的一部分。

3.1.18

可容许风险　tolerable risk

按当今社会价值取向在一定范围内可以接受的风险。

[GB/T 20002.4—2015，定义 3.15]

3.2　缩略语

下列缩略语适用于本文件(见表 1)。

表 1　本标准使用的缩略语

缩略语	全称	解释
ALARP	As Low As Reasonably Practicable	最低合理可行原则
BPCS	Basic Process Control System	基本过程控制系统
CCF	Common Cause Failure	共因失效
HAZOP	Hazard And Operability	危险与可操作性
IPL	Independent Protection Layer	独立保护层
LOPA	Layer Of Protection Analysis	保护层分析
PFD	Probability Of Dangerous Failure On Demand	要求时危险失效概率
PHA	Process Hazard Analysis	过程危险分析
P&ID	Pipe And Instrument Diagram	管道和仪表流程图
SIF	Safety Instrument Function	安全仪表功能
SIL	Safety Integrity Level	安全完整性等级
SIS	Safety Instrumented System	安全仪表系统

4　保护层分析(LOPA)原理

4.1　目的

保护层分析(LOPA)的目的是在定性危险分析的基础上，进一步对具体的场景的风险进行相对量化(准确到数量级)的研究，包括对场景的准确表述及识别已有的独立保护层，从而判定该场景发生时系统所处的风险水平是否达到可容许风险标准的要求，并根据需要增加适当的保护层，以将风险降低至可容许风险标准所要求的水平。

4.2　基本假设

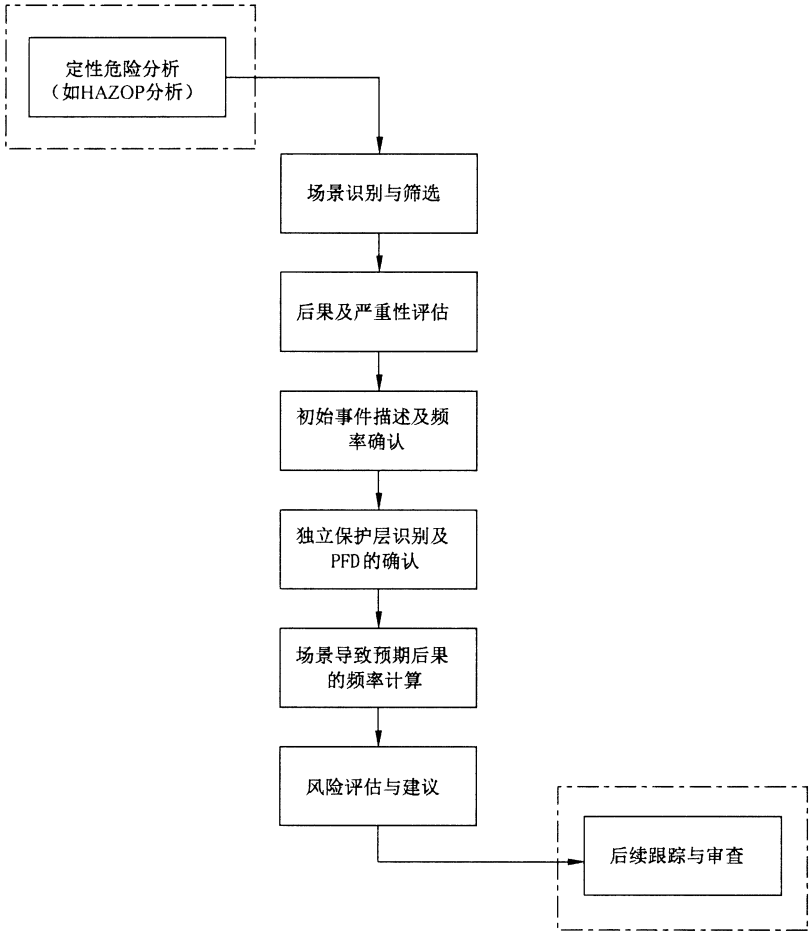
LOPA 的一个基本假设就是不存在不失效的保护层。

具体示例参见附录 A。

5 保护层分析基本程序和应用时机

5.1 基本程序

保护层分析的过程包括：场景识别与筛选、后果及严重性评估、初始事件描述及频率确认、独立保护层识别及 PFD 的确认、场景导致预期后果的频率计算、风险评估与建议。以上过程流程图见图 1。



注：图中虚框所含内容不在本标准范围之内。

图 1 保护层分析流程图

5.2 应用时机

LOPA 一般用于：

a) 场景过于复杂，不能采用完全定性的方法作出合理的风险判断；

b) 场景后果过于严重而不能只依靠定性方法进行风险判断。

LOPA 也用于以下几种场景：

a) 确定安全仪表功能的安全完整性等级；

b) 识别过程中安全关键设备；

c) 识别操作人员关键安全行为和关键安全响应；

d) 确定场景的风险等级以及场景中各种保护层降低的风险水平；

e) 其他适用 LOPA 的场景等(如设计方案分析和事故调查)。

LOPA 的应用示例参见附录 B 和附录 C。

6 分析过程

6.1 场景识别与筛选

6.1.1 场景应满足的基本要求

场景应满足以下基本要求:

a) 每个场景应至少包括两个要素:
   1) 引起一连串事件的初始事件;
   2) 该事件继续发展所导致的后果。
b) 每个场景应有唯一的初始事件及其对应后果;
c) 除了初始事件和后果外,一个场景还可能包括:
   1) 使能事件或使能条件;
   2) 防护措施失效。
d) 如果使用人员死亡、商业或环境损害作为后果,则场景还可能包括下列部分或全部因素,或条件修正因子:
   1) 可燃物质被引燃的可能性;
   2) 人员出现在事件影响区域的概率;
   3) 火灾、爆炸或有毒物质释放的暴露致死率(在场人员逃离的可能性);
   4) 其他可能的修正因子。

6.1.2 场景信息来源

场景识别信息通常来源于对新、改、扩建或在役工艺系统完成的危害评估,如 HAZOP 分析所识别的存在较大风险的场景。

HAZOP 中可导出的用于 LOPA 分析的数据见表 A.1。

值得一提的是,HAZOP 分析过程中所提出的现有安全措施可能是不完整的,在开展 LOPA 分析时,需要重新仔细检查是否遗漏了现有的措施,被遗漏的这些安全措施可能是独立保护层。

用于 LOPA 场景识别的信息来源还包括:

a) 生产运行问题,包括意外行为或正常范围之外的操作条件等;
b) 变更;
c) 事故事件;
d) 安全仪表功能审查。

6.1.3 场景筛选与开发

对场景进行详细分析与记录,记录表格示例见表 A.2。

对在记录过程中发现的,或独立保护层和初始事件频率评估中发现的新的场景,可能需要筛选开发新的场景,作为另一起 LOPA 分析的对象。

6.2 后果及严重性评估

在 LOPA 分析开始前,应确定场景后果的严重程度:

a) 宜采用定性或定量的方法对场景后果的严重性进行评估;

b) 典型的后果种类包括：人员伤亡、财产损失、环境污染、声誉影响等；

c) 后果严重性评估方法包括：释放规模/特征评估、简化的伤害/致死评估、需要进行频率校正的简化伤害/致死评估、详细的伤害/致死评估等；

d) 后果严重性评估分级应与可容许风险分级相一致。

后果等级、严重性分类等详细信息示例见表 A.3。

6.3 初始事件确认

6.3.1 初始事件类型

初始事件一般包括外部事件、设备故障和人的失效，分类见表 2。

表 2 初始事件类型

类别	外部事件	设备故障	人的失效
分类	a) 地震、海啸、龙卷风、飓风、洪水、泥石流和滑坡等自然灾害 b) 空难 c) 临近工厂的重大事故 d) 破坏或恐怖活动 e) 雷击和外部火灾 f) 其他外部事件	a) 控制系统失效 1) 元件失效 2) 软件失效 3) 控制支持系统失效(如电力系统、仪表空气系统) b) 机械系统故障 1) 磨损、疲劳或腐蚀造成的容器或管道失效 2) 设计、技术规程或制造/制作缺陷造成的容器或管道失效 3) 超压造成的容器或管道失效(如热膨胀、清管/吹扫)或低压失效(如真空) 4) 振动导致的失效(如转动设备) 5) 维护/维修不完善(包括使用不合适的替代材料)造成的失效 6) 高温或低温，以及脆性断裂引起的失效 7) 湍流或水击引起的失效 8) 内部爆炸、分解或其他失效反应造成的失效 9) 其他机械系统故障 c) 公用工程故障 d) 其他故障	a) 对给出的条件或其他提示未能正确观察或响应 b) 未能按正确的顺序执行任务步骤 c) 未能按操作规程进行操作(如误开/误关) d) 维护失误 e) 其他行为失效

6.3.2 初始事件确定原则

在确定初始事件时，应遵循以下原则：

a) 审查场景中所有的原因，以确定该初始事件为有效初始事件；

b) 应确认已辨识出所有的潜在初始事件，并确保无遗漏；

c) 应将每个原因细分为独立的初始事件（如“冷却失效”可细分为冷却剂泵故障、电力故障或控制回路失效），以便于识别独立保护层；

d) 在识别潜在初始事件时，应确保已经识别和审查所有的操作模式（如正常运行、开车、停车、设备停电）和设备状态（如待机、维护）下的初始事件；

e) 当人的失效作为初始事件时，应制定人员失误概率评估的统一规则并在分析时严格执行；

f) 以下事件不宜作为初始事件：

1) 操作人员培训不完善；

2) 测试或检查不完善；

3) 保护装置不可用；

4) 其他类似事件。

6.4 独立保护层评估

6.4.1 典型的保护层

一个典型的化工过程包含各种独立的或非独立的保护层，典型的保护层示例见表 A.6。

6.4.2 独立保护层的确定原则

并不是所有的保护层都可作为独立保护层。设备、系统或行动需满足以下条件才能作为独立保护层：

a) 有效性：按照设计的功能发挥作用，应有效地防止后果发生：

1) 应能检测到响应的条件；

2) 在有效的时间内，应能及时响应；

3) 在可用的时间内，应有足够的能力采取所要求的行动。

b) 独立性：独立于初始事件和任何其他已经被认为是同一场景的独立保护层的构成元件：

1) 应独立于初始事件的发生及其后果；

2) 应独立于同一场景中的其他独立保护层；

3) 应考虑共因失效或共模失效的影响。

c) 可审查性：对于阻止后果的有效性和 PFD 应以某种方式（通过记录、审查、测试等）进行验证。审查程序应确认如果独立保护层按照设计发生作用，它将有效地阻止后果：

