ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 32857—2025
代替 GB/T 32857—2016

保护层分析(LOPA)应用导则

Application directives for layer of protection analysis(LOPA)

2025-12-02 发布　　2026-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 32857—2016《保护层分析（LOPA）应用指南》，与 GB/T 32857—2016 相比，除结构调整和编辑性改动外，主要技术变化如下：

——增加了条件修正因子（见 3.2）、原始风险（见 3.5）、中间事件（见 3.7）、残余风险（见 3.12）、风险点（见 3.13）、风险降低因子（见 3.14）、复合场景（见 3.16）、安全仪表功能（见 3.17）、（SIF 的）运行模式（见 3.20）、安全关键动作（见 3.21）等 10 个术语和定义；

——更改了基本过程控制系统（见 3.1，2016 年版的 3.1.2）、使能事件或使能条件（见 3.4，2016 年版的 3.1.12）、初始事件（见 3.6，2016 年版的 3.1.5）、保护层分析（见 3.8，2016 年版的3.1.1）、保护层（见 3.9，2016 年版的 3.1.3）、独立保护层（见 3.10，2016 年版的 3.1.7）、安全完整性等级（见 3.18，2016 年版的 3.1.11）、安全仪表系统（见 3.19，2016 年版的 3.1.13）、可容忍风险（见 3.22，2016 年版的 3.1.18）等 9 个术语和定义；

——删除了事件（见 2016 年版的 3.1.4）、频率（见 2016 年版的 3.1.6）、共因失效（见 2016 年版的 3.1.14）等 3 个术语和定义；

——增加了保护层分析（LOPA）的基本要求（见 5.2）、应用范围（见 5.3）、人员要求（见 5.4）；

——增加了在工程实践中 LOPA 可选择单一场景分析法或复合场景分析法的描述及适用情况（见第 6 章）；

——增加了风险点识别的来源（见 7.1）；

——更改了场景识别的来源（见 7.2.2，2016 年版的 6.1.2）、场景筛选的规则（见 7.2.3，2016 年版的 6.1.3）；

——增加了场景补充要求（见 7.2.4）；

——更改了后果及严重性评估的要求（见 7.3，2016 年版的 6.2）；

——更改了初始事件分类（见表 1，2016 年版的表 2）；

——增加了初始事件频率确认依据（见 7.4.3）；

——增加了使能条件确认要求（见 7.5）；

——增加了条件修正因子确认要求（见 7.6）；

——更改了独立保护层识别要求（见 7.7.1，2016 年版的 6.4.3）和独立保护层 PFD 的确认要求（7.7.2，2016 年版的 6.4.4）；

——更改了单一场景分析法后果频率的计算（见 7.8，2016 年版的 6.5）；

——增加了复合场景分析法后果频率的计算（见 7.9）；

——更改了风险评估与建议的内容（见 7.10，2016 年版的 6.6）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国机械工业联合会提出。

本文件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。

本文件起草单位：机械工业仪器仪表综合技术经济研究所、中石化国家石化项目风险评估技术中心有限公司、中国寰球工程有限公司、南京南瑞继保工程技术有限公司、中科合成油技术有限公司、北京风

控工程技术股份有限公司、天津保泰安全技术服务有限公司、北京联合普肯工程技术股份有限公司。

本文件主要起草人：刘瑶、帅冰、王建伟、王雪梅、范咏峰、袁小军、孙舒、朱明露、施隋靖、娄清辉、肖松青、乔靖玉、史学玲、程泱、包伟华、张少华、刘飞舟、姜巍巍、张武涛、葛春涛、徐德腾、孙勇、吕峰、马欣欣、妥少辉、韩占武、杨柳、李秋娟、刁宇、朱旭营、王杰、张炜、赵俊丹、赵焱、薛永刚、张雪、朱弘毅、王哲蓓、刘万里、孙爱、熊文泽。

本文件及其所代替文件的历次版本发布情况为：

——2016 年首次发布为 GB/T 32857—2016；

——本次为第一次修订。

引　言

本文件的目的是描述保护层分析(LOPA)的原理和分析过程,为应用 LOPA 方法开展危险分析与风险评估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估方法,它通过分析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可容忍风险标准所要求的水平。它的优点如下。

- 与定性方法相比较,LOPA 可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,可应用 LOPA 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 是安全完整性等级(SIL)的重要评估工具,与图表法相比较,LOPA 可提供更加准确的结果。
- 通过 LOPA,可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,可选择更加经济合理的保护措施来降低风险。
- LOPA 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 LOPA,可发现可行方案,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 方法,作为一种简化的半定量的风险评估方法,使得对场景的分析比其他定量风险分析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,并且将其与可容忍风险比较,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 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 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 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估方法既可以减少定性分析方法的主观性,又较定量分析方法更容易实行,在风险评估中越来越广泛地被应用。

保护层分析(LOPA)应用导则

1 范围

本文件规定了保护层分析(LOPA)的一般要求、基本程序、分析过程以及文档要求。

本文件适用于指导各行业开展保护层分析工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 20438.4—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

GB/T 21109.1—2022 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、硬件和应用编程要求

3 术语和定义

GB/T 20438.4—2017 和 GB/T 21109.1—2022 界定的以及下列术语和定义适用于本文件。

3.1

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

对来自过程及其相关设备、其他可编程系统和/或操作员的输入信号作出响应并生成输出信号使过程及其相关设备按照期望的方式运行的系统,但它不执行任何 SIF。

注1:BPCS包括确保过程以期望的方式运行的所有必要设备。

注2:BPCS通常支持执行多种功能,如过程控制功能、监视、报警。

[来源:GB/T 21109.1—2022,3.2.3]

3.2

条件修正因子 conditional modifiers

场景风险计算时使用的可能性概率之一。

注:通常表现为影响后果(例如:人员伤亡、点火概率、致死率)而不是主要损失事件后果(例如:泄漏、容器破裂)时使用。

3.3

后果 consequence

某一特定事件的结果。

注:通常包括人员伤亡、财产损失、环境污染、声誉影响等。

3.4

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

不直接导致场景后果发生的事件或条件。

注:是使初始事件转变为场景后果的某种必要的操作状态或条件。

3.5

原始风险　initial risk

不考虑任何保护措施作用下场景的风险。

3.6

初始事件　initial event

使事故序列开始扩展所需的失效或错误的最小组合。

注：由一个单独的初始原因、多个原因或有使能条件的初始原因组成。

3.7

中间事件　intermediate event

初始事件发展成后果之前的关键事件。

注：通常是一个可被检测到的事件，如某压力容器压力高、某储罐液位高。需要指出的是，特殊场景可能由初始事件直接发展成为不良后果，不存在中间事件。

3.8

保护层分析　layer of protection analysis；LOPA

对降低不期望事件发生频率和/或后果严重性的独立保护层的有效性进行评估的一种方法或体系。

3.9

保护层　layer of protect；PL

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。

注：本文件中提及的保护措施属于保护层。

3.10

独立保护层　independent protection layer；IPL

能有效地防止场景向不期望的后果发展，与场景的初始事件或其他保护层的行动无关。

注1：保护层的一种。

注2：独立保护层的有效性和独立性能够被审查。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。

3.11

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

当受控设备或受控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。

注：本文件中PFD指独立保护层执行规定安全功能时的平均安全不可用性。

[来源：GB/T 20438.4—2017，3.6.17，有修改]

3.12

残余风险　residual risk

采取保护措施以后仍存在的风险。

[来源：GB/T 20438.4—2017，3.1.8，有修改]

3.13

风险点　risk point

伴随风险的设备、设施或位置以及在特定设备、设施或位置出现的危险场景的集合。

3.14

风险降低因子　risk reduction factor；RRF

量化保护层降险能力的参数，为要求时危险失效概率的倒数。

注：RRF=1/PFD。

3.15

场景　scenario

可能导致不期望后果的事件序列。

注：事件序列一般包括初始事件、中间事件和最终后果。

3.16

复合场景　multi scenario

可能导致同一不期望后果的多个事件序列的组合，这些事件序列的初始事件互相独立不相关。

3.17

安全仪表功能　safety instrumented function；SIF

由安全仪表系统(SIS)实现的安全功能。

注：SIF 设计用来达到一个要求的 SIL，SIL 由其他参与降低相同风险的保护层决定。

[来源：GB/T 21109.1—2022，3.2.66]

3.18

安全完整性等级　safety integrity level；SIL

为规定 SIS 应达到的安全完整性要求而分配给 SIF 的离散等级(4 个等级中的一个)。

注 1：SIL 等级越高，期望的 PFD_{avg} 越低，或者导致危险事件的危险失效平均频率越低。

注 2：SIL4 是安全完整性的最高等级，SIL1 是最低等级。

注 3：此定义和 GB/T 20438.4—2017 中的定义有差别，从而反应过程领域术语中的差异。

[来源：GB/T 21109.1—2022，3.2.69，有修改]

3.19

安全仪表系统　safety instrumented system；SIS

用来实现一个或多个 SIF 的仪表系统。

注 1：SIS 由任意组合的传感器、逻辑解算器及最终元件组成。它也包括通信和辅助设备(如电缆、管道、电源、取压管、伴热)。

注 2：SIS 还包括软件。

注 3：SIS 也包括人为动作作为 SIF 的一部分。

[来源：GB/T 21109.1—2022，3.2.67，有修改]

3.20

(SIF 的)运行模式　mode of operation(of a SIF)

SIF 的运行方式，低要求模式、高要求模式或连续模式。

a) 低要求模式：在这种运行模式下，SIF 只有在要求时才动作，以将过程导入一个特定的安全状态，并且要求的频率不大于一年一次。

b) 高要求模式：在这种运行模式下，SIF 只有在要求时才动作，以将过程导入一个特定的安全状态，并且要求的频率大于一年一次。

c) 连续模式：在这种运行模式下，SIF 作为正常运行的一部分保持过程处于一种安全状态。

[来源：GB/T 21109.1—2022，3.2.39]

3.21

安全关键动作　safety critical actions

SIF 中将过程导入安全状态的直接动作，不包括出于维护或装置再启动等相关安全或便捷考虑的执行动作。

3.22

可容忍风险　tolerable risk

根据当前社会发展水平在一定范围内能够接受的风险。

4　缩略语

下列缩略语适用于本文件。

ALARP：合理可行的低原则（As Low As Reasonably Practicable）
BPCS：基本过程控制系统（Basic Process Control System）
HAZOP：危险与可操作性（Hazard and Operability）
IE：初始事件（Initial Event）
IPL：独立保护层（Independent Protection Layer）
LOPA：保护层分析（Layer of Protection Analysis）
PFD：要求时危险失效概率（Probability of Dangerous Failure on Demand）
PFD_{avg}：要求时危险失效平均概率（Average Probability of Dangerous Failure on Demand）
P&ID：管道和仪表流程图（Pipe and Instrument Diagram）
RRF：风险降低因子（Risk Reduction Factor）
SIF：安全仪表功能（Safety Instrument Function）
SIL：安全完整性等级（Safety Integrity Level）
SIS：安全仪表系统（Safety Instrumented System）
TI：检验测试间隔（Test Interval）

5 一般要求

5.1 目的

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半定量分析（准确到数量级），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忍风险标准的要求，并根据需要增加适当的独立保护层，以将风险降低至可容忍风险标准所要求的水平。

