ICS 25.040
N 10

团 体 标 准

T/CPI XXXX-2023

炼化企业安全仪表系统安全完整性等级（SIL）评估技术规范

Technical Specification for Safety integrity level (SIL) Assessment of Safety instrumented system of Refinery and Chemical Companies

（征求意见稿）

2023-XX-XX 发布　　2023-XX-XX 实施

中国石油和石油化工设备工业协会

目 次

前 言 1

1 范围 1

2 规范性引用文件 1

3 术语、定义和缩略语 1

4 基本要求 3

5 SIL 定级 4

5.1 SIL 定级的步骤 4

5.2 确定风险可接受准则 4

5.3 场景识别与筛选 4

5.4 初始事件确认 5

5.5 独立保护层辨识 5

5.6 场景频率计算 6

5.7 评估 SIL 等级 6

6 SIL 验证 7

6.1 基本要求 7

6.2 验证步骤 7

6.3 验证准则 7

6.4 判定结构约束 SIL 等级 8

6.5 计算随机失效 SIL 等级 8

6.6 系统性安全完整性验证 8

6.7 验证结果 9

7 跟踪管理要求 9

附 录 A （资料性） SIL 定级报告内容 10

附 录 B （资料性） SIL 验证报告内容 11

附 录 C （资料性） 典型风险可接受准则示例 12

附 录 D （资料性） 典型初始事件频率 15

附 录 E （资料性） 典型独立保护层要求时的失效概率 17

附 录 F （规范性） 安全完整性等级确定原则 19

附 录 G （资料性） 典型仪表设备共因失效因子参考值 20

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。

本文件由中国石油和石油化工设备工业协会提出并归口。

本文件起草单位：

本文件主要起草人：

炼化企业安全仪表系统安全完整性等级（SIL）评估技术规范

1 范围

本文件规定了炼化企业安全仪表系统安全完整性等级评估的基本要求、定级方法、验证方法及跟踪管理要求。

本文件适用于炼化企业安全仪表系统安全完整性等级评估工作。

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　电气/电子/可编程电子安全相关系统的功能安全

GB/T 21109　过程工业领域安全仪表系统的功能安全

GB/T 32857　保护层分析（LOPA）应用指南

AQ/T 3033　化工建设项目安全设计管理导则

AQ/T 3054　保护层分析（LOPA）方法应用导则

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

安全仪表系统 safety instrumented system

用于实现一个或几个安全仪表功能的仪表系统，可以由测量仪表、逻辑控制器和最终执行元件构成。

3.1.2

安全仪表功能 safety instrumented function

为达到功能安全所必需的具有特定安全完整性等级的安全功能。

3.1.3

安全完整性等级 safety integrity level

用于规定分配给安全仪表系统的安全仪表功能的安全完整性要求的离散等级。SIL4 是安全完整性的最高等级，SIL1 为最低等级。炼化企业使用的最高等级为 SIL3。

3.1.4

场景 scenario

可能导致不期望后果的一种事件或事件序列。

3.1.5

初始事件 initiating event

事件/事故场景的初始原因。

3.1.6

后果 consequence

某一事件/事故导致的影响。通常包括人员伤亡、财产损失、环境污染、非财务性影响与社会影响。

3.1.7

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。

3.1.8

独立保护层 independent protection layer

独立的一种设备、系统或行动，能阻止场景向不期望后果发展。其独立性表示保护层的执行能力不受初始事件或其他保护层失效的影响。

3.1.9

保护层分析 layer of protection analysis

对降低事件/事故发生频率或后果严重性的独立保护层的有效性进行评估的一种方法。

3.1.10

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

当受保护设备或受保护设备控制系统发生要求时，设备或系统不能响应的概率。

3.1.11

要求时的平均失效概率 average probability of failure on demand

当受保护设备或受保护设备控制系统发生要求时，设备或系统不能响应的平均概率。

3.1.12

危险失效平均频率 probability of failure per hour

一个 E/E/PE 安全相关系统在一个给定的时间周期内执行规定安全功能时的危险失效平均频率。

3.1.13

硬件故障裕度 hardware fault tolerance

一个部件或子系统在有一个或几个硬件危险故障的情况下，仍能继续承担所要求的安全仪表功能的能力。

3.1.14

安全失效分数 safety failure fraction

安全相关组件的属性，定义为平均安全失效率加上检测出的平均危险失效率，与平均安全失效率加上平均危险失效率之比。

3.1.15

SIF 运行模式 operating mode of SIF

SIF 的运行方式分为低要求模式、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。

3.1.16

有限可变语言　limited variability language

用于商业或工业可编程电子控制器的编程语言，其能力仅限于在相关安全手册中定义的应用。这种语言的记法可能是文本或图形或二者皆有。

3.1.17

全可变语言　full variability language

计算机编程者易于理解，并可提供实现各种各样功能和应用的能力的一种语言。FVL 的例子包括：Ada、C、Pascal、指令表、汇编程序语言、C++、Java 和 SQL。