1) 审查应确认独立保护层的设计、安装、功能测试和维护系统的合适性，以取得独立保护层特定的 PFD；

2) 功能测试应确认独立保护层所有的构成元件（传感器、逻辑解算器、最终元件等）运行良好，满足 LOPA 的使用要求；

3) 审查过程应记录发现的独立保护层条件、上次审查以来的任何修改以及跟踪所要求的任何改进措施的执行情况。

6.4.3 独立保护层的确定

应依据 6.4.2 来确定防护措施是否是独立保护层。过程工业典型独立保护层的确定示例见表 A.7。

以下防护措施不宜作为独立保护层：

a) 培训和取证：在确定操作人员行动的 PFD 时，需要考虑这些因素，但是它们本身不是独立保护层。

b) 程序：在确定操作人员行动的 PFD 时，需要考虑这些因素，但是它们本身不是独立保护层。

c) 正常的测试和检测：正常的测试和检测将影响某些独立保护层的 PFD，延长测试和检测周期可能增加独立保护层的 PFD。

d) 维护：维护活动将影响某些独立保护层的 PFD。

e) 通信：作为一种基础假设，假设工厂内具有良好的通信。差的通信将影响某些独立保护层的 PFD。

f) 标识：标识自身不是独立保护层。标识可能不清晰、模糊、容易被忽略等。标识可能影响某些独立保护层的 PFD。

6.4.4 独立保护层 PFD 的确定

独立保护层 PFD 的确认原则有：

a) 独立保护层的 PFD 为系统要求独立保护层起作用时该独立保护层不能完成所要求的任务的概率；

b) 如果安装的独立保护层处于“恶劣”环境与条件（如易污染或易腐蚀环境中），则应考虑使用更高的 PFD 值；

c) 表 A.8 提供了过程工业典型独立保护层的 PFD 值，实际 LOPA 应用过程中，PFD 值的确定应参照企业标准或行业标准，经分析小组共同确认或进行适当的计算以确认 PFD 值取值的合适性，并将其作为 LOPA 分析中的统一规则严格执行。

6.5 场景频率的计算

场景频率的计算内容有：

a) 本节仅规定单一场景的频率计算，同样后果的多个场景频率求和不在本节的规定范围内。

b) 本节仅针对低要求模式进行分析计算。

c) 单一场景后果的频率为初始事件发生频率乘以所有独立保护层要求时危险失效概率，场景后果的频率可能需要使用下面的两种系数进行修正：

1) 假如场景的发生需要使能事件或使能条件时，需要乘以使能事件或使能条件的发生概率；

2) 假如需要计算危险物质释放后的后续后果发生频率时，需要乘以条件修正因子，常见的条件修正因子如下：

- 可燃物质点火概率；
- 人员出现在事件影响区域的概率；
- 火灾、爆炸或有毒物质释放的暴露致死率；
- 其他。

d) 场景频率计算分为低要求模式后果频率计算和高要求模式后果频率计算。

e) 低要求模式的后果发生频率按式(1)计算：

$$f_i^{C} = f_i^{I} \times P_i^{E} \times P_i^{C} \times \prod_{j=1}^{J} \mathrm{PFD}_{ij} \qquad \cdots\cdots(1)$$

式中：

f_i^{C} ——初始事件 i 造成后果 C 的频率，单位为次每年；

f_i^{I} ——初始事件 i 的发生频率，单位为次每年；

P_i^{E} ——使能事件或使能条件发生的概率，假如没有使能事件或使能条件，则 P^{E} 取 1；

P_i^C ——条件修正因子，假如没有任何条件修正，则 P^C 取 1；

PFD_{ij} ——初始事件 i 中第 j 个阻止后果 C 的独立保护层要求时危险失效概率(PFD)。

f) 高要求模式下后果发生频率的计算参见附录 D。

6.6 风险的评估与建议

风险的评估与建议内容有：

a) 本节只研究单一场景的风险评估，多个场景的累计风险计算不在本节规定范围内。

b) 各公司应制定适合自己企业的单一场景风险可容许标准。常见的风险评估分析方法有矩阵法、数值风险法(每个场景最大容许风险)，独立保护层(IPL)信用值法。矩阵法示例见表A.9，数值风险法示例见表 A.10～表 A.12。

c) 通过 6.2 的后果及严重性评估与 6.5 的场景频率计算，得出选定场景的后果等级以及后果发生概率，可以与风险矩阵进行比较，或者与数值风险法中的相关事件可接受频率比较。

d) 根据风险比较结果：

1) 计算风险小于场景可容许风险，继续下一场景的 LOPA 分析；

2) 计算风险大于场景可容许风险，LOPA 分析小组应建议满足可容许风险标准所需采取的措施，并确定拟采取措施的 PFD ，以将风险降低到可容许风险之下。

e) 一个简单的示例参见附录 E。

7 LOPA 文档

LOPA 分析应完整、准确地记录场景评估过程中获得的信息。记录文件应包括不期望场景后果的事件链，以便其他分析小组或分析师审查 LOPA 过程中做出的假设，以及当场景不能满足企业可容许风险时，应用其他保护层是否可以防止事件发生或降低事故风险。LOPA 文档记录可采用多种形式。

记录表格应包含如下信息，样表见表 A.2：

a) 后果

后果描述应给出风险评估(矩阵法或数值风险法)中的事故类别，以便进行风险评估。

b) 可容许风险

记录表格中选取的可容许风险应和事故后果类别一致，可容许的频率值符合公司可容许标准值。

c) 初始事件

记录表格中应清晰记录场景初始事件，同时应给出初始事件频率。

d) 使能事件或使能条件

应对初始事件的使能事件或使能条件进行描述，并给出使能事件发生的概率。

e) 条件修正

如果选取的场景后果为物料泄漏以后的后果，计算场景频率时，在评估人员具有相关经验及数据支持下可使用条件修正。条件修正因子可能包括：

1) 可燃物质点火概率；

2) 人员出现在事件影响区域的概率；

3) 火灾、爆炸或有毒物质释放的暴露致死率；

4) 其他。

应表明这些假定值的参考依据，且对标准值的任何修改必须说明理由并记录在案。

f) 减缓前的后果频率

减缓前的后果频率是初始事件频率和所有使能事件或使能条件发生概率以及条件修正因子的乘积。

g） 独立保护层

应写出所有现有的及建议的独立保护层，包括每个独立保护层失效概率。如果独立保护层的失效概率不同于企业内采用的标准值，则应阐明调整理由。

h） 防护措施（非独立保护层）

如果现有的防护措施不能作为独立保护层，应当说明理由，以便让人更容易理解分析的依据。

示例：系统安装有安全阀，但安全阀的泄放量小于计算的场景物料的泄放量，则这个安全阀不能作为这个场景的独立保护层。

i） 减缓后的后果频率

减缓后的后果频率为减缓前的后果频率乘以所有独立保护层的失效频率后的值。

j） 能否满足可容许风险

使用减缓后的后果频率与采用的可容许风险进行比较，假如减缓后的后果频率小于采用的可容许风险中的事故频率，则场景满足可容许风险，否则为不满足。

k） 满足可容许风险需要采取的行动

假如场景的计算风险大于企业可容许风险，则写出需要采取进一步的措施，采取的行动中需要给出负责人，以及预计行动完成日期。

假如场景的计算风险大于企业可容许风险，但企业目前又不得不接受这样的风险，这种特殊情况可能需要高级管理人员的签字，并附在分析文档中。

l） 备注

应包括所有背景资料，或记录与场景或采取行动相关的此类信息。

m） 参考资料

任何有关的工艺流程图、P&ID、SIF 描述或联锁逻辑图、仪表清单、设备清单、操作规程和测试程序等参考资料，从而完整地记录分析的依据，以便协助审查或执行分析的结果。

n） LOPA 分析人员

LOPA 分析人员姓名、职责。

附 录 A
（资料性附录）
LOPA 分析各阶段数据（示例）

A.1 从 HAZOP 导出的可用于 LOPA 分析的数据

从 HAZOP 导出的可用于 LOPA 分析的数据见表 A.1。

表 A.1 从 HAZOP 导出可用于 LOPA 的数据

LOPA 要求的信息	HAZOP 所导出的信息
场景背景与描述	偏差
初始事件	引起偏差的原因
后果描述	偏差导致的后果
独立保护层	现有的安全措施
注 1：HAZOP 所导出的信息在应用于 LOPA 分析时应再次判断。例如：HAZOP 分析中的现有安全措施并不都是独立保护层。 注 2：来自 HAZOP 分析的建议安全措施是否可作为独立保护层，也可在 LOPA 分析时再次判断。	

A.2 LOPA 分析记录表

LOPA 分析记录表（示例）见表 A.2。

表 A.2 LOPA 分析记录表（示例）

场景编号：	设备编号：	场景名称：	
日期：	场景背景与描述：	概率	频率 年$^{-1}$
后果描述/分类			
可容许风险（分类/频率）	不可接受（大于）		
	可以接受（小于或等于）		
初始事件 （一般给出频率）			
使能事件或使能条件			
条件修正 （如果适用）	点火概率		
	影响区域内人员存在概率		
	致死概率		
	其他		
减缓前的后果频率			

表 A.2（续）

场景编号：	设备编号：	场景名称：	
日期：	场景背景与描述：	概率	频率 年$^{-1}$
独立保护层			
基本过程控制系统			
人为缓解			
安全仪表功能			
压力缓解设备			
其他保护层 （应判别）			
其他保护措施 （非独立保护层）			
所有独立保护层总 PFD			
减缓后的后果频率			
是否满足可容许风险？（是/否）：			
满足可容许风险需要采取的行动：			
备注：			
参考资料（PHA 报告、P&ID 等）：			
LOPA 分析人员：			

填表注意事项：

a） 识别从初始事件发展到后果的所有重要环节；

b） 记录所有可能会影响后果出现的频率、后果大小或类型计算的因素；

c） 识别包括：维护特定初始事件、特定后果以及特定独立保护层之间的关联；

d） 对于已确定某一场景，分析人员识别初始事件，并确定事件导致预期的后果是否需要任何使能事件或使能条件；

e） 列出场景所有的防护措施；

f） 小组对列出的多种防护措施进行分析，确定真正的独立保护层；

g） 场景开发应该随着对工艺或系统理解的加深或者新的可用信息的加入而不断修改和完善；有些情况下，可能需要筛选开发出新的场景。

A.3 后果及严重性等信息

A.3.1 后果分类及严重性等级等的信息来源

后果分类及严重性等级等的信息来源包括：

a) 国际惯例或通用数据源；
b) 国家标准或行业规范；
c) 公司根据自身风险可接受水平制定的准则或规范；
d) 长期的行业经验或实践积累。

A.3.2 后果的分类

考虑后果分析的详细程度，可按照影响对象分为：
a) 人员伤亡；
b) 财产损失；
c) 环境污染；
d) 声誉影响等。
按照量化程度，后果评估的不同方法包括：
a) 释放规模/特征评估；
b) 简化的伤害/致死评估；
c) 需要进行频率校正的简化伤害/致死评估；
d) 详细的伤害/致死评估。

A.3.3 严重性分级

表 A.3 给出了简化的化学物质释放后果分级方法的示例，表 A.4 和表 A.5 分别给出了简化的伤害致死后果分级示例，以及简化的经济损失后果分级示例。

注：表 A.3～表 A.5 中的后果分级示例仅用于理解后续案例，不可供实际工程直接使用。

表 A.3 简化的物质释放后果分级表(示例)

