ICS 13.200
C 67
备案号：49407—2015

AQ

中华人民共和国安全生产行业标准

AQ/T 3054—2015

保护层分析(LOPA)方法应用导则

Guidelines for layer of protection analysis(LOPA)

2015-03-09 发布　　2015-09-01 实施

国家安全生产监督管理总局　　发布

目　　次

前　言

本标准编制依据 GB/T 1.1—2009 给出的规则起草。

本标准由国家安全生产监督管理总局提出。

本标准由全国安全生产标准化技术委员会化学品安全分技术委员会(SAC/TC 288/SC 3)归口。

本标准主要起草单位:中国石油化工股份有限公司青岛安全工程研究院、国家石化项目风险评估技术中心、中国石化洛阳工程有限公司。

本标准主要起草人:白永忠、韩中枢、党文义、万古军、文科武、张广文、于安峰、王全国、武志峰、沈郁、赵文芳。

引　言

一个典型的化工过程包含各种保护层，如本质安全设计、基本过程控制系统(BPCS)、报警与人员干预、安全仪表功能(SIF)、物理保护(安全阀等)、释放后保护设施、工厂应急响应和社区应急响应等。这些保护层降低了事故发生的频率。在开展化工过程工艺危害分析时，保护层是否足够，能否有效防止事故的发生是分析人员最为关注的一个问题。保护层分析(layer of protection analysis，LOPA)是在定性危害分析的基础上，进一步评估保护层的有效性，并进行风险决策的系统方法，其主要目的是确定是否有足够的保护层使过程风险满足企业的风险可接受标准。LOPA 是一种半定量的风险评估技术，通常使用初始事件频率、后果严重程度和独立保护层(IPL)失效频率的数量级大小来近似表征场景的风险。

本标准主要对 LOPA 基本程序进行了明确的规范和详细的描述，重点规定了 LOPA 场景与筛选、初始事件确认、独立保护层(IPL)、场景频率计算、风险评估与决策等方面的技术要求。本标准的制定，可为国内化工企业开展 LOPA 提供技术指导，同时可为 LOPA 的规范化和标准化奠定基础。

保护层分析(LOPA)方法应用导则

1 范围

本标准规定了化工企业采用LOPA方法的技术要求,包括LOPA基本程序、场景识别与筛选、初始事件确认、独立保护层评估、场景频率技术、风险评估与决策、LOPA报告和LOPA后续跟踪及审查。

本标准适用于化工企业新建、改建、扩建和在役装置(设施)的保护层分析。

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 21109.1 过程工业领域安全仪表系统的功能安全 第1部分:框架、定义、系统、硬件和软件要求

AQ/T 3034 化工企业工艺安全管理实施导则

3 术语、定义和缩略语

下列术语、定义和缩略语适用于本文件。

3.1 术语和定义

3.1.1

场景 scenario

可能导致不期望后果的一种事件或事件序列。每个场景至少包含两个要素:初始事件及其后果。

3.1.2

初始事件 initiating event

事故场景的初始原因。

3.1.3

后果 consequence

事件潜在影响的度量,一种事件可能有一种或多种后果。

3.1.4

保护层 protection layer

能够阻止场景向不期望后果发展的设备、系统或行动。

3.1.5

独立保护层 independent protection layer

能够阻止场景向不期望后果发展,并且独立于场景的初始事件或其他保护层的设备、系统或行动。

3.1.6

保护层分析 layer of protection analysis

通过分析事故场景初始事件、后果和独立保护层,对事故场景风险进行半定量评估的一种系统方法。

3.1.7

要求时的失效概率　probability of failure on demand

系统要求独立保护层起作用时，独立保护层发生失效，不能完成一个具体功能的概率。

3.1.8

风险评估　risk assessment

将风险分析的结果和风险可接受标准进行对比，进行风险决策的过程。

3.1.9

安全仪表功能　safety instrumented function

为了达到功能安全所必需的具有特定安全完整性水平的安全功能。

3.1.10

安全关键设备　safety critical equipment

可提供独立保护层降低场景风险等级，或将场景的风险由“不可接受风险”转变为“可接受风险”的工程控制设备。

3.1.11

使能必要事件或条件　enabling event or condition

不直接导致场景的事件或条件，但是对于场景的继续发展，这些事件或条件应存在。

3.1.12

根原因　root cause

事故发生的根本原因。根原因通常是管理上存在的某种缺陷。

3.1.13

安全仪表系统　safety instrumented system

用来实现一个或几个仪表安全功能的仪表系统，可由传感器、逻辑控制器和最终元件的任何组合组成。

3.1.14

防护措施　safeguard

可能中断初始事件后的事件链或减轻后果的任何设备、系统或行动。

3.1.15

“尽可能合理降低”原则　as low as reasonably practicable

在当前的技术条件和合理的费用下，对风险的控制要做到在合理可行的原则下“尽可能的低”。

3.2　缩略语

本标准使用的缩略语见表1。

表1　本标准使用的缩略语

缩略语	解释	全称
ALARP	“尽可能合理降低”原则	as low as reasonably practicable
BPCS	基本过程控制系统	basic process control system
HAZOP	危险与可操作性分析	hazard and operability study
IE	初始事件	initiating event
IPL	独立保护层	independent protection layer
LOPA	保护层分析	layer of protection analysis

表 1　本标准使用的缩略语（续）

缩略语	解释	全称
P&ID	管道和仪表流程图	piping and instrumentation diagram
PFD	要求时的失效概率	probability of failure on demand
SIF	安全仪表功能	safety instrumented function
SIL	安全完整性等级	safety integrity level
SIS	安全仪表系统	safety instrumented system

4　LOPA 基本程序

4.1　基本程序

4.1.1　保护层分析(LOPA)是在定性危害分析的基础上,进一步评估保护层的有效性,并进行风险决策的系统方法。其主要目的是确定是否有足够的保护层使风险满足企业的风险标准。

4.1.2　LOPA 基本流程图见附录 A,主要过程包括:

a)　场景识别与筛选;
b)　初始事件(IE)确认;
c)　独立保护层(IPL)评估;
d)　场景频率计算;
e)　风险评估与决策;
f)　后续跟踪与审查。

4.1.3　在使用 LOPA 前,应确定以下分析标准:

a)　后果度量形式及后果分级方法;
b)　后果频率的计算方法;
c)　IE 频率的确定方法;
d)　IPL 要求时的失效概率(PFD)的确定方法;
e)　风险度量形式和风险可接受标准;
f)　分析结果与建议的审查及后续跟踪。

4.2　应用时机

4.2.1　在过程危害分析中出现以下情形时,可使用 LOPA:

a)　事故场景后果严重,需要确定后果的发生频率;
b)　确定事故场景的风险等级及事故场景中各种保护层降低的风险水平;
c)　确定安全仪表功能(SIF)的安全完整性等级(SIL);
d)　确定过程中的安全关键设备或安全关键活动;
e)　其他适用 LOPA 的情形等。

4.2.2　LOPA 应用时机参见附录 B。当无法确定事故场景的风险时,可采用定量方法进行定量风险评价。

4.2.3　LOPA 的应用有以下局限性:

a)　LOPA 不是识别危险场景的工具,LOPA 的正确执行取决于定性危险评价方法所得出的危险场景的准确性,包括初始事件和相关的安全措施是否正确和全面。

b） 当使用 LOPA 时，只有满足如下条件才能进行场景风险的对比：

1） 选择失效数据的方法相同；

2） 采用相同的风险标准。

c） LOPA 是一种简化的方法，其计算结果并不是场景风险的精确值。

4.3 小组组成

4.3.1 LOPA 由一个小组完成。LOPA 小组成员可包括但不限于以下人员：

a） 组长；

b） 记录员；

c） 设计人员；

d） 操作人员；

e） 工艺人员；

f） 设备工程师；

g） 仪表工程师；

h） 安全工程师。

4.3.2 根据需要，可要求以下人员参加 LOPA：

a） 工艺包供应商；

b） 成套工艺设备供应商；

c） 公用工程工程师；

d） 电气工程师；

e） 其他专业工程师。

4.3.3 如果 LOPA 是基于 HAZOP 分析的结果，LOPA 小组人员组成宜包括 HAZOP 分析小组成员。

5 场景识别与筛选

5.1 场景基本要求

场景应满足以下基本要求：

a） 每个场景应有唯一的 IE 及其对应的单一后果；

b） 当同一 IE 导致不同的后果时，或多种 IE 导致同一后果时，应假设多个场景；

c） 当场景中存在使能必要事件或条件，应将其包含在场景中。

5.2 场景识别与信息来源

5.2.1 场景信息来源于危险分析的结果，包括：

a） 采用 HAZOP 分析方法进行危害分析的结果；

b） 采用 AQ/T 3034 中的工艺危害分析方法进行危害分析的结果；

c） 事故分析结果；

d） 工艺变更分析；

e） 安全仪表功能审查结果；

f） 其他危害分析结果等。

5.2.2 当利用 HAZOP 分析结果进行 LOPA 时，两者之间的信息对应关系参见附录 C。

5.2.3 当利用已有的定性危害分析结果进行 LOPA 时，宜对定性危害分析的结果进行审查，确保识别出所有的危害后果及导致后果的所有原因。

5.3 场景筛选

5.3.1 宜采用定性或定量的方法对场景后果的严重性进行评估，并根据后果严重性评估结果对场景进行筛选。

5.3.2 典型的后果种类包括人员伤害、财产损失、环境和声誉影响等。

6 初始事件确认

6.1 IE 一般包括外部事件、设备故障和人员失误，具体分类见表 2。

表 2 IE 类型

类别	外部事件	设备故障	人员失误
分类	a)地震、海啸、龙卷风、飓风、洪水、泥石流、滑坡和雷击等自然灾害 b)空难 c)临近工厂的重大事故 d)破坏或恐怖活动 e)邻近区域火灾或爆炸 f)其他外部事件	a)控制系统故障(如硬件或软件失效、控制辅助系统失效) b)设备故障： 1)机械故障(如泵密封失效、泵或压缩机停机) 2)腐蚀/侵蚀/磨蚀 3)机械碰撞或振动 4)阀门故障 5)管道、容器和储罐失效 6)泄漏等 c)公用工程故障(如停水、停电、停气、停风等) d)其他故障	a)操作失误 b)维护失误 c)关键响应错误 d)作业程序错误 e)其他行为失误