5.2 基本要求

5.2.1 LOPA 的一个基本原则就是不存在不失效的保护层。典型独立保护层 PFD 举例见附录 A 的表 A.8。

5.2.2 LOPA 的场景识别主要来源于定性危险分析方法（如 HAZOP 分析）所得出的危险场景。

注：LOPA 不是识别危险场景的工具。

5.2.3 应在 LOPA 前确定可容忍风险标准，分析过程应采用相同的可容忍风险标准。

注：各企业需制定适合自己的可容忍风险标准。确定可容忍风险标准的常见方法有矩阵法、数值风险法（每个场景最大容忍风险）等，示例见 A.6。

5.2.4 应在 LOPA 前确认输入资料。一旦输入资料发生变化，需对 LOPA 结果进行复审，必要时重新开展 LOPA。

5.2.5 当使用 LOPA 方法开展 SIL 定级分析时，应明确参与 SIF 的仪表设备、安全关键动作及其逻辑/冗余关系。

5.2.6 在开展 LOPA 时，最终建议的提出可遵循 ALARP。可容忍风险与 ALARP 的关系见图 1。

注：ALARP 原则建议“在合理可行的范围内”将风险降低，或降低到“尽可能低的合理可行水平”。如果风险介于两个极端（即不可容忍区域和广泛可接受区域）之间，并且应用了 ALARP 原则，则由此产生的风险就是该特定应用的可容忍风险。

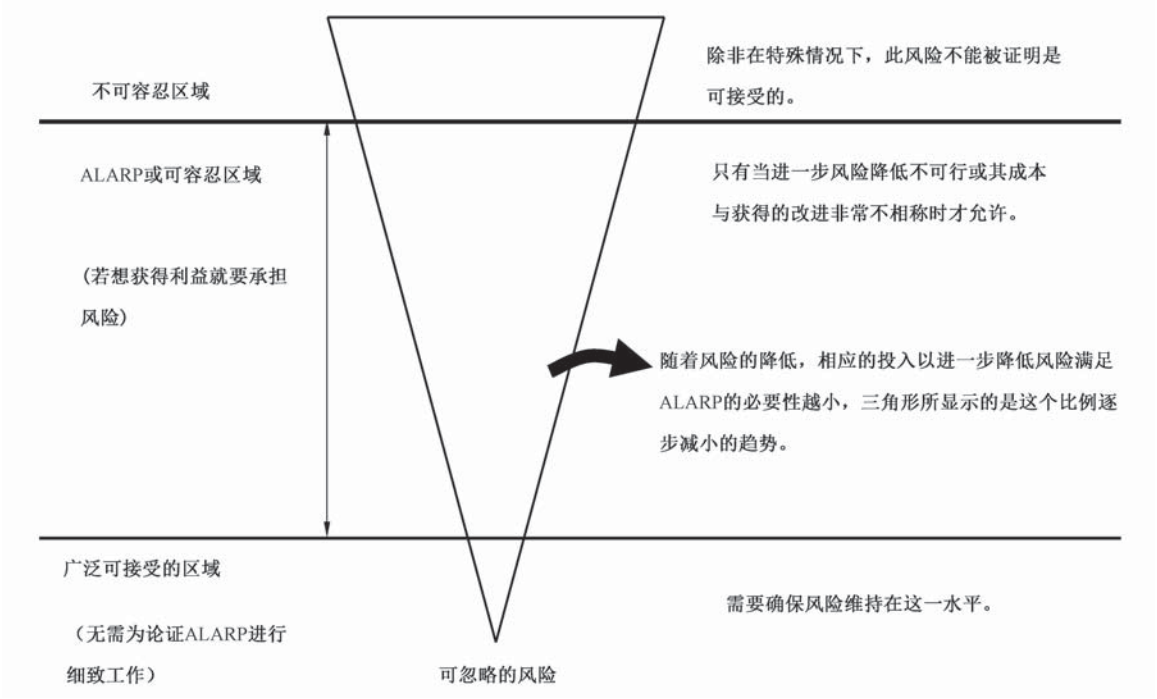


图 1　可容忍风险和 ALARP

5.3　应用范围

LOPA 可用于以下场合。

a）　以下两种情况的风险判断：

　　1）　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；

　　2）　场景后果过于严重而不能只依靠定性方法进行风险判断。

b）　确定 SIF 的 SIL。

c）　识别过程中安全关键设备。

d）　识别操作人员关键安全行为和关键安全响应。

e）　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。

f）　其他适用 LOPA 的场合（如设计方案分析和事故调查）。

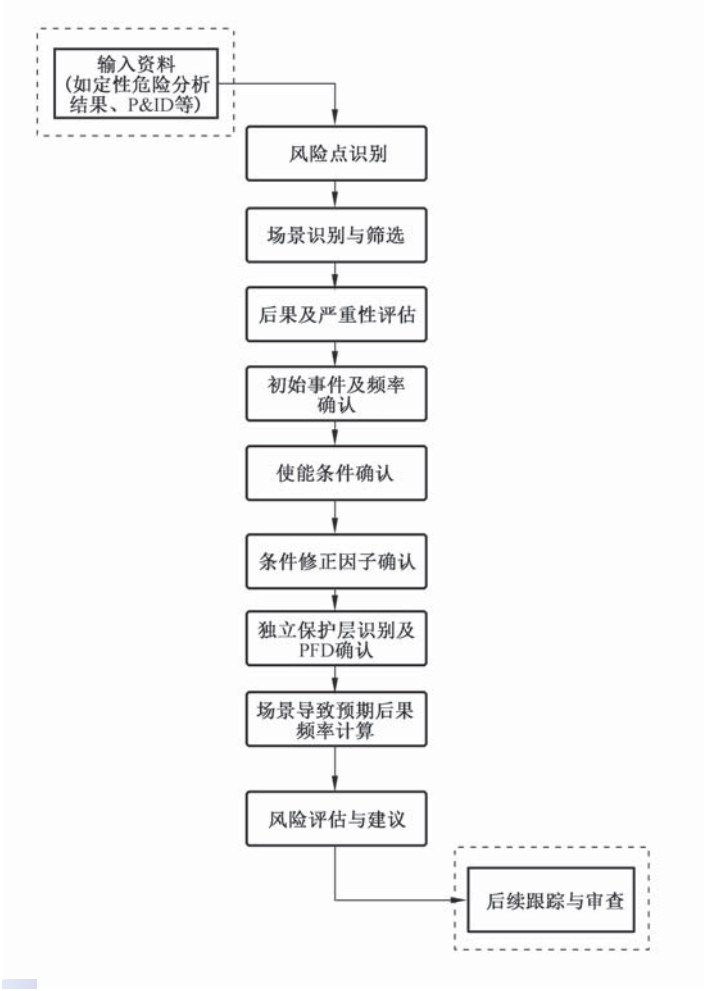
LOPA 的应用举例见附录 B、附录 C。

5.4　人员要求

LOPA 小组宜由分析主席、分析秘书和分析成员组成。分析主席和秘书应来自分析单位，分析成员宜来自运行单位、分析单位、设计方，必要时还包括承包商。

6　基本程序

保护层分析的过程应包括：风险点识别、场景识别与筛选、后果及严重性评估、初始事件及频率确认、使能条件确认、条件修正因子确认、独立保护层识别及 PFD 确认、场景导致预期后果频率计算、风险评估与建议。以上工作流程见图 2。



注：图中虚框所含内容不在本文件范围之内。

图 2　保护层分析流程图

在工程实践中 LOPA 可选择单一场景分析法或复合场景分析法。复合场景分析法是将导致同一后果的多个场景在考虑现有保护措施基础上对后果发生频率求和计算的方法，单一场景分析法是将导致同一后果的不同场景在考虑现有保护措施基础上分别计算后果发生频率并取高值作为计算结果的方法。因此，复合场景分析法相对于单一场景分析法评估结果更保守。

7　分析过程

7.1　风险点识别

应识别并确定待开展 LOPA 的风险点，可包括以下 3 类：

a）　危险与风险分析（如 HAZOP 分析）中原始后果为高后果和/或原始风险为高风险的场景及其他需要分析的重要风险点；

b）　设有联锁保护功能的风险点；

c）　通过危险与风险分析（如 HAZOP 分析）提出增设联锁保护功能的风险点。

7.2 场景识别与筛选

7.2.1 场景应满足的基本要求

场景应满足以下基本要求。

a) 每个场景至少包括两个要素：
   1) 引起事件序列的初始事件；
   2) 初始事件继续发展所导致的后果。
b) 每个场景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，场景还可能包括使能事件或使能条件。
d) 如果使用人员伤亡、财产损失或环境影响作为后果，则场景还可能包括下列部分或全部的条件修正因子：
   1) 点火概率；
   2) 人员出现在后果影响区域的概率；
   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) 其他适用的条件修正因子。

7.2.2 场景识别

场景识别信息通常来源于危险与风险分析(如 HAZOP 分析)，HAZOP 分析中可导出的用于 LOPA 的数据见表 A.1。

根据风险点的类别，场景识别的方法分为：

——针对 7.1a)类风险点，识别原始后果为高后果和/或原始风险为高风险及其他明确需要分析的所有场景；

——针对 7.1b)类风险点，识别保护措施中待分析联锁保护功能的所有场景；

——针对 7.1c)类风险点，识别建议增加联锁保护功能的所有场景。

7.2.3 场景筛选

根据风险点的类别，按照 7.2.2 完成场景识别后，开展场景筛选的规则为：

——针对 7.1a)类风险点，将后果描述相同且原始后果严重性等级相同的场景归类为同一风险点，生成对应 LOPA 记录表；

——针对 7.1b)类风险点，将同一联锁、后果描述相同且原始后果严重性等级相同的场景归类为同一风险点，生成对应 LOPA 记录表；

——针对 7.1c)类风险点，将建议增设联锁涉及的后果描述相同且原始后果严重性等级相同的场景归类为同一风险点，生成对应 LOPA 记录表。

7.2.4 场景补充

对场景进行详细分析与记录，记录表格示例见表 A.2 和表 A.3。

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场景，经识别和筛选后可能作为另一起 LOPA 的对象。

7.3 后果及严重性评估

7.3.1 后果分析应满足的基本要求

后果分析应符合以下要求：

a） 后果分析覆盖可容忍风险标准中的所有后果分类；

b） 分析至最终后果，并描述所有后果分类（如人员伤亡、财产损失、环境影响等）的严重性情况；

注 1：例如，若后果仅描述为“安全阀动作”或“压缩机停机”等，均不是最终后果，不符合本文件要求。

c） 后果分析为假设任何已有的保护措施都失效时导致的最终不利的可信后果。

注 2：可信后果指基于现场实际情况和科学的推导方法确定的最终不利后果。

7.3.2 后果严重度评估

应确定场景后果的严重程度，后果严重度分级应与可容忍风险分级相一致。后果分类、严重性分级等详细信息示例见表 A.4、表 A.5、表 A.6。

7.4 初始事件及频率确认

7.4.1 初始事件类型

初始事件一般包括外部事件、设备故障和人因失效，分类见表 1。

表 1 初始事件分类

类别	外部事件	设备故障	人因失效
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） 邻近工厂的重大事故 d） 破坏或恐怖活动 e） 雷击和外部火灾 f） 大气压力及环境温度快速变化等气候影响 g） 其他外部事件	a） 控制系统失效 1） 硬件失效 2） 软件失效 b） 仪表设备故障 c） 通信设备故障 d） 电气设备故障 e） 机械设备故障 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 f） 辅助系统故障 g） 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） 未能按操作规程进行操作 c） 未能按维护规程进行操作 d） 未按管理规定作业 e） 其他错误行为

