湖北省化工安全仪表系统
安全功能评估技术指南

2020-3-15 发布　　2020-3-15 实施

湖北省应急管理厅　发布

目　次

前 言

安全仪表系统是化工生产装置出现可能导致安全事故情况时，瞬间准确动作，使生产过程完全停止运行或自动导入预定安全状态，防止化工装置事故的重要保护层，近年来国内外发生的重大化工事故大都与安全仪表失效或设置不当有关。为全面提升化工生产装置本质安全程度，根据《国家安全监管总局关于加强化工安全仪表系统管理的指导意见》（安监总管三〔2014〕116 号）要求，依照有关标准规范，结合我省实际情况，制定本安全仪表系统安全功能评估技术指南，规范我省化工生产装置或设施危险与风险分析、安全完整性等级确定、安全仪表系统设计选型等全生命周期管理工作。

本指南由湖北省应急管理厅提出。

主编单位：湖北省安全生产技术协会

参编单位：湖北省缘达化工工程有限公司、中国石油化工股份有限公司武汉分公司、湖北中环智安科技有限公司、武汉华挚系统工程公司

主要起草人：周　彪　戴海霞　金　浩

主要审查人：夏浩中　刘一鸣　吴祥林　詹学贵　董元炜　方群伟　陈连和　张华慧　彭　维　吴　惠　郝　超　徐佐清

1 适用范围

本指南适用涉及“两重点一重大”的在役化工生产装置或设施的企业。

其他化工装置风险评估程度为风险矩阵中（附录 C 表 C.2）红色、橙色等级的，应依照本技术指南开展安全仪表系统安全功能评估。

2 规范性引用文件

下列文件中的条款通过在本指南的引用而成为本指南的条文。凡是注日期的引用文件，其随后的修改（不包括勘误的内容）或修订版均不适用本指南，然而，鼓励根据本指南达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用本指南。

《化工企业工艺安全管理实施导则》AQ/T3034

《危险与可操作性分析（HAZOP 分析）应用导则》AQ/T3049

《危险与可操作性分析（HAZOP 分析）应用指南》GB/T 35320

《保护层分析（LOPA）方法应用导则》AQ/T3054

《保护层分析（LOPA）方法应用指南》GB/T 32857

《电气/电子/可编程电子安全相关系统的功能安全》GB/T20438

《过程工业领域安全仪表系统的功能安全》GB/T21109

《石油化工安全仪表系统设计规范》GB/T50770

《石油化工可燃气体和有毒气体检测报警设计规范》GB50493

3 缩略语和术语、定义

3.1 缩略语

本指南使用的缩略语见表 1。

表 1 本指南使用缩略语

缩略语	全称	解释
ALARP	As low as reasonably practicable	“尽可能合理降低”原则
HAZOP	Hazard and operability study	危险与可操作性分析
IE	Initiating event	初始事件
IPL	Independent protection layer	独立保护层

缩略语	全称	解释
LOPA	Layer of protection analysis	保护层分析
P&ID	Piping and instrumentation diagram	管道和仪表流程图
PFD	Probability of failure on demand	要求时的失效概率
SIF	Safety instrumented function	安全仪表功能
SIL	Safety integrity level	安全完整性等级
SIS	Safety instrumented system	安全仪表系统

3.2 术语、定义

3.2.1 场景

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。

3.2.2 初始事件（IE）

事故场景的初始原因。

3.2.3 后果

事件潜在影响的度量，一种事件可能有一种或多种后果。

3.2.4 保护层

能够阻止场景向不期望后果发展的设备、系统或行动。

3.2.5 独立保护层（IPL）

能够阻止场景向不期望后果发展，并独立于场景的初始或其它保护层的设备、系统或行动。

3.2.6 保护层分析（LOPA）

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。

3.2.7 要求时的失效概率（PFD）

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。

3.2.8 风险评估

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。

3.2.9 安全仪表功能（SIF）

为了防止、减少危险事件发生或保持过程安全状态，用测量仪表、逻辑控制器、最终元件及相关软件等实现的安全保护功能或安全控制功能。

3.2.10 安全完整性等级（SIL）

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

3.2.11 安全关键设备

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，如安全仪表系统、安全泄压设施等。

3.2.12 使能必要事件或条件

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。

3.2.13 根原因

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。

3.2.14 化工安全仪表系统

包括安全联锁系统、紧急停车系统和有毒有害、可燃气体检测保护系统等，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。

3.2.15 防护措施

可能中断初始事件的事件链或减轻后果的任何设备、系统或行动。

3.2.16 “尽可能合理降低”原则（ALARP）

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靠的原则下“尽可能的低”。

3.2.17 安全仪表完整性等级（SIL）评估

通过工艺危险分析和风险评估，采用保护层分析法（半定量）、风险图法（定性）等方法，评估化工装置安全仪表完整性等级（SIL）和对设置的安全仪表系

统安全完整性等级进行验证的系列活动。

4 安全完整性等级（SIL）确定

4.1 安全完整性等级（SIL）分级

用来规定分配给安全仪表系统的仪表安全功能的安全完整性要求的离散等级，一般分为 4 级，石化化工工厂或装置的安全仪表系统工作于低要求模式，其安全完整性等级不应高于 SIL3 级。安全仪表功能的安全完整性等级（低要求模式）：

（1）SIL4，平均失效概率 PFDavg≥10^{-5} 且＜10^{-4}

（2）SIL3，平均失效概率 PFDavg≥10^{-4} 且＜10^{-3}

（3）SIL2，平均失效概率 PFDavg≥10^{-3} 且＜10^{-2}

（4）SIL1，平均失效概率 PFDavg≥10^{-2} 且＜10^{-1}

4.2 保护层分析法（LOPA）（方法一）

4.2.1 评估小组及职能

（1）小组成员可以包括但不限于以下人员：

① 组长；

② 记录员；

③ 设计人员；

④ 工艺人员；

⑤ 仪表工程师；

⑥ 设备工程师；

⑦ 安全工程师；

⑧ 操作人员。

（2）根据需要，可邀请以下人员参与

① 工艺包供应商；

② 成套工艺设备供应商；

③ 电气工程师；

④ 其他专业工程师。

主要工作包括分析节点选取、工艺危险分析和风险评估、控制回路确定、SIL确定等。各项分析、评估、确认活动应召集评估小组成员参加，充分听取大家意见后形成决议，并做好记录存档。

评估小组成员应具备危险分析、风险评估、安全仪表的相关知识，并经安全仪表系统（SIS）培训学习，具有相应能力。

4.2.2 开展工艺危险分析及无保护层事故后果预测

已开展过工艺危险分析的装置，对分析结果进行提炼，未开展工艺危险分析的，按《化工企业工艺安全管理实施导则》（AQ/T3034）推荐的工艺危险分析方法，建议选用 HAZOP 进行工艺危险分析，预测无保护层事故后果，评估风险等级。

4.2.3 事故后果的初始事件确认

初始事件（IE）一般包括外部事件、设备故障和人员失误，具体分类见下表：

表 2　IE 类型

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

在确定 IE 时，应遵循以下原则：

（1）宜对后果的原因进行审查，确保该原因为后果的有效 IE；

（2）应将每个原因细分为具体的失效事件，如“冷却失效”可细分为冷却剂失效、电力故障或控制回路等失效；

（3）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。

每个事故或事件场景都有唯一的 IE 及其对应的单一后果。当同一 IE 导致不同的后果时，或多种 IE 导致同一后果时，应分别建立对应关系，便于采取相应的风险降低措施。

4.2.4 独立保护层分析

4.2.4.1 保护层措施可靠性

涉及“两重点一重大”的在役化工生产装置或设施应重点分析以下 5 个方面的独立保护层措施，并审查其可靠性。

（1）仪表设置分析

主要分析装置是否设置了连续监测的压力、温度、流量、液位等仪表，并处于完好的状态；能准确反应装置的工作状态。

（2）联锁系统的审查

主要审查装置是否设置了基本过程控制系统，通过压力、温度、流量、液位等传感器的监测数据，通过响应过程或者操作人员的输入信号，产生输出信息，使生产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。

（3）安全阀、爆破片、阻火器的审查

主要对安全阀、爆破片、阻火器等物理保护措施进行审查，是否按要求设置了安全阀、爆破片、阻火器等必要的安全设施，并能保证其处于完好状态。

（4）报警作为安全措施的审查

审查报警作为安全措施的可行性，主要审查内容包括：操作人员是否能够得到采取行动的指示或报警；操作人员是否训练有素，能够完成特定报警所要求的操作任务；操作人员是否有足够的响应时间；操作人员的身体是否适合等。

（5）围堰、防爆墙的审查

主要审查装置是否按要求设置了围堰、防火堤、集液池等收集处理系统来降低事故后果的保护措施；建筑物是否按要求设置了防爆墙等防止冲击波破坏的措施。

4.2.4.2 化工安全仪表作为 IPL 时应满足的要求

（1）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它 IPL；

（2）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 在可能的时间内，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。

（3）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。

（4）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。

（5）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达到 IPL 的要求。

化工企业典型的保护层及作为 IPL 的要求见附录 A。

4.2.5 独立保护层评估

选择事故后果定性分级严重程度为 5、4、3 等级（分级见附录 C 表 C.3）的场景，按照 AQ/T 3054 场景频率计算方法，确定初始事件发生的频率，分析 IPL 的 PFD,确定保护层提供保护措施后的风险程度及是否可接受。

场景频率计算方法如下：

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

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。

初始事件发生频率和 IPL 的 PFD 数据可采用：

（1）行业统计数据；

（2）企业历史统计数据；

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

（4）其他可用数据，如典型 IE 发生频率和典型 IPL 的 PFD，见附录 B。

4.2.6 安全完整性等级（SIL）确定

对于需要增加的安全仪表功能，SIL 确定是将现有的独立保护层风险评估结果与风险控制目标进行比较，确定需增加的安全仪表功能的 SIL。按该等级要求设置安全仪表系统后，装置才能达到风险控制目标水平。在定级过程中，应首先考虑通过增加其它独立保护层或者优化工艺的方式，并尽量避免出现 SIL3 的安全仪表功能回路。