6.2 在确定 IE 时，应遵循以下原则：

a) 宜对后果的原因进行审查，确保该原因为后果的有效 IE；

b) 应将每个原因细分为具体的失效事件，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；

c) 人员失误的根原因(如培训不完善)、设备的不完善测试和维护等不宜作为 IE。

7 独立保护层评估

7.1 IPL 确定原则

化工企业保护层作为 IPL 时，应满足以下基本要求：

a) 独立性：

1) 独立于 IE 的发生及其后果；

2) 独立于同一场景中的其他 IPL。

b) 有效性：

1) 能检测到响应的条件；

2) 在有效的时间内，能及时响应；

3) 在可用的时间内，有足够的能力采取所要求的行动；

4) 满足所选择的 PFD 的要求。

c) 安全性。应使用管理控制或技术手段减少非故意的或未授权的变动。

d) 变更管理。设备、操作程序、原料、过程条件等任何改动应执行变更管理程序，以满足变更后保护层的 IPL 要求。

e) 可审查性。应有可用的信息、文档和程序可查，以说明保护层的设计、检查、维护、测试和运行活动能够使保护层达到 IPL 的要求。

7.2 化工企业典型保护层及作为 IPL 的要求

化工企业典型保护层及作为 IPL 的要求见表 3。

表 3 化工企业典型保护层及作为 IPL 的要求

保护层	描述	说明	示例	作为 IPL 的要求	
				具体要求	通用要求
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	容器或管道设计可承受事故后果产生的高温、高压等	1)当本质安全设计用来消除某些场景时，不应作为 IPL 2)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	对于所有的保护层，作为 IPL 应满足以下要求： 1)应有控制手段防止非故意的或未授权的变动 2)应执行严格的变更管理程序，以满足变更后保护层的 IPL 要求 3)应有可用的信息、文档和程序可查，以说明保护层的设计、检查、维护、测试和运行活动能够使保护层达到 IPL 的要求
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，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。由传感器、逻辑控制器和最终执行元件组成	BPCS 可以提供三种不同类型的安全功能作为 IPL： 1)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 IE 发生 2)报警行动：识别超出正常范围的过程偏差，并向操作人员提供报警信息，促使操作人员采取行动(控制过程或停车) 3)逻辑行动：行动将导致停车或采取动作使过程处于安全状态	精馏塔、加热炉等基本过程控制系统	1)BPCS 作为 IPL 应满足以下要求： ——BPCS 应与安全仪表系统(SIS)在物理上分离，包括传感器、逻辑控制器和最终执行元件 ——BPCS 故障不是造成 IE 的原因 2)在同一个场景中，当满足 IPL 的要求时，具有多个回路的 BPCS 宜作为一个 IPL。BPCS 多个回路作为 IPL 的具体评估方法可参见附录 D 3)当 BPCS 通过报警或其他形式提醒操作人员采取行动时，宜将这种保护考虑为报警和人员响应保护层	

表 3　化工企业典型保护层及作为 IPL 的要求（续）

保护层	描述	说明	示例	作为 IPL 的要求	
				具体要求	通用要求
报警和人员响应	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	反应器温度高报警和人员响应	1)操作人员应能够得到采取行动的指示或报警 2)操作人员应训练有素，能够完成特定报警所要求的操作任务 3)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 4)操作人员应有足够的响应时间 5)操作人员身体条件合适等	对于所有的保护层，作为 IPL 应满足以下要求： 1）应有控制手段防止非故意的或未授权的变动 2）应执行严格的变更管理程序，以满足变更后保护层的 IPL 要求 3）应有可用的信息、文档和程序可查，以说明保护层的设计、检查、维护、测试和运行活动能够使保护层达到 IPL 的要求
安全仪表功能（SIF）	安全仪表功能通过检测超限（异常）条件，控制过程进入功能安全状态。一个安全仪表功能由传感器、逻辑控制器和最终执行元件组成，具有一定的 SIL	安全仪表功能 SIF 在功能上独立于 BPCS。SIL 分级可见 GB/T 21109	1）安全仪表功能 SIL1 2）安全仪表功能 SIL2 3）安全仪表功能 SIL3	1)SIF 在功能上独立于 BPCS 2)SIF 的规格、设计、调试、检验、维护和测试应按 GB/T 21109 的有关规定执行	
物理保护	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	1)安全阀 2)爆破片 3)安全阀和爆破片串联 4)放空阀	1)独立于场景中的其他保护层 2)在确定安全阀、爆破片等设备的 PFD 时，应考虑其实际运行环境中可能出现的污染、堵塞、腐蚀、不恰当维护等因素对 PFD 进行修正 3)当物理保护作为 IPL 时，应考虑物理保护起作用后可能造成的其他危害，并重新假设 LOPA 场景进行评估	

表 3　化工企业典型保护层及作为 IPL 的要求（续）

保护层	描述	说明	示例	作为 IPL 的要求	
				具体要求	通用要求
释放后保护设施	危险物质释放后，用来降低事故后果的保护设施（如防止大面积泄漏扩散、降低受保护设备和建筑物的冲击波破坏、防止容器或管道火灾暴露失效、防止火焰或爆轰波穿过管道系统等）	一般需要对事故后果进行定量评估，根据评估结果选择针对性释放后保护设施或确定保护设施的设计参数	1）火气系统：可燃气体和有毒气体检测报警系统、泄漏或火灾后紧急切断系统、火灾报警系统等 2）拦蓄或收集设施：防火堤、集液池及收集系统等 3）释放后安全处理系统：洗涤设施、有毒气体捕集及处理系统等 4）减少蒸发扩散的设施：如用于 LNG 的高倍数泡沫系统 5）防火设施：耐火涂层、防火门、阻火器、消防系统（水幕、自动灭火系统等） 6）防爆设施：防爆墙或防爆舱、隔爆器、泄压板、水雾系统、减爆剂、惰化系统等 7）防中毒设施：正压防护系统、中和系统等 8）其他：与消防联动的电视监视系统	1）独立于场景中的其他保护层 2）在确定阻火器、隔爆器等设备的 PFD 时，应考虑其实际运行环境中可能出现的污染、堵塞、腐蚀、不恰当维护等因素对 PFD 进行修正	对于所有的保护层，作为 IPL 应满足以下要求： 1）应有控制手段防止非故意的或未授权的变动 2）应执行严格的变更管理程序，以满足变更后保护层的 IPL 要求 3）应有可用的信息、文档和程序可查，以说明保护层的设计、检查、维护、测试和运行活动能够使保护层达到 IPL 的要求
工厂和社区应急响应	在初始释放之后被激活，其整体有效性受多种因素影响		主要包括消防队、工厂撤离、社区撤离、避难所和应急预案等	应确认其有效性	

7.3　不作为 IPL 的防护措施

通常不作为 IPL 的防护措施见表 4。

表 4　通常不作为 IPL 的防护措施

防护措施	说明
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 IPL
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 IPL

表 4　通常不作为 IPL 的防护措施（续）

防护措施	说明
正常的测试和检测	正常的测试和检测将影响某些 IPL 的 PFD，延长测试和检测周期可能增加 IPL 的 PFD
维护	维护活动将影响某些 IPL 的 PFD
通信	差的通信将影响某些 IPL 的 PFD
标识	标识自身不是 IPL，标识可能不清晰、模糊、容易被忽略等。标识可能影响某些 IPL 的 PFD
火灾保护	火灾保护的可用性和有效性受到所包围的火灾/爆炸的影响。如果在特定的场景中，企业能够证明它满足 IPL 的要求，则可将其作为 IPL

8　场景频率计算

8.1　风险和频率的定量计算

8.1.1　场景的发生频率计算如下：

$$f_i^{C} = f_i^{I} \times \prod_{j=1}^{J} PFD_{ij}$$
$$= f_i^{I} \times PFD_{i1} \times PFD_{i2} \times \cdots \times PFD_{ij} \quad \cdots\cdots(1)$$

式中：

f_i^{C} ——初始事件 i 的后果 C 的发生频率，单位为/a；

f_i^{I} ——初始事件 i 的发生频率，单位为/a；

PFD_{ij} ——初始事件 i 中第 j 个阻止后果 C 发生的 IPL 的 PFD。

8.1.2　在计算场景频率时，可根据需要对场景频率进行修正。

a）　存在使能事件或条件时：

$$f_i^{C} = f_i^{I} \times f_i^{E} \times \prod_{j=1}^{J} PFD_{ij} \quad \cdots\cdots(2)$$

式中：

f_i^{E}——使能事件或条件发生概率。

b）　采用点火概率、人员暴露和具体伤害的概率对不同后果场景频率进行修正。

1）　火灾发生的频率：

$$f_i^{fire} = f_i^{I} \times \left(\prod_{j=1}^{J} PFD_{ij}\right) \times P_{ig} \quad \cdots\cdots(3)$$

式中：

P_{ig}——点火概率。

2）　人员暴露于火灾中的频率：

$$f_i^{fire-exp} = f_i^{I} \times \left(\prod_{j=1}^{J} PFD_{ij}\right) \times P_{ig} \times P_{ex} \quad \cdots\cdots(4)$$

式中：

P_{ex}——人员暴露概率。

3）　火灾引起人员受伤的频率：

$$f_i^{fire-injury} = f_i^{I} \times \left(\prod_{j=1}^{J} PFD_{ij}\right) \times P_{ig} \times P_{ex} \times P_d$$

$$\cdots\cdots(5)$$

式中：

P_d——人员受伤或死亡概率。

4） 对于毒性影响，人员伤害的频率方程与火灾伤害方程相似，毒性影响不需要点火概率，式(5)变为：

$$f_i^{\text{toxic}} = f_i^{\text{I}} \times \left(\prod_{j=1}^{J} PFD_{ij}\right) \times P_{ex} \times P_d \quad \cdots\cdots(6)$$

8.2 初始事件发生频率和 IPL 的 PFD

8.2.1 初始事件发生频率和 IPL 的 PFD 数据可采用：

a） 行业统计数据；

b） 企业历史统计数据；

c） 基于失效模式、影响和诊断分析(FMEDA)及故障树分析(FTA)等的数据；

d） 其他可用数据等。

8.2.2 选择失效数据时，应满足以下要求：

a） 在整个分析过程中，使用的所有失效数据的选用原则应一致；

b） 选择的失效率数据应具有行业代表性或能代表操作条件；

c） 使用企业历史统计数据时，只有该历史数据充足并具有统计意义时才能使用；

d） 使用普通的行业数据时，可根据企业的具体条件对数据进行修正；

e） 可对失效频率数据取整至最近的整数数量级。

8.2.3 在确定 IE 发生频率和典型 IPL 的 PFD 时，应考虑实际的运行环境对发生频率或 PFD 的影响：

a） 当系统或操作不连续(装载/卸载、间歇工艺等)时，应根据其实际的运行时间对失效频率数据进行修正；

b） 在确定安全阀、阻火器或隔爆器等设备的 PFD 时，应考虑其实际运行环境中可能出现的污染、堵塞、腐蚀、不恰当维护等因素对 PFD 进行修正；

c） 典型 IE 发生频率和典型 IPL 的 PFD 参见附录 E。

9 风险评估与决策

9.1 对事故场景风险，可根据场景频率计算结果和后果等级，使用定量数值风险标准、风险矩阵等形式进行风险等级评估，定量数值风险标准和风险矩阵示例参见附录 F。

9.2 根据事故场景风险等级进行风险决策，风险决策宜采取 ALARP 原则，将事故场景风险降低到可接受风险水平，ALARP 和可接受风险水平概念参见附录 F。

10 LOPA 报告

10.1 LOPA 分析结束时，应生成 LOPA 记录表和报告。LOPA 分析案例和记录表形式可参见附录 G。

10.2 LOPA 报告应包括以下内容：

a） 场景的信息来源说明；

b） 企业的风险标准；

c） IE 发生频率和 IPL 的 PFD；

d） 场景中 IPL 和非 IPL 的评估结果；

e） 场景的风险评估结果；

f） 满足风险标准要求采取的行动及后续跟踪；

g） 如果有必要，对需要采取不同技术进行深入研究的问题提出建议；

h） 对分析期间所发现的不确定情况及不确定数据的处理；

i） 分析小组使用的所有图纸、说明书、数据表和危险分析报告等的清单(包括引用的版本号)；

j） 参加分析的小组成员名单。

10.3 LOPA 报告应经小组成员签字确认。若 LOPA 小组不能达成一致意见，应记录原因。

11 LOPA 后续跟踪及审查

11.1 宜对 LOPA 分析结果的执行情况进行后续跟踪，对 LOPA 提出的降低风险行动的实施情况进行落实。

11.2 LOPA 的程序和分析结果可接受相关的审查。

附 录 A
（规范性附录）
LOPA 基本程序

LOPA 基本程序如图 A.1 所示，包括：

a） 场景识别与筛选。LOPA 通常评估先前危害分析研究中识别的场景。分析人员可采用定性或定量的方法对这些场景后果的严重性进行评估，并根据后果严重性评估结果对场景进行筛选。