7.4.2 初始事件确定要求

在确定初始事件时，遵循以下要求。

a) 应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) 每个场景的初始事件应追溯至分析对象范围内最初始原因。
d) 在识别潜在初始事件时，应识别和审查所有操作模式（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) 当人因失效作为初始事件时，应制定人因失效频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) 操作人员培训不充分；
   2) 测试或检查不完善；
   3) 物理保护功能失效（如安全阀等）。

7.4.3 初始事件频率确认

应结合行业经验及现场实际确定初始事件发生频率，常见的初始事件及其频率值示例见表 A.13。

注：在分析记录表或报告中需标明初始事件发生频率的确定依据。

7.5 使能条件确认

7.5.1 使能条件应用要求

在确定使能条件时，应遵循以下要求：
a) 使能条件的确认给出充分理由；
b) 独立于场景初始事件或任意独立保护层（IPL）；
c) 使能条件概率代表真实的风险削减因素，并且不随时间变化而变化。

7.5.2 常用的使能条件

7.5.2.1 常用的使能条件包括时效使能和操作使能。在开展 LOPA 时，当考虑使能条件时应在记录表中详细说明其取值依据。除非有特别有效数据支持，单一使能条件取值不宜低于 0.1，单一场景中使用的所有使能条件取值的乘积不宜小于 0.01。

7.5.2.2 时效使能 P^{E} 及操作使能 P^{E} 按公式（1）计算：

$$P^{E}=\frac{t_{E}}{t_{0}} \qquad \cdots\cdots(1)$$

式中：
P^{E} ——时效使能/操作使能条件系数；
t_{E} ——给定时间段（如 1 年）内时效使能/操作使能所占的平均时长，单位为小时（h）；
t_{0} ——给定时间段（如 1 年）内的实际运行时间，单位为小时（h）。

注：时效使能和操作使能具体描述及示例详见附录 D。

7.6 条件修正因子确认

7.6.1 常见的条件修正因子

常见的条件修正因子包括：
——点火概率；
——人员出现在后果影响区域的概率；
——暴露致死率；
——其他适用的条件修正因子。

7.6.2 赋值要求

7.6.2.1 使用条件修正因子时不应重复消减。

7.6.2.2 在开展 LOPA 时，当考虑修正因子时应在记录表中详细说明其取值依据。单一场景中使用的所有修正因子取值的乘积不宜小于 0.01。

注：需表明所使用假定值的参考依据，且对标准值的任何修改需说明理由并记录在案。

7.6.2.3 分析对象存在可燃介质时，点火概率取值宜考虑：

——介质的组成成分及其燃烧性；

——介质泄漏后的最终状态，如液态、气态；

——介质泄漏所处环境温度与自燃点的关系；

——泄漏形式，是连续还是瞬时释放；

——介质所处装置类型：固定/移动、生产/储存/装卸；

——装置区周边点火源情况；

——泄漏速率；

——现场的安全条件，包括防爆、接地、液体防流散措施、防火安全措施等；

——事故历史经验。

7.6.2.4 人员出现在后果影响区域的概率取值宜考虑。

——人员出现在后果影响区域的概率是指当损失事件发生时人可能出现在后果影响区域内的时间比例。人员出现在后果影响区域的概率宜考虑日常操作工况下影响区域内的所有人员，包括：巡检人员、维护人员等。对可能会受到影响的区域实行限制出入控制通常不作为人员出现在后果影响区域概率修正因子。

——人员出现在后果影响区域的概率修正因子应独立于所评估的场景。潜在后果影响范围较大（如群死群伤事件）的情况、瞬态或短期操作如开停车、维修及异常工况处置等可能有大量人员暴露的情况，不宜使用人员出现在后果影响区域的概率修正因子或需要单独进行评估。

——若操作规程要求报警时人员要去现场进行响应时，不宜使用人员暴露概率修正因子或需要单独进行评估。

7.6.2.5 暴露致死率取值宜考虑：

——暴露致死率修正因子描述了当人员出现于后果影响区域内时可能发生伤亡的概率；

——考虑暴露致死率时应参考装置发生事故时的伤亡半径、燃烧事故的热辐射强度、爆炸事故的冲击波强度等数据；

——没有适用的、可信的数据来源时不宜使用暴露致死率修正因子，暴露致死率修正因子取值不宜小于 0.1。

7.7 独立保护层识别及 PFD 确认

7.7.1 独立保护层识别

典型的工艺流程保护层示例见表 A.7，并不是所有的保护层都可作为独立保护层，保护层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。应满足以下要求：

1) 能检测到响应的条件；

2) 在有效的时间内，能及时响应，响应时间应满足过程安全时间要求；

3) 在需要时，有足够的能力采取所要求的行动。

注：保护措施是否有足够能力采取所要求的行动的确认，包括保护措施本身的选型、现场的管理和响应以及泄放类措施的通量和容器的容量等。例如：系统安装有安全阀，若安全阀的泄放通量小于计算的场景物料的泄放通

量，或安全阀连接的泄放罐容量小于该场景可能的最大泄放量，则这个安全阀不能作为这个场景的独立保护层，并需在分析表中给出说明。

b） 独立性，应同时满足以下要求：

1） 独立于初始事件的发生及其后果；

2） 独立于同一场景中的其他独立保护层。

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。应满足以下要求：

1） 审查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。

以下保护措施不宜作为独立保护层：

a） 培训和取证；

b） 操作规程；

c） 定期的测试和检测；

d） 维修维护；

e） 警示标识。

危险与风险分析过程中所提出的已有保护措施可能是不完整的，在开展 LOPA 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。

7.7.2 独立保护层 PFD 的确认

应依据以下要求确认独立保护层的 PFD：

a） 独立保护层的 PFD 为系统要求独立保护层执行规定安全功能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），则考虑使用更高的 PFD 值；

c） 表 A.8 给出了过程工业典型独立保护层的 PFD 值示例，实际 LOPA 过程中，PFD 值的确定符合国家标准、行业标准或企业标准，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 中的统一规则严格执行；

d） 考虑共因失效或共模失效对 PFD 的影响。

7.8 单一场景分析法后果频率计算

单一场景分析法后果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。

a） 单一场景分析法后果频率为初始事件发生频率乘以所有独立保护层的 PFD，还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见 7.2.1。

b） 低要求模式下各类后果（如人员伤亡、财产损失、环境影响等）发生频率按公式（2）计算：

$$f_n^{\mathrm{C}} = f_n^{\mathrm{I}} \times P_n^{\mathrm{E}} \times P_n^{\mathrm{C}} \times \prod_{j=1}^{J} \mathrm{PFD}_{nj} \quad \cdots\cdots (2)$$

式中：

f_n^C ——初始事件 n 造成后果 C 的频率，单位为次每年(次/年)；

f_n^I ——初始事件 n 的发生频率，单位为次每年(次/年)；

P_n^E ——初始事件 n 的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取 1；

P_n^C ——初始事件 n 的条件修正因子，假如没有任何条件修正则取 1；

注：存在多个适用的条件修正因子时，P_n^C 为各条件修正因子的乘积。

PFD_{nj} ——初始事件 n 中第 j 个阻止后果 C 的独立保护层 PFD；

J ——本场景中使用到的独立保护层数量。

c) 高要求模式下后果频率的计算见附录 E。

7.9 复合场景分析法后果频率计算

复合场景分析法后果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。

a) 低要求模式下复合场景分析法后果频率通过公式(3)计算：

$$f^C = \sum_{n=1}^{N} \left(f_n^I \times P_n^E \times P_n^C \times \prod_{j=1}^{J} PFD_{nj} \right) \quad \cdots\cdots (3)$$

式中：

f^C ——当前分析风险点产生后果 C 的频率，单位为次每年(次/年)；

N ——当前分析风险点所含场景的个数；

f_n^I ——场景 n 的初始事件发生频率，单位为次每年(次/年)；

P_n^E ——场景 n 的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取 1；

P_n^C ——场景 n 的初始事件的条件修正因子，假如没有任何条件修正则取 1；

注 1：存在多个适用的条件修正因子时，P_n^C 为各条件修正因子的乘积。

PFD_{nj} ——引发场景 n 的初始事件中第 j 个独立保护层 PFD；

J ——本场景中使用到的独立保护层数量。

也可对各场景均用到的独立保护层和条件修正因子合并同类项，通过公式(4)计算：

$$f^C = \left[\sum_{n=1}^{N} \left(f_n^I \times P_n^E \times \prod_{j=1}^{J} PFD_{nj} \right) \right] \times P_n^C \times \prod_{k=1}^{K} PFD_k \quad \cdots\cdots (4)$$

式中：

f^C ——当前分析风险点产生后果 C 的频率，单位为次每年(次/年)；

f_n^I ——场景 n 的初始事件发生频率，单位为次每年(次/年)；

P_n^E ——场景 n 的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取 1；

P_n^C ——条件修正因子，假如没有任何条件修正则取 1；

注 2：存在多个适用的条件修正因子时，P_n^C 为各条件修正因子的乘积。

PFD_{nj} ——引发场景 n 的初始事件中第 j 个独立保护层 PFD；

J ——场景 n 中使用到的与其他场景不同的独立保护层数量；

PFD_k ——该风险点各场景均用到的第 k 个 IPL 或非独立保护层 PFD；

K ——各场景均用到的独立保护层数量。

b) 高要求模式下后果频率的计算见附录 E。

7.10 风险评估与建议

风险评估与建议有以下内容。

a) 通过 7.3 的后果及严重性评估与 7.8、7.9 的场景频率计算，得出选定场景的后果等级以及后果频率，可与可容忍风险频率比较。

b) 若计算得出的后果频率不大于可容忍风险频率，当前设置已满足风险降低要求。

c) 若计算得出的后果频率大于可容忍风险频率，LOPA 小组应提出满足可容忍风险标准所需采取的措施及其负责人和预计行动完成日期，并确定拟采取保护措施的 PFD 或 RRF 值，以将风险降低到可容忍风险之下。其中 RRF 的计算公式如下：

1) 对于单一场景分析法，按公式(5)计算：

$$RRF = \frac{f_n^C}{f_t} \quad \cdots\cdots(5)$$

式中：

f_t ——可容忍风险频率，单位为次每年(次/年)；

f_n^C ——初始事件 n 造成后果 C 的频率，单位为次每年(次/年)。

2) 对于复合场景分析法，按公式(6)计算：

$$RRF = \frac{f^C}{f_t} \quad \cdots\cdots(6)$$

式中：

f_t ——可容忍风险频率，单位为次每年(次/年)；

f^C ——当前分析风险点产生后果 C 的频率，单位为次每年(次/年)。

8 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忍风险时，应用其他保护层是否可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。

记录表见表 A.2 或表 A.3，宜包含如下信息：

a) 后果；

b) 可容忍风险标准；

c) 初始事件；

d) 使能事件或使能条件；

e) 条件修正；

f) 独立保护层；

g) 保护措施(非独立保护层)；

h) 后果频率；

i) 能否满足可容忍风险标准；

j) 为满足可容忍风险标准需要采取的行动；

k) 备注；

l) 参考资料。

附 录 A
（资料性）
LOPA 各阶段数据（示例）

A.1 从 HAZOP 分析导出的可用于 LOPA 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 分析导出的可用于 LOPA 的数据