（1）对事故场景风险评估，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，通过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参见附录 C。

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

（3）已有安全仪表系统的 SIL 等级评估应从提供的保护程度和硬件配置匹配性两个方面进行，其提供的保护程度（明确的安全完整性等级）是否满足保护层要求的风险控制目标水平，硬件配置的匹配（核实传感器、逻辑解算器、最终执行元件及附件的组合）是否满足明确的安全完整性等级要求。

4.3 风险图分析法（方法二）

4.3.1 工艺危险分析

已开展过工艺危险分析的装置，对分析结果进行提炼，未开展工艺危险分析的，按 AQ/T3034 推荐的工艺危险分析方法，建议选用 HAZOP 进行工艺危险分析。必要时也可直接由评估小组采取会议形式进行工艺危险分析，辨识可能需要增加的 SIF 回路。

4.3.2 风险参数分析

风险图方法是基于定性的等级评估方法，属 GB/T 21109 推荐评估方法之一。风险允许的水平蕴含在风险图的结构中，风险图分析使用 4 个参数来确定安全完整性水平：后果（C）、处于危险区域的时间（F）、避开危险的概率（P）和不期望发生的后果（W）。参数选择原则详见附录 D。

4.3.3 安全完整性等级（SIL）确定

安全仪表功能（SIF）的安全完整性等级(SIL)是通过评估安全功能失效后的风险而确定的。

评估人员一旦确定了后果（C）、处于危险区域的时间（F）、避开危险的概率（P）和不期望发生的后果（W）4 项参数，根据附录 D 图 D.1，就能查明基于安全需求的安全仪表功能完整性等级。

5 安全完整性等级（SIL）确定报告

将 SIL 评估表等过程文件汇编，形成《SIL 确定报告》，内容包括现有工艺过程介绍、评估组成员、工艺危险分析及无保护层事故后果预测、事故后果的初始事件、独立保护层分析评估、SIL 确定、评估依据等内容。具体内容与选用的评估方法关联：

（1）评估整改前 P&ID 工艺流程图；

（2）评估场景介绍（工艺装置及保护层介绍）；

（3）事故后果分析（选用 LOPA 分析法时，可选用附录 C 表 C.3 后果定性分级表进行后果分析；选用风险图法时，根据附录 D 表 D.1 进行后果分析）；

（4）风险评估结果（选用 LOPA 分析法时，参照附录 C 表 C.2 风险评估矩阵进行风险评估）；

（5）场景频率计算或风险参数分析；

（6）评估活动记录及其他。

6 安全完整性等级（SIL）验算

企业应组织对设置的安全仪表系统安全完整性等级进行验算，并形成相应的《验算说明》。

6.1 安全完整性等级（SIL）验算目的、要求及方法

SIL 验算的目的通过可靠性建模来验证在役或完成设计的安全仪表系统的每个回路安全完整性等级（SIL）是否满足确定的 SIL，在 GB/T 20119 中明确规定，每个安全仪表功能（SIF）的要求时的失效概率 PFD 应等于或低于指定的目标值，并且应通过计算确认。SIL 验算的最终结果要满足三个方面的要求：

（1） 硬件故障裕度满足标准结构约束要求；

（2）低要求操作模式下的平均故障失效概率 PFDavg，通过计算满足标准要求的等级；依照 GB/T 50770 规定：“通常石油化工工厂和装置的安全仪表系统工作于低要求操作模式”，故下文中的参数均是低要求操作模式下的认证参数。

（3）系统完整性要求，根据 GB/T20438 认证的产品或先前使用（prior Use）过的；安全仪表系统运行及检修技术文件。

SIL 验算常用的建模方法有可靠性框图、故障树和马尔可夫（Markov）模型等。本指南推荐采用可靠性框图法，可靠性框图法是一种传统的可靠性分析方法，它用图形的方式来表示系统内部元件的传递过程，显示了相关元件的串并联关系，具有简单、清楚直观的特点。

6.2 验算流程

（1）成立专业验算项目组；

（2）准备验算资料；

① SIF 一览表:表格中应包含安全仪表回路及其 SIL 等级、所用仪表设备信息、设备失效数据、正在执行的检验测试周期等；

② 对在役装置的安全仪表系统不仅需要有原始设计资料，还应包含运行周期中所有详细的变更与故障资料，通常应具备下列资料：装置相关 P&ID 图、SIF 的 SIL 确定报告、SIS 的安全要求规格书（SRS）、生产周期间的所有变更和故障记录等。

（3）可靠性框图建模；

（4）计算出安全失效分数(SFF)，结合硬件故障裕度(HFT)，得出结构约束的安全完整性等级；

（5）根据失效数据和可靠性模型，计算要求时的失效概率 PFD，并符合 SIL 要求时的检验测试周期；

（6）系统完整性验证：应使用根据 GB/T20438 认证的产品或先前使用（prior use）过的产品；建立安全仪表系统运行和检修技术文件等，并落实，满足安全仪表系统安全生命周期管理。

（7）形成验算说明：SIL 验算说明是对 SIL 验算工作过程的总结，内容包括验算项目组、需要验算的 SIF 回路资料、系统结构约束验证、要求时的失效概率 PFD_G 、验算结果、符合 SIL 要求的检验测试周期及建议措施等内容。

SIL 等级验算流程见附录 F、验算示例见附录 I。

7 安全仪表系统（SIS）安全生命周期

7.1 安全生命周期的概念

安全仪表系统的安全生命周期是指安全仪表系统实现过程中所必须的生命活动，这些活动发生在从一项工程的概念阶段开始，直至安全仪表系统停止使用为止的一段时间内。安全生命周期内的活动有：

（1）定义 SIS 安全生命周期各阶段的活动（准备工作）

（2）危险和风险分析

（3）将安全功能分配到保护层

（4）制定 SIS 安全要求规格书（SRS）

（5）SIS 的设计与开发

（6）SIS 的安装和试运行

（7）安全功能的确认和验证

（8）SIS 的操作维护（含定期测试）与修理

（9）SIS 的修改和改型

（10）SIS 的停用和处理

7.2 安全仪表系统（SIS）安全生命周期关键活动的要求

7.2.1 制定 SIS 的安全要求规格书 （SRS）

制定安全要求规格书是整个 SIS 安全生命周期最重要的活动之一。有关 SIS 的安全要求规格书必须包含以下主要内容：

（1）基本要求；

（2）选型原则；

（3）控制器；

（4）操作员站；

（5）辅助操作台；

（6）工程师站和事件顺序记录站；

（7）应用软件组态；

（8）系统通信；

（9）系统负荷；

（10）维护和安全、可靠性；

（11）系统供电及接地；

（12）验收测试要求；

（13）环境要求；

（14）机械要求；

（15）技术服务；

（16）质量保证；

（17）文档资料。

7.2.2 安全仪表系统（SIS）设计与实施

化工安全仪表系统的设计单位必须应具备工程设计综合甲级、石油化工行业甲级、石油化工行业（化工工程）专业甲级资质之一；按制定的《安全要求规格书》进行设计；安全仪表系统的安装施工单位应具备石油化工施工过程总承包三级或电子与智能化工程专业承包二级及以上资质；按照设计图纸施工。

7.2.3 安全仪表系统（SIS）定期测试与拆除

SIS 定期测试一般指周期性的离线检验测试和 SIS 系统的在线诊断测试。周期性的离线检验测试是 SIS 投入操作运行后，重要的维护活动，是保持 SIF 持续地满足安全完整性要求的保障。他将 SIS 被测设备脱离开工艺流程，对其进行人工检测，可发现变送器膜盒损坏、引压管堵塞、阀门腐蚀内漏、阀芯卡死等故障。离线检测测试一般安排在停车大修期间进行，故设计要求的检验测试时间间隔（TI）大于、至少等于装置的停车检修时间间隔。

安全仪表系统中任一元器件和系统一般情况下，运行期间不得拆除，除非能确保拆除后，所要求的的 SIF 仍可保持正常。

7.3 安全仪表系统（SIS）安全生命周期要求

在执行 SIS 安全生命周期各阶段的活动时，首先制定目标要求和行动计划，在提交输出前，要对活动执行的相关细节进行确认，要保证一活动结束转交到下一项活动时，必须是准确无误的。每个阶段的活动，还应详细记录输入内容、工作记录、输出成果，便于溯源、查询。

附 录 A
（资料性附录）
化工企业典型的保护层及作为 IPL 的要求

化工企业典型的保护层及作为IPL的要求见表A.1。

表A.1 化工企业典型的保护层及作为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
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	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 AQ/T3054 附录 D； 3）当 BPCS 通过报警或其他形式提醒	

保护层	描述	说明	示例	作为 IPL 的要求	
				具体要求	通用要求
		车或采取动作使过程处于安全状态。		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。	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。
报警和人员响应	报警和人员响应是操作人员或其它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它任务； 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。	
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。	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	

保护层	描述	说明	示例	作为 IPL 的要求	
				具体要求	通用要求
				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。	
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，如耐火涂层、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，如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。	
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。	

附 录 B
（资料性附录）
失效数据

表B.1 初始事件IE典型频率值

IE	频率范围（/a）
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B.2　某公司采用的IE典型频率值

分类	IE	频率（/a）
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}
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 BLEVE	1×10^{-6}
	4. 球罐 BLEVE	1×10^{-4}
	5. 容器小孔（≤50mm）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（≤150mm）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/年）	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它转动设备失去流量	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	1. 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. 易燃蒸汽云爆炸	1×10^{-3}