b） 初始事件(IE)确认。首先，选择一个事故场景，LOPA 一次只能选择一个场景；然后确定场景 IE。IE 包括外部事件、设备故障和人员行为失效。

c） 独立保护层(IPL)评估。评估现有的防护措施是否满足 IPL 的要求是 LOPA 的核心内容。

d） 场景频率计算。将后果、IE 频率和 IPL 的 PFD 等相关数据进行计算，确定场景风险。

e） 风险评估与决策。根据风险评估结果，确定是否采取相应措施降低风险。然后，重复步骤 b）至步骤 e)直到所有的场景分析完毕。

f） 后续跟踪与审查。LOPA 分析完成后，对提出降低风险措施的落实情况应进行跟踪。应对 LOPA 的程序和分析结果进行审查。

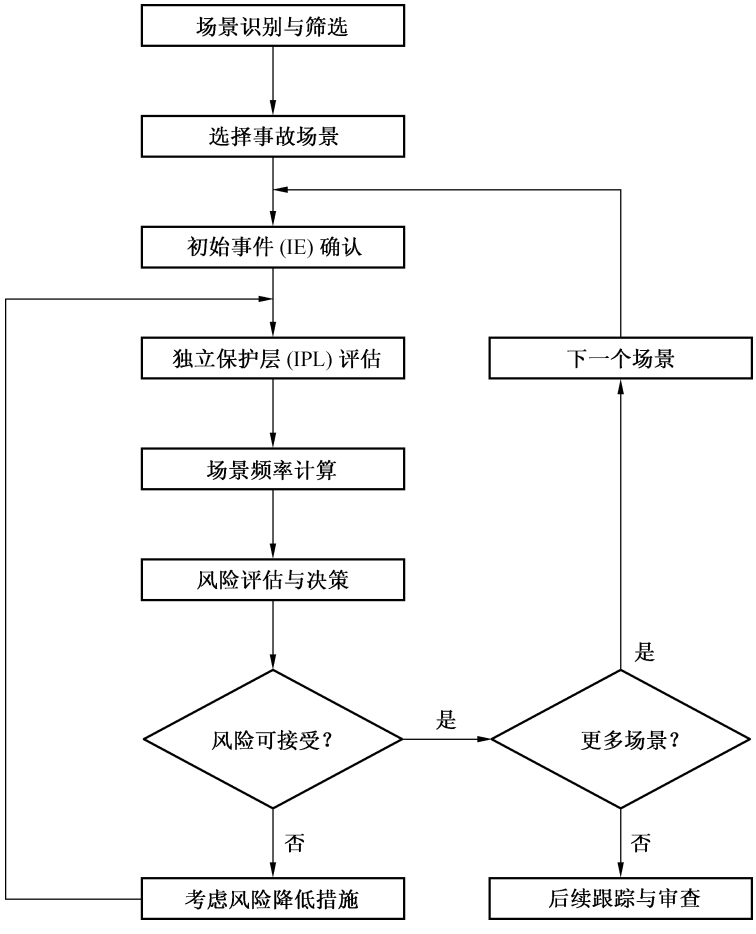
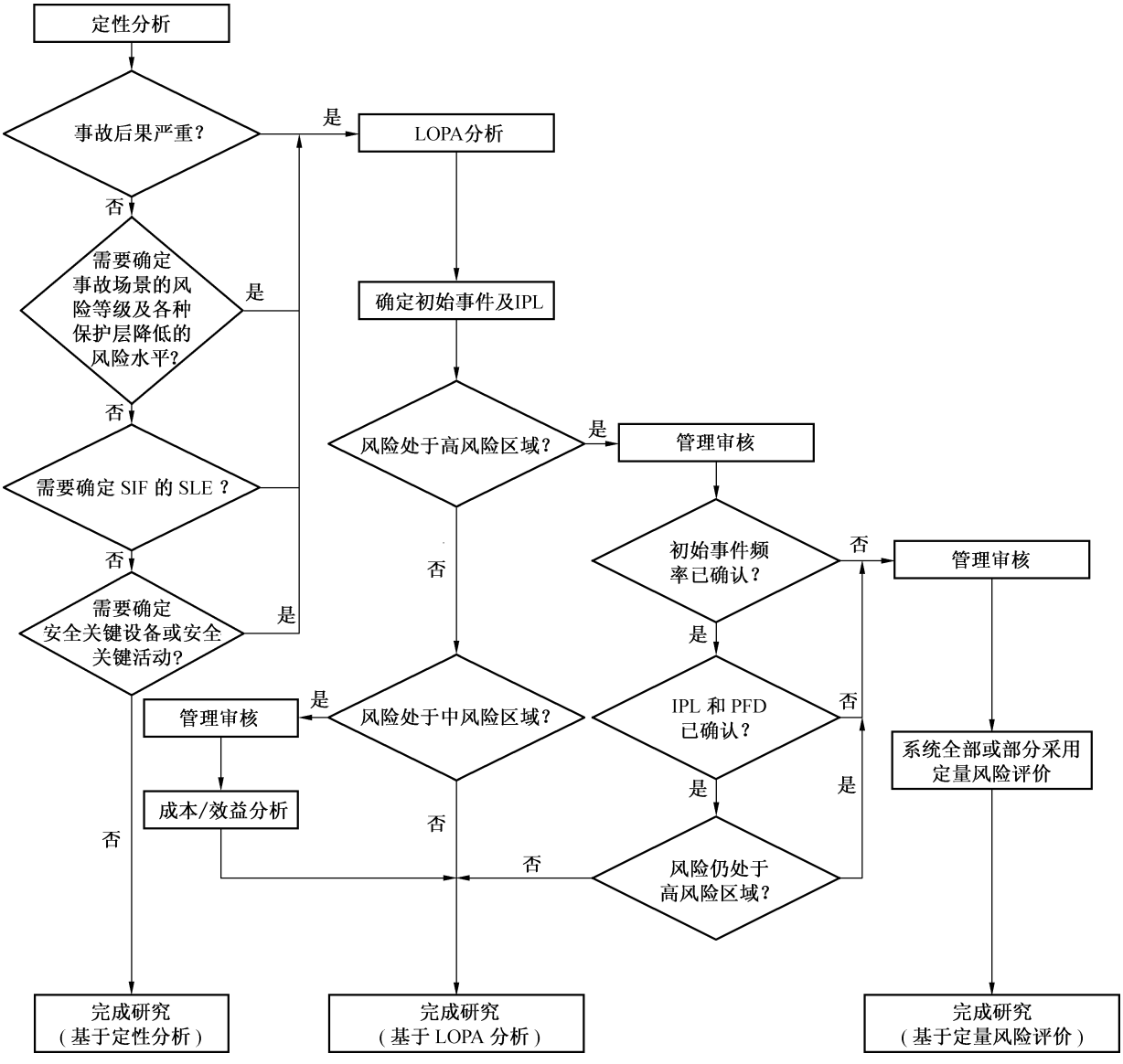


图 A.1 LOPA 基本程序

附 录 B
（资料性附录）
LOPA 应用时机



注： 事故后果是否严重可根据企业的风险标准确定，以表 F.3 为例，通常可认为 4 级及以上的后果为严重后果。

图 B.1 LOPA 的应用时机

附 录 C
（资料性附录）
HAZOP 信息与 LOPA 信息的关系

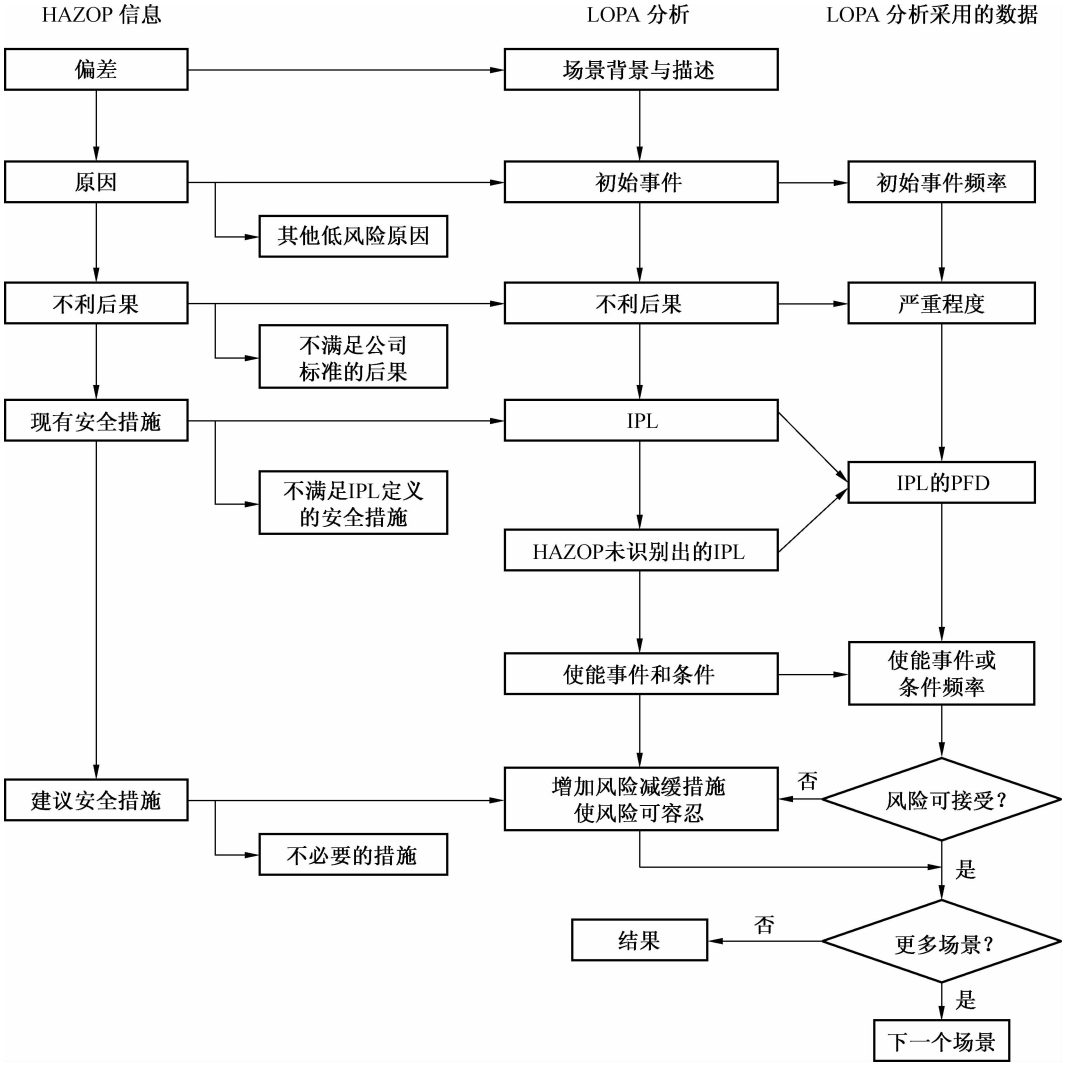


图 C.1 HAZOP 信息与 LOPA 信息的关系

附 录 D
（资料性附录）
BPCS 多个回路作为 IPL 的评估方法

D.1 同一 BPCS 多个功能回路作为 IPL 的评估方法

D.1.1 在同一场景中，当同一 BPCS 具有多个功能回路时，其 IPL 的评估可使用方法 A 或方法 B。

D.1.2 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控制器的 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。