LOPA 要求的信息	从 HAZOP 分析导出的信息
待分析风险点	• 原始后果为高后果和/或原始风险为高风险的场景及其他需要分析的重要风险点； • 设有联锁保护功能的风险点； • 建议增设联锁保护功能的风险点
场景描述	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	现有的保护措施
注 1：HAZOP 导出的信息在应用于 LOPA 时需再次判断。例如：HAZOP 分析中的现有保护措施并不都是独立保护层。 注 2：HAZOP 分析建议新增的保护措施是否作为独立保护层，也需在 LOPA 时再次判断。	

A.2 LOPA 记录表

单一场景 LOPA 记录表示例见表 A.2。

表 A.2 单一场景 LOPA 记录表（示例）

风险点编号：	风险点名称：		
日期：	描述	概率	频率（次/年）
后果描述			
后果严重性等级	人员： 级；财产： 级；环境： 级；声誉： 级		
可容忍风险（分类/频率）	人员：		
	财产：		
	环境：		
	声誉：		
初始事件（一般给出频率）			
使能事件或使能条件（如果适用）			

表 A.2　单一场景 LOPA 记录表(示例)(续)

风险点编号：	风险点名称：		
日期：	描述	概率	频率 (次/年)
独立保护层			
本质安全设计			
基本过程控制系统			
关键报警及人员响应			
安全仪表功能			
物理保护			
其他独立保护层			
其他保护措施(为可选填项)(非独立保护层)			
所有独立保护层总 PFD			
后果频率			
是否满足可容忍风险？(是/否)：			
满足可容忍风险需要采取的行动：			
备注：			
参考资料(P&ID 图号等)：			

注：填表注意事项如下：

a) 记录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) 记录包括：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) 列出场景所有的保护措施；

f) 小组对列出的多种保护措施进行分析，确定真正的独立保护层；

g) 场景开发需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。

复合场景 LOPA 记录表示例见表 A.3。

表 A.3　复合场景 LOPA 记录表(示例)

风险点编号：	风险点名称：		
日期：	描述	概率	频率 (次/年)
后果描述			
后果严重性等级	人员：　级;财产：　级;环境：　级;声誉：　级		
可容忍风险(分类/频率)	人员：		
	财产：		
	环境：		
	声誉：		
场景 1			
初始事件 1(一般给出频率)			
使能事件或使能条件			
初始事件 1 的 IPL			
场景 2			
初始事件 2(一般给出频率)			
使能事件或使能条件			
初始事件 2 的 IPL			
场景 *n*			
初始事件 *n*(一般给出频率)			
使能事件或使能条件			
初始事件 *n* 的 IPL			
中间事件频率			
条件修正 (如果适用)	点火概率		
	人员出现在后果影响区域的概率		
	致死概率		
	其他		
独立保护层(所有初始事件共用的)			
本质安全设计			
基本过程控制系统			
关键报警及人员响应			

表 A.3　复合场景 LOPA 记录表(示例)(续)

<table>
<tr><td>风险点编号：</td><td colspan="3">风险点名称：</td></tr>
<tr><td>日期：</td><td>描述</td><td>概率</td><td>频率
(次/年)</td></tr>
<tr><td>安全仪表功能</td><td></td><td></td><td></td></tr>
<tr><td>物理保护</td><td></td><td></td><td></td></tr>
<tr><td>其他保护层(需判别)</td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">其他保护措施(所有初始事件共用的)(非独立保护层)</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>所有独立保护层总 PFD</td><td></td><td></td><td></td></tr>
<tr><td rowspan="4">残余风险及其所需 RRF</td><td>人员伤亡</td><td></td><td></td></tr>
<tr><td>财产损失</td><td></td><td></td></tr>
<tr><td>环境影响</td><td></td><td></td></tr>
<tr><td>声誉影响</td><td></td><td></td></tr>
<tr><td colspan="4">是否满足可容忍风险？(是/否)：</td></tr>
<tr><td colspan="4">满足可容忍风险需要采取的行动：</td></tr>
<tr><td colspan="4">备注：</td></tr>
<tr><td colspan="4">参考资料(P&ID 图号等)：</td></tr>
<tr><td colspan="4">注：填表注意事项如下：
a)　表 A.2 单一场景 LOPA 记录表(示例)的填表注意事项都需关注；
b)　填入表 A.3 中的初始事件为导致同一后果的多个独立不相关事件；
c)　初始事件 n 的 IPL 为非所有初始事件共用的 IPL；
d)　独立保护层格中填写的为所有初始事件共用的 IPL；
e)　其他保护措施为所有初始事件共用的保护措施。</td></tr>
</table>

A.3　后果及严重性示例

表 A.4、表 A.5 和表 A.6 分别给出了简化的人员伤亡后果分级示例、简化的经济损失后果分级示例以及简化的环境影响后果分级示例。

注：表 A.4、表 A.5、表 A.6 中的后果分级示例仅用于理解后续案例，不适用于供实际工程直接使用。

表 A.4　简化的人员伤亡后果分级(示例)

人员伤亡				
等级 1	等级 2	等级 3	等级 4	等级 5
造成 3 人以下轻伤	造成 3 人(含)以下重伤,或者 3 人(含)以上 10 人以下轻伤	造成 3 人以下死亡,或者 3 人(含)以上 10 人以下重伤,或者 10 人(含)以上轻伤	造成 3 人(含)以上 10 人以下死亡,或者 10 人以上 50 人(含)以下重伤	10 人(含)及以上死亡

表 A.5　简化的经济损失后果分级(示例)

经济损失				
等级 1	等级 2	等级 3	等级 4	等级 5
造成 1 000 元以上 10 万元(含)以下直接经济损失	造成 10 万元以上 100 万元(含)以下直接经济损失	造成 100 万元以上 1 000 万元(含)以下直接经济损失	造成 1 000 万元以上 5 000万元(含)以下直接经济损失	造成 5 000 万元以上直接经济损失

表 A.6　简化的环境影响后果分级(示例)

环境影响				
等级 1	等级 2	等级 3	等级 4	等级 5
a) 因环境污染疏散、转移人员 100 人以下的。 b) 因环境污染造成直接经济损失 50 万元以下的	a) 因环境污染直接导致 3 人以下中毒或者重伤的。 b) 因环境污染疏散、转移人员 100 人以上 1 000 人以下的。 c) 因环境污染造成直接经济损失 50 万元以上 200 万元以下的。 d) 放射性同位素和射线装置失控导致人员受到超过年剂量限值的照射的	a) 因环境污染直接导致 3 人以下死亡,或者 3 人以上 10 人以下中毒或者重伤的。 b) 因环境污染疏散、转移人员 1 000 人以上 5 000 人以下的。 c) 因环境污染造成直接经济损失 200 万元以上 500 万元以下的。 d) 因环境污染造成跨县级行政区域纠纷,引起一般性群体影响的。 e) Ⅳ、Ⅴ类放射源丢失、被盗的;放射性物质泄漏,造成厂区内或者设施内局部辐射污染后果的	a) 因环境污染直接导致 3 人以上 10 人以下死亡或者 10 人以上 50 人以下中毒或者重伤的。 b) 因环境污染疏散、转移人员 5 000 人以上 1 万人以下的。 c) 因环境污染造成直接经济损失 500 万元以上 2 000万元以下的。 d) 因环境污染造成国家重点保护的动植物物种受到破坏的。 e) 因环境污染造成乡镇集中式饮用水水源地取水中断的。 f) Ⅲ类放射源丢失、被盗的;放射性同位素和射线装置失控导致 10 人以下急性重度放射病、局部器官残疾的;放射性物质泄漏,造成小范围辐射污染后果的。 g) 造成跨设区的市级行政区域影响的突发环境事件	a) 因环境污染直接导致 10 人以上死亡或者 50 人以上中毒或者重伤的。 b) 因环境污染疏散、转移人员 1 万人以上的。 c) 因环境污染造成直接经济损失 2 000 万元以上的。 d) 因环境污染造成区域生态功能部分丧失或者该区域国家重点保护野生动植物种群大批死亡的。 e) 因环境污染造成县级以上城市集中式饮用水水源地取水中断的。 f) Ⅰ、Ⅱ类放射源丢失、被盗的、失控并造成大范围严重辐射污染后果的;放射性同位素和射线装置失控导致急性死亡或者 10 人以上急性重度放射病、局部器官残疾的;放射性物质泄漏,造成较大范围辐射污染后果的。 g) 造成跨省级行政区域以上影响的突发环境事件

A.4 典型的保护层

典型的工艺流程保护层示例见表 A.7，包括保护层的描述、相关说明以及作为独立保护层的相关要求。表 A.8 给出了典型独立保护层 PFD 值。

表 A.7 典型的工艺流程保护层

保护层	描述	说明	作为独立保护层的要求
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	a) 当本质安全设计用来消除某些场景时，不作为 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)	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	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 控制回路需与 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，需有更全面的信息来支撑，具体评估方法见 A.5
关键报警和人员响应	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，需慎重考虑人员行动作为独立保护层的有效性。 关键报警需有充分的人员响应时间	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) 操作人员能够得到采取行动的指示或报警，这种指示或报警需始终对操作人员可用； b) 操作人员训练有素，能够完成特定报警所触发的操作任务； c) 任务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　典型的工艺流程保护层（续）

保护层	描述	说明	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	SIF 在功能上独立于 BPCS	a）SIF 在功能上独立于 BPCS，是一种独立保护层； b）SIF 的规格、设计、调试、检验、维护和测试都需参考 GB/T 21109 的有关规定。 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	包括安全阀、爆破片等，其有效性受服役条件的影响较大	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，需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，需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		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	$[1\times10^{-6},1\times10^{-1}]$
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	$[1\times10^{-1},1\times10^{0}]$
关键报警和人员响应	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	$[1\times10^{-1},1\times10^{0}]$
	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	$[1\times10^{-2},1\times10^{-1}]$
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	$[1\times10^{-2},1\times10^{-1})$
	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	$[1\times10^{-3},1\times10^{-2})$
	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	$[1\times10^{-4},1\times10^{-3})$
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	$[1\times10^{-3},1\times10^{-1}]$
	爆破片	防止系统超压。其有效性对服役条件比较敏感	$[1\times10^{-3},1\times10^{-1}]$
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	$[1\times10^{-3},1\times10^{-2}]$
	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	$[1\times10^{-3},1\times10^{-2}]$
	开式通风口	防止超压	$[1\times10^{-3},1\times10^{-2}]$
	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	$[1\times10^{-3},1\times10^{-2}]$
	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	$[1\times10^{-3},1\times10^{-2}]$

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，且需独立于 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。当 BPCS 逻辑解算器的 PFD 比 BPCS 回路其他部件的 PFD 至少低两个数量级时，方法 B 允许同一 BPCS 有两个 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。

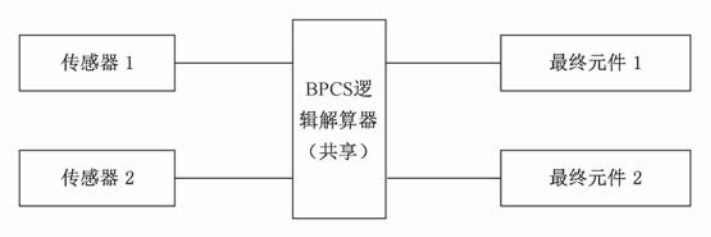


图 A.1 同一场景下多个回路的典型 BPCS 逻辑解算器

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，需满足：

a) BPCS 具有完善的安全访问程序，需确保将 BPCS 编程、变更或操作上潜在的人因失效降低到可接受水平；

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，则多个回路不能作为多个 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，则这两个 BPCS 回路也只能作为一个 IPL。