表B.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，将大大的降低相关场景后果的频率	1×10^{-1}～1×10^{-6}
BPCS		如果与 IE 无关，BPCS 可作为一种 IPL	1×10^{-1}～1×10^{-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	1.0～1×10^{-1}
	人员对 BPCS 指示或报警的响应，有 40min 的响应时间		1×10^{-1}
	人员行动，有 40 min 的响应时间		1×10^{-1}～1×10^{-2}
安全仪表功能	安全仪表功能 SIL 1	见 GB/T 21109	1×10^{-1}～1×10^{-2}
	安全仪表功能 SIL 2		1×10^{-2}～1×10^{-3}
	安全仪表功能 SIL 3		1×10^{-3}～1×10^{-4}
物理保护	安全阀	此类系统有效性对服役的条件比较敏感	1×10^{-1}～1×10^{-3}
	爆破片		1×10^{-1}～1×10^{-3}
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	1×10^{-2}～1×10^{-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	1×10^{-2}～1×10^{-3}
	开式通风口	防止超压	1×10^{-2}～1×10^{-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	1×10^{-2}～1×10^{-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	1×10^{-2}～1×10^{-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进入容器或储罐内的潜在回火	1×10^{-1}～1×10^{-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	1×10^{-1}～1×10^{-2}

附　录　C
（资料性附录）
风险标准和 ALARP 原则

C.1　风险标准

表C.1 数值风险标准（厂外个体风险）

部门	可容许风险（/a）	可忽略风险（/a）
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}
国内（新建和在役装置）	**新建：**1×10^{-5} **在役：**3×10^{-5}	-

表C.2 风险评估矩阵

后果等级	10^{-6}~10^{-7}	10^{-5}~10^{-6}	10^{-4}~10^{-5}	10^{-3}~10^{-4}	10^{-2}~10^{-3}	10^{-1}~10^{-2}	1~10^{-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C.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	释放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

C.2 ALARP原则

1、ALARP原则

ALARP原则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：

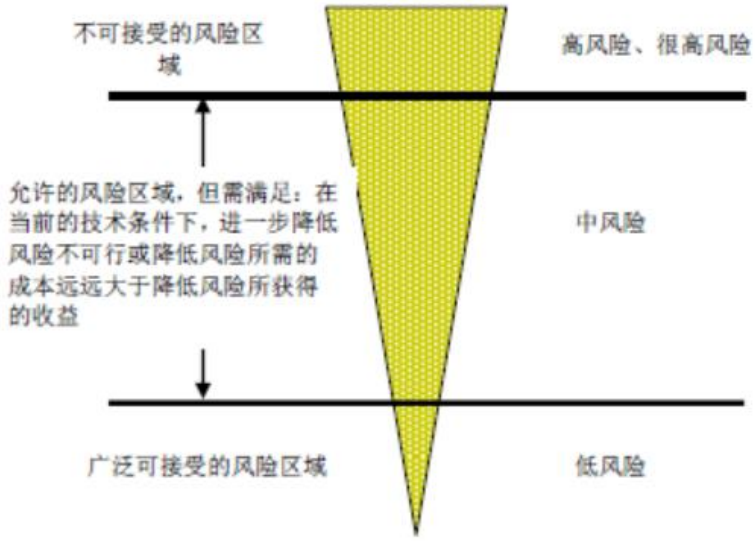
（1）不可接受的风险区域。在本指南C.2中指高风险和很高风险区域。在这个区域，除非特殊情况，风险是不可接受的 ；

（2）允许的风险区域。在本指南C.2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

（3）广泛可接受的风险区域。在本指南C.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C.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。

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。

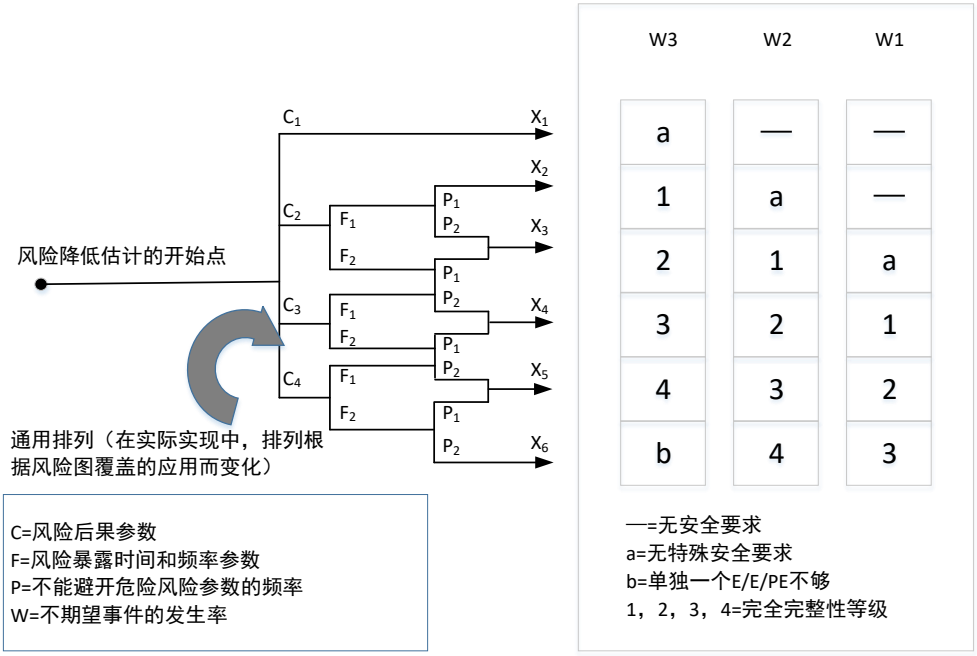
附 录 D
（资料性附录）
风险图法相关参数示例及风险图

风险图法中风险参数的有关示例如下表D.1。

表D.1 风险图法风险参数的有关数据示例

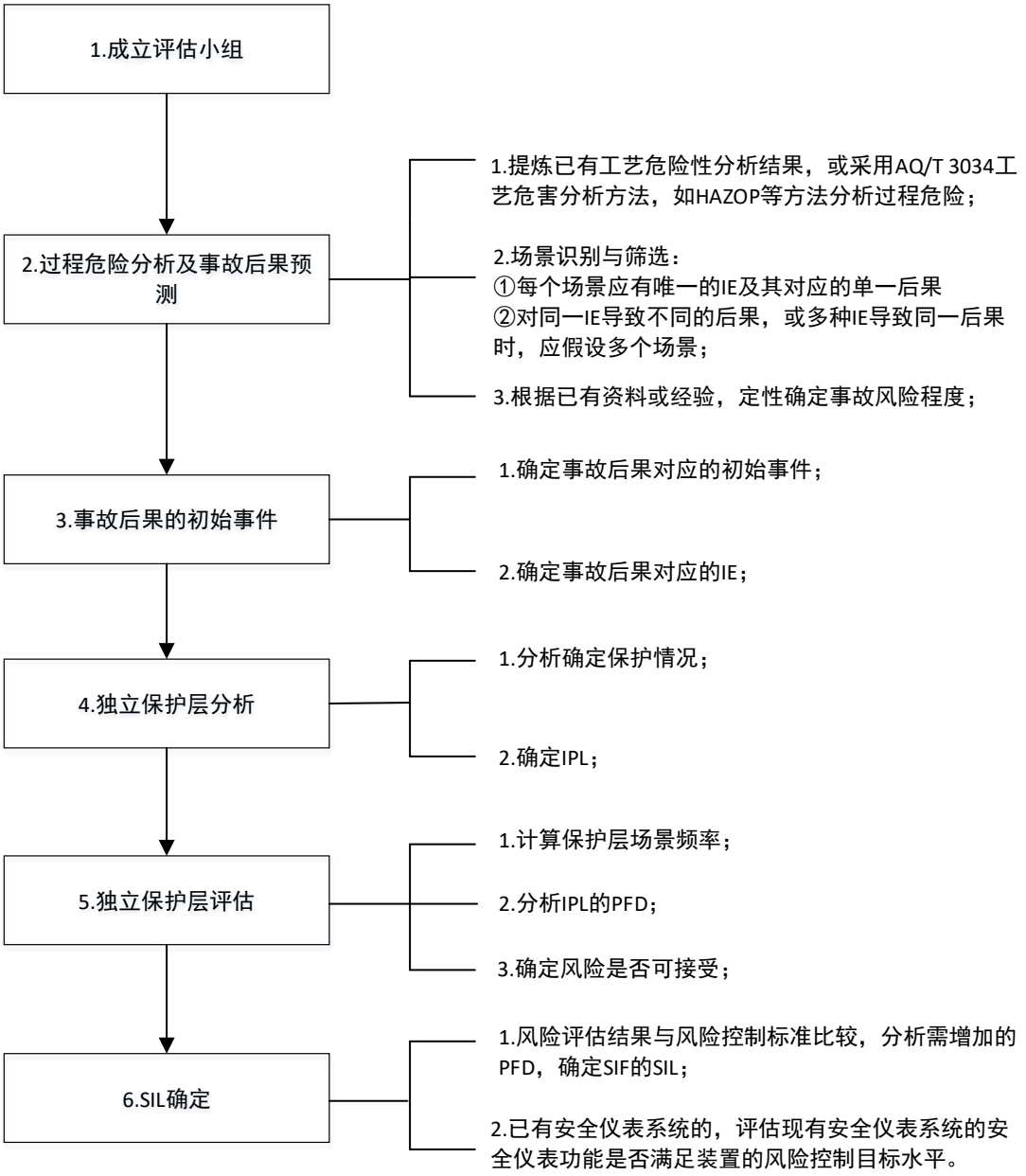
风险参数		分类	备注
后果（C）	C1 C2 C3 C4	微小伤害 对一人或多人的严重永久伤害;一人死亡 几人死亡 多人死亡	1.开发分类系统用于处理对人的伤害或死亡，需开发其他分类系统处理对环境的破坏或物质破坏。 2.对于C1、C2、C3、C4的解释，应考虑意外的后果和正常康复
在危险区域中的频率和暴露时间（F）	F1 F2	极少至较多暴露在危险区域 经常至永久暴露在危险区域	3.见上栏1。
避开危险事件的概率（P）	P1 P2	在一定条件下不可能 几乎不可能	4.参数考虑 —过程操作（被监督，即由熟练或不熟练人员操作，或未被监督） —危险事件的发生速率（如突然、快速或缓慢） —识别危险的难易（如立即看到，通过技术措施或不通过技术措施探测） —危险事件的避免（如在特定条件下可能或不可能的逃生路线） —实际安全经验（有无相同的EUC或类似EUC使用经验）
不期望事件的发生概率W	W1 W2 W3	出现不期望事件的发生概率非常小并且只有很少不期望事件可能出现 出现不期望事件发生概率小并且只有少量不期望事件有可能出现 不期望事件的发生概率相对高并且不期望事件有可能频繁出现	5.W因素的目的是估计不期望事件在没有任何附加安全相关系统（E/E/PE或其他技术系统）的情况下发生的频率，但包括任何外部风险降低设施 6.如果只有很少或没有使用EUC或EUC控制系统，或类似系统的经验，W因素的估计可以通过计算得出，在这种情况下应当做最坏。