释放物特性	释放规模					
	0.5 kg～5 kg	5 kg～50 kg	50 kg～500 kg	500 kg～5 000 kg	5 000 kg～50 000 kg	>50 000 kg
剧毒，温度>B.P	等级 3	等级 4	等级 5	等级 5	等级 5	等级 5
剧毒，温度<B.P 或高毒性，温度>B.P	等级 2	等级 3	等级 4	等级 5	等级 5	等级 5
高毒性，温度<B.P 或易燃，温度>B.P	等级 2	等级 2	等级 3	等级 4	等级 5	等级 5
易燃，温度<B.P	等级 1	等级 2	等级 2	等级 3	等级 4	等级 5
可燃液体	等级 1	等级 1	等级 1	等级 2	等级 2	等级 3
注 1：B.P 表示常压沸点。 注 2：在很难定量评估人员伤亡数量和伤亡严重程度时，帮助小组做出更准确的相对风险判断。						

表 A.4 简化的伤害致死后果分级(示例)

后果特征	等级 1	等级 2	等级 3	等级 4	等级 5	等级 6
人员伤害/致死	人员受伤但歇工不足 1 个工作日	无重伤及死亡歇工 1 个工日及以上	1～2 人重伤	1～2 人死亡或 3～9 人重伤	3～9 人死亡或 10 人及以上重伤	10 人及以上死亡

表 A.5 简化的经济损失后果分级(示例)

后果特征	等级 1	等级 2	等级 3	等级 4	等级 5	等级 6
经济损失	直接经济损失2万元以下,并未构成公司级事故的非计划停工事故 或总损失(直接加上间接)为以上直接损失值的10倍	直接经济损失2万元以上,10万元以下 或总损失(直接加上间接)为以上直接损失值的10倍	直接经济损失10万元及以上,50万元以下;或造成3套及以上生产装置停产,影响日产量50%及以上 或总损失为以上直接损失值的10倍	直接经济损失50万元及以上,100万元以下 或总损失(直接加上间接)为以上直接损失值的10倍	直接经济损失100万元及以上,500万元以下 或总损失(直接加上间接)为以上直接损失值的10倍	直接经济损失500万元及以上 或总损失(直接加上间接)为以上直接损失值的10倍

A.4 典型的保护层

6.4.1 介绍了典型的保护层,一个典型的化工过程包含各种独立的或非独立的保护层,表 A.6 为典型的保护层的描述及相关说明,表 A.7 为介绍独立保护层的确定,包括独立保护层的描述及作为独立保护层的要求,表 A.8 给出了典型独立保护层 PFD 值。

表 A.6 典型的保护层

保护层	描述	说明
采用本质安全设计	从根本上消除或减少工艺系统存在的危害	企业可根据具体场景需要,确定是否将其作为 IPL
基本过程控制系统(BPCS)	基本过程控制系统 BPCS 是执行持续监测和控制日常生产过程的控制系统。BPCS 中的控制回路通过响应过程或操作人员的输入信号,产生输出信息,使过程以期望的方式运行,该控制回路正常运行时能避免特定危险事件的发生,该控制回路的故障不会作为起因引起特定危险事件的发生。一个 BPCS 控制回路由传感器、控制器和最终元件组成	BPCS 控制回路作为 IPL,可能包括以下两种形式: a) 连续控制行动:保持过程参数维持在规定的正常范围以内,防止初始事件发生; b) 逻辑行动:状态控制器(逻辑解算器或控制继电器)采取自动行动来跟踪过程,而不是试图使过程返回到正常操作范围内。行动将导致停车,使过程处于安全状态
关键报警和人员干预	关键报警和人员响应是操作人员或其他工作人员对报警响应,或在系统常规检查后,采取的防止不良后果的行动	通常认为人员响应的可靠性较低,应慎重考虑人员行动作为独立保护层的有效性。 关键报警应有充分的人员响应时间
安全仪表系统(SIS)	安全仪表功能 SIF 针对特定危险事件通过检测超限等异常条件,控制过程进入功能安全状态。一个安全仪表功能 SIF 由传感器、逻辑解算器和最终元件组成,具有一定的 SIL	安全仪表功能 SIF 在功能上独立于 BPCS

表 A.6（续）

保护层	描述	说明
物理保护 （释放措施）	提供超压保护，防止容器的灾难性破裂	包括安全阀、爆破片等，其有效性受服役条件的影响较大
释放后物理保护 （防火堤、隔堤）	释放后保护设施是指危险物质释放后，用来降低事故后果（如大面积泄漏扩散、受保护设备和建筑物的冲击波破坏、容器或管道火灾暴露失效、火焰或爆轰波穿过管道系统等）的保护设施	
工厂和周围社区的应急响应	在初始释放之后被激活，其整体有效性受多种因素影响	

表 A.7　独立保护层的确定

保护层	描述	作为独立保护层的要求
工艺设计	从根本上消除或减少工艺系统存在的危害	a）当本质安全设计用来消除某些场景时，不应作为 IPL； b）当考虑本质安全设计在运行和维护过程中的失效时，在某些场景中，可将其作为一种 IPL
基本过程控制系统（BPCS）	基本过程控制系统 BPCS 是执行持续监测和控制日常生产过程的控制系统。BPCS 中的控制回路通过响应过程或操作人员的输入信号，产生输出信息，使过程以期望的方式运行，该控制回路正常运行时能避免特定危险事件的发生，该控制回路的故障不会作为起因引起特定危险事件的发生。一个 BPCS 控制回路由传感器、控制器和最终元件组成	如果 BPCS 控制回路的正常操作满足以下要求，则可作为独立保护层： a）BPCS 控制回路应与安全仪表系统（SIS）功能安全回路 SIF 在物理上分离，包括传感器、控制器和最终元件； b）该控制回路正常运行时能避免特定危险事件的发生； c）该控制回路的故障不会作为起因引起特定危险事件的发生。 BPCS 控制回路是一个相对较弱的独立保护层，内在测试能力有限，防止未授权变更内部程序逻辑的安全性有限。如果要考虑多个独立保护层的话，应有更全面的信息来支撑，具体评估方法见 A.5
关键报警和人员干预	关键报警和人员响应是操作人员或其他工作人员对报警响应，或在系统常规检查后，采取的防止不良后果的行动	当报警或观测触发的操作人员行动满足以下要求，确保行动的有效性时，则可作为独立保护层： a）操作人员应能够得到采取行动的指示或报警，这种指示或报警应始终对操作人员可用； b）操作人员应训练有素，能够完成特定报警所触发的操作任务； c）任务应具有单一性和可操作性，不宜要求操作人员执行 IPL 要求的行动时同时执行其他任务； d）操作人员应有足够的响应时间； e）操作人员的工作量及其身体条件合适等

表 A.7（续）

保护层	描述	作为独立保护层的要求
安全仪表系统(SIS)	安全仪表功能 SIF 针对特定危险事件通过检测超限等异常条件，控制过程进入功能安全状态。一个安全仪表功能 SIF 由传感器、逻辑解算器和最终元件组成，具有一定的 SIL	a) 安全仪表功能 SIF 在功能上独立于 BPCS，是一种独立保护层； b) 安全仪表功能 SIF 的规格、设计、调试、检验、维护和测试都应按 GB/T 21109 的有关规定执行； c) 安全仪表功能 SIF 的风险削减性能由其 PFD 所确定，每个安全仪表功能 SIF 的 PFD 基于传感器、逻辑解算器和最终元件的数量和类型，以及系统元件定期功能测试的时间间隔
物理保护 （释放措施）	提供超压保护，防止容器的灾难性破裂	a) 如果这类设备(安全阀、爆破片等)的设计、维护和尺寸合适，则可作为独立保护层，它们能够提供较高程度的超压保护； b) 但是，如果这类设备的设计或者检查和维护工作质量较差，则这类设备的有效性可能受到服役时污垢或腐蚀的影响
释放后物理保护 （防火堤、隔堤）	释放后保护设施是指危险物质释放后，用来降低事故后果(如大面积泄漏扩散、受保护设备和建筑物的冲击波破坏、容器或管道火灾暴露失效、火焰或爆轰波穿过管道系统等)的保护设施	为独立保护层，这些独立保护层是被动的保护设备，如果设计和维护正确，这些独立保护层可提供较高等级的保护
厂区的应急响应	在初始释放之后被激活，其整体有效性受多种因素影响	厂区的应急响应(消防队、人工喷水系统、工厂撤离等措施)通常不作为独立保护层，因为它们是在初始释放后被激活，并且有太多因素影响了它们在减缓场景方面的整体有效性。当考虑它作为独立保护层时，应提供足够证据证明其有效性
周围社区的应急响应	在初始释放之后被激活，其整体有效性受多种因素影响	周围社区的应急响应(社区撤离和避难所等)通常不作为独立保护层，因为它们是在初始释放之后被激活，并且有太多因素影响了它们在减缓场景方面的整体有效性。当考虑它作为独立保护层时，应提供足够证据证明其有效性

表 A.8 典型独立保护层 PFD 值

独立保护层的 PFD 范围独立保护层	说明	PFD （来自文献和工业数据）
“本质安全”设计	如果正确地执行，将大大地降低相关场景后果的频率	$1\times10^{-5}\sim1\times10^{-1}$
基本过程控制系统(BPCS)	如果与初始事件无关，BPCS 中的控制回路可确认为一种独立保护层	$1\times10^{-2}\sim1\times10^{-1}$ (IEC 规定 $1\times10^{-1}\sim1\times10^{-0}$)

表 A.8（续）

独立保护层的 PFD 范围独立保护层		说明	PFD （来自文献和工业数据）
关键报警和人员干预	人员行动，有 10 min 的响应时间	简单的、记录良好的行动，行动要求具有清晰可靠的指示	$1\times10^{-1}\sim1\times10^{-0}$
	人员对 BPCS 指示或报警的响应，有 40 min 的响应时间	简单的、记录良好的行动，行动要求具有清晰可靠的指示	1×10^{-1}
	人员行动，有 40 min 的响应时间	简单的、记录良好的行动，行动要求具有清晰可靠的指示	$1\times10^{-2}\sim1\times10^{-1}$
安全仪表系统(SIS)	SIL 1	典型组成： 单个传感器＋单个逻辑解算器＋单个最终元件	$1\times10^{-2}\sim1\times10^{-1}$
	SIL 2	典型组成： 多个传感器＋多个通道逻辑解算器＋多个最终元件	$1\times10^{-3}\sim1\times10^{-2}$
	SIL 3	典型组成： 多个传感器＋多通道逻辑解算器＋多个最终元件	$1\times10^{-4}\sim1\times10^{-3}$
物理保护（释放措施）	安全阀	防止系统超压。其有效性对服役条件比较敏感	$1\times10^{-5}\sim1\times10^{-1}$
	爆破片	防止系统超压。其有效性对服役条件比较敏感	$1\times10^{-5}\sim1\times10^{-1}$
释放后物理保护	防火堤	降低储罐溢流、破裂、泄漏等严重后果(大面积扩散)的频率	$1\times10^{-3}\sim1\times10^{-2}$
	地下排污系统	降低储罐溢流、破裂、泄漏等严重后果(大面积扩散)的频率	$1\times10^{-3}\sim1\times10^{-2}$
	开式通风口	防止超压	$1\times10^{-3}\sim1\times10^{-2}$
	耐火材料	减少热输入率，为降压/消防等提供额外的响应时间	$1\times10^{-3}\sim1\times10^{-2}$
	防爆墙/舱	通过限制冲击波，保护设备/建筑物等，降低爆炸重大后果的频率	$1\times10^{-3}\sim1\times10^{-2}$