3.1.18

诊断覆盖率　diagnostic coverage

通过自动在线诊断测试检测到的危险失效分数。危险失效分数是由检测到的危险失效率除以总危险失效率计算出的。

3.2　缩略语

下列缩略语适用于本文件。

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 studies）

LOPA：保护层分析（Layer of protection analysis）

IPL：独立保护层（Independent protection layer）

SIF：安全仪表功能（Safety instrumented function）

SIL：安全完整性等级（Safety integrity level）

PFD：要求时的失效概率（Probability of failure on demand）

PFD_{avg}：要求时的平均失效概率（Average probability of failure on demand）

PFH：危险失效平均频率（Probability of failure per hour）

HFT：硬件故障裕度(Hardware fault tolerance)

MTTF：平均无故障时间（Mean time to failure）

DD：可检测到的危险失效（Dangerous failure detected）

DU：未检测到的危险失效（Dangerous failure undetected）

SD：可检测到的安全失效（Safety failure detected）

SU：未检测到的安全失效（Safety failure undetected）

β：共因失效因子（Common cause failure factor）

RRF：风险降低因子（Risk reduction factor）

SRS：安全要求规格书（Safety requirements specification）

4　基本要求

4.1　安全仪表系统应独立于基本过程控制系统，能够独立完成安全保护功能。

4.2 企业应组织对安全仪表系统中每一个安全仪表功能的安全完整性等级进行评估，包括SIL定级和SIL验证。

4.3 新建、改建和扩建项目设计阶段应开展安全仪表系统SIL定级和SIL验证工作。设计初期时，为了避免后期验算不通过带来的设计修改，可进行SIL预验证，采用拟用产品证书数据或通用数据进行验证计算。

4.4 企业应结合HAZOP分析结果开展SIL定级工作，依据定级结果开展SIS系统工程设计。

4.5 安全仪表系统设备选型确定后，应对每一个安全仪表功能进行SIL验证，不能满足要求的安全仪表功能应进行整改。

4.6 SIL评估小组应包含工艺、仪表、设备、安全、电气等专业人员，SIL评估主持人应具有石油石化行业工艺、仪控、安全相关的设计、咨询或运行经验，取得功能安全工程师或相关专业工程师资格证书。

4.7 企业应建立安全仪表功能的日常管理档案，包括但不限于联锁功能、设定值、变更信息、停车记录、校验记录、故障信息等数据资源。

5 SIL 定级

5.1 SIL 定级的步骤

SIL定级宜采用LOPA方法，定级过程包含以下步骤：

a）确定风险可接受准则；

b）场景识别与筛选；

c）初始事件确认；

d）独立保护层辨识；

e）场景频率计算；

f）评估SIL等级。

5.2 确定风险可接受准则

企业应依据行业相关要求结合自身实际情况制定风险可接受准则，作为 SIL 定级工作的基础。典型风险可接受准则示例参见附录 C。

5.3 场景识别与筛选

5.3.1 场景识别信息通常来源于新建、改建、扩建项目或在役系统开展HAZOP分析识别的风险场景，主要包括：

a）工艺设计意图，例如联锁设计时考虑保护的事故场景；

b）生产运行问题，包括意外行为或正常范围之外的操作条件等；

c）事故事件，尤其类似工厂及行业发生过的事故事件案例。

5.3.2 场景基本要求包括以下内容：

a）每个场景要素应包括但不限于：

1）引起事件或事件序列发生的初始事件；

2）该事件继续发展所导致的后果。

b）每个场景应有唯一的初始事件及其对应后果；

c）当同一初始事件导致不同的后果时，或多种初始事件导致同一后果时，应假设多个场景；

d）当场景中存在使能事件或使能条件时，应将其包含在场景中；

e）如果考虑人员伤害、财产损失或环境影响作为后果，则场景应考虑下列因素或条件修正因子：

1）可燃物质被引燃的可能性；

2）人员出现在事件影响区域的概率；

3）火灾、爆炸或有毒物质释放的暴露致死率（在场人员逃离的可能性）；

4）其他可能的修正因子。

5.3.3 推荐采用定性或半定量的方法对场景后果的严重性进行评估，并根据后果严重性对场景进行筛选。典型的后果种类包括人员伤害、财产损失、环境影响、非财务性影响与社会影响。