D.1.3 方法 B 假设一个 BPCS 回路失效，最有可能是传感器或最终控制元件失效，而 BPCS 逻辑控制器仍能正常运行。BPCS 逻辑控制器的 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 D.1 所示，两个 BPCS 回路使用相同的逻辑控制器。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。

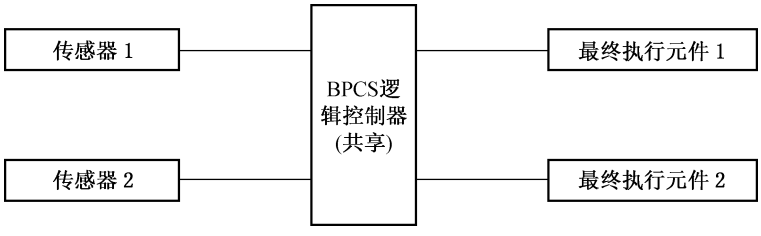


图 D.1 同一场景下共享同一 BPCS 逻辑控制器的多条回路

D.2 同一场景下，同一 BPCS 多个功能回路同时作为 IPL 的要求

D.2.1 同一场景下，同一 BPCS 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执行元件在 BPCS 回路的所有部件中具有最高的失效概率值。

D.2.2 如果传感器或最终执行元件是场景中其他 IPL 的公共组件或是 IE 的一部分，则多个回路不应作为多个 IPL。如图 D.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，如果最终执行元件（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。

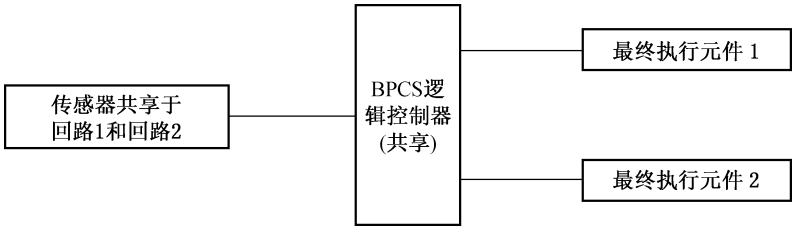
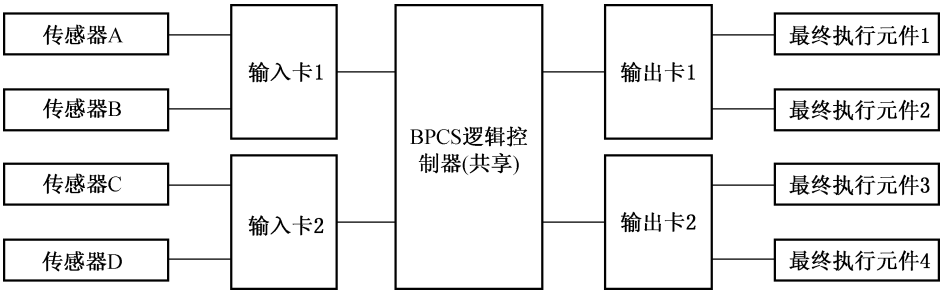


图 D.2 同一场景下共享传感器的 BPCS 回路

D.2.3 共享逻辑控制器输入卡或输出卡的额外 BPCS 回路不宜同时作为 IPL。如图 D.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→逻辑控制器→输出卡 1→最终执行元件 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→逻辑控制器→输出卡 2→最终执行元件 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→逻辑控制器→输出卡 1→最终执行元件 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。



注： 1～4 是最终执行元件。

图 D.3 相同场景下共享输入/输出卡的影响

D.2.4 如果 IE 不涉及 BPCS 逻辑控制器失效，每一个回路均满足 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 D.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，最多只有两个回路被作为 IPL。

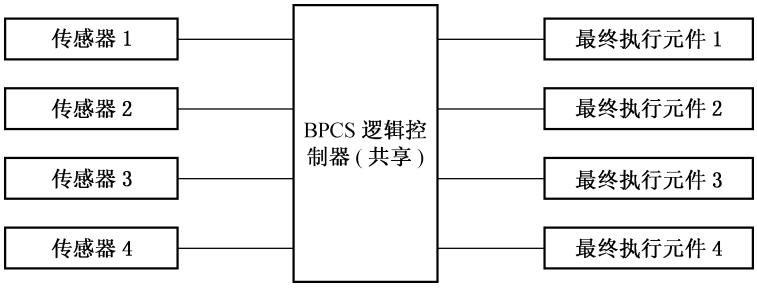


图 D.4 相同场景下 BPCS 功能回路作为 IPL 的最大数量

D.2.5 所有 BPCS 回路 IPL 总的 PFD，不宜低于 1×10^{-2}。

D.2.6 最终执行元件可以是机械动作（如关闭阀门、启动泵）或一种是机械动作，另一种是要求人员采取行动的报警。在同一场景中，不宜将两个人员响应同时作为 IPL，除非证明它们完全独立并且满足人员行动作为 IPL 的所有要求。

D.2.7 IE 或使能事件涉及 BPCS 回路失效时，在同一场景中，宜只将 1 个 BPCS 回路作为 IPL。如果人员失效是 IE，不宜将启动人员行动的 BPCS 报警视为 IPL。

D.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

D.3.1 对数据与数据分析的要求如下：

a) 方法 B 假设 BPCS 逻辑控制器的 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：

1) BPCS 逻辑控制器、输入/输出卡、传感器、最终执行元件、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。

b） 对这些数据的分析应包括：

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 逻辑控制器 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。

D.3.2 对分析人员的要求如下：

a） 分析人员应能够：

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。

b） 分析小组或人员应具有相关专业知识，例如：

1） 对 BPCS 逻辑控制器具有足够低的 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。

c） 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。

附 录 E
（资料性附录）
失效数据

表 E.1 IE 典型频率值

单位为每年

IE	频率范围
压力容器疲劳失效	10^{-5}～10^{-7}
管道疲劳失效－100m－全部断裂	10^{-5}～10^{-6}
管线泄漏(10%截面积)－100m	10^{-3}～10^{-4}
常压储罐失效	10^{-3}～10^{-5}
垫片/填料爆裂	10^{-2}～10^{-6}
涡轮/柴油发动机超速,外套破裂	10^{-3}～10^{-4}
第三方破坏(挖掘机、车辆等外部影响)	10^{-2}～10^{-4}
起重机载荷掉落	(10^{-3}～10^{-4})/起吊
雷击	10^{-3}～10^{-4}
安全阀误开启	10^{-2}～10^{-4}
冷却水失效	1～10^{-2}
泵密封失效	10^{-1}～10^{-2}
卸载/装载软管失效	1～10^{-2}
BPCS 仪表控制回路失效	1～10^{-2}
调节器失效	1～10^{-1}
小的外部火灾(多因素)	10^{-1}～10^{-2}
大的外部火灾(多因素)	10^{-2}～10^{-3}
LOTO(锁定、标定)程序失效(多个元件的总失效)	(10^{-3}～10^{-4})/次
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^{-1}～10^{-3})/次

表 E.2 某公司采用的 IE 典型频率值

单位为每年

分类	IE	频率
阀门	1)单向阀完全失效	1
	2)单向阀卡涩	1×10^{-2}
	3)单向阀内漏(严重)	1×10^{-5}
	4)垫圈或填料泄漏	1×10^{-2}
	5)安全阀误开或严重泄漏	1×10^{-2}
	6)调节器失效	1×10^{-1}
	7)电动或气动阀门误动作	1×10^{-1}

表 E.2 某公司采用的 IE 典型频率值（续）

单位为每年

分类	IE	频率
容器和储罐	1)压力容器灾难性失效	1×10^{-6}
	2)常压储罐失效	1×10^{-3}
	3)过程容器沸腾液体扩展蒸气云爆炸(BLEVE)	1×10^{-6}
	4)球罐沸腾液体扩展蒸气云爆炸(BLEVE)	1×10^{-4}
	5)容器小孔(≤50 mm)泄漏	1×10^{-3}
公用工程	1)冷却水失效	1×10^{-1}
	2)断电	1
	3)仪表风失效	1×10^{-1}
	4)氮气(惰性气体)系统失效	1×10^{-1}
管道和软管	1)泄漏(法兰或泵密封泄漏)	1
	2)弯曲软管微小泄漏(小口径)	1
	3)弯曲软管大量泄漏(小口径)	1×10^{-1}
	4)加载或卸载软管失效(大口径)	1×10^{-1}
	5)中口径(≤150 mm)管道大量泄漏	1×10^{-5}
	6)大口径(>150 mm)管道大量泄漏	1×10^{-6}
	7)管道小泄漏	1×10^{-3}
	8)管道破裂或大泄漏	1×10^{-5}
施工与维修	1)外部交通工具的冲击(假定有看守员)	1×10^{-2}
	2)吊车载重掉落(起吊次数/a)	1×10^{-3}
	3)操作维修加锁加标记(LOTO)规定没有遵守	1×10^{-3}
操作失误	1)无压力下的操作失误(常规操作)	1×10^{-1}
	2)有压力下的操作失误(开停车、报警)	1
机械故障	1)泵体坏(材质变化)	1×10^{-3}
	2)泵密封失效	1×10^{-1}
	3)有备用系统的泵和其他转动设备失去流量	1×10^{-1}
	4)透平驱动的压缩机停转	1
	5)冷却风扇或扇叶停转	1×10^{-1}
	6)电机驱动的泵或压缩机停转	1×10^{-1}
	7)透平或压缩机超载或外壳开裂	1×10^{-3}
仪表	BPCS(基本过程控制系统)回路失效	1×10^{-1}
外部事件	1)雷电击中	1×10^{-3}
	2)外部大火灾	1×10^{-2}
	3)外部小火灾	1×10^{-1}
	4)易燃蒸气云爆炸	1×10^{-3}