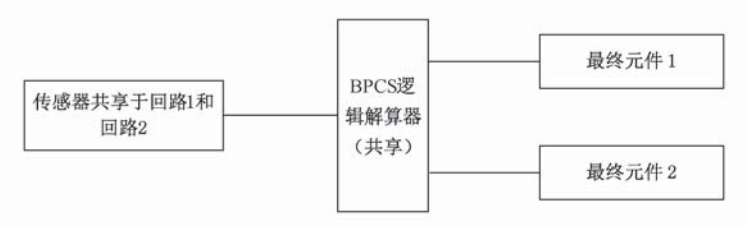
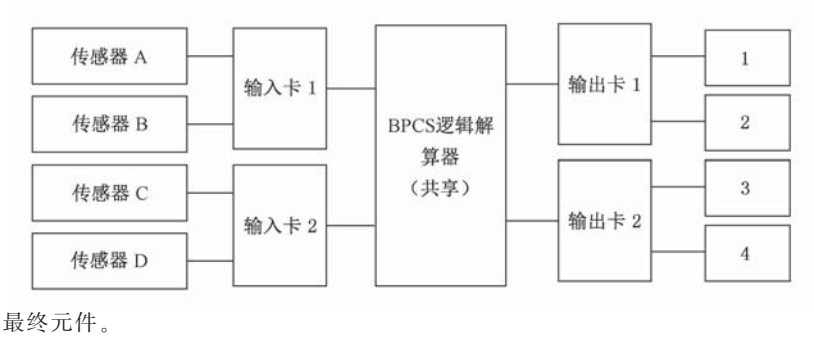


图 A.2 同一场景下共享传感器的 BPCS 回路

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），则此回路也可确定为 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），则此回路不能作为 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 B→输入卡 1→逻辑解算器→输出卡 2→最终元件 4），则此回路也因为输入卡 1 共用在两个回路中而不能作为独立保护层。



注：1、2、3、4 是最终元件。

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 回路不能超过 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。

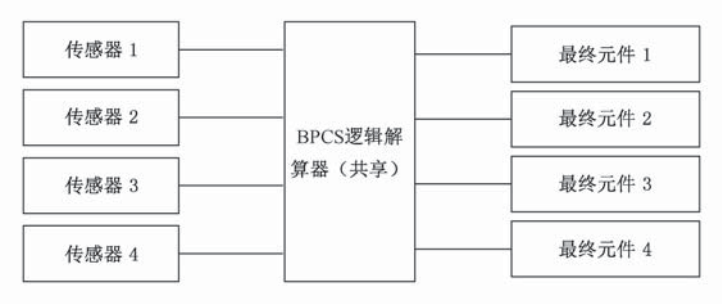


图 A.4　同一场景下 BPCS 功能回路作为 IPL 的最大数量

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

同一场景下，同一 BPCS 多个功能回路同时作为 IPL 的数据和人员需满足以下内容。

a）　对数据分析需满足如下内容。

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，需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：

1）　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；

2）　系统制造商提供的数据；

3）　检查、维护和功能性测试数据；

4）　仪表图、管道和仪表流程图（P&ID）、回路图、标准规范等资料；

5）　访问 BPCS，进行程序更改、旁路报警等安全访问 BPCS 的信息。

对这些数据的分析需包括：

1）　计算设备或系统 BPCS 回路组件的有效失效率；

2） 各种组件，特别是 BPCS 逻辑解算器 PFD 数据的比较；

3） 逻辑输入/输出卡及相关回路的独立性评估；

4） 安全访问控制充分性评估；

5） 使用多重 BPCS 回路作为同一场景下的多个 IPL 的合适性评估。

b） 对分析人员的能力需满足如下内容。

分析人员能够：

1） 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；

2） 了解仪表的设计和 BPCS 系统是否满足独立性要求；

3） 理解建议的 IPL 对工艺或系统的影响。

分析小组或人员需具有相关专业知识，如：

1） 对 BPCS 逻辑解算器具有足够低的 PFD 的独立第三方认证；

2） 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；

3） 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，则在判断 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.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
$10^{-1}\sim10^{0}$	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）
$10^{-2}\sim10^{-1}$	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）
$10^{-3}\sim10^{-2}$	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）
$10^{-4}\sim10^{-3}$	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）
$10^{-5}\sim10^{-4}$	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）
$10^{-6}\sim10^{-5}$	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）
$10^{-7}\sim10^{-6}$	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	不需要采取行动

人员伤亡、环境影响、财产损失对应的可容忍风险（示例）标准见表 A.10、表 A.11、表 A.12。

表 A.10　数值分析法-安全与健康相关事件的可容忍风险(示例)

严重程度	安全与健康相关的后果	可容忍风险频率 (次/年)
5 级,灾难性的	10 人(含)及以上死亡	1×10^{-7}
4 级,严重的	造成 3 人(含)以上 10 人以下死亡,或者 10 人以上 50 人(含)以下重伤	1×10^{-6}
3 级,较大的	造成 3 人以下死亡,或者 3 人以上 10 人(含)以下重伤,或者 10 人(含)以上轻伤	1×10^{-5}
2 级, 较小的	造成 3 人(含)以下重伤,或者 3 人(含)以上 10 人以下轻伤	1×10^{-3}
1 级,微小的	造成 3 人以下轻伤	1×10^{-1}

表 A.11　数值分析法-环境相关事件的可容忍风险(示例)

严重程度	环境相关的后果	可容忍风险频率 (次/年)
5 级,灾难性的	a)　因环境污染直接导致 10 人以上死亡或者 50 人以上中毒或者重伤的。 b)　因环境污染疏散、转移人员 1 万人以上的。 c)　因环境污染造成直接经济损失 2 000 万元以上的。 d)　因环境污染造成区域生态功能部分丧失或者该区域国家重点保护野生动植物种群大批死亡的。 e)　因环境污染造成县级以上城市集中式饮用水水源地取水中断的。 f)　Ⅰ、Ⅱ类放射源丢失、被盗的、失控并造成大范围严重辐射污染后果的;放射性同位素和射线装置失控导致急性死亡或者 10 人以上急性重度放射病、局部器官残疾的;放射性物质泄漏,造成较大范围辐射污染后果的。 g)　造成跨省级行政区域以上影响的突发环境事件	1×10^{-6}
4 级,重大的	a)　因环境污染直接导致 3 人以上 10 人以下死亡或者 10 人以上 50 人以下中毒或者重伤的。 b)　因环境污染疏散、转移人员 5 000 人以上 1 万人以下的。 c)　因环境污染造成直接经济损失 500 万元以上 2 000 万元以下的。 d)　因环境污染造成国家重点保护的动植物物种受到破坏的。 e)　因环境污染造成乡镇集中式饮用水水源地取水中断的。 f)　Ⅲ类放射源丢失、被盗的;放射性同位素和射线装置失控导致 10 人以下急性重度放射病、局部器官残疾的;放射性物质泄漏,造成小范围辐射污染后果的。 g)　造成跨设区的市级行政区域影响的突发环境事件	1×10^{-5}

表 A.11　数值分析法-环境相关事件的可容忍风险(示例)(续)

严重程度	环境相关的后果	可容忍风险频率 (次/年)
3 级,较大的	a)　因环境污染直接导致 3 人以下死亡,或者 3 人以上 10 人以下中毒或者重伤的。 b)　因环境污染疏散、转移人员 1 000 人以上 5 000 人以下的。 c)　因环境污染造成直接经济损失 200 万元以上 500 万元以下的。 d)　因环境污染造成跨县级行政区域纠纷,引起一般性群体影响的。 e)　Ⅳ、Ⅴ类放射源丢失、被盗的;放射性物质泄漏,造成厂区内或者设施内局部辐射污染后果的	1×10^{-4}
2 级,较小的	a)　因环境污染直接导致 3 人以下中毒或者重伤的。 b)　因环境污染疏散、转移人员 100 人以上 1 000 人以下的。 c)　因环境污染造成直接经济损失 50 万元以上 200 万元以下的。 d)　放射性同位素和射线装置失控导致人员受到超过年剂量限值的照射的	1×10^{-2}
1 级,微小的	a)　因环境污染疏散、转移人员 100 人以下的。 b)　因环境污染造成直接经济损失 50 万元以下的	1×10^{-1}

表 A.12　数值风险法-财产相关事件的可容忍风险(示例)

严重程度	财产相关的后果	可容忍风险频率 (次/年)
5 级,灾难性的	造成 5 000 万元以上直接经济损失	1×10^{-6}
4 级,重大的	造成 1 000 万元以上 5 000 万元(含)以下直接经济损失	1×10^{-5}
3 级,较大的	造成 100 万元以上 1 000 万元(含)以下直接经济损失	1×10^{-4}
2 级,较小的	造成 10 万元以上 100 万元(含)以下直接经济损失	1×10^{-2}
1 级,微小的	造成 1000 元以上 10 万元(含)以下直接经济损失	1×10^{-1}

A.7　初始事件频率示例

常用初始事件频率示例见表 A.13。

表 A.13　常用初始事件频率(示例)

初始事件	频率范围 (次/年)
压力容器疲劳失效	$10^{-7}\sim10^{-5}$
管道疲劳失效－100 m－全部断裂	$10^{-6}\sim10^{-5}$
管线泄漏(10%截面积)－100 m	$10^{-4}\sim10^{-3}$
常压储罐失效	$10^{-5}\sim10^{-3}$
垫片/填料爆裂	$10^{-6}\sim10^{-2}$

表 A.13　常用初始事件频率(示例)(续)

初始事件	频率范围 (次/年)
涡轮/柴油发动机超速,外套破裂	10^{-4}～10^{-3}
第三方破坏(挖掘机、车辆等外部影响)	10^{-4}～10^{-2}
起重机载荷掉落	10^{-4}～10^{-3}
雷击	10^{-4}～10^{-3}
安全阀误开启	10^{-4}～10^{-2}
冷却水失效	10^{-2}～1
泵密封失效	10^{-2}～10^{-1}
卸载/装载软管失效	10^{-2}～1
BPCS 仪表控制回路失效	10^{-2}～1
调节器失效	10^{-1}～1
小的外部火灾(多因素)	10^{-2}～10^{-1}
大的外部火灾(多因素)	10^{-3}～10^{-2}
LOTO(锁定、标定)程序失效(多个元件的总失效)	10^{-4}～10^{-3}
操作员失效(执行常规程序,假设得到较好的培训、不紧张、不疲劳)	10^{-3}～10^{-1}

附 录 B
（资料性）
反应器系统 LOPA 应用

B.1 概述

B.2～B.4 列出了《保护层分析——简化的过程风险评估》中的案例，B.5 以此为基础开展 LOPA 复合场景分析的应用。

B.2 问题描述

以图 B.1 中的 P&ID 图为基础进行 LOPA。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。