A.5 BPCS 多个回路作为 IPL 的评估方法

A.5.1 同一 BPCS 多个功能回路作为 IPL 的评估方法

有两种方法可用于评估涉及 BPCS 回路或功能的 IPLs 的独立性，以确定某特定场景中存在多少独立保护层。使用方法 A，规则明确且保守。如果分析人员经验丰富，并且关于 BPCS 逻辑解算器设计及实际性能的数据充足可用时，可使用方法 B。

a） 方法 A

方法 A 假设一个单独 BPCS 回路失效，则其他所有共享相同逻辑解算器的 BPCS 回路都失效。对

单一的 BPCS，只允许有一个 IPL，且应独立于 IE 或任何使能事件。

b） 方法 B

方法 B 假设一个 BPCS 回路失效，最有可能是传感器或最终元件失效，而 BPCS 逻辑解算器仍能正常运行。BPCS 逻辑解算器的 PFD 比 BPCS 回路其他部件的 PFD 至少低两个数量级。方法 B 允许同一 BPCS 有一个以上的 IPL。

如图 A.1 所示，两个 BPCS 回路使用相同的逻辑解算器。假设这两个回路满足作为同一场景下 IPL 的其他要求，方法 A 只允许其中一个回路作为 IPL，方法 B 允许两个回路都作为同一场景下的 IPL。

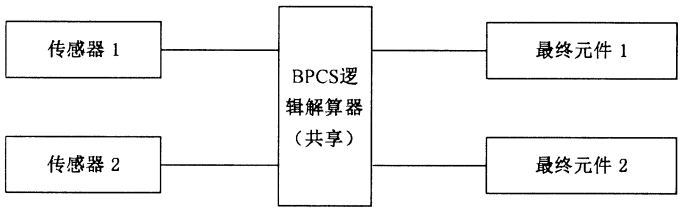


图 A.1 同一场景下多个回路的典型 BPCS 逻辑计算器

A.5.2 同一场景下，同一 BPCS 多个功能回路同时作为 IPL 的要求

同一场景下，同一 BPCS 的多个功能回路同时作为 IPL 时，应满足：

a） BPCS 具有完善的安全访问程序，应确保将 BPCS 编程、变更或操作上潜在的人为失误降低到可接受水平；

b） BPCS 回路中的传感器与最终元件在 BPCS 回路的所有部件中具有最高的失效概率值。

如果传感器或最终元件是场景中其他 IPL 的公共组件或是初始事件的一部分，则多个回路不应作为多个 IPL。如图 A.2 所示，BPCS 回路 1 和回路 2 均使用同一传感器，在这个场景下，则这两个 BPCS 回路只能作为一个 IPL。同样，如果最终元件（或相同报警和操作人员响应）被共享在两个 BPCS 回路，那么这两个 BPCS 回路也只能作为一个 IPL。

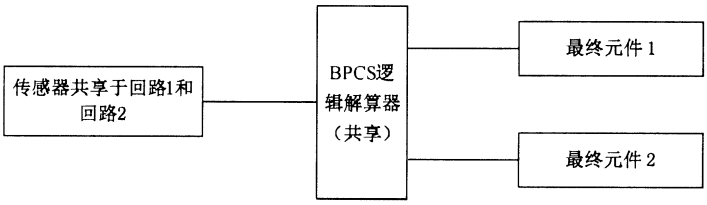


图 A.2 同一场景下共享传感器的 BPCS 回路

共享逻辑解算器输入卡或输出卡的额外 BPCS 回路不宜同时作为 IPL。如图 A.3 所示，假设满足 IPL 的所有其他要求，则回路（传感器 A→输入卡 1→逻辑解算器→输出卡 1→最终元件 1）可确定为 IPL。如果第二个控制回路的路径为（传感器 D→输入卡 2→逻辑解算器→输出卡 2→最终元件 4），那么此回路也可确定为 IPL。但是，如果第二个回路的路径为（传感器 D→输入卡 2→逻辑解算器→输出卡 1→最终元件 2），那么此回路不能作为 IPL，因为输出卡 1 共享在两个回路中。相似的，如果第二个回路的路径为（传感器 D→输入卡 2→逻辑解算器→输出卡 1→最终元件 2），那么此回路也因为输出卡 1 共用在两个回路中而不能作为独立保护层。

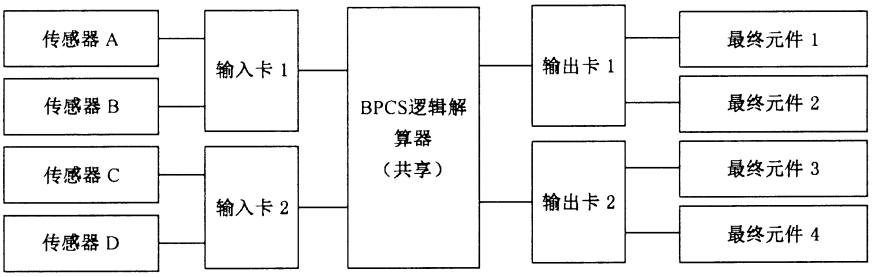


图 A.3　同一场景下共享输入/输出卡的 BPCS 回路

如果初始事件不涉及 BPCS 逻辑解算器失效，每一个回路都满足 IPL 的所有要求，在同一场景下，作为 IPL 的 BPCS 回路不应超过 2 个。如图 A.4 所示，如果所有 4 个回路各自满足相同场景下 IPL 的要求，在使用方法 B 时，通常仅有两个回路被作为 IPL。在使用方法 A 时，只有一个回路被作为独立保护层。

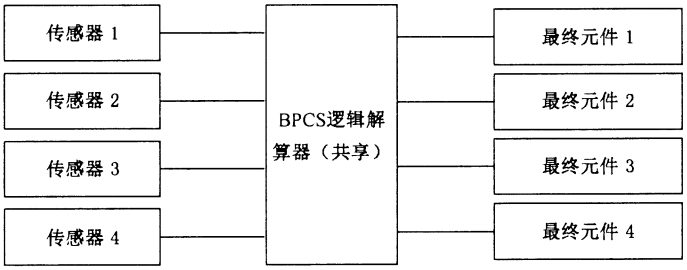


图 A.4　同一场景下 BPCS 功能回路作为 IPL 的最大数量

A.5.3　同一场景下，同一 BPCS 多个功能回路同时作为 IPL 的数据和人员要求

A.5.3.1　对数据与数据分析的要求

方法 B 假设 BPCS 逻辑解算器的 PFD 比 BPCS 回路其他部件的 PFD 至少低两个数量级，应具有支持这个假设的数据，并对数据进行分析。这些数据包括：

a）　BPCS 逻辑解算器、输入/输出卡、传感器、最终元件、人员响应等历史性能数据；

b）　系统制造商提供的数据；

c）　检查、维护和功能性测试数据；

d）　仪表图、管道和仪表流程图(P&ID)、回路图、标准规范等资料；

e）　访问 BPCS，进行程序更改、旁路报警等安全访问 BPCS 的信息。

对这些数据的分析应包括：

a）　计算设备或系统 BPCS 回路组件的有效失效率；

b）　各种组件，特别是 BPCS 逻辑解算器 PFD 数据的比较；

c）　逻辑输入/输出卡及相关回路的独立性评估；

d）　安全访问控制充分性评估；

e）　使用多重 BPCS 回路作为同一场景下的多个 IPL 的合适性评估。

A.5.3.2　对分析人员的要求

分析人员应能够：

a）　判断是否有足够和完整的数据，这些数据是否能满足足够精度的计算；

b） 了解仪表的设计和 BPCS 系统是否满足独立性要求；

c） 理解建议的 IPL 对工艺或系统的影响。

分析小组或人员应具有相关专业知识，如：

a） 对 BPCS 逻辑解算器具有足够低的 PFD 的独立第三方认证；

b） 对历史性能数据和维修记录的分析，建立设计标准使多个 BPCS 回路满足 IPL 的要求；

c） 设计并执行多个 BPCS 回路系统使之满足独立性与可靠性要求等。

如果分析小组或人员不能满足以上要求，那么在判断 BPCS 回路作为 IPL 时，宜使用方法 A 进行分析。

A.6 风险评估与建议矩阵法示例

表 A.9 给出具有不同行动要求的风险矩阵(示例)。表 A.10～表 A.12 给出了数值分析法相关事件的可容许风险(示例)。

表 A.9 具有不同行动要求的风险矩阵(示例)

后果频率	后果等级				
	等级 1	等级 2	等级 3	等级 4	等级 5
10^{0}～10^{-1}	可选择 (评估方案)	可选择 (评估方案)	采取行动 (通知公司)	立即采取行动 (通知公司)	立即采取行动 (通知公司)
10^{-1}～10^{-2}	可选择 (评估方案)	可选择 (评估方案)	可选择 (评估方案)	采取行动 (通知公司)	立即采取行动 (通知公司)
10^{-2}～10^{-3}	不需要采取行动	可选择 (评估方案)	可选择 (评估方案)	采取行动 (通知公司)	采取行动 (通知公司)
10^{-3}～10^{-4}	不需要采取行动	不需要采取行动	可选择 (评估方案)	可选择 (评估方案)	采取行动 (通知公司)
10^{-4}～10^{-5}	不需要采取行动	不需要采取行动	不需要采取行动	可选择 (评估方案)	可选择 (评估方案)
10^{-5}～10^{-6}	不需要采取行动	不需要采取行动	不需要采取行动	不需要采取行动	可选择 (评估方案)
10^{-6}～10^{-7}	不需要采取行动	不需要采取行动	不需要采取行动	不需要采取行动	不需要采取行动

表 A.10 数值分析法——安全与健康相关事件的可容许风险(示例)

严重程度	安全与健康相关的后果	可接受频率 年$^{-1}$
5 级，灾难性的	大范围的人员死亡，重大区域影响	1×10^{-6}
4 级，严重的	人员死亡，大范围的人员受伤和严重健康影响，大的社区影响	1×10^{-5}
3 级，较大的	严重受伤和中等健康损害，永久伤残，大范围的人员轻微伤，小范围的社区影响	1×10^{-4}
2 级，较小的	轻微受伤或轻微的健康影响，药物治疗，超标暴露	1×10^{-2}
1 级，微小的	没有人员受伤或健康影响，包括简单的药物处理	1×10^{-1}

表 A.11　数值分析法——环境相关事件的可容许风险(示例)

严重程度	环境相关的后果	可接受频率 年$^{-1}$
5 级,灾难性的	超过 10 m^3 溢油的环境污染,不可复原的环境影响	1×10^{-5}
4 级,重大的	在 1 m^3～10 m^3 之间的溢油,灾难性的环境影响	1×10^{-4}
3 级,较大的	在 0.1 m^3～1 m^3 之间的溢油,严重的环境影响,大范围的损害	1×10^{-3}
2 级,较小的	在 0.01 m^3～0.1 m^3 之间的溢油,较小的环境影响,暂时的和短暂的	1×10^{-2}
1 级,微小的	小于 0.01 m^3 溢油	1×10^{-1}