表 E.3 化工行业典型 IPL 的 PFD

IPL		说明 （假设具有完善的设计基础、充足的检测和维护程序、良好的培训）	PFD
本质安全设计		如果正确执行，将大大地降低相关场景后果的频率	$1\times10^{-1}\sim1\times10^{-6}$
BPCS		如果与 IE 无关，BPCS 可作为一种 IPL	$1\times10^{-1}\sim1\times10^{-2}$
关键报警和人员响应	人员行动，有 10 min 的响应时间	行动应具有单一性和可操作性	$1.0\sim1\times10^{-1}$
	人员对 BPCS 指示或报警的响应，有 40 min 的响应时间		1×10^{-1}
	人员行动，有 40 min 的响应时间		$1\times10^{-1}\sim1\times10^{-2}$
安全仪表功能	安全仪表功能 SIL 1	见 GB/T 21109	$\geqslant1\times10^{-2}\sim<1\times10^{-1}$
	安全仪表功能 SIL 2		$\geqslant1\times10^{-3}\sim<1\times10^{-2}$
	安全仪表功能 SIL 3		$\geqslant1\times10^{-4}\sim<1\times10^{-3}$
物理保护	安全阀	此类系统有效性对服役的条件比较敏感	$1\times10^{-1}\sim1\times10^{-5}$
	爆破片		$1\times10^{-1}\sim1\times10^{-5}$
释放后保护措施	防火堤	降低由于储罐溢流、断裂、泄漏等造成严重后果的频率	$1\times10^{-2}\sim1\times10^{-3}$
	地下排污系统	降低由于储罐溢流、断裂、泄漏等造成严重后果的频率	$1\times10^{-2}\sim1\times10^{-3}$
	开式通风口	防止超压	$1\times10^{-2}\sim1\times10^{-3}$
	耐火涂层	减少热输入率，为降压、消防等提供额外的响应时间	$1\times10^{-2}\sim1\times10^{-3}$
	防爆墙/舱	限制冲击波，保护设备/建筑物等，降低爆炸重大后果的频率	$1\times10^{-2}\sim1\times10^{-3}$
	阻火器或防爆器	如果、安装和维护合适，这些设备能够防止通过管道系统或进入容器或储罐内的潜在回火	$1\times10^{-1}\sim1\times10^{-3}$
	遥控式紧急切断阀	切断物料，防止事故发生或事故后果扩大	$1\times10^{-1}\sim1\times10^{-2}$

附 录 F
（资料性附录）
风险标准和 ALARP 原则

F.1 风险标准

表 F.1 数值风险标准(厂外个体风险)

单位为每年

部 门	可容许风险	可忽略风险
荷兰环境保护和城市规划部 VROM(现存装置)	1×10^{-5}	1×10^{-8}
荷兰环境保护和城市规划部 VROM(新建设施)	1×10^{-6}	1×10^{-8}
英国健康和安全局 HSE(现有设施)	1×10^{-4}	1×10^{-6}
英国健康和安全局 HSE(新建居民区)	3×10^{-6}	3×10^{-7}
英国(新建核电站)	1×10^{-5}	1×10^{-6}
英国(新建危险品运输)	1×10^{-4}	1×10^{-6}
香港(新建和已建装置)	1×10^{-5}	—
新加坡(新建和已建装置)	5×10^{-5}	1×10^{-6}
马来西亚(新建和已建装置)	1×10^{-5}	1×10^{-6}
澳大利亚(新建和已建装置)	5×10^{-5}	5×10^{-7}
加拿大	1×10^{-4}	1×10^{-6}
巴西(新建和已建装置)	1×10^{-5}	1×10^{-6}

表 F.2 风险评估矩阵

后果等级	$10^{-6}\sim10^{-7}$	$10^{-5}\sim10^{-6}$	$10^{-4}\sim10^{-5}$	$10^{-3}\sim10^{-4}$	$10^{-2}\sim10^{-3}$	$10^{-1}\sim10^{-2}$	$1\sim10^{-1}$
5	低	中	中	高	高	很高	很高
4	低	低	中	中	高	高	很高
3	低	低	低	中	中	中	高
2	低	低	低	低	中	中	中
1	低	低	低	低	低	中	中
频率等级/a							

风险等级说明：

低：不需采取行动。

中：可选择性的采取行动。

高：选择合适的时机采取行动。

很高：立即采取行动。

表 F.3 后果定性分级方法

等级	严重程度	分类			
		人员	财产	环境	声誉
1	低后果	医疗处理，不需住院；短时间身体不适	损失极小	事件影响未超过界区	企业内部关注，形象没有受损
2	较低后果	工作受限，轻伤	损失较小	事件不会受到管理部门的通报或违反允许条件	社区、邻居、合作伙伴影响
3	中后果	严重伤害，职业相关疾病	损失较大	事件受到管理部门的通报或违反允许条件	本地区内影响；政府管制，公众关注负面后果
4	高后果	1～2 人死亡或丧失劳动能力，3～9 人重伤	损失很大	重大泄漏，给工作场所外带来严重影响	国内影响；政府管制，媒体和公众关注负面后果
5	很高后果	3 人以上死亡，10 人以上重伤	损失极大	重大泄漏，给工作场所外带来严重的环境影响，且会导致直接或潜在的健康危害	国际影响

F.2 ALARP 原则

F.2.1 ALARP 原则

ALARP 原则(图 F.1)指在当前的技术条件和合理的费用下，对风险的控制要做到在合理可行的原则下“尽可能的低”。按照 ALARP 原则，风险区域可分为：

a) 不可接受的风险区域。在本标准 F.2 中指高风险和很高风险区域。在这个区域，除非特殊情况，风险是不可接受的。

b) 允许的风险区域。在本标准 F.2 中指中风险区域。在这个区域内必须满足以下条件之一时，风险才是可允许的：

   1) 在当前的技术条件下，进一步降低风险不可行；

   2) 降低风险所需的成本远远大于降低风险所获得的收益。

c) 广泛可接受的风险区域。在本标准 F.2 中指低风险区域。在这个区域，剩余风险水平是可忽略的，一般不要求进一步采取措施降低风险。

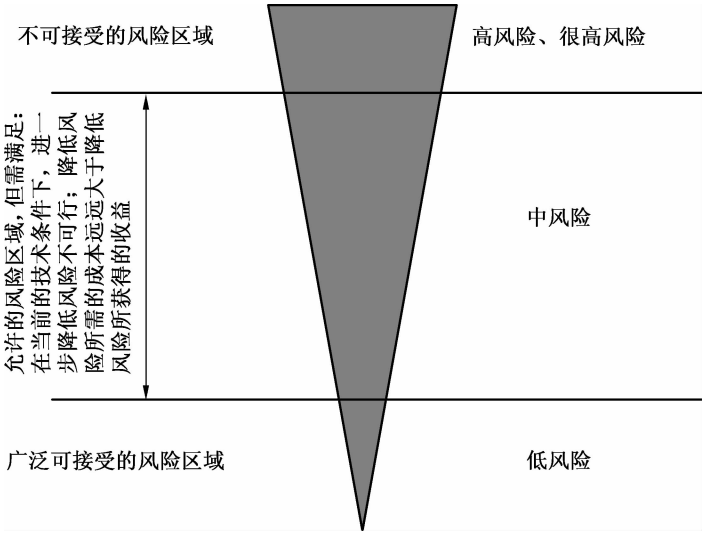


图 F.1　ALARP 原则

ALARP 原则推荐在合理可行的情况下，把风险降低到“尽可能的低”。如果一个风险位于两种极端情况（高风险及以上不可接受区域和广泛可接受的风险区域）之间，如果使用了 ALARP 原则，则所得到的风险可认为是可允许的风险。

如果风险处于高风险及以上区域，则该风险是不可接受的，应把它降低到可接受风险水平。

在广泛可接受的低风险区域，不需要进一步降低风险，但有必要保持警惕以确保风险维持在这一水平。

F.2.2　可接受风险水平

根据 ALARP 原则，可接受风险水平指允许的风险区域或广泛可接受的风险区域。

附 录 G
（资料性附录）
LOPA 示例

G.1 正己烷缓冲罐溢流

G.1.1 工艺描述

简化 P&ID 示例见图 G.1。示例的详细描述可参见 *Layer of Protection Analysis—Simplified Process Risk Assessment*。来自上游工艺单元的正己烷进入正己烷缓冲罐 T-401。正己烷供料管道总是带压。正己烷缓冲罐液位受液位控制回路(LIC-90)控制,LIC-90 检测储罐液位,通过调节液位阀(LV-90)控制液位。正己烷输往下游工艺使用。LIC 回路包括提醒操作人员的高液位报警(LAH-90)。储罐总容量为 30 t,通常盛装一半的容量。储罐位于防火堤内,该防火堤能够容纳 45 t 正己烷。

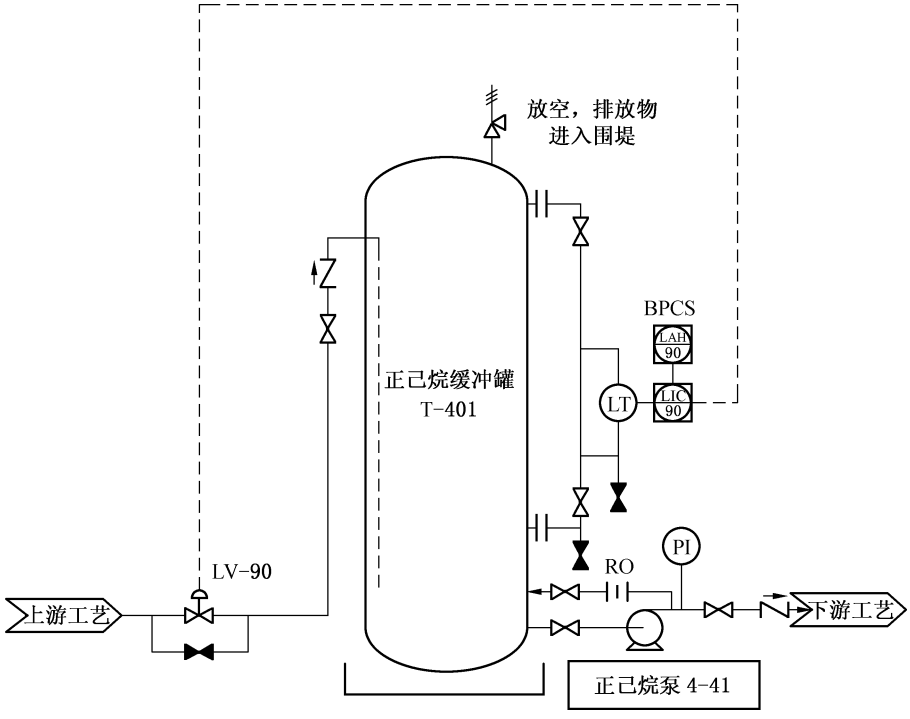


图 G.1 正己烷缓冲罐溢流

G.1.2 场景识别与筛选

采用前期进行的 HAZOP 分析作为场景信息来源。正己烷缓冲罐 T-401 的 HAZOP 分析结果见表 G.1。根据表 F.3 筛选进行 LOPA 分析的场景。本例选择分析的场景为正己烷缓冲罐溢流,防火堤发生失效,导致大面积火灾,造成人员的伤亡,后果等级为 5 级。