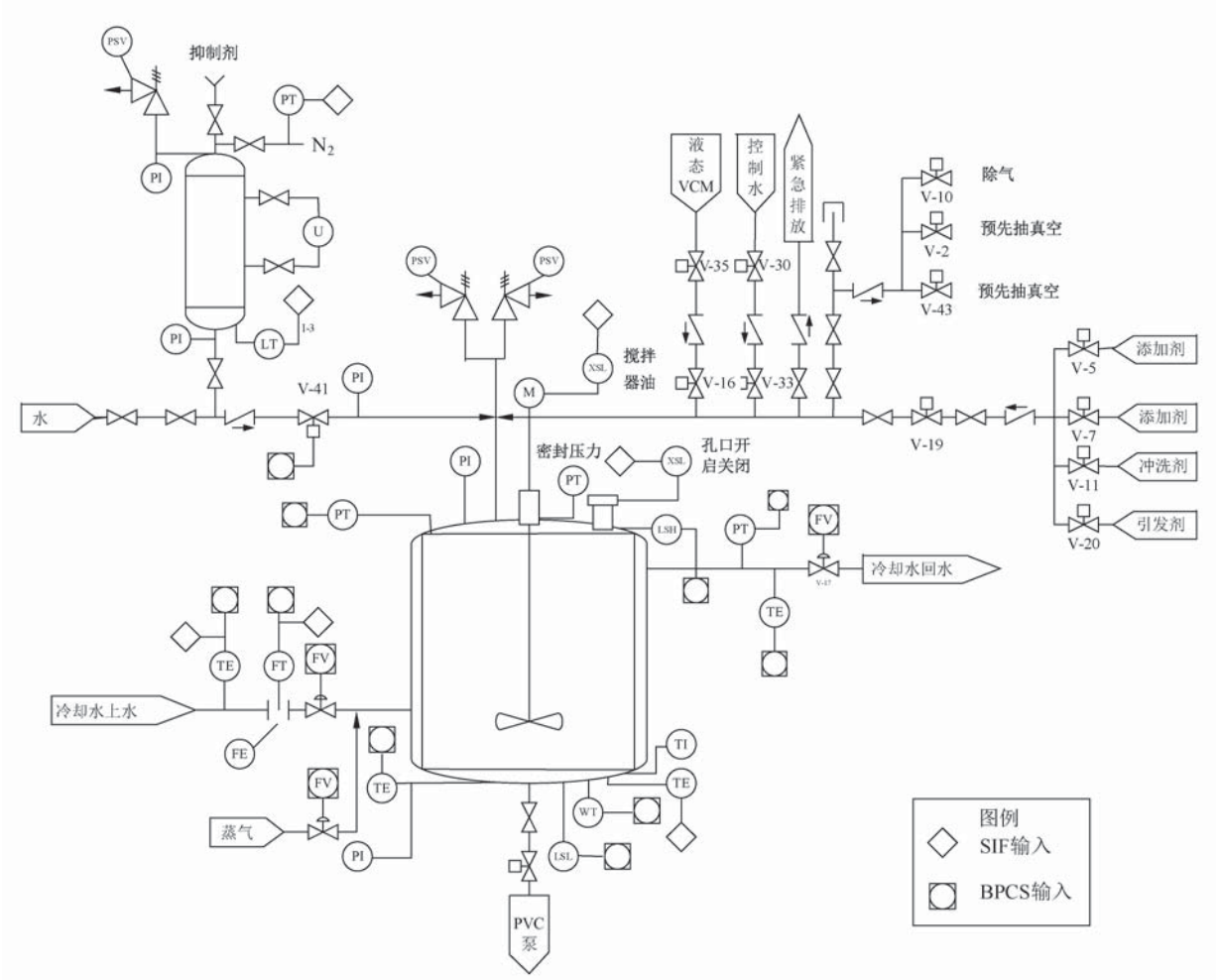
在表 B.1 中列出了所要分析的 8 个场景。表 B.2～表 B.9 包括了针对这些场景的 LOPA 汇总表。

B.3 问题讨论

使用风险矩阵后果等级和可容忍风险，根据场景的顺序进行 LOPA。

表 B.1 分析场景案例

场景一：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
场景二：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
场景三：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
场景四：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
场景五：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
场景六：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
场景七：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
场景八：搅拌器密封失效的使 VCM 泄漏并诱发着火，爆炸，伤害和死亡的可能性



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

开展 LOPA 分析，步骤如下。

a)　可容忍风险标准

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，事件频率大于每年 1×10^{-4} 即无法接受，需采取行动对其进行改正。事件频率等于或小于每年 1×10^{-6} 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忍风险，而对处于灰色安全地带的现役装置，则进行成本效益分析。

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 批/年

此处假定每批料仅加一次催化剂，且每批料运转 3 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忍风险的方法中，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

独立保护层具有有效性、独立性和可审查性。

1） 有效性

对于多数场景，均建议增加承担减压功能的 SIF。反应器顶部管线既用于减压阀和安全阀 PSV 的排放管线，又是反应器添加引发剂、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，则需采用 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 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，所以通风系统没有问题。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 结果，假定独立保护层 IPL 的 PFD 为 1×10^{-1}，尽管表 B.9 的一个注释还要求对该 IPL 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可被考虑为独立保护层 IPL 做分析。

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）。所以将低占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 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，然后用手动方式让反应器“冒泡”的方式来混合介质，在 LOPA 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（$PFD=1\times10^{-2}$）与排气阀 SIF（$PFD=1\times10^{-3}$）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

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，操作员人员的两个操作步骤（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。

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 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 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 至 B.9 中直接描述。而确认和审计可能会包括：

- 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、反应动力学等的以支持该结论；
- 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

本条对图 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。

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。

还需考虑在 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，则需采用 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，需参照 Guidelines for Pressure Relief and Effluent Handling Systems 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亦适用于排气阀 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（如上）的 PFD 及可容忍风险决定了 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，也需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。若有足够的培训、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	风险点名称：反应器超压		
场景描述：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/（次/年）
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		
可容忍风险（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（一般给出频率）	冷却水故障停		1×10^{-1}
使能事件或使能条件（如果适用）	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 （/反应器）	
条件修正（如果适用）	点火概率	不适用	
	人员出现在后果影响区域的概率	不适用	
	致死概率	不适用	
	其他	不适用	
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}	
保护措施（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		

表 B.2　场景 1 分析案例（续）

场景编号：1	风险点名称：反应器超压		
场景描述：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/（次/年）
所有独立保护层的总 PFD		1×10^{-6}	
减缓后的后果频率			5×10^{-8}
是否满足可容忍风险？（是/否）	是 但需增加 SIF（安全仪表功能）系统		
满足可容忍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		

表 B.3　场景 2 分析案例

场景编号：2	风险点名称：反应器超压		
场景描述：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/（次/年）
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		
可容忍风险（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（如果适用）	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）	点火概率	不适用	
	人员出现在后果影响区域的概率	不适用	
	致死概率	不适用	
	其他	不适用	
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}	
保护措施（非独立保护层）	操作员操作（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）		

表 B.3　场景 2 分析案例（续）

场景编号：2	风险点名称：反应器超压		
场景描述：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/（次/年）
所有独立保护层总 PFD		1×10^{-5}	
减缓后的后果频率			5×10^{-7}
是否满足可容忍风险？（是/否）	是 但需增加 SIF（安全仪表功能）系统		
满足可容忍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		

表 B.4　场景 3 分析案例

场景编号：3	风险点名称：反应器超压		
场景描述：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/（次/年）
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、受伤、死亡 后果等级 5		
可容忍风险（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（如果适用）	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）	点火概率	不适用	
	人员出现在后果影响区域的概率	不适用	
	致死概率	不适用	
	其他	不适用	
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}	
保护措施（非独立保护层）	操作员操作（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）		

表 B.4　场景 3 分析案例（续）

场景编号：3	风险点名称：反应器超压		
场景描述：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/（次/年）
所有独立保护层总 PFD		1×10^{-5}	
减缓后的后果频率			5×10^{-7}
是否满足可容忍风险？（是/否）	是 但需增加 SIF（安全仪表功能）系统		
满足可容忍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 PFD1×10^{-2}。若有更高的安全要求，则考虑提高放空阀 SIF 的 PFD		

表 B.5　场景 4 分析案例

场景编号：4	风险点名称：反应器超压		
场景描述：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/（次/年）
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、受伤、死亡 后果等级 5		
可容忍风险（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（如果适用）	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）	点火概率	不适用	
	人员出现在后果影响区域的概率	不适用	
	致死概率	不适用	
	其他	不适用	
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}	

表 B.5　场景 4 分析案例（续）

场景编号：4	风险点名称：反应器超压		
场景描述：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/（次/年）
保护措施（非独立保护层）	操作员响应（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}
是否满足可容忍风险？（是/否）	是 但需增加 SIF（安全仪表功能）系统		
满足可容忍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 PFD1×10^{-2}。若有更高的安全要求，则考虑提高放空阀 SIF 的 PFD		

表 B.6　场景 5 分析案例

场景编号：5	风险点名称：反应器超压		
场景描述：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/（次/年）
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、受伤、死亡 后果等级 5		
可容忍风险（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）	操作员误操作，添加 2 次催化剂		1×10^{-2}
使能事件或使能条件（如果适用）	添加催化剂（每 3 天一次——每年 121 次）	121	
条件修正（如果适用）	点火概率	不适用	
	人员出现在后果影响区域的概率	不适用	
	致死概率	不适用	
	其他	不适用	
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}	

表 B.6　场景 5 分析案例（续）

场景编号：5	风险点名称：反应器超压		
场景描述：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/（次/年）
SIF	SIF 打开放空阀，场景 5 确定了其 PFD 值	1×10^{-3}	
保护措施（非独立保护层）	操作员操作（不能作为独立保护）（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			1.21×10^{-6}
是否满足可容忍风险？（是/否）	是 但需增加 SIF（安全仪表功能）系统		
满足可容忍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		

表 B.7　场景 6 分析案例

场景编号：6	风险点名称：反应器超压		
场景描述：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/（次/年）
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、受伤、死亡 后果等级 5		
可容忍风险（分类或频率）	不可接受（大于）		1×10^{-4}
	可接受（小于或等于）		1×10^{-6}
初始事件（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（如果适用）	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）	点火概率	不适用	
	人员出现在后果影响区域的概率	不适用	
	致死概率	不适用	
	其他	不适用	
独立的保护层			
泄压阀	修正系统	1×10^{-2}	

表 B.7　场景 6 分析案例（续）

场景编号：6	风险点名称：反应器超压		
场景描述：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/（次/年）
SIF	SIF 打开放空阀，场景 5 确定了其 PFD 值	1×10^{-3}	
保护措施（非独立保护层）	操作员响应（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}
是否满足可容忍风险？（是/否）	是 但需增加 SIF（安全仪表功能）系统		
满足可容忍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		

表 B.8　场景 7 分析案例

场景编号：7	风险点名称：反应器超压		
场景描述：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/（次/年）
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、受伤、死亡 后果等级 5		
可容忍风险（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（如果适用）	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）	点火概率	不适用	
	人员出现在后果影响区域的概率	不适用	
	致死概率	不适用	
	其他	不适用	
独立的保护层			
泄压阀	要修改系统	1×10^{-2}	

表 B.8　场景 7 分析案例（续）

场景编号：7	风险点名称：反应器超压		
场景描述：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/（次/年）
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}	
保护措施（非独立保护层）	操作员响应（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}
是否满足可容忍风险？（是/否）	是 但需增加 SIF（安全仪表功能）系统		
满足可容忍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 PFD1×10^{-2}。若有更高的安全要求，则考虑提高放空阀 SIF 的 PFD		