表 A.12　数值风险法——财产相关事件的可容许风险(示例)

严重程度	财产相关的后果	可接受频率 年$^{-1}$
5 级,灾难性的	超过 1 000 万元直接财产损失,长时间生产中断	1×10^{-4}
4 级,重大的	在 100 万元～1 000 万元之间的直接财产损失,生产中断	1×10^{-3}
3 级,较大的	在 10 万元～100 万元之间的直接财产损失	1×10^{-2}
2 级,较小的	在 1 万元～10 万元之间的直接财产损失	1×10^{-1}
1 级,微小的	小于 1 万元的直接财产损失	1

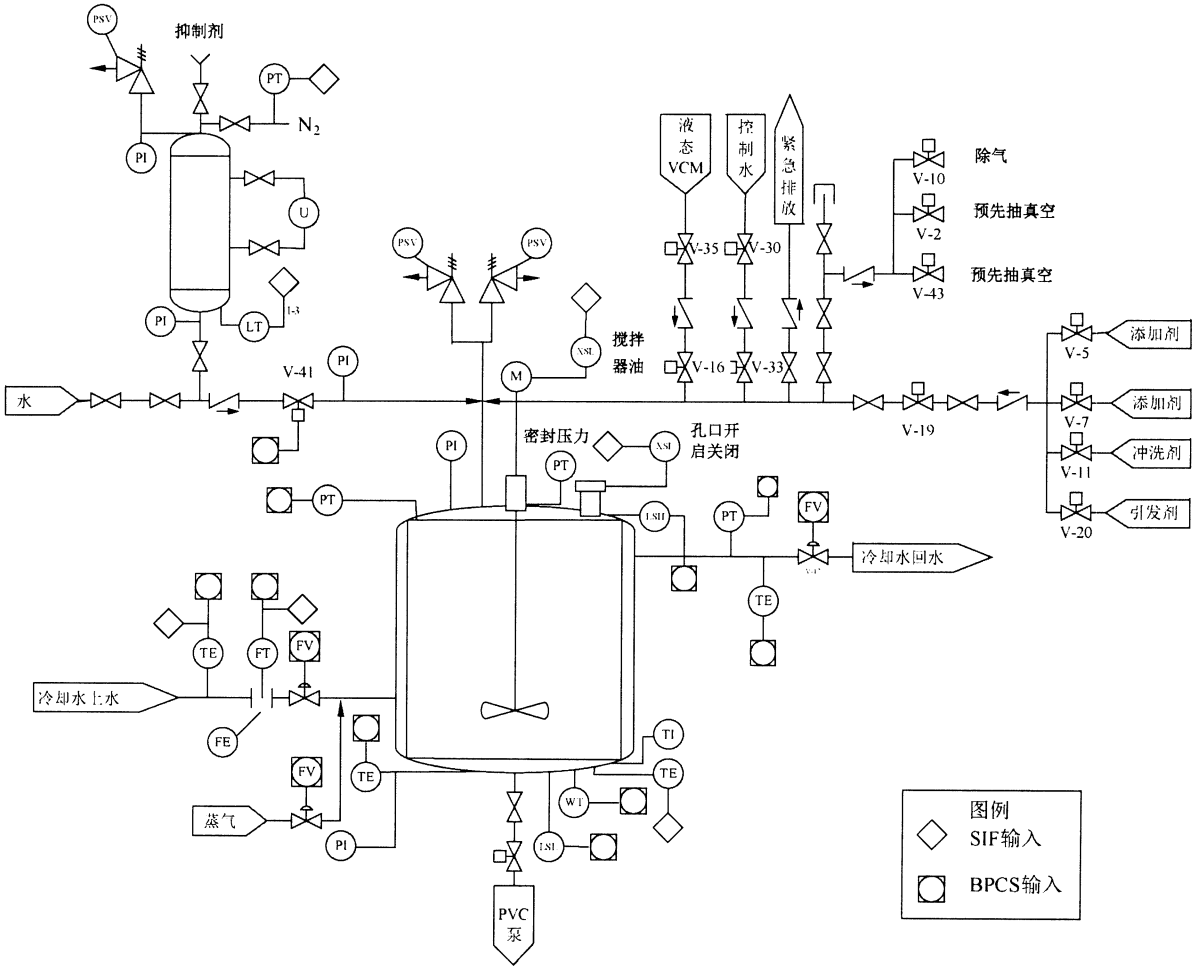
附 录 B
（资料性附录）
反应器系统 LOPA 应用

B.1 简介

本附录用摘选自《化工工艺安全自动化(CCPS,1993b)指南》中的案例来演示 LOPA 的应用。

B.2 问题描述

本附录以图 B.1 中的 P&ID 图为基础进行 LOPA 分析。该工艺为由氯乙烯单体(VCM)转化为聚氯乙烯(PVC)的间歇聚合操作。通过同一喷嘴将水、液态 VCM、引发剂和添加剂加入到带搅拌的夹套反应器中。加料喷嘴还与紧急排气阀和卸压阀(PSV)相连。中止液可通过同一喷嘴加入。



注：一些 SIFs(如火灾、气体和手动跳车)没有绘制出。

图 B.1 简化流程——聚氯乙烯(PVC)的间歇聚合操作流程图

在表 B.1 中列出了所要分析的 8 个场景。表 B.2～表 B.9 包括了针对这些场景的 LOPA 总结表。

表 B.1 安全自动化场景案例

场景	场景描述
场景 1	冷却水故障，反应失控，可能导致反应器超压、泄漏、破裂及人员伤亡
场景 2	搅拌器电机驱动器故障，反应失控，可能导致反应器超压、泄漏、破裂及人员伤亡
场景 3	大范围停电，反应失控，可能导致反应器超压、泄漏、破裂及人员伤亡
场景 4	冷却水泵故障(停电)，反应失控，可能导致反应器超压、泄漏、破裂及人员伤亡
场景 5	人为误操作，催化剂量加倍，反应失控，可能导致反应器超压、泄漏、破裂及人员伤亡
场景 6	BPCS 液位控制功能失效导致反应器满罐，可能导致反应器超压、泄漏、破裂及人员伤亡
场景 7	在点火步骤中 BPCS 温度控制发生故障导致反应器超温，反应失控，可能导致反应器超压、泄漏、破裂及人员伤亡
场景 8	搅拌器密封失效使 VCM 泄漏并诱发着火，爆炸，伤害和死亡的可能性

B.3 问题讨论

使用风险矩阵后果等级和可容许风险，根据场景的顺序进行 LOPA 分析。

a) 可容许风险

评估改造措施时，风险矩阵更加灵活。对于表 A.9 等级 5 的后果，事件频率大于 1×10^{-4} 年$^{-1}$即无法接受，应采取行动对其进行改正。事件频率等于或小于 1×10^{-6} 年$^{-1}$为可接受，无需采取行动。而介于此二者之间的场景则依成本、可行性等允许有一定的灵活性。通用原则为，风险矩阵法要求一个新装置要达到最严格的可容许风险，而对处于灰色安全地带的现役装置，则须进行成本效益分析。

b) 使能事件或使能条件

对于间歇反应器如果其(1)在使用中，(2)初始事件发生，而导致了飞温超压的后果。LOPA 方法假定上述两个条件同时存在的可能性为 0.5。

同样地，加倍注入催化剂量的频率等于每年投料批次乘以催化剂加错的几率。

若我们假定在该过程中出现错误的可能性为 0.01，则加倍注入催化剂量的频率为：

365 天/年×1 批/3 天×0.01= 1.21/年

此处假定每批料仅加一次催化剂，且每批料运转三天。

注：若使用催化剂装填和人为错误的设定值，则此事件的场景确定了泄压系统(SIF)的 PFD。

c) 条件修正因子

在某些使用火灾或死亡频率作为可容许风险的方法中，用条件修正因子对初始事件进行修正从而获得其频率。

d) 独立保护层 IPL

独立保护层应具有：有效性、独立性和可审查性。下面对这几个特性逐步介绍。

1) 有效性

对于多数场景，均建议增加由安全仪表系统(SIS)控制的减压系统(SIF)。反应器顶部管线既用于减压阀和安全阀 PSV 的排放管线，又为反应器添加引发剂、水和添加剂及更重要的中止液的入口管线。这就产生了一个问题，当排气阀或安全阀 PSV 打开时，上述任何一种物料是否能通过该管线同时流入容器，对于许多情景，认为加入中止液为独立保护层 IPL，其中减压系统和 PSV 也是独立保护层 IPL。

这样，也许需要置疑是否能假定加入中止液与通过相同喷嘴进行系统排放将不会同时发生。

因此，使用 LOPA 方法的分析师将会置疑如图 B.1 中配置的放空系统 PSV 和中止液添加系统的有

效性，在建议的管道设计中它们是否都应被视为独立保护层 IPL。

可能会提到的其他问题为：反应器卸压时（采用安全阀 PSV 或排气阀），在管道和阀门是否会出现两相流。

若此情况有可能发生，则应采用 DIERS 或类似技术就尺寸、机械强度及处理问题等进行计算。

在场景 4，操作员有两个操作步骤（打开蒸汽动力冷却水泵及加入中止液）。在本标准中展示的 LOPA 方法中，若操作员在应对报警时效率低下，则其不可能正确执行第二项任务。所以在 LOPA 中，这些行动中仅有一项会被认为是有效的独立保护层 IPL。

在场景 8 中，一个现场通风系统的工艺设计可以认定为一个独立保护层 IPL，因为其可防范因搅拌器轴封故障而导致的 VCM 泄漏。轴封的设计据称可限制可能泄漏的 VCM 最大量，所以通风系统无虞。该排放系统的设计基础是否恰当取决于对轴封执行的分析等级及通风系统风扇等的合理历史故障率。为取得表 B.9 中所示的 LOPA 分析结果，假定独立保护层 IPL 的 PFD 为 1×10^{-1}，尽管该表的一个注释还要求对该 IPL 进行进一步分析。

下面对在场景 8 中反应器区域的低使用率是否应被考虑为独立保护层 IPL 做探讨。

例如，若一个密封面临问题，有可能有人员在附近观察和讨论该密封，或其实际上正在密封上工作。若当时出现破裂，实际上在该区域中可能会比正常情况下有更多的人（注意：至少有一个导致了多人死亡的事故是由于有多人在爆炸源附近正在调查设备故障）。所以将低使用率称为独立保护层 IPL 可能并不恰当。

在表 B.9 所示的 LOPA 分析中，因为上述原因的关系，其不能被视为有效或独立于初始事件之外，因此低使用率并未被视为独立保护层 IPL；此外，对其 PFD 进行量化也比较困难。

在评估操作人员的行为是否是独立保护层 IPL 时也可考虑其行为的有效性。在某些场景下，当搅拌器不运转时，操作员添加中止液，然后采用手动让反应器“冒泡”的方式来混合介质，在 LOPA 分析中，该行动并未被视为独立保护层 IPL。