表 G.1　正己烷缓冲罐 T-401 HAZOP 分析

序号	偏差	原因	后果	现有防护措施	建议
1	液位高	流量控制阀 LV-90 误开大(如液位控制 LIC 失效，操作人员失误等)导致至正己烷缓冲罐 T-401 管线流量大	高压(见 5)	1)液位监测，高液位报警 2)单元操作程序	建议安装一个 SIS，在 T-401 高液位时切断进料
2	液位低	上游工艺至正己烷缓冲罐 T-401 管线流量小或无流量	无后果：在下游倒空供料罐前，如果不填充，将引起潜在的过程中断		
3	温度高		无关心的后果		
4	温度低	低的环境温度，而缓冲罐内有水(见 7)	缓冲罐底部或缓冲罐排水线或仪表线积累的水冻结，导致排水线断裂和泄漏		
5	压力高	高液位(见 1)	1)正己烷通过释放阀泄放到防火堤内；如果防火堤不能包容释放物，可能造成大面积火灾 2)泄漏(如果超压值超过缓冲罐额定压力)(见 8)		
6	压力低	在蒸气吹扫后，冷却前缓冲罐发生堵塞	真空下缓冲罐塌陷导致设备破坏	标准程序和容器蒸气吹扫检查	
7	污染物浓度高	在蒸气吹扫和冲洗后，水没有完全排出	在低的环境温度期间，缓冲罐内积累的水可能冻结(见 4)		
8	包容物损失	1)腐蚀/侵蚀 2)外部影响(如火灾) 3)液位高(见 1) 4)垫片、填料或密封失效 5)不适当的维护 6)仪表或仪表线失效 7)材质缺陷 8)采样阀泄漏 9)通风口和排水阀泄漏 10)低温(见 4)	正己烷泄漏，如果防火堤不能包容释放物，可能造成大面积火灾，造成人员伤亡	1)操作和维护程序，需要时隔离 2)能手动隔离缓冲罐 3)按照规范和标准进行预防性检测 4)安全阀，释放到缓冲罐防火堤内 5)防火堤容积能容纳正己烷 45 t(1.5 倍缓冲罐能力) 6)紧急响应程序	

G.1.3　IE 确认

本例选定 IE 为 BPCS 液位控制回路失效，根据表 E.1，其失效频率为 1×10^{-1}/a。

G.1.4 IPL 评估

对场景的防护措施开展 IPL 评估，包括：

a） 防火堤。一旦发生罐体溢流，合适的防火堤可以包容这些溢流物。如果防火堤失效，将发生大面积扩散，从而发生潜在的火灾、损害和死亡。防火堤满足 IPL 所有的要求，包括：

1） 如果按照设计运行，防火堤可有效地包容储罐的溢流；

2） 防火堤独立于任何其他独立保护层和 IE；

3） 可以审查防火堤的设计、建造和目前的状况。

对于本例，根据表 E.3，防火堤的 PFD 取 1×10^{-2}。

b） BPCS 报警和人员响应行动。在本例中，人员行动不作为 IPL，原因如下：

1） 由于操作人员不总是在现场，在防火堤失效导致重大释放前，不能假设独立于任何报警的操作人员行动能有效地检测和阻止释放。

2） BPCS 液位控制回路失效(IE)导致系统不能产生报警，从而不能提醒操作人员采取行动以阻止缓冲罐进料。因此，BPCS 产生的任何报警不能完全独立于 BPCS 系统，不能作为独立保护层。

c） 安全阀。缓冲罐上的安全阀无法防止缓冲罐发生溢流，因此，对于本场景，安全阀不是 IPL。

G.1.5 场景频率计算

取点火概率为 1，人员暴露概率为 0.5，人员伤亡概率为 0.5，则后果发生频率为：

$$\begin{aligned} f_i^{C} &= f_i^{I} \times PFD_{\text{dike}} \times P_{ig} \times P_{ex} \times P_d \\ &= (1\times10^{-1}/\text{a}) \times (1\times10^{-2}) \times 1 \times 0.5 \times 0.5 \\ &= 2.5\times10^{-4}/\text{a} \\ &= 2\times10^{-4}/\text{a}(\text{取整}) \end{aligned}$$

式中：

f_i^{C} ——初始事件 i 的后果 C 的发生频率，单位为 /a；

f_i^{I} ——初始事件 i 的发生频率，单位为 /a；

PFD_{dike} ——防火堤的 PFD；

P_{ig} ——点火概率；

P_{ex} ——人员暴露概率；

P_d ——人员伤亡概率。

G.1.6 风险评估与决策

缓冲罐 LIC 失效，溢流物未被防火堤包容，溢出物被点燃，造成人员伤亡，后果等级为 5 级。事件发生的频率为 2×10^{-4}/a。根据后果等级为 5 级和频率为 2×10^{-4}/a，查询表 F.2，其风险等级为高风险，要求：选择合适的时机采取行动。

分析小组决定安装一个独立的 SIF，用于检测和阻止溢流。本 SIF 采用独立的液位传感器、逻辑控制器和独立的截断阀，见图 G.2 中粗线部分。当检测到高液位时，该 SIF 联锁关流量控制阀 LV-90 和远程截断阀。可根据企业具体的风险控制要求，确定该 SIF 的 SIL。在本例中，确定该 SIF 的 FPD 为 1×10^{-2}(SIL1)。对于场景，SIF 将释放事件的频率从 2×10^{-4}/a 降低到 2×10^{-6}/a。在风险矩阵中，对于后果等级为 5 级、频率为 2×10^{-6}/a 的事件，其风险等级为中风险，要求：可选择性地采取行动。此时，企业可采用成本效益分析，决定是否需采用额外的措施进一步降低风险。

G.1.7 LOPA 记录表

本案例 LOPA 记录表见表 G.2。

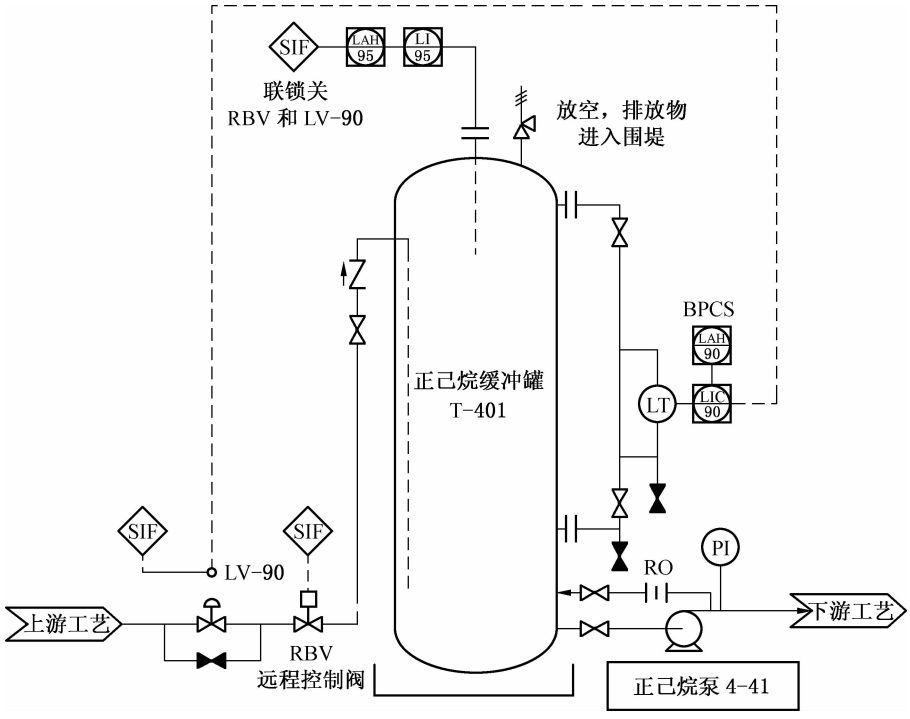


图 G.2　正己烷缓冲罐溢流(增加 IPL 后)

表 G.2 LOPA 记录表

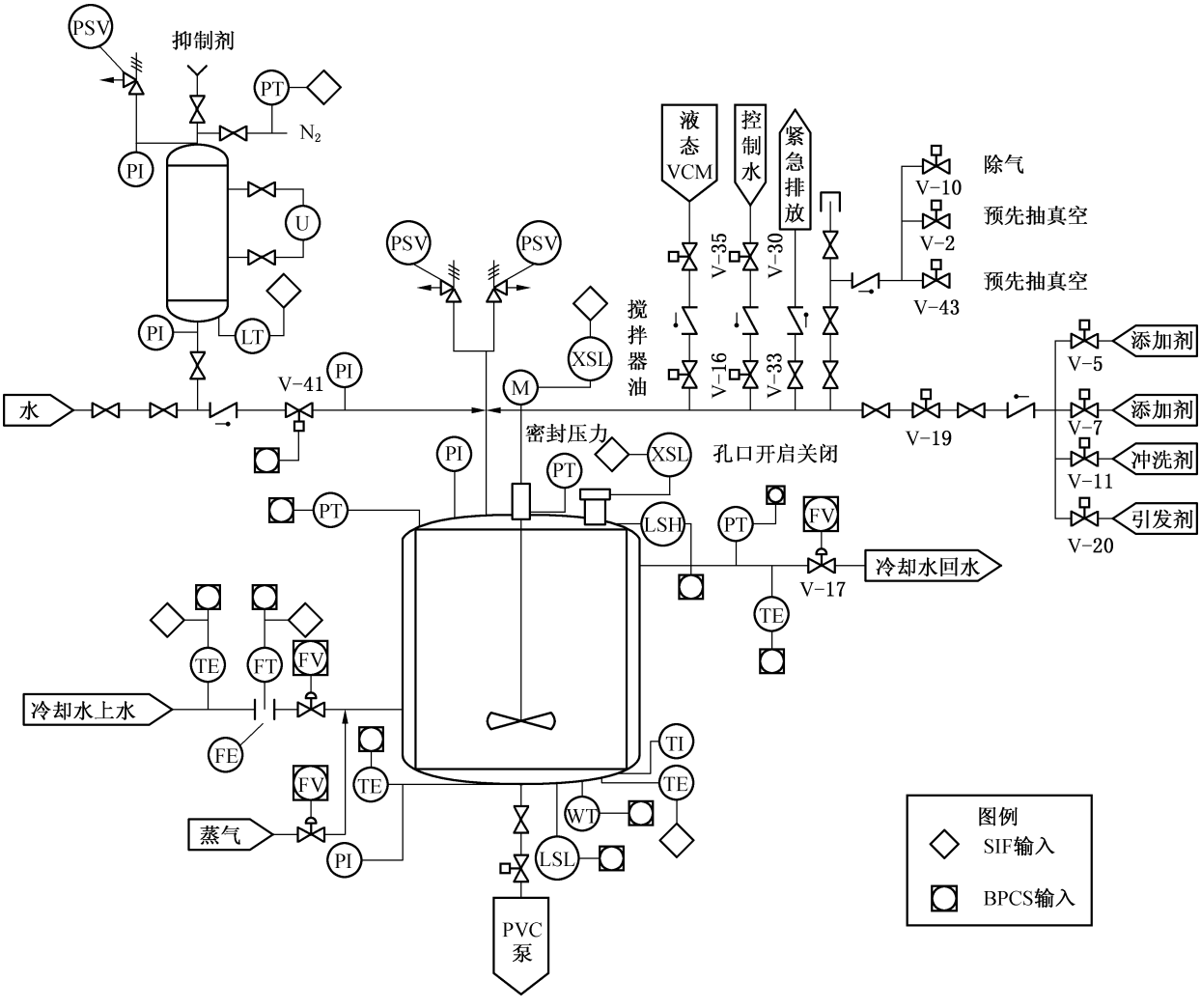
公司名称		装置名称		时间	
工艺单元		分析组成员		图纸号	
分析节点	正己烷缓冲罐				