表 B.9　场景 8 分析案例

场景编号：8	风险点名称：反应器泄漏		
场景描述：搅拌器密封失效使 VCM 泄漏并诱发着火，爆炸、伤害和死亡			
日期：	描述	概率	频率/（次/年）
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），可能造成受伤和死亡 后果等级 3		
可容忍风险（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（如果适用）			
条件修正（如果适用）	点火概率	不适用	
	人员出现在后果影响区域的概率	不适用	
	致死概率	不适用	
	其他	不适用	

表 B.9　场景 8 分析案例（续）

场景编号：8	风险点名称：反应器泄漏		
场景描述：搅拌器密封失效使 VCM 泄漏并诱发着火，爆炸、伤害和死亡			
日期：	描述	概率	频率/（次/年）
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}	
保护措施（非独立保护层）	操作员操作（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}
是否满足可容忍风险？（是/否）	是 但需增加 SIF（安全仪表功能）系统		
满足可容忍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			

B.5　基于复合场景分析得出的供考虑的设计改进

对于表 B.2～表 B.8 分析的 7 个场景，其中场景 1、场景 2、场景 3、场景 4、场景 5、场景 6、场景 7 共 7 个场景均导致了同一个后果，即：反应器超压、泄漏、破裂和人员伤亡，且此 7 个场景的初始事件为相互独立事件，因此可使用复合场景分析方法开展分析，分析过程见表 B.10。

表 B.10　复合场景分析案例

风险点编号：1	风险点名称：反应器超压		
日期：	描述	概率	频率/（次/年）
后果描述	反应器失控和可能导致反应器超压、泄漏、破裂及人员伤亡		
后果严重性等级	人员：5 级		
可容忍风险（分类/频率）	人员：		$\leqslant1\times10^{-6}$
	财产：		—
	环境：		—
	声誉：		—

表 B.10　复合场景分析案例（续）

风险点编号：1	风险点名称：反应器超压		
日期：	描述	概率	频率/（次/年）
场景 1			
初始事件 1（一般给出频率）	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（/反应器）	
初始事件 1 的 IPL	当反应器温度高报时，添加中止液	1×10^{-1}	
初始事件 1 的保护措施（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	—	
场景 2			
初始事件 2（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（/反应器）	
初始事件 2 的 IPL			
初始事件 2 的保护措施（非独立保护层）	操作员操作（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）		
场景 3			
初始事件 3（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（/反应器）	
初始事件 3 的 IPL			
初始事件 3 的保护措施（非独立保护层）	操作员操作（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）		
场景 4			
初始事件 4（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（/反应器）	
初始事件 4 的 IPL	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}	

表 B.10　复合场景分析案例（续）

风险点编号:1	风险点名称:反应器超压		
日期:	描述	概率	频率/(次/年)
初始事件 4 的保护措施(非独立保护层)	操作员响应(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)		
场景 5			
初始事件 5(一般给出频率)	添加催化剂(每 3 天一次——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}	
初始事件 5 的 IPL	当反应器温度高报时,添加中止液	1×10^{-1}	
初始事件 5 的保护措施(非独立保护层)	操作员操作(不能作为独立保护)(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)		
场景 6			
初始事件 6(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 (/反应器)	
初始事件 6 的 IPL			
初始事件 6 的保护措施(非独立保护层)	操作员响应(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)		
场景 7			
初始事件 7(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 (/反应器)	
初始事件 7 的 IPL	SIF 添加紧急冷却水	1×10^{-1}	
初始事件 7 的保护措施(非独立保护层)	操作员响应(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)		
中间事件频率			2.86×10^{-1}
条件修正(如果适用)	点火概率	不适用	
	人员出现在后果影响区域的概率	不适用	
	致死概率	不适用	
	其他	不适用	
独立保护层(所有初始事件共用的)			
泄压阀	对系统进行改进后	1×10^{-2}	

表 B.10　复合场景分析案例（续）

风险点编号：1	风险点名称：反应器超压		
日期：	描述	概率	频率/（次/年）
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}	
保护措施（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		
所有独立保护层的总 PFD		1×10^{-5}	
残余风险及其所需 RRF			2.86×10^{-6}/RRF＝3
是否满足可容忍风险？（是/否）	否，需增加 SIF（安全仪表功能）系统		
满足可容忍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		

附 录 C
（资料性）
LOPA 方法在 SIL 定级中的应用

C.1 LOPA 示例 1

LOPA 方法在 SIL 定级中应用示例 1 见表 C.1。

表 C.1 LOPA 示例 1

P&ID 图号：	LOPA-SAMPLE-DW-001-6 REV.3C
SIF 编号	I-1234
风险点/SIF 名称	PAHH 1001 压力高高
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	严重度	初始事件频率	条件修正		独立保护层			减缓后频率	可容忍后果频率	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	1×10^{-1}	使用率		基本设计	不适用		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	不适用							
					点火概率	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	不适用							

C.2 LOPA 示例 2

LOPA 方法在 SIL 定级中应用示例 2 见表 C.2。

表 C.2 LOPA 示例 2

P&ID 图号：	LOPA-SAMPLE-DW-001-6 REV.3C																										
SIF 编号：	I-1234																										
风险点/SIF 名称	PAHH 1001 压力高高																										
SIF 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																										
后果描述：	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		后果类别	严重性等级		可容忍后果频率		后果频率		目标 RRF		SIL 定级结论				是否 SIF											
			人员	5		1×10^{-6}		3×10^{-3}		3 000		SIL3，RRF≥3 000				是											
			财产	3		1×10^{-4}		1.5×10^{-2}		150																	
			环境	3		1×10^{-4}		1.5×10^{-2}		150																	
编号	初始事件	初始事件频率	后果类别	独立保护层							使能条件			条件修正					中间频率	建议	责任方	备注					
				IPL1			IPL2			…	EC1		…	CM1		CM2		…									
				类型	描述	PFD	类型	描述	PFD	…	描述	概率	…	描述	概率	描述	概率	…									
1	进料 FIC 0001/ PIC 0002 串级回路故障-PV 开度过大	1×10^{-1}	人员	关键报警和人员响应	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}	物理保护	见备注	1	…	间歇工况	不适用	…	点火概率	0.5	人员暴露概率	0.2	…	1×10^{-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				
			财产			1×10^{-1}			1	…		不适用	…		0.5		不适用	…	5×10^{-3}								
			环境			1×10^{-1}			1	…		不适用	…		0.5		不适用	…	5×10^{-3}								

表 C.2　LOPA 示例 2（续）

编号	初始事件	初始事件频率	后果类别	独立保护层							使能条件			条件修正					中间频率	建议	责任方	备注
				IPL1			IPL2			…	EC1		…	CM1		CM2		…				
				类型	描述	PFD	类型	描述	PFD	…	描述	概率	…	描述	概率	描述	概率	…				
2	下游压缩机故障跳车	2×10^{-1}	人员	关键警报和人员响应	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}			1	…	间歇工况	不适用	…	点火概率	0.5	人员暴露概率	0.2	…	2×10^{-3}			
			财产			1×10^{-1}			1	…		不适用	…		0.5		不适用	…	1×10^{-2}			
			环境			1×10^{-1}			1	…		不适用	…		0.5		不适用	…	1×10^{-2}			
3	…		人员			…			…	…		…	…		…		…	…	…			
			财产			…			…	…		…	…		…		…	…	…			
			环境			…			…	…		…	…		…		…	…	…			

C.3 LOPA 示例 3

LOPA 方法在 SIL 定级中应用示例 3 见表 C.3。

表 C.3 LOPA 示例 3

风险点编号:01	风险点名称:PAHH 1001 压力高高		
日期:	描述	概率	频率/(次/年)
后果描述	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		
后果严重性等级	人员:5 级;财产:3 级;环境:3 级		
可容忍风险(分类/频率)	人员:		1×10^{-6}
	财产:		1×10^{-4}
	环境:		1×10^{-4}
场景 1			
初始事件 1(一般给出频率)	进料 FIC 0001/ PIC 0002 串级回路故障(PV 开度过大)		1×10^{-1}
使能事件或使能条件			
初始事件 1 的 IPL	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	0.1	
场景 2			
初始事件 2(一般给出频率)	下游压缩机故障跳车		2×10^{-1}
使能事件或使能条件			
初始事件 2 的 IPL	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	0.1	
中间事件频率			3×10^{-2}
条件修正 (如果适用)	点火概率	0.5	
	人员出现在后果影响区域的概率	0.2	
	致死概率	不适用	
	其他	不适用	
独立保护层(所有初始事件共用的)			
本质安全设计			
后果描述	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		
后果严重性等级	人员:5 级;财产:3 级;环境:3 级		
可容忍风险(分类/频率)	人员:		1×10^{-6}
	财产:		1×10^{-4}
	环境:		1×10^{-4}

表 C.3　LOPA 示例 3（续）

风险点编号：01	风险点名称：PAHH 1001 压力高高		
日期：	描述	概率	频率/（次/年）
基本过程控制系统			
关键报警及人员响应			
安全仪表功能	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		
物理保护	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		
其他保护层（需判别）			
其他保护措施（所有初始事件共用的）（非独立保护层）			
所有独立保护层总 PFD			
残余风险及其所需 RRF	人员伤亡		3×10^{-3}/ RRF＝3 000
	财产损失		1.5×10^{-2}/ RRF＝150
	环境影响		1.5×10^{-2}/ RRF＝150
是否满足可容忍风险？（是/否）：否			
满足可容忍风险需要采取的行动： 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保护功能应实现 SIL3，RRF≥3 000			
备注：			
参考资料（P&ID 图号等）：			

C.4　LOPA 示例 4

LOPA 方法在 SIL 定级中应用示例 4 见表 C.4。

表 C.4　LOPA 示例 4

风险点编号：01	风险点名称：PAHH 1001 压力高高		
日期：	描述	概率	频率/（次/年）
后果描述	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		

表 C.4　LOPA 示例 4（续）

风险点编号：01	风险点名称：PAHH 1001 压力高高		
日期：	描述	概率	频率/（次/年）
后果严重性等级	人员：5 级；财产：3 级；环境：3 级		
可容忍风险（分类/频率）	人员：		1×10^{-6}
	财产：		1×10^{-4}
	环境：		1×10^{-4}
场景 1			
初始事件 1（一般给出频率）	进料 FIC 0001/ PIC 0002 串级回路故障（PV 开度过大）		1×10^{-1}
使能事件或使能条件			
初始事件 1 的 IPL	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	0.1	
条件修正（如果适用）	点火概率	0.5	
	人员出现在后果影响区域的概率	0.2	
	致死概率	不适用	
	其他	不适用	
独立保护层（所有初始事件共用的）			
本质安全设计			
基本过程控制系统			
关键报警及人员响应			
安全仪表功能	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		
物理保护	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		
其他保护层（需判别）			
其他保护措施（所有初始事件共用的）（非独立保护层）			
所有独立保护层总 PFD			
后果频率	人员伤亡		1×10^{-3}
	财产损失		5×10^{-3}
	环境影响		5×10^{-3}
场景 2			
初始事件 2（一般给出频率）	下游压缩机故障跳车		2×10^{-1}