5.4 初始事件确认

5.4.1 初始事件一般包括外部事件、设备故障和人为失误，初始事件确认时应遵循以下原则：

a）审查场景中所有的原因，以确定该初始事件为有效初始事件；

b）应确认已辨识出所有的潜在初始事件；

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

d）在识别潜在事件时，应确保已经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）当人为失误作为初始事件时，应制定人为失误频率评估的统一规则并在分析时严格执行。

5.4.2 以下事件不宜作为初始事件：

a）操作人员培训不到位；

b）测试或检查不完善；

c）保护装置不可用；

d）其他类似事件。

5.5 独立保护层辨识

5.5.1 典型的独立保护层包括：

a）本质安全设计；

b）基本过程控制系统；

c）关键报警及人员响应；

d）安全仪表系统；

e）物理保护（释放措施）；

f）释放后保护措施。

5.5.2 独立保护层应满足独立性要求：应独立于初始事件及其后果和同一场景中的其他独立保护层。

5.5.3 独立保护层应满足有效性要求：执行动作以后可以有效防止事故后果的发生。

5.5.4 独立保护层应满足可审查性要求：对有效性、独立性以及PFD值可以某种方式（通过记录、审查、测试等）进行验证。

5.5.6 以下措施不宜作为独立保护层：培训和取证、操作程序、正常的测试和检测、标识。

5.6 场景频率计算

5.6.1 初始事件发生频率和IPL的PFD数据参见附录D和附录E。实际应用时，PFD值的确定应经评估小组共同确认，如有必要可进行适当的修正以确认PFD取值的合适性，并作为分析过程的统一规则执行。初始事件发生频率应优先使用企业的经验数据，其次使用行业通用数据。

5.6.2 单一场景后果的频率为初始事件发生频率乘以所有IPL的PFD，场景后果频率可以由以下两种系数进行修正：

a) 当场景的发生需要使能事件或使能条件时，应乘以使能事件或使能条件的发生概率；

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

1) 可燃物质点火概率；

2) 人员出现在事件影响区域的概率；

3) 火灾、爆炸或有毒物质释放的暴露致死概率；

4) 其他，如工程经验。

5.6.3 场景频率按式（1）计算：

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

式中：

f_i^C— 初始事件 i 造成后果 C 的频率，单位为次每年；

f_i^I — 初始事件 i 的发生频率，单位为次每年；

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

P_i^C— 条件修正因子，假如没有任何条件修正，则P^C取1；

$\prod_{j=1}^{J} PFD_{ij}$ — 初始事件i中j个阻止后果C的IPL的PFD的总乘积。

5.7 评估 SIL 等级

5.7.1 根据式（2）计算场景所需安全仪表功能的 PFD。

$$PFD_{SIF} = F / f_i^C \quad (2)$$

式中：

PFD_{SIF} — 安全仪表功能要求时的失效概率；

F — 风险可接受频率，具体根据5.3.3场景后果严重性评估结果查阅风险可接受准则进行确定；

f_i^C — 初始事件i造成后果C的频率，单位为次每年；

5.7.2 根据PFD_{SIF}计算结果查阅表F.1，确定单一场景安全仪表功能需要达到的SIL等级。

5.7.3 同一初始事件导致多个事故场景的，逐个场景进行分析，该安全仪表功能SIL等级取场景需要达到SIL等级的最高值。多个初始事件导致同一事故后果的，场景频率计算时宜考虑进

行叠加。

5.7.4 安全仪表功能定级结果达到 SIL3 以上时，应增加独立保护层或修改工程设计方案，降低对该安全仪表功能的 SIL 等级要求。

6 SIL 验证

6.1 基本要求

6.1.1 安全仪表功能的测量仪表、逻辑控制器和最终执行元件等厂家规格型号确定后，应进行 SIL 验证计算，以判断现有安全仪表系统是否能够达到 SIL 定级时要求的 SIL 等级。对未达到 SIL 等级要求的安全仪表系统应采取整改措施，以满足系统 SIL 等级的要求。