有效性还包括被称为独立保护层 IPL 的失效概率 PFD。该类的一个例子为对比安全阀 PSV 的分值（PFD=1×10^{-2}）与排气阀 SIF（PFD=1×10^{-3}）的分值。对于此类设备，可能是由于聚合物沉积或排气过程中带有聚合材料而产生的阀门或管道阻塞/冻结的原因，安全阀的 PFD 相对较高。而如果设计正确，SIF 以 1×10^{-3} 的失效概率 PFD，检测操作条件、传送信号并打开排气阀，看起来阀门和管道不大可能比安全阀受阻塞影响的程度低。

若此说法正确，则图 B.1 中所示的设计中安全阀和排气阀的 PFD 均应假定为 1×10^{-2} 是可能的。因为除通用喷嘴外，两个安全阀共享一个共同的入口管线、两个排气阀也共享一个共同的入口管线时，此种假设尤为正确。

2） 独立性

下面讨论独立保护层 IPL 的独立性。一旦认同了使用共同的喷嘴和管道，中止液添加系统、排气系统 SIF 及 PSV 的独立性就要受到挑战。这将导致它们是否均应被视为独立保护层的讨论。

考虑独立性时的另一问题是初始事件与潜在独立保护层之间或相同场景下已确定的独立保护层与另一潜在的独立保护层之间是否有关联。此处的案例为：

场景 4 中单一冷却水低流量报警后，操作员的两个操作步骤（启动蒸汽驱动冷却水泵及加入中止液）来应对报警，在 LOPA 中不能认为是为独立保护层。因为：

若单一低流量报警故障，则两个行动都可能无效，因为操作员可能并不知道冷却水故障。这是通过一个共同传感器而缺乏独立性的一个例证。

若操作员没能圆满完成各项任务中的一项，则不大可能正确执行第二项行动。这是经由最后控制单元（操作员行动）而缺乏独立性的一个例证。

在 LOPA 的基础方法中，若工艺控制系统 BPCS 出现故障，会导致失去执行两个独立保护层行动的能力。在一定场景下，在对工艺控制系统设计和性能有特殊要求时，可在评估该问题时降低保守

程度。

场景 6 中工艺控制系统的液位控制回路故障导致反应器满溢而成为初始事件。在 LOPA 分析中，液位和重量单元报警不能视为独立保护层 IPL，因为若控制系统故障是初始事件，就不允许假定 BPCS 还将保持探测、处理和采取行动(启动警报)以让操作员采取行动的能力。

场景 7 工艺控制系统中的温度控制回路故障成为初始事件。在 LOPA 分析中，不能假定工艺控制系统仍旧能够探测到该情况并警示操作员采取行动，因为工艺控制系统的一部分(初始事件)故障并不能被假定为其可让相同工艺控制系统的另一部分处于可采取有效行动探测、处理和发送信息的状态。这样，初始事件和纠正行为并非是独立的，该行动不能被视为独立保护层。

3) 可审查性

保护系统的详细设计未在 CCPS(1993b)或表 B.2～表 B.9 中直接描述。而确认和审查可能会包括：

- 显示设计基础、管道尺寸选择方法(即 DIERS)、水力和机械计算(或其参考)(CCPS 1998b)的 PSV 汇总表；
- 工艺设计依据，能证明针对该场景而选择的设计方案的原因，并提供所需的模型、VLE、反应动力学等以支持该结论；
- 工艺控制系统和安全仪表的设计细节；
- SIF 设计细节以证明所称 PFD 值是恰当的；
- 所要求的检查、测试和维护程序细节；
- 检查、测试和维护频率和结果的记录文件。

B.4 供考虑的设计改进

本章对图 B.1 所示的设计提出了改进意见，这些改变包括对 IPL 的数量及其 PFD 造成的影响。这些均基于表 B.2～表 B.9 所示的 LOPA 分析。

a) PSV 系统的改进

此处建议改进管道系统以使每个 PSV 均通过其自己的喷嘴和管道系统与反应器相连。这将确保 PSV 和中止液注入系统的独立性，消除在正常操作或排放动作过程中单个喷嘴被聚合物阻塞而使 PSV 失效的可能性。

还应考虑在 PSV 增加氮气吹扫以将管道中或阀门入口处的聚合物沉积/冻结的可能性降至最低。若还未曾考虑，应采用 DIERS 技术确定在排放过程中管道和阀门中是否会出现两相流。如果可行，应参照《卸压和排放液处理系统指南》设计管道和阀门。这些改变将使 PSV 和中止液系统被视为 IPL。通过建议的管道改进和氮气吹扫的加入——若恰当且实用，PSV 系统的 PFD 很可能会显著改善。

b) 排气阀 SIF 系统的改进

对 PSV 系统设计的相同改进也适用于排气阀 SIF 系统。这样，就要求在反应器顶部还需有两个新喷嘴。也需考虑在两相流、聚合等方面的相同设计问题。

这些改进都会使排气阀 SIF 系统和中止液添加系统被视为 IPL。假定的 PSV 的 PFD 及可容许风险决定了 SIF 系统的 PFD。系统的最终设计(传感器数量、最终控制元素、处理系统类型、测试频率和类型等)将由该 IPL 所要求的 PFD 决定。

举个例子，若在每批料之间测试完整的排气阀 IPL(从信号探测到排气阀打开)，则对于所给出的设计，测试时间会很短，且与每年才测试一次的相同设计相比，会有改善。既要考虑频繁测试的实用性、成本和人力，也应考虑简易系统的低成本。

c) 人为独立保护层

除非分析证明传感器、报警器和操作员是独立的，对于每一种场景来说，人为行动仅可被用作一道

IPL。应有足够的培训、测试和程序，才能将人作为 IPL。

表 B.2　场景 1 分析案例

场景编号：1	设备编号：	场景名称：冷却水故障引起反应失控，可能导致反应器超压、泄漏、破裂及人员伤亡。假定有搅拌		
日期：		描述	概率	频率 $年^{-1}$
后果描述/等级		反应器失控和可能导致反应器超压、泄漏、破裂及人员伤亡 后果等级 5		
可容许风险 （分类/频率）		不可接受（大于）		1×10^{-4}
		可接受（小于或等于）		1×10^{-6}
初始事件（频率）		冷却水故障停		1×10^{-1}
使能事件或使能条件		反应器处于因冷却失效而出现失控反应条件下的概率（以年为基础）	0.5 （每个反应器）	
条件修正 （如果适用）		着火的概率	N/A	
		影响区域内人员存在概率	N/A	
		死伤概率	N/A	
		其他	N/A	
减缓前的后果频率				5×10^{-2}
独立保护层				
BPCS 报警和人为动作		当反应器温度高报时，添加中止液	1×10^{-1}	
泄压阀		对系统进行改进（见行动项）	1×10^{-2}	
SIF（要求 PFD＝1×10^{-3}）（对于反应器是部分 SIS）		SIF 打开放空阀，场景 5 确定了其 PFD 值	1×10^{-3}	
防护措施（非独立保护层）		操作员行动（同一操作员的其他操作步骤不独立于报警和人为动作）。 紧急冷却水系统（汽轮机）。未记为 IPL，因为有太多共同因素（管道、阀门、护套等）都可能已启动了初始冷却水故障		
所有独立保护层总 PFD			1×10^{-6}	
减缓后的后果频率				5×10^{-8}
是否满足可容许风险？（是/否）		是 但应增加 SIF（安全仪表功能）系统		
满足可容许风险需要采取的行动		在反应器上安装 SIS。SIF 的最低 PFD 为 1×10^{-3}，为高温打开放空阀；每个放空阀有独立进出管线，每个 PSV 安装独立的泄压管线以最大限度地减少堵塞；考虑 N_2 吹扫所有的放空阀和 PSV		
备注		确保操作员对高温报警的反应速度及应对符合 IPL 的要求，确保 RV 的设计、安装和维修，符合要求 PFD1$\times10^{-2}$。若有更高的安全要求，则考虑提高放空阀 SIF 的 PFD		

注：N/A 表示不适用。

表 B.3　场景 2 分析案例

场景编号:2	设备编号:	场景名称:搅拌器电动机故障,反应失控、可能导致反应器超压、泄漏、破裂及人员伤亡		
日期:		描述	概率	频率 年$^{-1}$
后果描述/等级		反应器失控和可能导致反应器超压、泄漏、破裂及人员伤亡 后果等级 5		
风险承受能力 (分类或频率)		不可接受(大于)		1×10^{-4}
		可以接受(小于或等于)		1×10^{-6}
初始事件 (一般给出频率)		出现搅拌器电机故障的频率		1×10^{-1}
使能事件或使能条件		反应器处于因冷却失效而出现失控反应条件下的概率(以年为基础)	0.5 (每个反应器)	
条件修正 (如果适用)		着火的概率	N/A	
		影响区域内人员存在概率	N/A	
		死伤概率	N/A	
		其他	N/A	
减缓前的后果频率				5×10^{-2}
独立保护层				
泄压阀		要修改系统	1×10^{-2}	
SIF 要求 PFD=1×10^{-3})(对于反应器是部分 SIS)		SIF 打开放空阀,场景 5 确定了其 PFD 值	1×10^{-3}	
防护措施(非独立保护层)		操作员干预(保护反应器和注中止液的操作步骤非常复杂) 紧急冷却系统(停电时搅拌器停,使得冷却无效)		
所有独立保护层总 PFD			1×10^{-5}	
减缓后的后果频率				5×10^{-7}
是否满足可容许风险?(是/否)		是 但应增加 SIF(安全仪表功能)系统		
满足可容许风险需要采取的行动		在反应器上安装 SIS。SIF 的最低 PFD 为 1×10^{-3},为高温打开放空阀;每个放空阀有独立进出管线,每个 PSV 安装独立的泄压管线以最大限度地减少堵塞;考虑 N_2 吹扫所有的放空阀和 PSV		
备注		确保操作员对高温报警的反应速度及应对符合 IPL 的要求,确保 RV 的设计、安装和维修,符合要求 PFD1$\times10^{-2}$。若有更高的安全要求,则考虑提高放空阀 SIF 的 PFD		

注:N/A 表示不适用。

表 B.4　场景 3 分析案例

场景编号:3	设备编号:	场景名称:停电(大面积),可能导致反应器超压、泄漏、破裂及人员伤亡		
日期:		描述	概率	频率 $年^{-1}$
后果描述/等级		反应器失控和可能出现的反应器超压、渗漏、破裂及人员伤亡 后果等级 5		
风险承受能力 (分类或频率)		不可接受(大于)		1×10^{-4}
		可以接受(小于或等于)		1×10^{-6}
初始事件 (一般给出频率)		出现停电(大面积)		1×10^{-1}
使能事件或使能条件		反应器处于因冷却失效而出现失控反应条件下的概率(以年为基础)	0.5 (每个反应器)	
条件修正 (如果适用)		着火的概率	N/A	
		影响区域内人员存在概率	N/A	
		致死概率	N/A	
		其他	N/A	
减缓前的后果频率				5×10^{-2}
独立的保护层				
泄压阀		要修改系统	1×10^{-2}	
SIF		SIF 打开放空阀,场景 5 确定了其 PFD 值	1×10^{-3}	
防护措施(非独立保护层)		操作员干预(保护反应器和注中止液的操作步骤非常复杂) 紧急冷却系统(停电时搅拌器停,使得冷却无效)		
所有独立保护层总 PFD			1×10^{-5}	
减缓后的后果频率				5×10^{-7}
是否满足可容许风险?(是/否)		是 但应增加 SIF(安全仪表功能)系统		
满足可容许风险需要采取的行动		在反应器上安装 SIS。SIF 的最低 PFD 为 1×10^{-3},为高温打开放空阀;每个放空阀有独立进出管线,每个 PSV 安装独立的泄压管线以最大限度地减少堵塞;考虑 N_2 吹扫所有的放空阀和 PSV		
备注		确保操作员对高温报警的反应速度及应对符合 IPL 的要求,确保 RV 的设计、安装和维修,符合要求 PFD1 $\times10^{-2}$。若有更高的安全要求,则考虑提高放空阀 SIF 的 PFD		