表 C.4　LOPA 示例 4（续）

风险点编号:01	风险点名称:PAHH 1001 压力高高		
日期:	描述	概率	频率/(次/年)
使能事件或使能条件			
初始事件 2 的 IPL	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	0.1	
条件修正 (如果适用)	点火概率	0.5	
	人员出现在后果影响区域的概率	0.2	
	致死概率	不适用	
	其他	不适用	
独立保护层(所有初始事件共用的)			
本质安全设计			
基本过程控制系统			
关键报警及人员响应			
安全仪表功能	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		
物理保护	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		
其他保护层(需判别)			
其他保护措施(所有初始事件共用的) (非独立保护层)			
所有独立保护层总 PFD			
后果频率	人员伤亡		2×10^{-3}
	财产损失		1×10^{-2}
	环境影响		1×10^{-2}
总的后果频率	人员伤亡		3×10^{-3}
	财产损失		1.5×10^{-2}
	环境影响		1.5×10^{-2}
残余风险及其所需 RRF	人员伤亡		3×10^{-3}/ RRF=3 000
	财产损失		1.5×10^{-2}/ RRF=150
	环境影响		1.5×10^{-2}/ RRF=150

表 C.4　LOPA 示例 4（续）

风险点编号：01	风险点名称：PAHH 1001 压力高高		
日期：	描述	概率	频率/（次/年）
是否满足可容忍风险？（是/否）：否			
满足可容忍风险需要采取的行动：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保护功能应实现 SIL3，RRF≥3 000			
备注：			
参考资料（P&ID 图号等）：			

附 录 D
（资料性）
使能条件的计算

使能条件包括时效使能和操作使能，其中：

a） 时效使能：只有当处在某一特定时间段内其条件才能使场景转变为失效事件。使用时效使能条件的前提是风险场景的初始事件为显性失效，即某个可能立刻引起系统指示/报警从而被发现的失效。使用时效使能条件应确保与初始事件原因相互独立。常见的时效使能条件包括下列几种情况：

- 季节性风险，极端温度情况；
- 某个过程在当发生故障的事故序列能继续发展为损失事件的非连续操作中的一个特定的部分。

时效使能 P^{E} 计算见公式(D.1)：

$$P^{E}=\frac{t_{PE}}{t_{0}} \qquad \cdots\cdots(D.1)$$

式中：

P^{E} ——时效使能条件系数；

t_{PE} ——给定时间段(如 1 年)内使场景转变为失效事件的特定时间段时长，单位为小时(h)；

t_{0} ——给定时间段(如 1 年)内的实际运行时间，单位为小时(h)。

b） 操作使能：操作使能条件与生产过程中不同时间或不同批次的原料(化学品、浓度、流量、数量)，催化剂，最终产品，操作条件和/或工艺流程等相关。使用操作使能条件应确保与初始事件原因相互独立。常见的操作使能条件包括下列几种情况：

- 仅当生产过程处于某种特殊的状态或工艺流程时，设备失效才会导致损失事件；
- 装置或装置的一部分仅在一年中的特定时间段运营。

操作使能 P^{E} 的计算见公式(D.2)：

$$P^{E}=\frac{t_{PE}\times n}{t_{0}} \qquad \cdots\cdots(D.2)$$

式中：

P^{E} ——操作使能条件系数；

t_{PE} ——给定时间段(如 1 年)内装置处于循环模式的平均时长，单位为小时(h)；

n ——给定时间段(如 1 年)内装置进入循环模式的次数；

t_{0} ——给定时间段(如 1 年)内的实际运行时间，单位为小时(h)。

附 录 E
（资料性）
高要求模式后果频率的计算

E.1 概述

计算高要求模式下的后果发生频率需采用一种近似的方法。公式(3)、公式(4)、公式(5)仅适用于低要求模式，如用于高要求模式将导致不精确的后果发生频率值，一般情况下其结果远大于实际后果发生频率的数值。

E.2 计算方法

E.2.1 单个 IPL，失效频率可以获得时

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，计算见公式(E.1)：

$$f_i^{\mathrm{C}} = f_i^{\mathrm{IPL}i1} P_i^{\mathrm{C}} \qquad \cdots\cdots (\mathrm{E.1})$$

式中：

f_i^{C} ——初始事件 f_i^{C} 造成后果 C 的频率，单位为次每年(次/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(次/年)；

P_i^{C} ——条件修正因子，假如没有任何条件修正，则取 1。

E.2.2 单个 IPL，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，则可用公式(E.2)替代：

$$f_i^{\mathrm{C}} = 2 \times \frac{1}{TI} \times \mathrm{PFD}_{\mathrm{IPL}} \times P_i^{\mathrm{C}} \qquad \cdots\cdots (\mathrm{E.2})$$

式中：

TI ——检验测试间隔，单位为年；

$\mathrm{PFD}_{\mathrm{IPL}}$ ——独立保护层的 PFD；

P_i^{C} ——条件修正因子，假如没有任何条件修正，则取 1。

E.2.3 多个 IPL，且第 1 个 IPL 的失效频率可获得时

高要求模式下，对于有多个 IPL，且有第 1 个 IPL 的失效频率时，使用第 1 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，代入公式(E.1)，即替代 $f_i^{\mathrm{IPL}i1} P_i^{\mathrm{C}}$ 进行计算，此时需要忽略第 1 个 IPL 的 PFD，见公式(E.3)。

$$f_i^{\mathrm{C}} = f_i^{\mathrm{IPL}i1} \qquad \cdots\cdots (\mathrm{E.3})$$

E.2.4 多个 IPL，且第 1 个 IPL 的失效频率未能获得时

高要求模式下，对于有多个 IPL，且没有第 1 个 IPL 的失效频率时，使用 2×(1/第 1 个 IPL 的检验测试间隔，次/年)×(第 1 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，代入公式(E.1)替代 $f_i^{\mathrm{IPL}i1} P_i^{\mathrm{C}}$ 进行计算，得到公式(E.4)。

$$f_i^{\mathrm{C}} = 2 \times \frac{1}{TI} \times \mathrm{PFD}_{\mathrm{IPL}} \qquad \cdots\cdots (\mathrm{E.4})$$

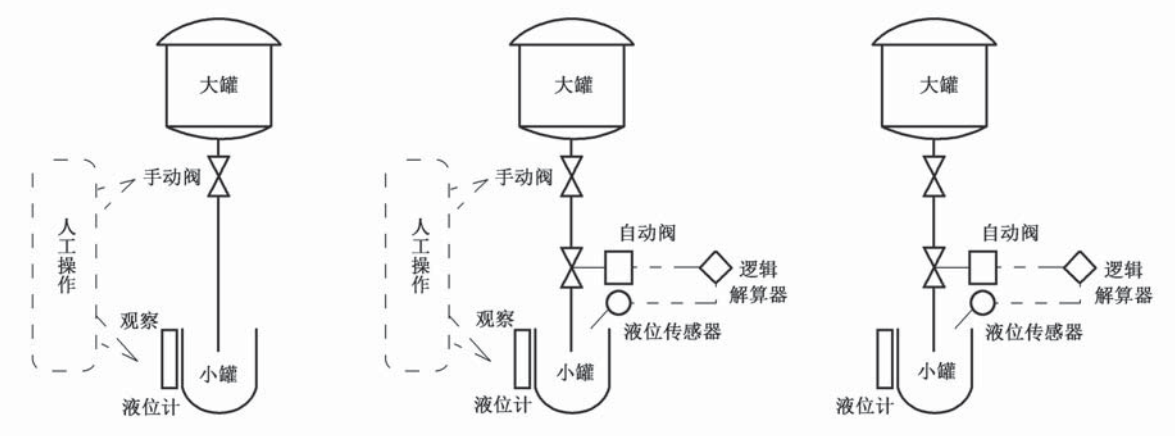
式中：

TI ——检验测试间隔，单位为年；

PFD_{IPL} ——独立保护层的 PFD。

E.3 示例 1

本示例引自《保护层分析——简化的过程风险评估》，小罐从大罐充液 1 400 次/年，其经历了 3 种操作方式（见图 E.1）。



a） 人工　　b） 低要求模式　　c） 高要求模式

图 E.1 3 种操作方式示例

a） 操作人员观察现场液位计，并在装满时，人工关闭手动阀。

b） 发生了一次溢流事故后，增加了液位传感器、逻辑解算器、自动阀组成的 IPL，用于高液位时停止充液，防止事故。人工继续观察液位，并关闭阀门：

1） 人工操作失误的概率为 0.000 5，操作失误的总次数为 0.7 次/年。计算过程为：1 400 次/年×0.000 5；

2） IPL 的要求频率为 0.7 次/年，小于 1 次/年，是低要求模式；

3） IPL 每年测试 1 次。IPL 的 PFD 是 0.01；

4） 本例无条件修正；

5） 溢流后果发生频率是 0.007 次/年。计算过程为：0.7 次/年×0.01。

c） 操作人员实际去做其他工作，依赖 IPL 停止充液：

1） IPL 的要求频率为 1 400 次/年，大于 1 次/年，是高要求模式；

2） 如此时直接使用低要求模式下的计算公式，则溢流后果频率的计算为：1 400 次/年×0.01＝14 次/年，很显然这个结果不现实，远高于实际情况；

3） 使用高要求模式的计算公式，如果有多个 IPL，且没有第 1 个 IPL 的失效频率时，采用公式（E.2），溢流后果频率的近似计算为：2×1 次/年（测试频率）×0.01（PFD）＝0.02 次/年。如果企业有 100 个这样的罐，预计每年发生 2 次溢流事故；

4） 如果只有一个 IPL，且 IPL 的失效频率未知时，采用公式（E.1），溢流后果频率的近似计算为：将初始事件频率设定为测试频率的 2 倍，计算结果为 0.02 次/年。本附录不详细说明这种计算方法。

E.4 示例 2

当要求汽车停止行驶时，刹车系统失效，后果是车无法制动停车。刹车系统是典型的高要求模式

IPL，数据如下：

a） 需要停车制动是常见场景，初始事件频率是 10^4 次/年；

b） 刹车系统的失效频率是 0.1 次/年；

c） 刹车系统的 PFD 是 2.6×10^{-2}；

d） 刹车系统的检验测试间隔是 1 次/年，即一年一检。

如果采用公式（E.1），后果频率的结果是 260 次/年。计算过程为：初始事件频率×刹车系统的 PFD＝$10^4\times2.6\times10^{-2}$＝260 次/年。计算结果与实际不符合，不可能一年发生 260 次无法制动停车的事故。

采用公式（E.1），实际的情况是，汽车需要停车时，刹车失效，汽车无法制动停车的频率只有 0.1 次/年，即十年一遇，计算结果与实际符合。

本示例的数据是假设的，用于说明典型情况，并非实际数据。

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/T 45111—2024 保护层分析(LOPA)、安全完整性等级(SIL)定级和验证质量控制导则

[3] CCPS (Center for Chemical Process Safety). Guidelines for Pressure Relief and Effluent Handling Systems[M], Hoboken, New Jersey: Wiley-AICHE, 1998.

[4] CCPS(Center for Chemical Process Safety). Guidelines for Safe Automation of Chemical Processes[M]. 2nd ed. Hoboken, New Jersey: Wiley-AICHE, 2017.

[5] 美国化工过程安全中心. 保护层分析——简化的过程风险评估[M]. 白永忠, 党文义, 于安峰, 译. 北京: 中国石化出版社, 2010.