6.1.2 SIL 验证的范围应包含所有 SIL1 及以上的安全仪表功能。

6.1.3 SIL 验证通常采用专业化软件进行建模计算，软件内嵌验算方法应符合 GB/T 20438、GB/T 21109 要求。

6.1.4 仪表设备可靠性数据宜来自以往使用数据、SIL 认证报告、公开发行的工业数据库或安全手册中的失效数据等。

6.2 验证步骤

SIL 验证过程包含以下步骤：

a) 明确验证准则；

b) 判定结构约束 SIL 等级；

c) 计算随机失效 SIL 等级；

d) 系统性安全完整性验证；

e) SIL 等级验证结果。

6.3 验证准则

6.3.1 安全仪表功能的 SIL 等级应同时满足结构约束 SIL 等级、随机失效 SIL 等级以及系统性安全完整性要求。

6.3.2 结构约束 SIL 等级确定应满足以下条件：

a) SIL 等级应满足表 1 对应最小 HFT 要求；

b) 全可变或有限可变语言可编程设备的诊断覆盖率应不小于 60%；

c) 失效量计算中使用的可靠性数据应由不小于 70%的统计置信区间上限确定。

表 1 不同 SIL 对应的最小 HFT 要求

SIL	要求的最小 HFT
1（任何模式）	0
2（低要求模式）	0
2（高要求/连续模式）	1
3（任何模式）	1

4（任何模式）	2
注：未使用全可变或有限可变语言可编程设备的 SIS 或 SIS 子系统，若采用本表规定的最小 HFT 将导致额外故障并导致整体过程安全降级，其 HFT 要求参照 GB/T21109.1 标准要求确定。	

6.3.3 随机失效 SIL 等级确定应满足以下条件：

a）低要求和高要求运行模式下安全仪表功能的 SIL 等级应根据表 F.1 或表 F.2 确定。

b）连续模式下运行的安全仪表功能的 SIL 等级应根据附录表 F.2 确定。

6.4 判定结构约束 SIL 等级

6.4.1 应对测量仪表、逻辑控制器、最终执行元件等子系统分别确定HFT，安全仪表功能结构约束SIL等级取决于各子系统结构约束SIL等级的最小值。

6.4.2 依据安全仪表功能中包含的测量仪表、逻辑控制器、最终执行元件等元器件相关的规格型号、冗余结构等信息，根据6.3.2要求确定安全仪表子系统的结构约束SIL等级。

注1：基于路线1H和2H确定结构约束SIL等级要求见GB/T20438.2，本文件中不做讨论。

6.5 计算随机失效 SIL 等级

6.5.1 依据安全仪表功能中包含的测量仪表、逻辑控制器、最终执行元件等元器件相关的规格型号、冗余结构、检验测试计划及规程等情况，综合可信数据库，确定各元器件可检测到的危险失效率（λ_{DD}）、未检测到的危险失效率（λ_{DU}）、可检测到的安全失效率（λ_{SD}）、未检测到的安全失效率（λ_{SU}），以及共因失效因子(共因失效因子 β 的选取可根据工程经验或参考附录 G 确定)、平均恢复时间、检验测试间隔、检验测试覆盖率等参数，通过建模计算安全仪表功能各子系统的 PFD_{avg}。

6.5.2 根据安全仪表功能各子系统的要求时的平均失效概率，按式（3）计算安全仪表功能的 $PFD_{avg-SIF}$。根据$PFD_{avg-SIF}$计算结果查阅附录F，确定安全仪表功能的随机失效SIL等级。

$$PFD_{avg-SIF} = PFD_{avg-S} + PFD_{avg-L} + PFD_{avg-FE} \quad (3)$$

式中：

$PFD_{avg-SIF}$ — 安全仪表功能要求时的平均失效概率；

PFD_{avg-S} — 测量仪表子系统要求时的平均失效概率；

PFD_{avg-L} — 逻辑控制器子系统要求时的平均失效概率；

PFD_{avg-FE} — 最终执行元件子系统要求时的平均失效概率。

6.6 系统性安全完整性验证

6.6.1 设备的系统性能力SC N（N =1,2,3）应满足SIF要求的SIL等级。宜根据厂商提供SIL认证报告查询设备可实现的系统性能力。

6.6.2 设备的系统性能力要求可通过满足GB/T20438路线1s、路线2s、路线3s之一实现。

6.6.3 对于某具有系统性能力SC N(N =1,2,3)的组件，若该组件的系统性故障并不会使指定安全功能失效，而仅在另一个具有系统性能力SC N 的组件同时发生系统故障时才会使指定功能失效，则在两个组件之间足够独立的前提下其组合的系统性能力可视为SC (N +1)。足够独立性的判定见GB/T20438.2第7.4.3.4条。