确定了后果（C）、处于危险区域的时间（F）、避开危险的概率（P）和不期望发生的后果（W）4项参数，依据下图确定安全仪表系统的安全完整性等级。

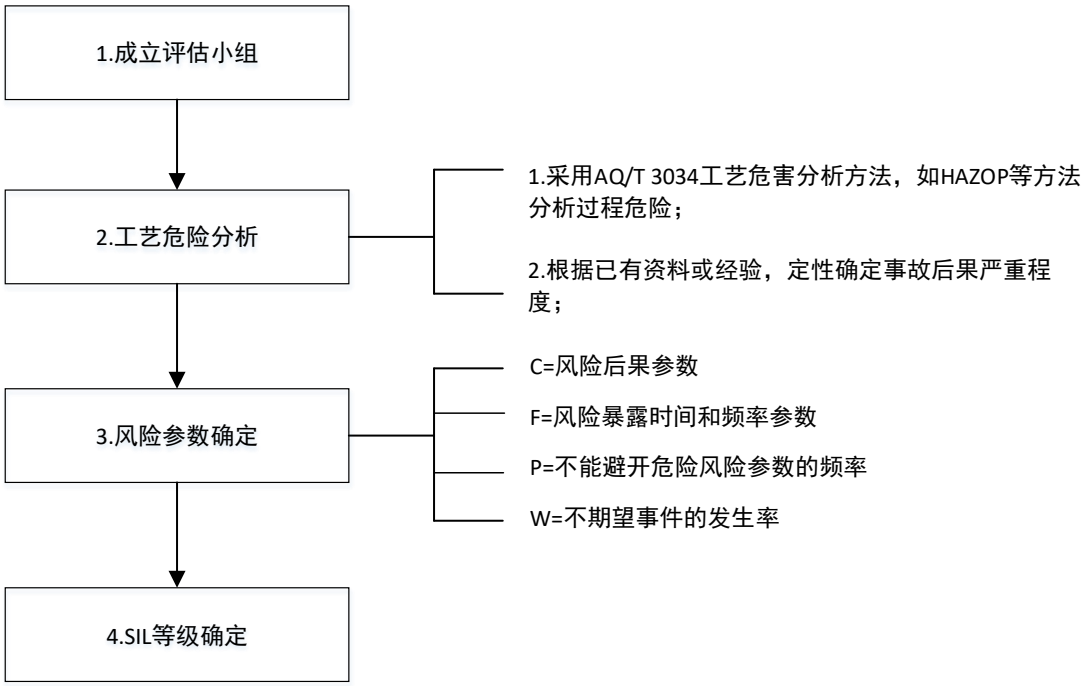


图D.1 风险图：总框图

附 录 E
（资料性附录）
安全完整性等级（SIL）确定流程图



图E.1 LOPA分析法SIL确定流程图



图E. 2　风险图分析法SIL确定流程图

附　录　F
（资料性附录）
安全完整性等级（SIL）验算流程图

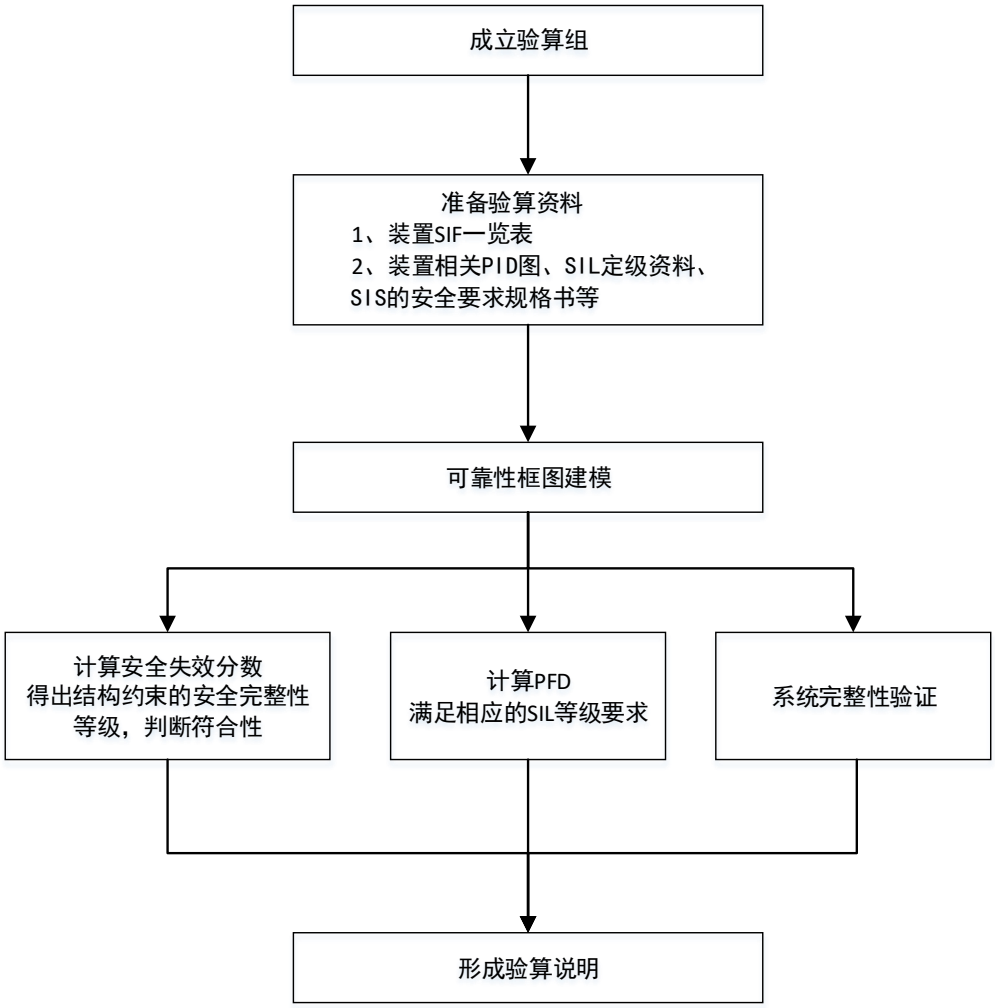


图 F.3　SIL 验算流程图

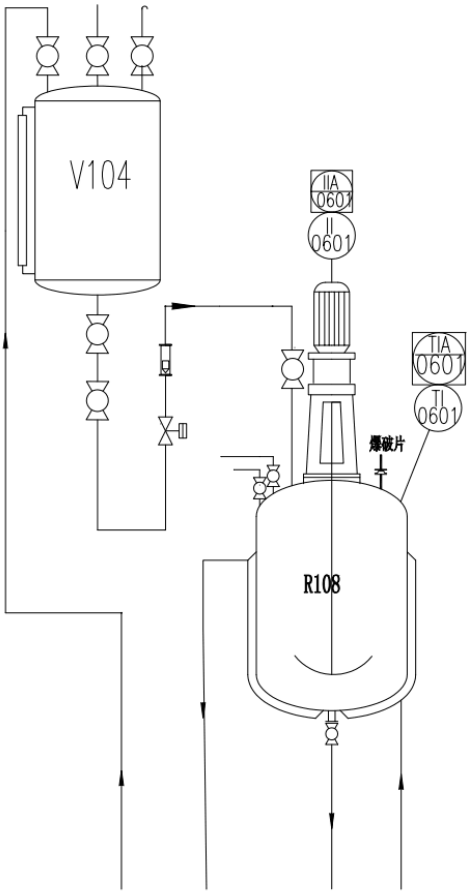
附 录 G
（资料性附录）
LOPA 分析法

附录G包含的示例旨在举例说明本指南中描述的LOPA分析法确定安全完整性等级的流程，示例中的二硝基氯化苯工艺装置工艺设计已进行了大幅度简化，仅用于演示；在任何情况下，这些示例不具备实际案例分析的复杂性。

G.1 现有工艺过程介绍

将定量的氯化苯加入有硝化反应釜中，打开夹套冷却水，启动搅拌。然后缓慢打开混酸阀门开始滴加混酸，操作人员随时观察反应釜温度，控制温度在**℃以内，根据温度变化随时调整滴加混酸阀门开度，直至混酸滴加完毕。当反应过程中温度超过**℃时，及时手动关闭进料阀，停止混酸进料。

反应釜设置了现场温度检测和远传显示报警，反应釜上设置了爆破片。P&ID简化图见图G.1。



图G.1 二硝基氯化苯硝化反应装置

G.2 评估组成员

组建评估组，评估组成员如下：

表G.1 评估组成员一览表

序号	姓名	组内职务	专业	职务/职称/能力
1	***	组长		
2	***	组员		
3	***	组员		
4	***	组员		
5	***	组员		
6	***	组员		
7	***	组员		
8	***	记录员		

G.3 工艺危险分析及无保护层事故后果预测

提炼前期进行HAZOP分析的结果，筛选出后果比较严重的场景，如下表：

表G.2 筛选出的LOPA场景

序号	描述	建议增设的控制回路
1	二硝基氯化苯硝化反应混酸滴加过程中，人工操作滴加阀门时开度控制不当，致使混酸滴加速度过快，反应釜温度升高，造成反应冲料或爆炸，导致设施破坏和人员伤亡。	过程控制系统(BPCS):建立温度、混酸流量自动调节系统，控制硝化反应的温度。 安全仪表功能(SIF)：硝化反应过程中监控反应釜反应温度，当温度超过**℃时，紧急关闭混酸进料切断阀。
2	二硝基氯化苯硝化反应釜反应压力异常，致使反应器超压，造成反应冲料或爆炸，导致设施破坏和人员伤亡。	略
3	二硝基氯化苯硝化反应过程中，搅拌装置失灵，反应不均匀，反应釜温度升高，可能造成冲料或爆炸，致使设施破坏和人员伤亡。	略
4	二硝基氯化苯硝化反应过程中，夹套冷却水水泵故障，冷却水压力为零，反应釜温度升高，可能造成反应冲料或爆炸，导致设施破坏和人员伤亡。	略

