附 录 A
（资料性）
LOPA 分析各阶段数据（示例）

A.1 从 HAZOP 分析导出的可用于 LOPA 的数据

表 A.1 从 HAZOP 分析导出可用于 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所导出的信息在应用于LOPA分析时需再次判断。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

表 A.2 LOPA 分析记录表-单一场景（示例）

风险点编号：	**风险点名称：**		
日期：	**描述**	**概率**	**频率** **年$^{-1}$**
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）**			

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			
本质安全设计			
基本过程控制系统			
关键报警及人员干预			
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）：			

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。

表 A.3 LOPA 分析记录表-复合场景（示例）

风险点编号：	**风险点名称：**		
日期:	**描述**	**概率**	**频率** **年$^{-1}$**
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）			

表 A.3　LOPA 分析记录表-复合场景（示例）（续）

<table>
<tr><td>本质安全设计</td><td></td><td></td><td></td></tr>
<tr><td>基本过程控制系统</td><td></td><td></td><td></td></tr>
<tr><td>关键报警及人员干预</td><td></td><td></td><td></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
（必须判别）</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>
</table>

填表注意事项：

a)　表 A.2 的填报注意事项都需关注；
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。

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害致死后果分级示例、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、A.5、A.6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.4　简化的人员伤害后果分级（示例）

后果特征	人员伤害/致死				
	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 人以下重伤，或者 3 人以上 10 人以下轻伤。	造成 3 人以下死亡，或者 3 人以上 10 人以下重伤，或者 10 人以上轻伤。	造成 3 人以上 10 人以下死亡，或者 10 人以上 50 人以下重伤。	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	经济损失				
	等级 1	等级 2	等级 3	等级 4	等级 5
-	造成 1000 元以上 10 万元以下直接经济损失。	造成 10 万元以上 100 万元以下直接经济损失。	造成 100 万元以上 1000 万元以下直接经济损失。	造成 1000 万元以上 5000 万元以下直接经济损失。	造成 5000 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）

后果特征	经济损失				
	等级 1	等级 2	等级 3	等级 4	等级 5
-	1. 因环境污染疏散、转移人员 100 人以下的。 2. 因环境污染造成直接经济损失 50 万元以下的。	1. 因环境污染直接导致 3 人以下中毒或者重伤的。 2. 因环境污染疏散、转移人员 100 人以上 1000 人以下的。 3. 因环境污染造成直接经济损失 50 万元以上 200 万元以下的。 4. 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. 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。 2. 因环境污染疏散、转移人员 1000 人以上 5000 人以下的。 3. 因环境污染造成直接经济损失 200 万元以上 500 万元以下的。 4. 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。 5. 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. 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。 2. 因环境污染疏散、转移人员 5000 人以上 1 万人以下的。 3. 因环境污染造成直接经济损失 500 万元以上 2000 万元以下的。 4. 因环境污染造成国家重点保护的动植物物种受到破坏的。 5. 因环境污染造成乡镇集中式饮用水水源地取水中断的。 6. 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。 7. 造成跨设区的市级行政区域影响的突发环境事件。	1. 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。 2. 因环境污染疏散、转移人员 1 万人以上的。 3. 因环境污染造成直接经济损失 2000 万元以上的。 4. 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。 5. 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。 6. 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。 7. 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）	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 控制回路应与 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，应有更全面的信息来支撑，具体评估方法见附录 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。	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。关键报警必须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) 操作人员应能够得到采取行动的指示或报警，这种指示或报警必须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。
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	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、维护和测试都应按 GB/T 21109 的有关规定执行。 SIF 的风险削减性能由其 PFD 所确定，

	器和最终元件组成，具有一定的 SIL。		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，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		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，将大大的降低相关场景后果的频率。	1×10^{-6}~1×10^{-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。	1×10^{-1}~1×10^{0}
关键报警和人员干预	人员行动，有 10min 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}~1×10^{0}
	人员对 BPCS 指示或报警的响应，有 40min 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 40min 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^{-2}~1×10^{-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	1×10^{-2}~1×10^{-1}

		元件。	
	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。	1×10^{-3}~1×10^{-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。	1×10^{-4}~1×10^{-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。	1×10^{-3}~1×10^{-1}
	爆破片	防止系统超压。其有效性对服役条件比较敏感。	1×10^{-3}~1×10^{-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。	1×10^{-3}~1×10^{-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。	1×10^{-3}~1×10^{-2}
	开式通风口	防止超压。	1×10^{-3}~1×10^{-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。	1×10^{-3}~1×10^{-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。	1×10^{-3}~1×10^{-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。