序号	场景	后果		初始事件		使能必要事件/条件		条件修正			IPL			其他保护措施	后果发生频率	现有风险等级	需求的 SIL 等级或建议的 IPL			减缓后的后果发生频率	减缓后的风险等级	备注
		描述	等级	描述	频率/a	描述	概率	点火概率	人员暴露率	致死概率	描述	IPL类别	PFD				描述	IPL类别	PFD			
1	正己烷缓冲罐溢流，溢流物未被防火堤包容	由于储罐溢流和防火堤失效，导致释放的正己烷流出防火堤，发生火灾和人员伤亡	5	BPCS LIC 控制回路失效	1×10^{-1}	—	—	1	0.5	0.5	防火堤	释放后保护设施	1×10^{-2}	人员响应行动	2.5×10^{-4}	高风险	增加一个独立的SIF，用于检测和阻止溢流	SIF	1×10^{-2}（SIL 1）	2.5×10^{-6}	中风险	1. 人员行动不作为IPL，原因如下： ——操作人员不总是在现场 ——BPCS液位控制回路失效（IE）导致系统不能产生报警，从而不能提醒操作人员采取行动以阻止缓冲罐进料 2. 企业可采用成本效益分析，决定是否需采用额外的措施进一步降低风险

G.2 PVC 反应器

G.2.1 工艺描述

图 G.3 为氯乙烯单体(VCM)生产聚氯乙烯(PVC)工艺的简化 P&ID 图。示例的详细描述可参见 *Layer of Protection Analysis—Simplified Process Risk Assessment*。此过程为间歇聚合反应。水、液态 VCM、引发剂和添加剂通过同一喷管注入搅动的夹套反应器内。注入喷管与安全阀(PSV)相连接,抑制剂也可通过同一喷管添加。



注: 一些 SIFs(如火灾、气体和手动跳车)没有绘制出。

图 G.3 PVC 工艺的简化 P&ID 图

G.2.2 场景识别与筛选

根据前期进行的危害分析,通过后果分级表 F.3,筛选进行 LOPA 的场景。表 G.3 为筛选出的 LOPA 场景。本例以场景 1 为例进行分析。场景 1 为冷却水失效,导致反应失控,反应器潜在的超压、泄漏、断裂,造成人员受伤和死亡,后果等级为 5 级。

表 G.3 筛选出的 LOPA 场景

场景 1	冷却水失效，导致反应失控，反应器潜在的超压、泄漏、断裂，潜在的受伤和死亡	场景 5	人员错误——注入 2 倍催化剂的量，导致潜在的反应失控，超压、泄漏、断裂，受伤和死亡
场景 2	搅拌机电动机转动失效，导致潜在的反应失控，超压、泄漏、断裂，受伤和死亡	场景 6	BPCS 液位控制失效，导致反应器溢流，潜在的反应器超压、泄漏、断裂，受伤和死亡
场景 3	停电(大面积)，导致潜在的反应失控，超压、泄漏、断裂，受伤和死亡	场景 7	在升温期间，BPCS 温度控制失效，潜在的反应器超压、泄漏、断裂，受伤和死亡
场景 4	冷却泵失效(停电)，导致潜在的反应失控，超压、泄漏、断裂，受伤和死亡	场景 8	搅拌器密封失效，导致潜在的 VCM 泄漏，潜在的火灾、爆炸、受伤和死亡

G.2.3 初始事件确认

本例选定 IE 为冷却水失效，根据表 E.1，其失效频率为 1×10^{-1}。冷却水损失引起反应失控的反应器条件概率为 0.5。

G.2.4 IPL 评估

对场景的防护措施开展 IPL 评估，包括：

a) BPCS 报警和人员响应行动。冷却水失效时，BPCS 将会产生低流量报警，人员添加抑制剂。BPCS 报警和人员响应可满足 IPL 的要求，包括：

1) BPCS 报警和人员响应独立于 IE 和其他独立保护层；
2) 仅要求操作人员执行添加抑制剂的行动，任务具有单一性和可操作性；
3) 操作人员有足够的响应时间；
4) 如果操作人员训练有素，身体条件合适，则能够完成报警所触发的操作任务。

对于本例，根据表 E.3，该 IPL 的 PFD 取 1×10^{-1}。

b) 安全阀。安全阀可防止反应器发生超压泄漏，但是由于安全阀放空与抑制剂的添加共用同一管道，无法保证安全阀放空与抑制剂的添加可以同时进行，因此需修改安全阀设计，安全阀安装独立的放空管线。此外，考虑在安全阀下增加氮气吹扫，以最小化管线或阀门进口聚合物沉积或冻结。变更后，如果安全阀安装和维护符合 IPL 的要求，可作为 IPL。

对于本例，根据表 E.3，变更后该 IPL 的 PFD 取 1×10^{-2}。

c) 紧急冷却系统(蒸气涡轮机)。在本例中，紧急冷却系统不能作为 IPL，因为其不独立于 IE，与冷却水系统有多个公共元件(管线、阀门等)。这些公共元件在引起冷却水失效时，也会导致紧急冷却系统失效。

G.2.5 场景频率计算

后果发生频率为：

$$\begin{aligned} f_i^{C} &= f_i^{I} \times P_c \times PFD_{BPCS} \times PFD_{PSV} \\ &= (1 \times 10^{-1}/a) \times 0.5 \times (1 \times 10^{-2}) \times 1 \times 10^{-1} \\ &= 5 \times 10^{-5}/a \end{aligned}$$

式中：

f_i^{C} ——IEi 的后果 C 的发生频率，单位为/a；

f_i^{I} ——IEi 的发生频率，单位为/a；

P_c ——条件概率；

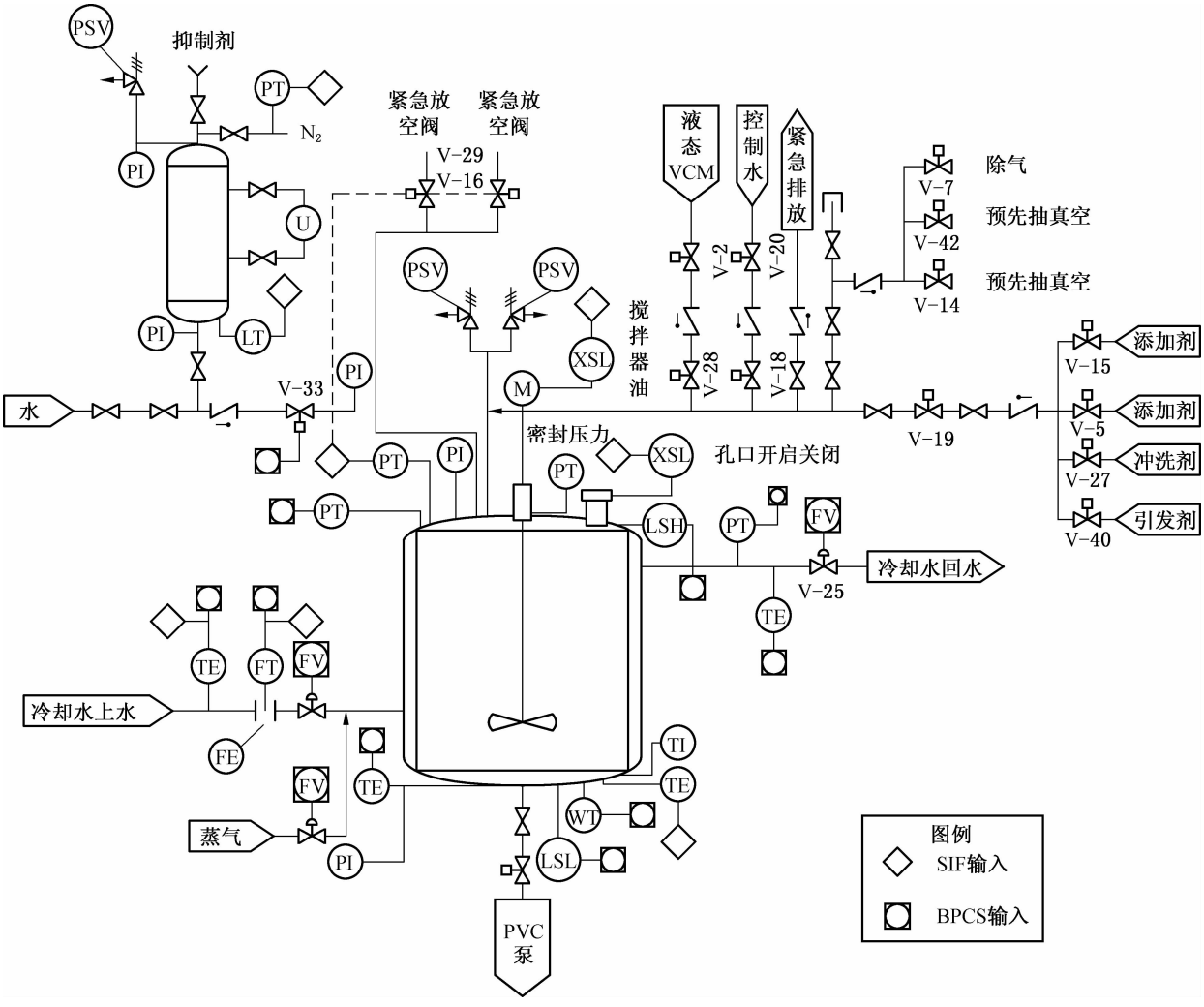
PFD_{BPCS} ——BPCS 报警和人员响应行动的 PFD；

PFD_{PSV} ——安全阀的 PFD。

G.2.6 风险评估与决策

冷却水失效，导致反应失控，反应器潜在的超压、泄漏、断裂，潜在的受伤和死亡，后果等级为 5 级。后果发生的频率为 5×10^{-5}/a。根据后果等级为 5 级和频率为 5×10^{-5}/a，查询表 F.2，风险等级为中风险，要求：可选择性的采取行动。

分析小组决定安装一个独立的 SIF，当检测到超压时，联锁打开放空阀。放空阀具有独立的放空管线，同样在放空阀下考虑增加氮气吹扫。该 SIF 的设置见图 G.4 粗线部分。可根据企业具体的风险控制要求，确定该 SIF 的 SIL。在本例中，确定该 SIF 的 FFD 为 1×10^{-2}（SIL1）。对于场景，SIF 将释放事件的频率从 5×10^{-5}/a 降低到 5×10^{-7}/a。根据表 F.2，对于后果等级为 5 级、频率为 5×10^{-7}/a 的事件，风险等级为低风险，不需采取行动。