参照附录C后果分级表C.3,硝化反应釜温度升高，反应冲料或爆炸，致使设施破坏和人员伤亡的场景，确定无保护层事故后果等级为5级。

G.4 事故后果的初始事件

根据表G.2分析，本例筛选第一个场景，即人员操作失误，致使混酸滴加速度过快，反应釜温度升高，造成反应冲料或爆炸，导致设施破坏和人员伤亡。

查附录B，该场景初始事件阀门操作失误率10^{-1}～10^{-3}/次,本示例取10^{-2}/次，假设该装置年生产300天，每天需要操作阀门2次，则初始事件概率为6/a。

G.5 独立保护层分析

爆破片可作为该场景的独立保护层，根据附录B失效数据表B.3化工行业典型IPL的PFD，爆破片的PFD取1×10^{-2}。

G.6 独立保护层风险评估

（1）场景频率

根据场景频率计算方法，场景后果频率a计算如下：

a=6/a（初始事件频率）×1（人员暴露概率）×1（受伤率）×1×10^{-2}（现有保护层爆破片失效概率）=6×10^{-2}/a

由于由人员现场操作失误引起，故人员暴露概率取1，人员处于危险源的中心，故受伤率也取1。

则后果频率为6×10^{-2}/a。

（2）评估风险是否可以接受

后果频率为6×10^{-2}/a，从附录C表C.2 《风险评估矩阵》查表知风险等级为很高。

根据“ALARP”原则，按在役装置取目标风险水平为3×10^{-5}/a。因而风险不能接受，需要增加其他独立保护层。

G.7 安全仪表功能的SIL确定

在本例中安全仪表功能（SIF）将场景的频率从6×10^{-2}降低3×10^{-5}以下，需要增加的保护层其PFD应小于：

（3×10^{-5}）/6×10^{-2}=0.5×10^{-3}

根据G.3，增加基本过程控制系统（BPCS），查附录B表B.3，取基本过程控制系统（BPCS）的失效概率为1×10^{-1}。

故需要增加的安全仪表功能（SIF）保护层的PFD应小于：

（3×10^{-5}）/（$6\times10^{-2}\times1\times10^{-1}$）=$5\times10^{-3}$

故该安全仪表功能（SIF）的安全完整性等级为SIL2。

G.8 评估表

表G.3 危险分析-风险评估-SIL定级（LOPA法）

序号	工艺简介	初始事件	后果/风险	偏差	安全仪表功能	LOPA 分析				
						现有独立保护层分析	IE 后果频率评估（a）	风险可接受水平（b）	需要增加保护水平(c)	SIL 等级确定
1	二硝基氯化苯主反应釜生产工艺描述：先将氯化苯投入硝化反应釜中，启动搅拌后，缓慢滴加混酸，在规定的温度下滴加至终点，依据反应温度调节滴加速度。	人员操作失误：人工操作混酸滴加阀门时，开度控制不当，致使混酸滴加速度过快	5	反应温度异常升高。	硝化反应过程中监控反应釜温度，当温度超过**℃时，紧急关闭混酸进料切断阀。	1、爆炸片取 1×10^{-2}	根据场景频率计算方法，初始事件阀门操作失误率 10^{-2}/次（假设该装置年生产 300 天，每天需要操作阀门 2 次。）；由于由人员现场操作失误引起，故人员暴露概率取 1，人员处于危险源的中心，故受伤率也取 1。考虑拟增设则后果频率为 **$6\times10^{-2}/a$**。	按附录 C 表 C.1 中在役装置目标水平为 **3×10^{-5}**	需要增加保护层的 PFD 应小于 5×10^{-3}	考虑增加过程控制系统后（保证独立性），基本过程控制系统的 PFD 为 **1×10^{-1}**，故该 SIF 安全完整性等级确定为 SIL2。
备注			1、可参见附录 C 表 C.2 后果定性分级方法。			1、可参见附录 A 表 B.1 化工行典型 IPL。	1、计算方法；根据场景频率计算。 2、初始事件频率确定见 G.4。 3、数据库来源：附录 B。	1、可以是与客户协商的风险目标水平，但不低于标准要求； 2、数据库来源（表 C.1 中在役装置目标风险水平）。	低于 b/a 的圆整值。	

评估组长： 评估成员： 记录员：

G.9 评估依据

1、《化工企业工艺安全管理实施导则》AQ/T 3034-2010
2、《危险与可操作性分析（HAZOP分析）应用导则》AQ/T 3049-2013
3、《保护层分析（LOPA）方法应用导则》AQ/T 3054-2015
4、《电气/电子/可编程电子安全相关系统的功能安全》GB/T 20438-2017
5、《过程工业领域安全仪表系统的功能安全》GB/T 21109-2007
6、《石油化工安全仪表系统设计规范》GB/T 50770-2013
7、《危险与可操作性分析（HAZOP分析）应用指南》GB/T 35320-2017
8、《保护层分析（LOPA）方法应用指南》GB/T 32857-2016

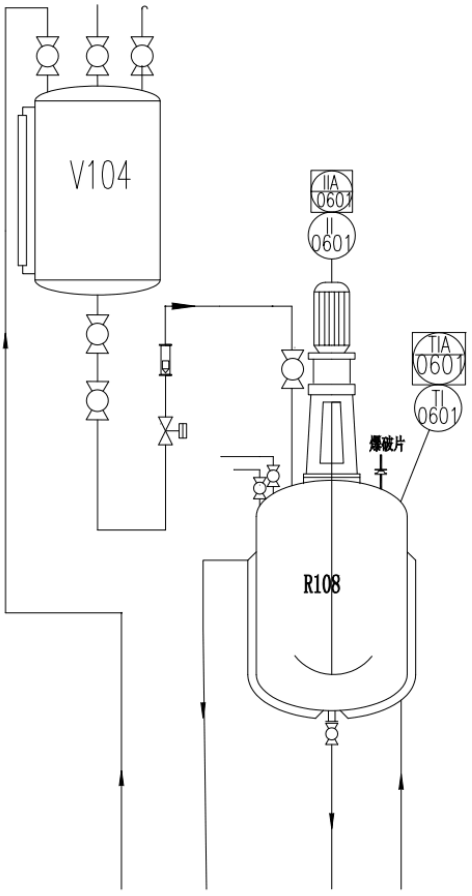
附　录　H
（资料性附录）
风险图分析法

附录B包含的示例旨在举例说明本指南中描述的风险图分析法确定安全完整性等级的流程，示例中的二硝基氯化苯工艺装置工艺设计已进行了大幅度简化，仅用于演示；在任何情况下，这些示例不具备实际案例分析的复杂性。

H.1　现有工艺过程介绍

将定量的氯化苯加入有硝化反应釜中，打开夹套冷却水，启动搅拌。然后缓慢打开混酸阀门开始滴加混酸，操作人员随时观察反应釜温度，控制温度在**℃以内，根据温度变化随时调整滴加混酸阀门开度，直至混酸滴加完毕。当反应过程中温度超过**℃时，及时手动关闭进料阀，停止混酸进料。

反应釜设置了现场温度检测和远传显示报警，反应釜上设置了爆破片。P&ID简化图见图H.1。



图H.1 二硝基氯化苯硝化反应装置

H.2 评估组成员

组建评估组，评估组成员如下：

表H.1 评估组成员一览表

序号	姓名	组内职务	专业	职务/职称/能力
1	***	组长		
2	***	组员		
3	***	组员		
4	***	组员		
5	***	组员		
6	***	组员		
7	***	组员		
8	***	记录员		

H.3 工艺危险分析

提炼前期进行HAZOP分析的结果，如下表：

表H.2 工艺危险性分析

序号	描述	建议增设的控制回路
1	二硝基氯化苯硝化反应混酸滴加过程中，人工操作滴加阀门时开度控制不当，致使混酸滴加速度过快，反应釜温度升高，造成反应冲料或爆炸，导致设施破坏和人员伤亡。	过程控制系统(BPCS):建立温度、混酸流量自动调节系统，控制硝化反应的温度。 安全仪表功能(SIF)：硝化反应过程中监控反应釜反应温度，当温度超过**℃时，紧急关闭混酸进料切断阀。
2	二硝基氯化苯硝化反应釜反应压力异常，致使反应器超压，造成反应冲料或爆炸，导致设施破坏和人员伤亡。	略
3	二硝基氯化苯硝化反应过程中，搅拌装置失灵，反应不均匀，反应釜温度升高，可能造成冲料或爆炸，致使设施破坏和人员伤亡。	略
4	二硝基氯化苯硝化反应过程中，夹套冷却水水泵故障，冷却水压为零，反应釜温度升高，可能造成反应冲料或爆炸，导致设施破坏和人员伤亡。	略

H.4 确定风险参数

本例筛选第一个场景分析

（1）C 确定

本指南表 D.1：造成现场几个死亡后果，后果（C）取 C3。

（2）F 确定

本指南表 D.1，现场操作时，经常至永久暴露在危险区域，风险时间和频率参数（F）取 F2。

（3）P 确定

本指南表 D.1，结合专家分析意见，现场设置了防爆片，避免危险事件后果的可能性（P）取 P1。

（4）W 确定

本指南表 D.1，结合专家意见，增设 BPCS 后，确定不期望事件的发生概率（W）取 W2。

H.5 SIL确定

根据 H.4 分析结果，即 C=C3，F=F2，P=P1，W=W2，依据本指南图 D.1 可知，实现该项安全仪表功能（SIF）的 SIS 系统的 SIL 认证等级应取 SIL2。

此处 SIL2，是在设置 BPCS 前提下的 SIL2。因此，首先增设 DCS 系统，实现温度变化联锁调节流量（滴加量）；同时设立 SIS 系统，当反应釜温度超高时，紧急切断滴加混酸的切断阀门。