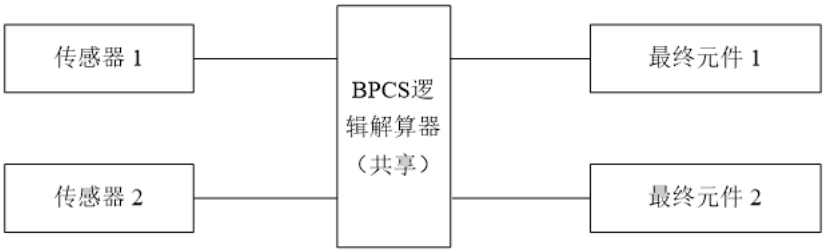


图 A.1 同一场景下多个回路的典型 BPCS 逻辑计算器

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。

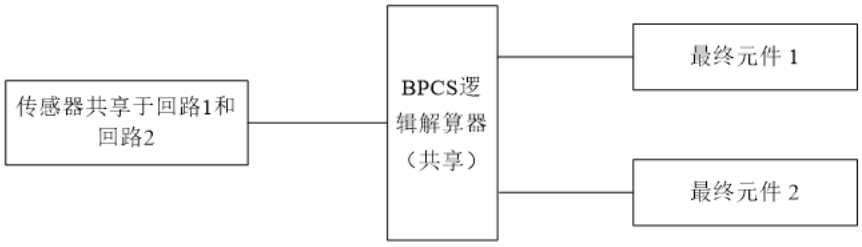
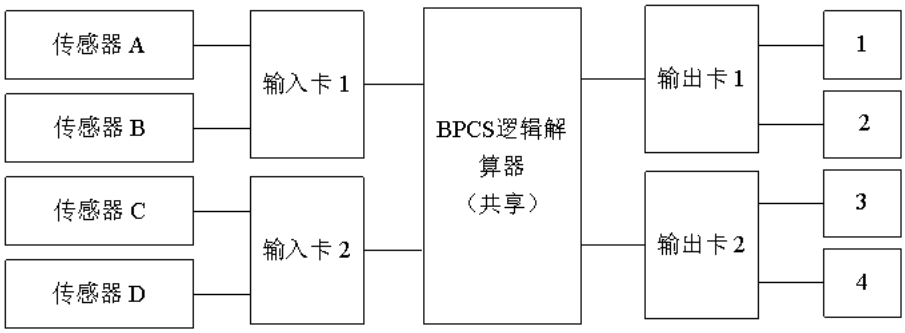


图 A.2 同一场景下共享传感器的 BPCS 回路

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。



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。

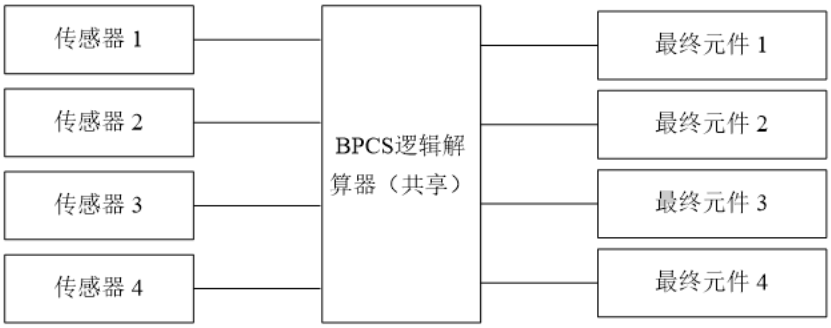


图 A.4 同一场景下 BPCS 功能回路作为 IPL 的最大数量

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) 对数据与数据分析的要求如下：

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：

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) 对分析人员的要求如下：

分析人员必须能够：

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。

分析小组或人员应具有相关专业知识，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，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.9 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 人及以上死亡。	1 x 10^{-7}
4 级，严重的	造成 3 人以上 10 人以下死亡，或者 10 人以上 50 人以下重伤。	1 x 10^{-6}
3 级，较大的	造成 3 人以下死亡，或者 3 人以上 10 人以下重伤，或者 10 人以上轻伤。	1 x 10^{-5}
2 级， 较小的	造成 3 人以下重伤，或者 3 人以上 10 人以下轻伤。	1 x 10^{-3}
1 级，微小的	造成 3 人以下轻伤。	1 x 10^{-1}

表 A.10 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	1. 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。 2. 因环境污染疏散、转移人员 1 万人以上的。 3. 因环境污染造成直接经济损失 2000 万元以上的。 4. 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。 5. 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。 6. 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。 7. 造成跨省级行政区域以上影响的突发环境事件。	1 x 10^{-6}
4 级，重大的	1. 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。 2. 因环境污染疏散、转移人员 5000 人以上 1 万人以下的。 3. 因环境污染造成直接经济损失 500 万元以上 2000 万元以下的。 4. 因环境污染造成国家重点保护的动植物物种受到破坏的。 5. 因环境污染造成乡镇集中式饮用水水源地取水中断的。 6. 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。 7. 造成跨设区的市级行政区域影响的突发环境事件。	1 x 10^{-5}
3 级，较大的	1. 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。 2. 因环境污染疏散、转移人员 1000 人以上 5000 人以下的。 3. 因环境污染造成直接经济损失 200 万元以上 500 万元以下的。 4. 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。 5. 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 x 10^{-4}
2 级，较小的	1. 因环境污染直接导致 3 人以下中毒或者重伤的。 2. 因环境污染疏散、转移人员 100 人以上 1000 人以下的。 3. 因环境污染造成直接经济损失 50 万元以上 200 万元以下的。 4. 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 x 10^{-2}
1 级， 微小的	1. 因环境污染疏散、转移人员 100 人以下的。 2. 因环境污染造成直接经济损失 50 万元以下的。	1 x 10^{-1}