注：一些 SIFs（如火灾、气体和手动跳车）没有绘制出。

图 G.4 PVC 工艺的简化 P&ID 图（增加 IPL 后）

G.2.7 LOPA 记录表

本案例 LOPA 记录表如表 G.4 所示。

表 G.4 LOPA 记录表

公司名称		装置名称		时间	
工艺单元		分析组成员		图纸号	
分析节点	PVC 反应器				

序号	场景	后果		初始事件		使能必要事件/条件		条件修正			IPL			其他保护措施	后果发生频率	现有风险等级	需求的 SIL 等级或建议的 IPL			减缓后的后果发生频率	减缓后的风险等级	备注
		描述	等级	描述	频率/a	描述	概率	点火概率	人员暴露概率	致死概率	描述	IPL类别	PFD				描述	IPL类别	PFD			
1	冷却水失效，反应失控，潜在的反应器超压、泄漏、断裂、受伤和死亡	反应失控，潜在的反应器超压、泄漏、断裂、受伤和死亡	5	冷却水损失	1×10^{-1}	冷却水损失引起反应失控的反应器条件概率	0.5	—	—	—	BP-CS 回路高报警，加制反应器温抑剂	报警和人员响应	1×10^{-1}	1. 紧急冷却系统（蒸气涡轮机）2. 操作人员行动	5×10^{-5}	高风险	反应器增加一个 SIF：安装一个在高压时打开的放空阀	SIF	1×10^{-2}（SIL1）	5×10^{-7}	低风险	1. 安全阀作为 IPL 应满足以下要求： ——对于每一个安全阀安装独立的放空管线 ——在所有放空阀/安全阀下考虑 N2 吹扫 2. 其他的操作人员行动不独立于已经确认的保护层的同一操作人员 3. 紧急冷却系统不能作为 IPL，因为其不独立于 IE，与冷却水系统有多个公共元件（管线、阀门等）。这些公共元件在引起冷却水失效时，也会导致紧急冷却系统失效
											安全阀	物理保护	1×10^{-2}									

G.3 循环氢加热炉

G.3.1 工艺描述

加氢裂化装置循环氢加热炉简化 P&ID 图见图 G.5。该循环氢加热炉为立管立式炉，介质流量为 6000 Nm^3/h，炉管的设计压力为 20 MPa，对流段设计热负荷为 1139 kW，辐射段设计热负荷为 3877 kW，用于加热循环氢。该炉子位于加氢裂化反应器入口，氢气经过炉子加热后与精制油、循环油、热高分来的常规液态烃混合进入加氢裂化反应器。

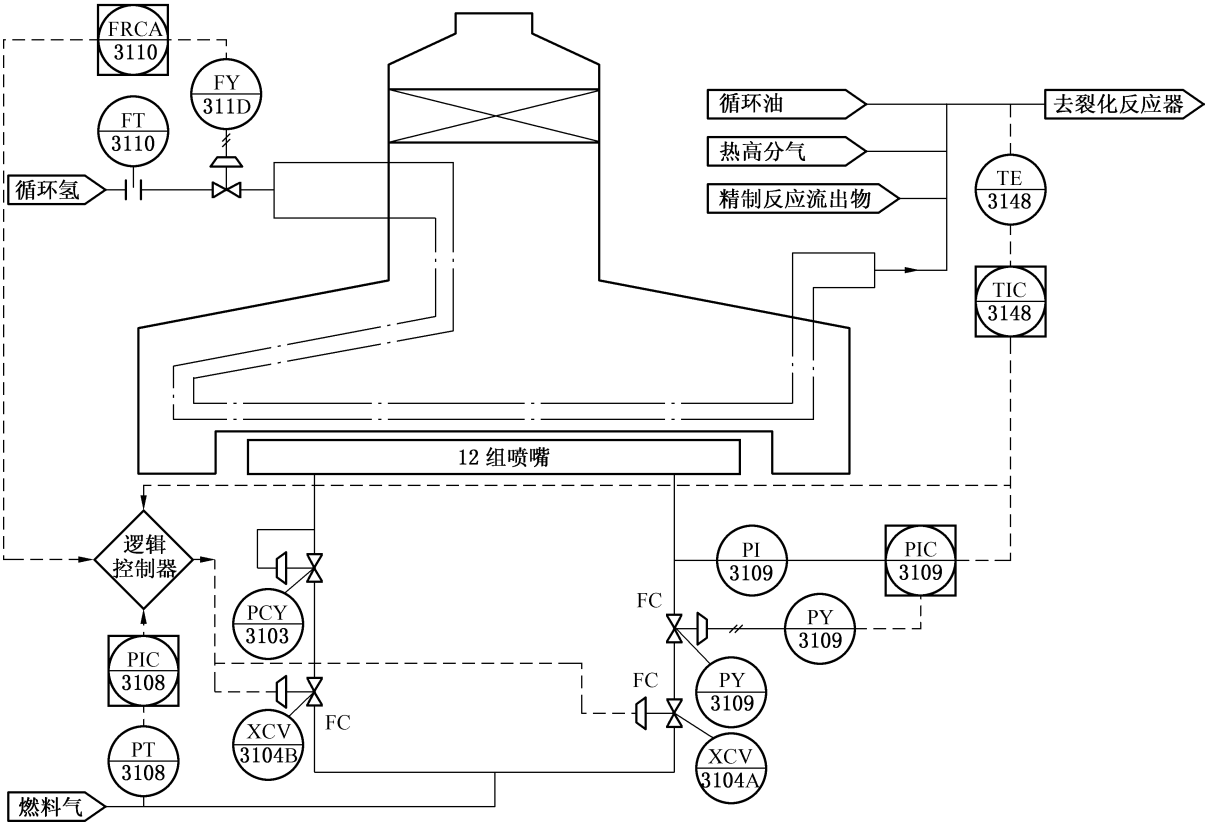


图 G.5 加氢裂化装置循环氢加热炉简化 P&ID 图

G.3.2 场景识别与筛选

采用 HAZOP 分析辨识工艺中存在的主要危险，通过后果分级表 F.3，筛选进行 LOPA 的场景。表 G.5 为筛选出的 LOPA 场景。本例以场景 2 为例进行分析。场景 2 为燃料气总管压力低造成加热炉熄火，炉内燃料气积聚导致遇明火爆炸。后果等级为 4 级。

表 G.5 筛选出的 LOPA 场景

场景 1	加热炉出口氢气温度高造成加氢裂化反应器入口温度过高，引起反应失控，损坏反应器
场景 2	燃料气总管压力低造成加热炉熄火，炉内燃料气积聚导致遇明火爆炸
场景 3	加热炉进料流量低造成加热炉炉管干烧而损坏

G.3.3 初始事件确认

本例选定IE为燃料气总管压力传感器故障，人员未及时响应，根据表E.1，其失效频率为1×10^{-2}。

G.3.4 IPL评估

燃料气总管压力设有SIF。当PT3108检测到燃料气压力过低时，SIF逻辑控制器输出信号关闭XCV31404A和XCV3104B，同时切断去主火嘴的燃料气和去长明灯的燃料气，熄灭火嘴和长明灯，防止加热炉内因熄火出现燃料气积聚而导致遇明火爆炸。但是，由于该SIF与人员响应得到的报警共用一个传感器，不独立于初始事件的发生，所以，该SIF不能作为IPL。

G.3.5 场景频率计算

后果发生频率为：

$$f_i^{C}=f_i^{I}=1\times10^{-2}/a$$

式中：

f_i^{C}——IEi的后果C的发生频率，单位为/a；

f_i^{I}——IEi的发生频率，单位为/a。

G.3.6 风险评估与决策

燃料气总管压力低造成加热炉熄火，炉内燃料气积聚导致遇明火爆炸，后果等级为4级。后果发生的频率为1×10^{-2}/a。根据后果等级为4和频率为1×10^{-2}/a，查询表F.2，风险等级为高风险，要求：选择合适的时机采取行动。

分析小组将燃料气总管压力低报警和人员响应系统与燃料气总管压力SIF在硬件上独立。此时，燃料气总管压力SIF可作为IPL。可根据企业具体的风险控制要求，确定该SIF的SIL。在本例中，确定该SIF的FFD为1×10^{-2}(SIL1)。对于场景，SIF将释放事件的频率从1×10^{-2}/a降低到1×10^{-4}/a。根据表F.2，对于后果等级为4级、频率为1×10^{-4}/a的事件，风险等级为中风险，企业可采用成本效益分析，决定是否需采用额外的措施进一步降低风险。

G.3.7 LOPA记录表

本案例LOPA记录表如表G.6所示。

表 G.6　LOPA 记录表

公司名称		装置名称		时间	
工艺单元		分析组成员		图纸号	
分析节点	循环氢加热炉				

序号	场景	后果		初始事件		使能必要事件/条件		条件修正			IPL			其他保护措施	后果发生频率	现有风险等级	需求的 SIL 等级或建议的 IPL			减缓后的后果发生频率	减缓后的风险等级	备　注
		描述	等级	描述	频率/a	描述	概率	点火概率	人员暴露概率	致死概率	描述	IPL类别	PFD				描述	IPL类别	PFD			
1	燃料气总管压力低造成加热炉熄火，炉内燃料气积聚导致遇明火爆炸	燃料气总管压力低造成加热炉熄火，炉内燃料气积聚导致遇明火爆炸，设备损坏	4	燃料气总管压力传感器故障，人员未及时响应	1×10^{-2}	—	—	—	—	—	—	—	—	燃料气总管压力SIF	1×10^{-2}	高风险	将燃料气总管压力低报警和人员响应与燃料气总管压力SIF在硬件上独立，此时该SIF可作为IPL	SIF	1×10^{-2}（SIL 1）	1×10^{-4}	中风险	将燃料气总管压力低报警和人员响应与燃料气总管压力SIF在硬件上独立

参 考 文 献

[1] Dowell M. A Layer of protection analysis for determining safety integrity level. ISA Transactions, 1998,37(3):155－165

[2] CCPS. Layer of Protection Analysis—Simplified Process Risk Assessment. New York: American Institute of Chemical Engineers, Center for Chemical Process Safety, 2001

[3] CCPS. Guidelines for Safe Automation of Chemical Processes. New York: American Institute of Chemical Engineers, Center for Chemical Process Safety, 1998

[4] CCPS. Guidelines for Safe and Reliable Instrumented Protective Systems. New York: American Institute of Chemical Engineers, Center for Chemical Process Safety, 2007

[5] CCPS. Guidelines for hazard evaluation procedures (third edition). New York: American Institute of Chemical Engineers, Center for Chemical Process Safety, 2008

[6] IEC. Functional safety—Safety instrumented systems for the process industry sector. International Electrotechnical Commission, 2003

[7] Bridges B. W, Clark T. Key issues with implementing LOPA (layer of protection ananlysis)—perspective from one of the originators of LOPA. 5th Global congress on process safety, 2009

[8] Dowell M. A. Is it really an independent protection layer. 6th Global congress on process safety, 2010

[9] Murphy F. W, Bridges W. Initiating events and independent protection layers for LOPA, a new CCPS guideline book. AIChE Spring National Meeting. 2009

[10] Young G. G, Crowe S. G. Modifying LOPA for improved performance. ASSE professional development conference and exposition, 2006