H.6　评估表

表H.3　危险分析-风险评估-SIL定级

<table>
<tr><td rowspan="2">序号</td><td rowspan="2">工艺简介</td><td rowspan="2">初始事件</td><td rowspan="2">后果/风险</td><td rowspan="2">偏差</td><td rowspan="2">安全仪表功能</td><td colspan="4">风险图评估</td><td rowspan="2">SIL 等级</td></tr>
<tr><td colspan="3">风险评估参数/选取</td><td>风险图应用</td></tr>
<tr><td rowspan="10">1</td><td rowspan="10">二硝基氯化苯主反应釜生产工艺描述：先将氯化苯投入硝化反应釜中，启动搅拌后，缓慢滴加混酸，在规定的温度下滴加至终点，依据反应温度调节滴加速度。</td><td rowspan="10">人工操作混酸滴加阀门时，开度控制不当，致使混酸滴加速度过快，温度过高，可能造成反应冲料或爆炸，导致设施破坏和人员伤亡；</td><td rowspan="10">造成人员伤亡、财产损失。</td><td rowspan="10">反应温度异常升高。</td><td rowspan="10">硝化反应过程中监控反应釜反应温度，监测反应温度，当温度超过**℃时，紧急关闭混酸进料切断阀。</td><td rowspan="4">后果严重程度（C）</td><td>C1</td><td></td><td rowspan="10">SIL2</td><td rowspan="10">增设 BPCS 后，该安全仪表功能的安全完整性等级为 SIL2。</td></tr>
<tr><td>C2</td><td></td></tr>
<tr><td>C3</td><td>C3</td></tr>
<tr><td>C4</td><td></td></tr>
<tr><td rowspan="2">接触程度（F）</td><td>F1</td><td></td></tr>
<tr><td>F2</td><td>F2</td></tr>
<tr><td rowspan="2">避开事件程度（P）</td><td>P1</td><td>P1</td></tr>
<tr><td>P2</td><td></td></tr>
<tr><td rowspan="3">后果概率（W）</td><td>W1</td><td></td></tr>
<tr><td>W2</td><td>W2</td></tr>
<tr><td>W3</td><td></td></tr>
<tr><td>备注</td><td></td><td></td><td></td><td></td><td></td><td colspan="3">应用表 D.1 选取。</td><td>应用图 D.1 选取。</td><td></td></tr>
</table>

评估组组长：　　评估组成员：　　记录员：

H.7 评估依据

1、《化工企业工艺安全管理实施导则》AQ/T 3034-2010
2、《危险与可操作性分析（HAZOP 分析）应用导则》AQ/T 3049-2013
3、《电气/电子/可编程电子安全相关系统的功能安全》GB/T 20438-2017
4、《过程工业领域安全仪表系统的功能安全》GB/T 21109-2007
5、《石油化工安全仪表系统设计规范》GB/T 50770-2013
6、《危险与可操作性分析（HAZOP 分析）应用指南》GB/T 35320-2017

附　录　I
（资料性附录）
二硝基氯化苯工艺 SIS 系统某 SIF 回路 SIL 验算说明

I.1　验算示例

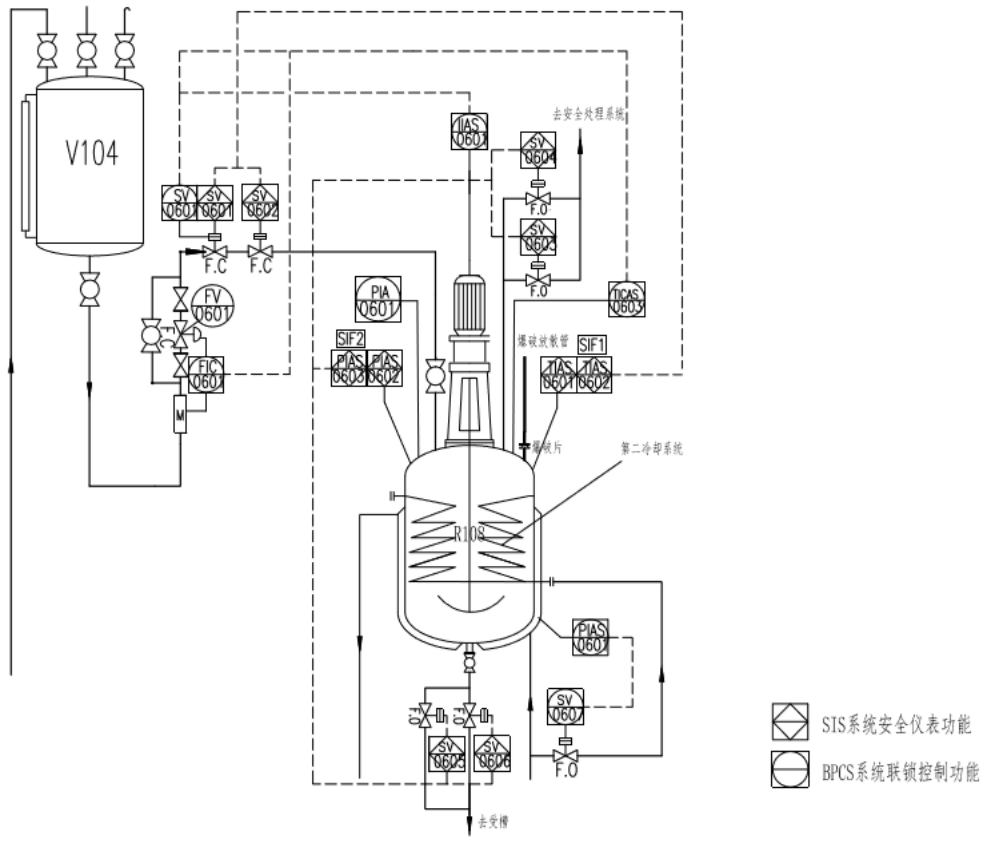
针对某设计单位提供的设计资料，对二硝基氯化苯工艺装置SIS系统的混酸滴加紧急切断功能（SIF1）进行等级验算，硝化反应过程中监控反应釜反应温度，当温度超过**℃时，紧急关闭混酸进料切断阀，其安全完整性等级为SIL2（详见附录G、附录H），本示例系不具备实际情况的复杂性，仅作验算演示。

1、SIL验算项目组（人员）

表（略）

2、验算资料：

（1）装置P&ID图（图I.1）



图I.1 某设计单位依据SIL定级结果针对二硝基氯化苯硝化反应装置设计的SIS系统P&ID图
[本例分析图中混酸滴加紧急切断功能（SIF1）]

（2）SIL确定评估表

表I.1　危险分析-风险评估-SIL确定（LOPA法）

序号	工艺简介	初始事件	后果/风险	偏差	安全仪表功能	LOPA 分析				
						现有独立保护层分析	IE 后果频率评估（a）	风险可接受水平（b）	需要增加保护水平(c)	SIL 等级确定
1	二硝基氯化苯主反应釜生产工艺描述：先将氯化苯投入硝化反应釜中，启动搅拌后，缓慢滴加混酸，在规定的温度下滴加至终点，依据反应温度调节滴加速度。	人员操作失误：人工操作混酸滴加阀门时，开度控制不当，致使混酸滴加速度过快	5	反应温度异常升高。	硝化反应过程中监控反应釜反应温度，当温度超过**℃时，紧急关闭混酸进料切断阀。	1、爆炸片取 1×10^{-2}	根据场景频率计算方法，初始事件阀门操作失误率 10^{-2}/次（假设该装置年生产 300 天，每天需要调节阀门 2 次。）；由于由人员现场操作失误引起，故人员暴露概率取 1，人员处于危险源的中心，故受伤率也取 1。考虑拟增设则后果频率为 **$6\times10^{-2}/a$**。	按附录 C 表 C.1 中在役装置目标水平为 **3×10^{-5}**	需要增加保护层的 PFD 应小于 5×10^{-3}	考虑增加过程控制系统后（保证独立性），基本过程控制系统的 PFD 为 **1×10^{-1}**，故该 SIF 安全完整性等级确定为 SIL2。
备注			1、可参见附录 C 表 C.2 后果定性分级方法。			1、可参见附录 A 表 B.1 化工行典型 IPL。	1、计算方法；根据场景频率计算。 2、初始事件频率确定见 G.4。 3、数据库来源：附录 B。	1、可以是与客户协商的风险目标水平，但不低于标准要求； 2、数据库来源（表 C.1 中在役装置目标风险水平）。	低于 b/a 的圆整值。	

评估组长：　　评估成员：　　记录员：

(3) 根据某设计单位出具的《二硝基氯化苯安全仪表系统设计资料》表明，该SIF功能设计依照《石油化工安全仪表系统设计规范》（GB/T 50770）的要求，对于评估为 SIL2 级安全仪表功能，测量仪表、控制阀、逻辑控制器均宜独立设置，并与基本过程控制过程系统分开。本回路（SIF1）温度测量仪表、逻辑控制器均为独立设置，采取“二选一”（1oo2）高安全性的逻辑结构，执行机构采用取得SIL认证的切断球阀，也采取“二选一”高安全性的逻辑结构(1oo2)，其中一个紧急切断阀与DCS系统共用（信号先进SIS系统）。

本回路（SIF1）硝化反应釜设置釜温超高高联锁关闭混酸滴加紧急切断球阀，传感单元为一体化温度变送器二台（TIAS-0601、TIAS-0602）；执行单元为混酸滴加进料管线上新增混酸紧急切断球阀两台（SV-0601、SV-0602）；系统逻辑控制单元为通过认证的符合SIL等级要求某品牌产品，该SIF回路完成以下功能：当釜内温度达到超高联锁温度时（“1oo2”），SIS 系统关闭紧急切断球阀（混酸滴加切断球阀SV-0601、SV-0602 (1oo2)）。