表 A.11 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 5000 万元以上直接经济损失。	1×10^{-6}
4 级，重大的	造成 1000 万元以上 5000 万元以下直接经济损失。	1×10^{-5}
3 级，较大的	造成 100 万元以上 1000 万元以下直接经济损失。	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 万元以下直接经济损失。	1×10^{-1}

A.7 初始事件频率示例

表 A.12 给出初始事件频率及有效性表（示例）。

表 A.12 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^{-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}
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}
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}

附 录 B
（资料性）
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

本附件以图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。

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

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分析。

表 B.1 安全自动化场景案例

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

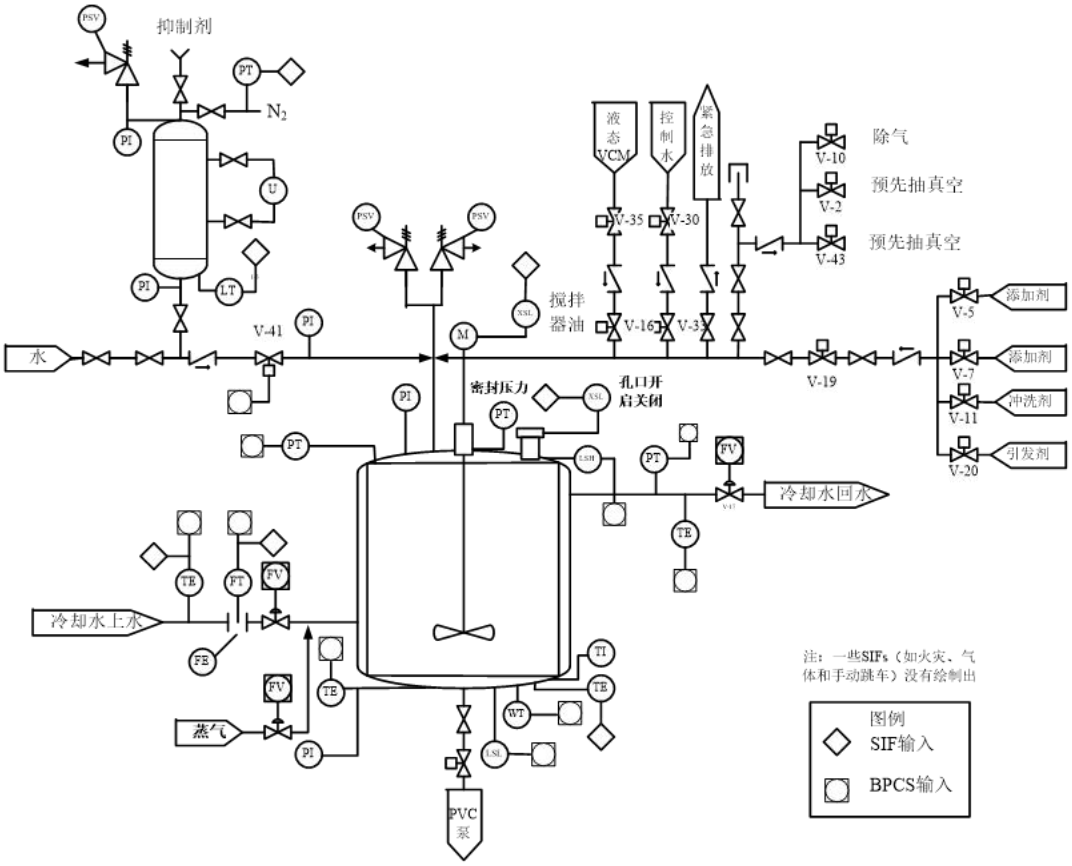


图 B.1 简化流程-聚氯乙烯（PVC）的间歇聚合操作流程图

a) 可容忍风险

评估改造措施时，风险矩阵更加灵活。对于附录表A.9等级5的后果，事件频率大于每年1×10^{-4}即无法接受，必须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，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

独立保护层的应具有：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，均建议增加安全仪表控制SIS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）。在本文件中展示的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，然后用手动方式让反应器“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) 可审计

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

本节对图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至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。必须有足够的培训、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（每年）**
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	N/A	
	人员出现在后果影响区域的概率	N/A	
	致死概率	N/A	
	其他	N/A	
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。		
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 但须增加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.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（每年）**
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	N/A	
	人员出现在后果影响区域的概率	N/A	
	致死概率	N/A	
	其他	N/A	
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）		
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 但必须增加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.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（每年）**
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	N/A	
	人员出现在后果影响区域的概率	N/A	
	致死概率	N/A	
	其他	N/A	
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）		
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 但必须增加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（每年）**
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	N/A	
	人员出现在后果影响区域的概率	N/A	
	致死概率	N/A	
	其他	N/A	
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}	
保护措施（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}
是否满足可容忍风险? (是/否)	是 但必须增加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。		