6.6.4 多个系统性能力为SC N 的组件组合后可声明的最高系统性能力为SC(N +1)。每个SC N 组件在这种方式下仅能使用一次，不允许继续增加SC N 组件达到或超过SC (N +2)。

6.7 验证结果

6.7.1 应以安全仪表功能结构约束SIL等级和随机失效SIL等级两者中的较小值作为该安全仪表功能可以达到的SIL等级，同时系统性能力SC应满足SIL等级要求。

6.7.2 安全仪表功能验证达到的SIL等级大于或等于SIL定级要求达到的SIL等级时，该安全仪表功能满足要求。宜考虑SIL定级结果RRF要求。

6.7.3 安全仪表功能验证达到的SIL等级低于SIL定级要求达到的SIL等级时，该安全仪表功能不满足要求，应进一步分析其冗余结构以及测量仪表、逻辑控制器和最终执行元件的PFD分布情况，提出整改措施。

6.7.4 装置不满足SIL等级要求时，可考虑采取以下整改措施以实现SIL等级要求：

a）增加独立保护层；

b）增设冗余结构；

c）更换危险失效率更低的元器件或提高设备诊断覆盖率；

d）设置部分行程测试；

e）调整安全仪表功能检验测试周期及检验测试覆盖率等。

7 跟踪管理要求

7.1 基础设计阶段宜开展SRS编制工作，并跟随设计和工程进度不断补充完善，以指导安全仪表系统全生命周期各阶段管理工作，SRS应符合GB/T21109.1要求。

7.2 安全仪表系统应定期检验测试，并详细记录测试过程和结果。

7.3 安全仪表系统测试方法应参考厂商安全手册或安装维护手册，并编制相应的检验测试规程及记录报告模板。

7.4 安全仪表系统检验测试周期应综合考虑法律法规与标准规范的要求、厂商建议、SIL 验证报告以及设备设施大修周期等因素确定。

7.5 安全仪表系统变更包括投用状态的变更（投用/摘除）、联锁设定值的变更、控制逻辑的变更、硬件的非同类替换或更换厂家、系统软件的版本变化等等，对安全仪表系统的所有变更均应保留相应信息，包括：