SIF回路具体结构内容详见表I.2 SIF仪表控制回路统计表、表I.3 SIF回路设备参数一览表。

表I.2　安全仪表系统SIF控制回路统计表

序号	回路号	功能描述	控制点位号	测量范围	控制范围	工程单位	执行器位号	控制规律	SIL 等级
1	SIF1	釜温超高高时，混酸滴加紧急切断。	TIAS-0601 TIAS-0602	**℃~**℃	**℃~**℃	℃	SV-0601 SV-0602	釜温 T>**℃,系统紧急关断混酸切断球阀 SV-0601 或者 SV-0602。	SIL2
……	……	……	……	……	……	……	……	……	……

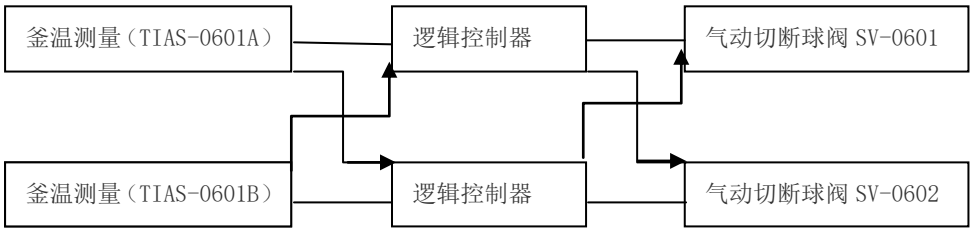
注：根据实际控制回路逐一列出；位号由P&ID图提供。

表I.3 SIF控制回路设备参数一览表

回路号	设备名	设备位号	子系统类别	硬件裕度	λDD/ Fit	λSD/ Fit	λSU /Fit	λDU /Fit	β	βD	T_I(h)	MTTR(h)	PFD_G
SIF1	一体化温度变送器	TIAS-0601 TIAS-0602	传感子系统	1oo2	258.0	0.00	84.0	32.0	10%	5%	8760	8	1.41E-05
	安全栅	Safe-A Safe-B	传感子系统	1oo2	1134.1	0.00	1020.7	113.4	10%	5%	8760	8	5.02E-05
	混酸滴加紧急切断球阀	SV-0601 SV-0602	最终执行子系统	1oo2	142	0.00	640	430	10%	5%	8760	8	1.91E-04
	电磁阀		最终执行子系统	1oo2	353	0.00	278	4	10%	5%	8760	8	1.90E-04
	安全逻辑控制器		逻辑控制子系统	1oo2	221.859	36.731	78.109	2.498	10%	5%	8760	8	1.18E-06

注：1Fit=1E-09；设备参数由设备厂家提供。

3、可靠性框图建模：依据设计单位提供设计资料绘制该SIF回路可靠性框图，如下图I.2二硝基氯化苯混酸滴加紧急切断（SIF1）系统可靠性框图：



图I.2　二硝基氯化苯混酸滴加紧急切断（SIF1）系统可靠性框图

4、系统结构约束验证：由图I.2可知，SIS系统传感部分（釜温测量为1oo2,HFT=1）、逻辑处理器部分为1oo2结构(HFT=1)，执行器为1oo2结构(HFT=1)。

依据表I.3提供参数计算各子系统安全失效分数:

$$SFF=（\lambda DD+\lambda SD+\lambda SU）/（\lambda DD+\lambda DU+\lambda SD+\lambda SU）$$

式中：

λDD 为检测到的子系统中通道每小时的危险失效率（它是在子系统通道中所有检测到的危险失效率的总和）；

λDU 为未检测到的子系统中通道每小时的危险失效率（它是在子系统通道中所有未检测到的危险失效率的总和）；

λSD 为子系统中被检测到的通道每小时的安全失效率（它是子系统通道中所有未被检测到的安全失效率的总和）；

λSU 为子系统中未被检测到的通道每小时的安全失效率（它是在子系统通道中所有未被检测到的安全失效率的总和）。

经计算结果如下：

执行元件气动球阀部分SFF=64.5%　　（A类安全相关子系统）

安全栅部分SFF=95.0%　　（A类安全相关子系统）

电磁阀部分SFF =99.4%　　（A类安全相关子系统）

传感器部分一体化温变SFF= 91.4%　　（B类安全相关子系统）

逻辑处理器部分SFF=99.3%　　（B类安全相关子系统）

表I.4　硬件安全完整性：A类安全相关子系统的结构约束 （GB/T 20438）

安全失效分数（SFF）	最低硬件故障裕度		
	0	1	2
＜60%	SIL1	SIL2	SIL3
60%~＜90%	SIL2	SIL3	SIL4
90%~＜99%	SIL3	SIL4	SIL4
≥99%	SIL3	SIL4	SIL4

表I.5　硬件安全完整性：B类安全相关子系统的结构约束 （GB/T 20438）

安全失效分数（SFF）	最低硬件故障裕度		
	0	1	2
＜60%	不允许	SIL1	SIL2
60%~＜90%	SIL1	SIL2	SIL3
90%~＜99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

将各子系统元件的安全失效分数SFF，按照各自所属类型（A、B）分别对应表I.4、表I.5核查，得出结论：该SIF回路硬件裕度满足SIL2等级结构约束。

5、 要求时的失效概率PFD_G 验证：由系统可靠性框图图I.2可知，SIS系统传感部分（釜温测量为1oo2）、逻辑处理器部分为1oo2结构，执行器为1oo2结构。

通常系统要求的失效概率为：

$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$

式中：PFD_{SYS} — SIS系统的安全功能在要求时的平均失效概率

PFD_S — 传感器子系统要求的平均失效概率

PFD_L — 逻辑子系统要求的平均失效概率

PFD_{FE} — 最终元件子系统要求的平均失效概率

依据表I.4所列参数及图I.2所列出不同仪表组合，通过可靠性框图推导出PFDavg计算公式得出：

对于传感子系统：一体化温度变送器和安全栅的PFD相加，即

PFD_s=1.41E-05+5.02E-05=6.43E-05；

对于逻辑子系统：PFD_L=1.18E-06；

对于最终元件子系统：混酸滴加紧急切断球阀和电磁阀的PFD相加，即：

PFD_{FE}=1.91E-04+1.90E-04=3.81E-04

本SIF回路要求时的失效概率：

$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$

=6.43E-05+1.18E-06+3.81E-04

=4.46E-04(满足SIL2)

6、验算结果

表I.6　二硝基氯化苯硝化反应混酸滴加紧急切断功能（SIF1）验算结果

验算项目	子系统	结构	HFT	SFF	PFD_{avg}（时间间隔为1年）	SIL 等级
硬件完整性	一体化温度变送器	1oo2	1,TypeB	91.4	1.41E-05	SIL3（适用）
	安全栅	1oo2	1,TypeA	95.0	5.02E-05	SIL3（适用）
	电磁阀	1oo2	1, TypeA	99.4	1.91E-04	SIL3（适用）
	气动切断球阀	1oo2	1, TypeA	64.5	1.90E-04	SIL3（适用）
	安全型逻辑处理器	1oo2	1, TypeB	99.3	1.18E-06	SIL3（适用）
系统完整性	系统能力约束	各子系统均采用符合GB/T 20438的产品；建立了完善的安全仪表运行及检修制度，并按要求落实。				系统能力符合要求
	SIF1系统				4.46E-04	SIL2（满足）

评估组长：　　评估成员：　　记录员：

验算结论：该SIF回路符合评定的安全完整性等级SIL2。当多个SIF验算时，应考虑共因失效。

I.2　安全仪表系统(SIS)SIF回路SIL等级的两种验算方法介绍

1、GB/T 20438中SIL验算方法

IEC 61508中的SIL验算方法适用于已取得SIL认证的仪表、控制逻辑器、执行元件等，取得SIL认证的产品参数由设备厂商提供，其中，λSD为被检测到的安全故障率；λSU为未被检测到的安全故障率；λDD为被检测到的危险故障率；λDU为未被检测到的危险故障率；λS为安全失效故障率；λD为危险失效故障率（故障率的单位为Fit，1 Fit=1×10^{-9}）；DC为诊断覆盖率；SFF为安全失效分数。计算公式如下所示：

$$\lambda S=\lambda SD+\lambda SU$$

$$\lambda D=\lambda DD+\lambda DU$$

$$DC=\lambda DD/\lambda D$$

$$SFF=(\lambda DD+\lambda S)/(\lambda D+\lambda S) \qquad (1)$$

式（1）中λSD，λSU，λDD，λDU可从仪表设备SIL认证证书中获取。根据GB/T 50770中4.1.3条规定：“通常石油化工工厂和装置的安全仪表系统工作于低要求操作模式”，故下文中的参数均是低要求操作模式下的认证参数。

通过式（1）的计算可得出安全失效分数，而表I.4和表I.5列出了硬件的SIL，其中A类仪表有浪涌保护器、液位开关、安全栅、电磁阀、阀体、执行机构、阀门定位器等，B类有安全型控制逻辑器、现场变送器等。

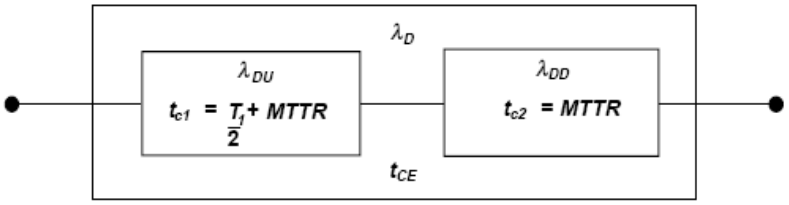
经验表明，通过SIL认证的温度变送器、压力变送器、流量计、液位计等B类子系统SFF多在90%～99%，符合SIL2的要求，可以通过冗余配置达到SIL3。而A类子系统SFF在90%～99%已满足SIL3要求。

SIS投入运行后需进行周期性的离线维护，某些故障或失效只能通过离线的人工测试才能发现，例如变送器的膜盒损坏、引压管的堵塞、测量精度、阀门的腐蚀内漏、阀芯的卡死等。大多数SIS设备的检验测试在装置的停车大修期间进行。在低操作要求模式下，检测平均时间间隔T1有3 d,6 d,1 a，一般选用T1=1 a=8760 h，平均恢复时间MTTR=8 h。