注: N/A 表示不适用。

表 B.5　场景 4 分析案例

场景编号:4	设备编号:	场景名称:冷却水泵(电机停)故障,反应失控,可能导致反应器超压、泄漏、破裂及人员伤亡		
日期:		描述	概率	频率 年$^{-1}$
后果描述/等级		反应器失控和可能出现的反应器超压、渗漏、破裂及人员伤亡 后果等级 5		
风险承受能力 (分类或频率)		不可接受(大于)		1×10^{-4}
		可以接受(小于或等于)		1×10^{-6}
初始事件 (一般给出频率)		出现冷却水泵(电机停)的频率		1×10^{-1}
使能事件或使能条件		出现反应器无冷却的概率	0.5 (每个反应器)	
条件修正 (如果适用)		着火的概率	N/A	
		影响区域内人员存在概率	N/A	
		致死概率	N/A	
		其他	N/A	
减缓前的后果频率				5×10^{-2}
独立的保护层				
BPCS 报警和人为动作		当反应器温度高报时,添加中止液,或冷却水流量低时启动透平泵	1×10^{-1}	
泄压阀		修正系统	1×10^{-2}	
SIF		SIF 打开放空阀,场景 5 确定了其 PFD 值	1×10^{-3}	
防护措施(非独立保护层)		操作员干预(因为不同的保护层由共同的操作员、报警和感应器完成,操作员有两个操作步骤,只有一步是 IPL)		
所有独立保护层总 PFD			1×10^{-6}	
减缓后的后果频率				5×10^{-8}
是否满足可容许风险?(是/否)		是 但应增加 SIF(安全仪表功能)系统		
满足可容许风险需要采取的行动		在反应器上安装 SIS。SIF 的最低 PFD 为 1×10^{-3},为高温打开放空阀;每个放空阀有独立进出管线,每个 PSV 安装独立的泄压管线以最大限度地减少堵塞;考虑 N_2 吹扫所有的放空阀和 PSV		
备注		确保操作员对高温报警的反应速度及应对符合 IPL 的要求,确保 RV 的设计、安装和维修,符合要求 PFD1$\times10^{-2}$。若有更高的安全要求,则考虑提高放空阀 SIF 的 PFD		

注:N/A 表示不适用。

表 B.6　场景 5 分析案例

场景编号:5	设备编号:	场景名称:人为误操作催化剂,可能导致反应器超压、泄漏、破裂及人员伤亡		
日期:		描述	概率	频率 年$^{-1}$
后果描述/等级		反应器失控和可能出现的反应器超压、渗漏、破裂及人员伤亡 后果等级 5		
风险承受能力 (分类或频率)		不可接受(大于)		1×10^{-4}
		可以接受(小于或等于)		1×10^{-6}
初始事件 (一般给出频率)		添加催化剂(每 3 天 1 次——每年 121 次)的频率		121
使能事件或使能条件		操作员添加 2 次催化剂的概率	1×10^{-2}	
条件修正 (如果适用)		着火的概率	N/A	
		影响区域内人员存在概率	N/A	
		致死概率	N/A	
		其他	N/A	
减缓前的后果频率				1.21
独立的保护层				
BPCS 报警和人为动作		当反应器温度高报时,添加中止液	1×10^{-1}	
泄压阀		要修改系统	1×10^{-2}	
SIF		SIF 打开放空阀,场景 5 确定了其 PFD 值	1×10^{-3}	
防护措施(非独立保护层)		操作员干预(不能作为独立保护)(不独立于 BPCS 感应器、报警、FCE) 操作员的失误作为初始事件		
所有独立保护层总 PFD			1×10^{-6}	
减缓后的后果频率				1.21×10^{-6}
是否满足可容许风险?(是/否)		是 但应增加 SIF(安全仪表功能)系统		
满足可容许风险需要采取的行动		在反应器上安装 SIS。SIF 的最低 PFD 为 1×10^{-3},为高温打开放空阀;每个放空阀有独立进出管线,每个 PSV 安装独立的泄压管线以最大限度地减少堵塞;考虑 N_2 吹扫所有的放空阀和 PSV		
备注		确保操作员对高温报警的反应速度及应对符合 IPL 的要求,确保 RV 的设计、安装和维修,符合要求 PFD1 $\times10^{-2}$。若有更高的安全要求,则考虑提高放空阀 SIF 的 PFD		

注: N/A 表示不适用。

表 B.7　场景 6 分析案例

场景编号:6	设备编号:	场景名称:BPCS 控制功能失效导致反应器满罐,可能导致反应器超压、泄漏、破裂及人员伤亡		
日期:		描述	概率	频率 年$^{-1}$
后果描述/等级		反应器满罐导致反应器可能出现超压、法兰渗漏、破裂及人员伤亡 后果等级 5		
风险承受能力 (分类或频率)		不能承受的频率(大于)		1×10^{-4}
		可以承受的频率(小于或等于)		1×10^{-6}
初始事件 (一般给出频率)		出现 BPCS 控制功能失效的频率		1×10^{-1}
使能事件或使能条件		反应器无冷却导致反应失控的概率	0.5 (每年)	
条件修正 (如果适用)		着火的概率	N/A	
		影响区域内人员存在概率	N/A	
		致死概率	N/A	
		其他	N/A	
减缓前的后果频率				5×10^{-2}
独立的保护层				
泄压阀		修正系统	1×10^{-2}	
SIF		SIF 打开放空阀,场景 5 确定了其 PFD 值	1×10^{-3}	
防护措施(非独立保护层)		操作员干预(不独立于 BPCS 感应器、报警 FCE) BPCS 添加抑制和冷却水系统回路(不独立于初始事件)		
所有独立保护层总 PFD			1×10^{-5}	
减缓后的后果频率				5×10^{-7}
是否满足可容许风险?(是/否)		是 但应增加 SIF(安全仪表功能)系统		
满足可容许风险需要采取的行动		在反应器上安装 SIS。SIF 的最低 PFD 为 1×10^{-3},为高温打开放空阀;每个放空阀有独立进出管线,每个 PSV 安装独立的泄压管线以最大限度地减少堵塞;考虑 N_2 吹扫所有的放空阀和 PSV		
备注		确保操作员对高温报警的反应速度及应对符合 IPL 的要求,确保 RV 的设计、安装和维修,符合要求 PFD1$\times10^{-2}$。若有更高的安全要求,则考虑提高放空阀 SIF 的 PFD		

注:N/A 表示不适用。

表 B.8　场景 7 分析案例

场景编号:7	设备编号:	场景名称:BPCS 温度控制发生故障导致反应器超温,可能导致反应器超压、泄漏、破裂及人员伤亡		
日期:		描述	概率	频率 年$^{-1}$
后果描述/等级		反应器失控和可能出现的反应器超压、渗漏、破裂及人员伤亡 后果等级 5		
风险承受能力 (分类或频率)		不可接受(大于)		1×10^{-4}
		可以接受(小于或等于)		1×10^{-6}
初始事件 (一般给出频率)		BPCS 温度控制的频率		1×10^{-1}
使能事件或使能条件		反应器无冷却导致反应失控的概率	0.5 (每个反应器)	
条件修正 (如果适用)		着火的概率	N/A	
		影响区域内人员存在概率	N/A	
		致死概率	N/A	
		其他	N/A	
减缓前的后果频率				5×10^{-2}
独立的保护层				
泄压阀		要修改系统	1×10^{-2}	
SIF		SIF 打开放空阀,场景 5 确定了 PFD 值 SIF 添加紧急冷却水	1×10^{-3} 1×10^{-1}	
防护措施(非独立保护层)		操作员干预(不独立于 BPCS 感应器、报警 FCE) BPCS 添加抑制和冷却水系统回路(不独立于初始事件)		
所有独立保护层总 PFD			1×10^{-6}	
减缓后的后果频率				5×10^{-8}
是否满足可容许风险?(是/否)		是 但应增加 SIF(安全仪表功能)系统		
满足可容许风险需要采取的行动		在反应器上安装 SIS。SIF 的最低 PFD 为 1×10^{-3},为高温打开放空阀;每个放空阀有独立进出管线,每个 PSV 安装独立的泄压管线以最大限度地减少堵塞;考虑 N_2 吹扫所有的放空阀和 PSV		
备注		确保操作员对高温报警的反应速度及应对符合 IPL 的要求,确保 RV 的设计、安装和维修,符合要求 PFD1$\times10^{-2}$。若有更高的安全要求,则考虑提高放空阀 SIF 的 PFD		

注:N/A 表示不适用。

表 B.9　场景 8 分析案例

场景编号:8	设备编号:	场景名称:搅拌器密封失效使 VCM 泄漏并诱发着火、爆炸及人员伤亡		
日期:		描述	概率	频率 年$^{-1}$
后果描述/等级		搅拌器密封泄漏(在大气压以下有 50 kg～500 kg 可燃物),可能造成及人员伤亡 后果等级 3		
风险承受能力 (分类或频率)		不可接受(大于)		1×10^{-1}
		可以接受(小于或等于)		1×10^{-4}
初始事件 (一般给出频率)		密封故障		1×10^{-1}
使能事件或使能条件				
条件修正 (如果适用)		着火的概率	N/A	
		影响区域内人员存在概率	N/A	
		致死概率	N/A	
		其他	N/A	
减缓前的后果频率				1×10^{-1}
独立的保护层				
搅拌器轴封的现场通风系统			1×10^{-1}	
SIF		SIF 打开放空阀,场景 5 确定了 PFD 值	1×10^{-3}	
防护措施(非独立保护层)		操作员干预(不独立于 BPCS 感应器、报警 FCE) 密封部位的可燃气检测仪(事后的补救措施且无法定量确定其效果)		
所有独立保护层总 PFD			1×10^{-4}	
减缓后的后果频率				1×10^{-5}
是否满足可容许风险?(是/否)		是 但应增加 SIF(安全仪表功能)系统		
满足可容许风险需要采取的行动		在反应器上安装 SIS。SIF 的最低 PFD 为 1×10^{-3},为高温打开放空阀;每个放空阀有独立进出管线,每个 PSV 安装独立的泄压管线以最大限度地减少堵塞;在搅拌器轴承密封处放空可有效将泄漏介质排放以避免火灾;考虑 N_2 吹扫所有的放空阀和 PSV		
备注				