a）变更的描述；

b）变更的理由；

c）变更活动对安全仪表系统的影响分析与风险评估；

d）变更审批记录、变更培训；

e）验证所有变更已正确实施，包括验证安全仪表系统可以按要求执行所进行的测试；

f）验证所有变更不会对未修改的安全仪表系统组成部分产生不利影响所进行的测试。

7.6 安全仪表系统发生变更时，应重新开展 SIL 定级及验证工作。

附 录 A
（资料性）
SIL 定级报告内容

SIL 定级报告大纲宜包括以下主要内容：

A.1 封皮

A.2 签字页

A.3 目录

A.4 正文

A.4.1 项目概述

A.4.2 工作范围

A.4.3 定级方法概述

A.4.4 风险可接受标准

A.4.5 条件修正假设

A.4.6 工艺描述

A.4.7 SIL 定级小组组成

A.4.8 SIL 定级进程

A.4.9 SIL 定级结果（含定级结果汇总表、统计分析表）

A.4.10 改进建议（含改进建议措施汇总表）

A.5 附件

A.5.1 SIL 分析定量数据

A.5.2 SIL 定级分析会议签到表

A.5.3 SIL 定级记录表

附 录 B
（资料性）
SIL 验证报告内容

SIL 验证报告大纲宜包括以下主要内容：

B.1 封皮

B.2 签字页

B.3 目录

B.4 正文

B.4.1 项目概述

B.4.2 工作范围

B.4.3 验证方法概述

B.4.4 验证假设说明

B.4.5 需验证回路统计

B.4.6 验证结果汇总

B.4.7 改进方案建议

B.5 附件

B.5.1 验证工作表（包括测量仪表、逻辑控制器、最终执行元件三个部分的 PFD_{avg}、MTTF、结构约束 SIL 等级等计算结果）

B.5.2 验证数据（包括测量仪表、逻辑控制器、最终执行元件等设备的厂家型号以及对应的失效数据，如 λ_{DD}、λ_{DU}、λ_{SD}、λ_{SU} 等）

附 录 C
（资料性）
典型风险可接受准则示例

C.1 概述

风险可接受准则是在确定的经济技术条件下，经过长期积累或反复验证后企业可以接受的风险频率，包括但不限于安全、环境、财产、非财务性影响与社会影响方面的风险。

C.2 安全相关风险的可接受频率

SIL定级过程中所采用的安全相关风险的可接受频率，如表C.1所示。

表 C.1 安全相关风险的可接受频率

严重程度	安全相关风险	可接受频率（/y）
5 级	造成 10 人以上死亡，或者 50 人以上重伤	1×10^{-7}
4 级	造成 3 人以上 10 人以下死亡，或者 10 人以上 50 人以下重伤	1×10^{-6}
3 级	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	1×10^{-5}
2 级	造成 3 人以下重伤，或者 3 人以上 10 人以下轻伤	1×10^{-3}
1 级	造成 3 人以下轻伤	1×10^{-1}

C.3 环境相关风险的可接受频率

SIL定级过程中所采用的环境相关风险的可接受频率，如表C.2所示。

表 C.2 环境相关风险的可接受频率

严重程度	环境相关风险	可接受频率（/y）
5 级	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	1×10^{-6}
4 级	重大泄漏，给工作场所外带来严重影响	1×10^{-5}
3 级	释放事件受到管理部门的通报或违反允许条件	1×10^{-4}
2 级	事件不会受到管理部门的通报或违反允许条件	1×10^{-2}

1 级	危险物质泄漏，不影响现场以外区域，微损，可很快清除	1×10^{-1}

C.4 财产相关风险的可接受频率

SIL定级过程中所采用的财产相关风险的可接受频率，如表C.3所示。

表 C.3 财产相关风险的可接受频率

严重程度	财产相关风险	可接受频率（/y）
5 级	造成 5000 万元以上直接经济损失	1×10^{-6}
4 级	造成 1000 万元以上 5000 万元以下直接经济损失	1×10^{-5}
3 级	造成 100 万元以上 1000 万元以下直接经济损失	1×10^{-4}
2 级	造成 10 万元以上 100 万元以下直接经济损失	1×10^{-2}
1 级	造成 1000 元以上 10 万元以下直接经济损失	1×10^{-1}

C.4 非财务性影响与社会影响相关风险的可接受频率

SIL定级过程中所采用的非财务性影响与社会影响的可接受频率，如表C.4所示。

表 C.4 非财务性影响与社会影响相关风险的可接受频率

严重程度	财产相关风险	可接受频率（/y）
5 级	1.引起了国家相关部门采取强制性措施； 2.在全国范围内造成严重的社会影响； 3.引起国内国际媒体重点跟踪报道或系列报道。	1×10^{-6}
4 级	1.引起国内或国际媒体长期负面关注； 2.造成省级范围内的不利社会影响；对省级公共设施的日常运行造成严重干扰； 3.引起了省级政府相关部门采取强制性措施； 4.导致失去当地市场的生产、经营和销售许可证。	1×10^{-5}
3 级	1.引起地方政府相关监管部门采取强制性措施； 2.引起国内或国际媒体的短期负面报道。	1×10^{-4}
2 级	1.存在合规性问题，不会造成严重的安全后果或不会导致地方政府相关监管部门采取强制性措施； 2.当地媒体的长期报道； 3.在当地造成不利的社会影响,对当地公共设施的日常运行造	1×10^{-2}

	成严重干扰。	
1 级	1.当地媒体的短期报道； 2.对当地公共设施的日常运行造成干扰（如:导致某道路在24 小时内无法正常通行）	1×10^{-1}

附 录 D
（资料性）
典型初始事件频率

表 D.1 给出了典型初始事件频率示例。

表 D.1 典型初始事件频率示例

分类	初始事件	频率（/y）
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）过程容器沸腾液体扩展蒸汽云爆炸（BLEVE）	1×10^{-6}
	4）球罐沸腾液体扩展蒸汽云爆炸（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（≤150mm）管道大量泄漏	1×10^{-5}

表 D.1 典型初始事件频率示例（续）

分类	初始事件	频率（/y）
	6）大口径（>150mm）管道大量泄漏	1×10^{-6}
	7）管道小泄漏	1×10^{-3}
	8）管道破裂或大量泄漏	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	BPCS 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}
注：该表摘自 AQ/T3054-2015，表 E.2		