工程设计中，常见的仪表组合有“1oo1”，“1oo2”，“2oo3”，通过下列步骤分别计算组合后的PFDavg。

以下列出不同仪表组合的通过可靠性框图计算推导出的PFDavg公式。

(1) 1oo1结构的可靠性框图



图I.3 1oo1可靠性框图

通道的等效平均停止工作时间表示如下：

$$t_{CE}=\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2}+MTTR\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR$$

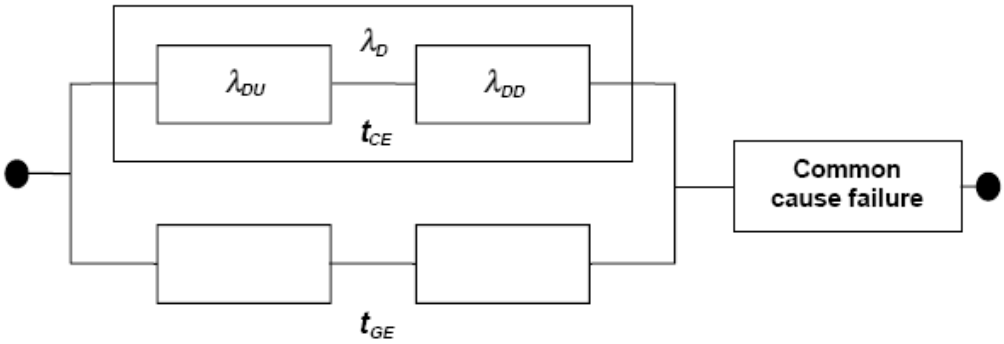
已被检测和未被检测到的危险失效率如下：

$$\lambda_{DU}=\frac{\lambda}{2}(1-DC)\quad ;\lambda_{DD}=\frac{\lambda}{2}DC$$

此结构在要求时的平均失效概率为：

$$PFD_G=(\lambda_{DU}+\lambda_{DD})t_{CE}$$

(2) 1oo2结构的可靠性框图



图I.4 1oo2可靠性框图

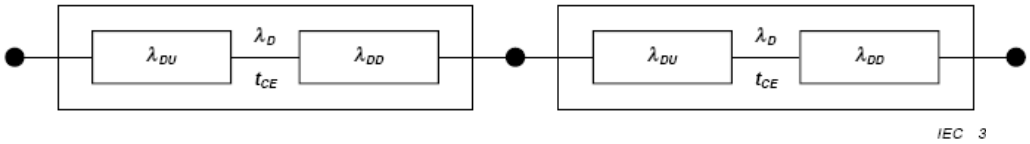
系统等效停止工作时间表示如下：

$$t_{GE}=\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3}+MTTR\right)+\frac{\lambda_{DU}}{\lambda_D}MTTR$$

此结构在要求时的平均失效概率为：

$$PFD_G=2(1-\beta)\lambda_{DU}\left((1-\beta)\lambda_{DU}+(1-\beta_D)\lambda_{DD}+\lambda_{SD}\right)t_{CE}t_{GE}+\beta_D\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)$$

（3） 2oo2结构的可靠性框图

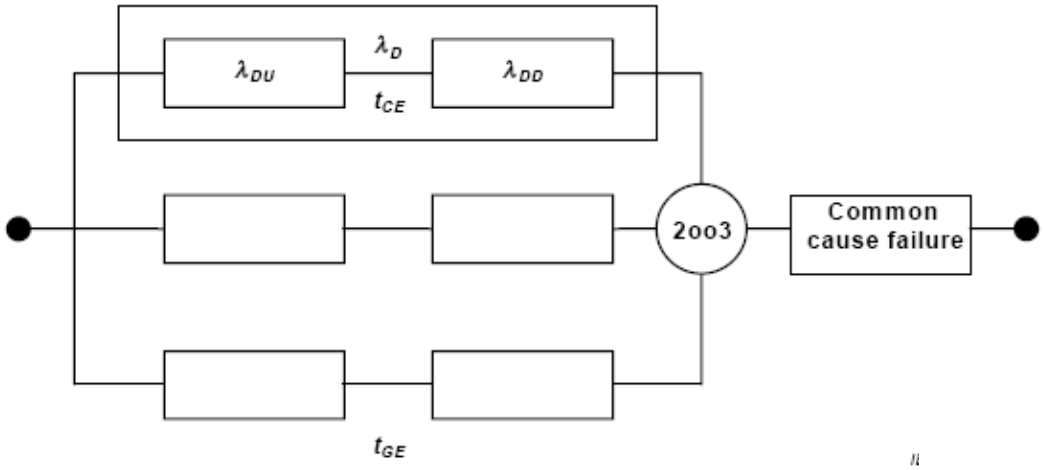


图I.5　2oo2可靠性框图

此结构在要求时的平均失效概率为：

$$\mathrm{PFD_G} = 2\lambda_\mathrm{D} t_\mathrm{CE}$$

（4） 2oo3结构的可靠性框图



图I.6　2oo3可靠性框图

此结构在要求时的平均失效概率为：

$$\mathrm{PFD_G} = 6\left((1-\beta_\mathrm{D})\lambda_\mathrm{DD} + (1-\beta)\lambda_\mathrm{DU}\right)^2 t_\mathrm{CE} t_\mathrm{GE} + \beta_\mathrm{D}\lambda_\mathrm{DD}\mathrm{MTTR} + \beta\lambda_\mathrm{DU}\left(\mathrm{T_1}/2 + \mathrm{MTTR}\right)$$

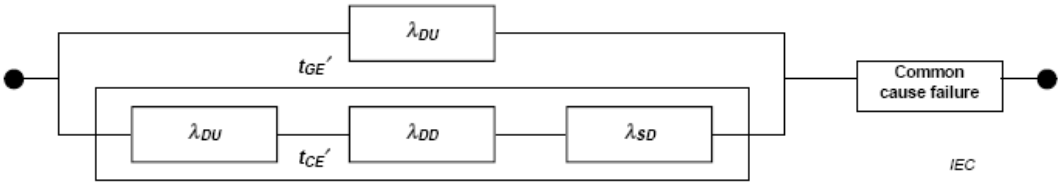
（5 ）1oo2D结构的可靠性框图

每个通道中被检测的安全失效率如下：

$$\lambda_\mathrm{SD} = \lambda / 2\mathrm{DC}$$

$$t'_\mathrm{CE} = \left[\lambda_\mathrm{DU}/\left(\mathrm{T_1}/2 + \mathrm{MTTR}\right) + \left(\lambda_\mathrm{DD} + \lambda_\mathrm{SD}\right)\mathrm{MTTR}\right]/\left(\lambda_\mathrm{DU} + \lambda_\mathrm{DD} + \lambda_\mathrm{SD}\right)$$

$$t'_\mathrm{GE} = \left[\lambda_\mathrm{DU}/\left(\mathrm{T_1}/3 + \mathrm{MTTR}\right) + \left(\lambda_\mathrm{DD} + \lambda_\mathrm{SD}\right)\mathrm{MTTR}\right]/\left(\lambda_\mathrm{DU} + \lambda_\mathrm{DD} + \lambda_\mathrm{SD}\right)$$



图I.7　1oo2D可靠性框图

此结构在要求时的平均失效概率为：

$$\mathrm{PFD_G} = 2(1-\beta)\lambda_\mathrm{DU} + \left((1-\beta)\lambda_\mathrm{DU} + (1-\beta_\mathrm{D})\lambda_\mathrm{DD} + \lambda_\mathrm{SD}\right)t_\mathrm{CE}\,'t_\mathrm{GE}\,' + \beta_\mathrm{D}\lambda_\mathrm{DD}\mathrm{MTTR} + \beta\lambda_\mathrm{DU}\left(\mathrm{T_1}/2 + \mathrm{MTTR}\right)$$

式中：βD——具有共同原因已被检测到的失效分数；β——具有共同原因没有被检测到的失效分数，β=2βD。

β的值可根据GB/T 20438.6通过评分获得，β取值有1%，2%，5%，10%；对应的βD分别为0.5%，1%，2.5%，5%。将上述数据分别代入式（5）中验算，结果相差无几，且β评分方法繁琐，为了方便工程计算，现场仪表可统一将β取值为10%，βD取值为5%。

（6）根据相应结构约束分别计算SIF回路中的传感器、逻辑系统、执行元件等的PFD_G后，计算SIF回路系统的平均失效概率：

$PFD_{SYS} = \sum PFD_S + \sum PFD_L + \sum PFD_{FE}$

式中：$\sum PFD_S$——传感器子系统平均失效概率；

$\sum PFD_L$——逻辑子系统平均失效概率；

$\sum PFD_{FE}$——执行元件子系统平均失效概率。

2、ISA TR 84.00.02标准中SIL的验算方法

ISA TR 84.00.02标准(美国仪器、系统和自动化协会颁布的标准，全称：ISA TR 84.00.02 Safety Instrumented Functions (SIF)—Safety Integrity Level(SIL) Evaluation Technique）中SIL的计算方法相对简单，未经SIL认证的普通仪表采用IEC 61508计算时，λSD，λSU，λDD，λDU无数据可查，此时可通过ISA TR 84.00.02 标准中的方法进行SIL验算，步骤如下所示：

1） 计算危险失效故障率λd： λd=1/MTTFd

式中： MTTFd——平均危险失效前时间,实际验算过程中精确的数值可从供货商处获取仪表平均故障时间MTBF，MTTFd=MTBF-MTTR，因MTTR时间很短为8 h，则MTTFd≈MTBF。在MTTFd无数据可循的情况下，可参考ISA TR 84.00.02 标准中part 1 表5.1中5个工厂经验值。

因λDU=λD×（1-DC），可假设未经过SIL认证的常规仪表诊断覆盖率DC=0，则λDU=λD。

① “1oo1”时的PFD_G：

$$PFD_G = \lambda DU \cdot \frac{T_I}{2}$$

② “1oo2”时的PFD_G：

$$PFD_G = \frac{(\lambda DU \cdot T_I)^8}{3}$$

③ “2oo3”时的PFD_G：

$$PFD_G = (\lambda DU \cdot T_I)^2$$

2） 根据公式$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$，计算SIF回路的$PFD_{SYS}$。