注:N/A 表示不适用。

附 录 C
（资料性附录）
LOPA 方法在 SIL 定级中的应用

C.1 LOPA 示例一

LOPA 示例一见表 C.1。

表 C.1 LOPA 示例一

P&ID 图号				LOPA-SAMPLE -DW-001-6 REV.3C											
SIF 编号				I-1234											
SIF 功能描述				PAHH 1001 压力高高触发联锁 I-1234 关断 TSSV-0051/ 0052 以避免下游管线及设备超压											
影响事件描述				下游管线及设备可能超压，引起管线破裂，从而导致天然气泄漏至外部环境，潜在火灾爆炸危害											
编号	初始事件	后果分类	严重程度	初始事件频率	条件修正		独立保护层			减缓后频率	可容许后果频率	目标 SIL 等级	备注	建议	责任方
					描述	概率	类型	描述	PFD						
1	FIC 0001/ PIC 0002 串级回路故障（PV 开度过大）	人员	5 级	1×10^{-1}	使用率		基本设计	N/A		1×10^{-3}	1×10^{-6}	3	管线上设置的安全泄放阀泄放管径核算时未考虑调压回路失效的影响，不能作为独立保护层考虑		
					人员暴露概率	0.2	工艺流程控制系统	N/A							
					点燃概率	0.5	报警及操作人员响应	PAH 0003 压力高报警可以提示操作人员及时切换另一条压力控制回路	1×10^{-1}						
							其他减缓措施，限制人员进入等	N/A							
注：N/A 表示不适用。															

C.2 LOPA 示例二

LOPA 示例二见表 C.2。

表 C.2 LOPA 示例二

场景	影响事件			初始事件		条件事件/条件修正		未减缓后果频率	安全措施（非独立保护层）	独立保护层				减缓后后果频率	风险可容许标准		建议措施
	描述	类别	严重程度	描述	初始事件发生频率	描述	概率			类型	描述	PFD	所有独立保护层总 PFD		频率	差距	
反应器夹套冷却水温度过高	聚合反应器温度、压力上升，可能飞温，形成堵塞，可能造成装置停车约2周	经济损失	3级	夹套冷却水冷媒控制回路失效（冷媒控门开度过大）	1×10^{-1}	使用率		1×10^{-1}	夹套冷却水冷媒低流量报警（因为冷媒流量控制回路失效是初始事件，所以其为非独立保护层）	基本设计	N/A		1×10^{-2}	1×10^{-3}	1×10^{-4}	1×10^{-1}	考虑将反应器温度高高联锁功能安全性等级提升为SIL 2级以满足风险可容许标准的要求
						点火概率	N/A			工艺流程控制系统	N/A						

表 C.2（续）

场景	影响事件			初始事件		条件事件/条件修正		未减缓后果频率	安全措施（非独立保护层）	独立保护层				减缓后后果频率	风险可容许标准		建议措施
	描述	类别	严重程度	描述	初始事件发生频率	描述	概率			类型	描述	PFD	所有独立保护层总PFD		频率	差距	
						人员暴露概率	N/A			报警及操作人员响应	反应器夹套冷却水温差报警及人员响应	1×10^{-1}					
										其他减缓措施，限制人员进入等	N/A						

表 C.2（续）

场景	影响事件			初始事件		条件事件/条件修正		未减缓后果频率	安全措施（非独立保护层）	独立保护层				减缓后后果频率	风险可容许标准		建议措施
	描述	类别	严重程度	描述	初始事件发生频率	描述	概率			类型	描述	PFD	所有独立保护层总PFD		频率	差距	
										其他独立保护层，安全泄放阀等	反应器温度高高触发联锁注入中止剂停止反应，SIF回路SIL等级为1	1×10^{-1}					

注： N/A 表示不适用。

附 录 D
（资料性附录）
高要求模式后果发生频率计算示例

D.1 概述

式(1)仅适用于低要求模式，对于高要求模式如果采用此公式将导致不精确的后果发生频率值，一般情况下会计算出一个远大于实际后果发生频率的数值。本附录采用一种近似的方法计算高要求模式下的后果发生频率。

D.2 单个 IPL 下的后果发生频率计算

D.2.1 单个 IPL 的失效频率可以获得时

在高要求模式下，对于只有一个 IPL，假如有这一个 IPL 的失效频率时，计算公式如式(D.1)：

$$f_i^{\mathrm{C}} = f_i^{\mathrm{IPL}_{-}i1} \times P_i^{\mathrm{C}} \quad \cdots\cdots\cdots\cdots\cdots\cdots (\mathrm{D.1})$$

式中：

f_i^{C} ——初始事件 i 造成后果 C 的频率，单位为次每年；

$f_i^{\mathrm{IPL}_{-}i1}$——对于初始事件 i，单个 IPL 对后果 C 防护的失效频率，单位为次每年；

P_i^{C} ——条件修正因子，假如没有任何条件修正，则 P_i^{C} 取 1。

D.2.2 单个 IPL 的失效频率未能获得时

高要求模式下，对于只有一个 IPL，且没有这一个 IPL 的失效频率时，由于 IPL 的 PFD 通常方便查找，则可以用简化公式式(D.2)替代：

$$f_i^{\mathrm{C}} = 2 \times \text{IPL 检验测试频率(次 / 年)} \times \text{IPL 的 PFD} \times P_i^{\mathrm{C}} \quad \cdots\cdots\cdots\cdots\cdots\cdots (\mathrm{D.2})$$

D.3 多个 IPL 下的后果发生频率计算

对于有多个 IPL 的高要求模式，且第 1 个 IPL 的失效频率可以获得，则使用第一个 IPL 的失效频率作为经过使能事件或条件修正过的初始事件的发生频率，即带入式(1)，即替代 $f_i^{\mathrm{I}} \times P_i^{\mathrm{E}}$ 进行计算，此时需要忽略第一个 IPL 的 PFD。假如第 1 个 IPL 的失效频率无法获得，则可以用 2×(第一个 IPL 检验测试频率，次/年)×(第一个 IPL 的 PFD)替代经过使能事件或条件修正过的初始事件的发生频率，即带入式(1)替代 $f_i^{\mathrm{I}} \times P_i^{\mathrm{E}}$ 进行计算，此时需要忽略第一个 IPL 的 PFD。

附 录 E
（资料性附录）
LOPA 分析表（示例）

本标准的 6.6 介绍了两种方法进行风险评估与建议，包括矩阵法和数值风险法。表 E.1 为风险矩阵法风险分析示例，表 E.2 为数值风险法风险分析示例。

表 E.1 风险矩阵法风险分析（示例）

场景编号：1	设备编号：T201	场景名称：正己烷缓冲罐溢流，溢流物溢出防火堤	
日期：2010 年 6 月 7 日	描述	概率	频率 年$^{-1}$
后果描述/分类	释放正已烷（500 kg～5 000 kg），由于溢流和防火堤失效，正已烷溢出防火堤，后果等级为 4		
可容许风险（分类/频率）	不可接受（大于）		$>1\times10^{-3}$
	可以接受（小于或等于）		$<1\times10^{-5}$
初始事件 （一般给出频率）	BPCS LIC 控制回路故障（PFD 来自××）		1×10^{-1}
使能事件或使能条件	无	N/A	
条件修正 （如果适用）	点火概率	N/A	
	影响区域内人员存在概率	N/A	
	致死概率	N/A	
	其他	N/A	
减缓前的后果频率			1×10^{-1}
独立保护层	防火堤（PFD 来自×××）	1×10^{-2}	
	安全仪表功能 SIF（将要增加——见采取的行动）	1×10^{-2}	
	无	N/A	
非独立保护层	LIC 液位控制回路不作为 IPL，因为 LIC 液位控制回路故障是初始事件，因此不能作为 IPL		
	无		
	无		
所有独立保护层总 PFD	两个独立保护层	1×10^{-4}	
减缓后的后果频率			1×10^{-5}
是否满足可容许风险？（是/否）：是，但应增加一个安全仪表功能（SIF）			
满足可容许风险需要采取的行动	增加一个 PFD 为 1×10^{-2} 的 SIF，负责人员为王号，完成日期为 2010 年 7 月 30 日		
备注	把增加此 SIF 的行动加到公司隐患整改跟踪表中		

表 E.1（续）

场景编号：1	设备编号：T201	场景名称：正己烷缓冲罐溢流，溢流物溢出防火堤	
日期：2010 年 6 月 7 日	描述	概率	频率 年$^{-1}$
参考资料(PHA 报告，P&ID 等)：2005 年 PHA 报告，P&ID 号：BD-DWG-DPPB-PR-0203			
LOPA 分析人员：王号，李波，万彬			
注：N/A 表示不适用。			

表 E.2　数值风险法风险分析(示例)

场景编号：1	设备编号：T201	场景名称：正己烷缓冲罐溢流，溢流物溢出防火堤	
日期：2010 年 6 月 7 日	描述	概率	频率 年$^{-1}$
后果描述/分类	由于溢流和防火堤失效，正己烷溢出防火堤，遇到点火源，造成火灾，导致人员死亡		
可容许风险(分类/频率)	容许频率(数据取自表 A.10)		$<1\times10^{-5}$
初始事件 (一般给出频率)	由于库存量控制失效，导致槽车向空间不足的储罐卸货(库存量控制失效频率基于工厂历史数据)		1
使能事件或使能条件	无	N/A	
条件修正 (如果适用)	点火概率(数据为工厂经验)	1	
	影响区域内人员存在概率(数据基于工厂运行情况)	0.5	
	致死概率(数据为工厂经验)	0.5	
	其他	N/A	
减缓前的后果频率			0.25
独立保护层	卸货前，操作工检查就地液位计(PFD 来自表×××)	1×10^{-1}	
	防火堤(PFD 来自×××)	1×10^{-2}	
	安全仪表功能 SIF(将要增加——见采取的行动)	1×10^{-2}	
非独立保护层	LIC 液位控制回路不作为 IPL，因为 LIC 液位控制回路故障是初始事件，因此不能作为 IPL		
	无		
	无		
所有独立保护层总 PFD	两个独立保护层	1×10^{-5}	

表 E.2（续）

场景编号：1	设备编号：T201	场景名称：正己烷缓冲罐溢流，溢流物溢出防火堤	
日期：2010 年 6 月 7 日	描述	概率	频率 年$^{-1}$
减缓后的后果频率			2.5×10^{-6}
是否满足可容许风险？（是/否）：是，但应增加一个安全仪表功能（SIF）			
满足可容许风险需要采取的行动	增加一个 PFD 为 1×10^{-2} 的 SIF，负责人员为王号，完成日期为 2010 年 7 月 30 日		
备注	把增加此 SIF 的行动加到公司隐患整改跟踪表中		
参考资料（PHA 报告，P&ID 等）：2005 年 PHA 报告，P&ID 号：BD-DWG-DPPB-PR-0203			
LOPA 分析人员：王号，李波，万彬			
注：N/A 表示不适用。			

参 考 文 献

[1] GB/T 21109—2007 过程工业领域安全仪表系统的功能安全

[2] Layer of protection analysis_ simplified process risk assessment.New York,2001

[3] 化工工艺安全自动化(CCPS,1993b)指南