附 录 E
（资料性）
典型独立保护层要求时的失效概率

表 E.1 给出了典型独立保护层要求时的失效概率。

表 E.1 典型独立保护层要求时的失效概率

IPL		PFD（GB/T 32857）	PFD（推荐值）	具体要求 （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）
本质安全设计		1×10^{-1}～1×10^{-6}	1×10^{-2}～1×10^{-4}	从根本上消除或减少工艺系统存在的危害，考虑本质安全设计在运行和维护过程中的失效时，在某些事故场景中，可将其作为一种 IPL。
BPCS		1×10^{-1}～1×10^{-2}	1×10^{-1}	a）BPCS 作为独立保护层应与初始事件无关； b）BPCS 取值小于 10^{-1}时应满足 GB/T 21109.1 相关要求。
关键报警和人员响应		1.0～1×10^{-1}	1×10^{-1}	a）操作人员应能够得到采取行动的指示或报警； b）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； 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它任务； d）操作人员应有足够的响应时间； e）操作人员身体条件合适等。
安全仪表功能	安全仪表功能 SIL1	≥1×10^{-2}～＜1×10^{-1}	1×10^{-1}或 SIL 评估 PFD 值	满足 GB/T 21109 要求
	安全仪表功能 SIL2	≥1×10^{-3}～＜1×10^{-2}	1×10^{-2}或 SIL 评估 PFD 值	满足 GB/T 21109 要求
	安全仪表功能 SIL3	≥1×10^{-4}～＜1×10^{-3}	1×10^{-3}或 SIL 评估 PFD 值	满足 GB/T 21109 要求
物理保护	安全阀	1×10^{-1}～1×10^{-5}	1×10^{-1}～1×10^{-2}	应考虑其实际运行环境中可能出现的污染、堵塞、腐蚀等因素确定 PFD
	爆破片	1×10^{-1}～1×10^{-5}	1×10^{-1}～1×10^{-2}	

表 E.1 典型独立保护层要求时的失效概率（续）

IPL		PFD（GB/T 32857）	PFD（推荐值）	具体要求 （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）
释放后保护措施	防火堤	1×10^{-2}～1×10^{-3}	1×10^{-2}	降低由于储罐溢流、断裂、泄漏等造成严重后果的频率
	地下排污系统	1×10^{-2}～1×10^{-3}	1×10^{-2}	降低由于储罐溢流、断裂、泄漏等造成严重后果的频率
	开式通风口	1×10^{-2}～1×10^{-3}	1×10^{-2}	防止超压
	防爆墙/舱	1×10^{-2}～1×10^{-3}	1×10^{-2}	限制冲击波，保护设备/建筑物等，降低爆炸重大后果的频率
	阻火器或防爆器	1×10^{-1}～1×10^{-3}	1×10^{-2}	防止通过管道系统或进入容器或储罐内的潜在回火事故后果

附 录 F
（规范性）
安全完整性等级确定原则

表 F.1 给出了要求运行模式下安全完整性等级确定的原则。

表 F.1 要求运行模式下安全完整性等级：要求时的失效概率

SIL	要求时的平均失效概率	要求的风险降低
4	10^{-5}～<10^{-4}	>10000～100000
3	10^{-4}～<10^{-3}	>1000～10000
2	10^{-3}～<10^{-2}	>100～1000
1	10^{-2}～<10^{-1}	>10～100

表 F.2 给出了连续运行模式或要求运行模式下安全完整性等级确定的原则。

表 F.2 连续运行模式或要求运行模式下安全完整性等级：SIF 的危险失效平均频率

连续运行模式或要求运行模式	
SIL	危险失效平均频率（每小时失效）
4	10^{-9}～<10^{-8}
3	10^{-8}～<10^{-7}
2	10^{-7}～<10^{-6}
1	10^{-6}～<10^{-5}

附 录 G
（资料性）
典型仪表设备共因失效因子参考值

表 G.1 给出了传感单元和执行单元的共因失效因子 β 参考值。

表 G.1 典型仪表设备 β 参考值

所属单元	元件	β 值
传感单元	开关	0.05
	变送器	0.04
执行单元	切断阀	0.03
	电磁阀	0.1
	控制阀	0.03
	泄压阀	0.05
	继电器	0.03
注：以上 β 值应根据现场实际情况进行修正		