ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 45111—2024

保护层分析(LOPA)、安全完整性等级(SIL)定级和验证质量控制导则

Quality control guidelines for layer of protection analysis(LOPA), safety integrity levels(SIL)determination and verification

国家标准全文公开系统专用，此文本仅供个人学习、研究之用，
未经授权，禁止复制、发行、汇编、翻译或网络传播等，侵权必究。
全国标准信息公共服务平台：https://std.samr.gov.cn

2024-12-31 发布　　2025-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅴ
引言 …… Ⅵ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 6
5　质量控制节点 …… 6
5.1　总体原则 …… 6
5.2　质量控制节点划分 …… 7
5.2.1　LOPA 工作质量控制节点 …… 7
5.2.2　SIL 定级质量控制节点 …… 8
5.2.3　SIL 验证质量控制节点 …… 8
6　LOPA 工作的质量控制 …… 9
6.1　控制要素 …… 9
6.1.1　人员 …… 9
6.1.2　资料 …… 9
6.1.3　流程和内容 …… 9
6.1.4　文档 …… 9
6.2　控制要求 …… 9
6.2.1　人员控制要求 …… 9
6.2.2　资料控制要求 …… 10
6.2.3　流程和内容控制要求 …… 11
6.2.4　文档控制要求 …… 21
6.3　审查要求 …… 22
7　SIL 定级的质量控制 …… 22
7.1　控制要素 …… 22
7.1.1　人员 …… 22
7.1.2　资料 …… 23
7.1.3　流程和内容 …… 23
7.1.4　文档 …… 23
7.2　控制要求 …… 23
7.2.1　人员控制要求 …… 23
7.2.2　资料控制要求 …… 23

7.2.3 流程和内容控制要求 …… 23
7.2.4 文档控制要求 …… 24
7.3 审查要求 …… 25
8 SIL 验证的质量控制 …… 25
8.1 控制要素 …… 25
8.1.1 人员 …… 25
8.1.2 资料 …… 25
8.1.3 流程和内容 …… 25
8.1.4 文档 …… 25
8.2 控制要求 …… 26
8.2.1 人员控制要求 …… 26
8.2.2 资料控制要求 …… 26
8.2.3 流程和内容控制要求 …… 27
8.2.4 文档控制要求 …… 34
8.3 审查要求 …… 34
附录 A(资料性) LOPA 记录表与报告示例 …… 35
附录 B(资料性) LOPA 工作质量控制审查样表 …… 37
附录 C(资料性) SIL 定级分析记录表与报告示例 …… 46
附录 D(资料性) SIL 定级质量控制审查样表 …… 48
附录 E(资料性) SIL 验证工作表与报告示例 …… 50
附录 F(资料性) SIL 验证质量控制审查样表 …… 52
参考文献 …… 58

图 1 LOPA 工作、SIL 定级和 SIL 验证的关系 …… 7
图 2 LOPA 工作流程图 …… 12
图 3 保护层模型 …… 17
图 4 SIL 验证基本工作流程 …… 28
图 A.1 LOPA 工作报告示例 …… 36
图 C.1 SIL 定级报告示例 …… 47
图 E.1 SIL 验证报告示例 …… 51

表 1 初始事件分类 …… 15
表 2 初始事件典型频率值 …… 15
表 3 典型的保护层 …… 17
表 4 独立保护层的确定 …… 19
表 5 低要求运行模式下的 SIL 要求(GB/T21109.1—2022 中表 4) …… 23
表 6 连续运行模式或高要求运行模式下的 SIL 要求(GB/T21109.1—2022 中表 5) …… 24

表 7　不同 SIL 对应的最小 HFT 要求 …… 30
表 8　A 类安全相关组件或子系统执行安全功能时的最大允许 SIL …… 30
表 9　B 类安全相关组件或子系统执行安全功能时的最大允许 SIL …… 31
表 10　验证计算使用参数及其范围 …… 32
表 A.1　LOPA 记录表示例 …… 35
表 B.1　LOPA 工作质量控制审查样表 …… 37
表 C.1　SIL 定级分析记录表示例 …… 46
表 D.1　SIL 定级质量控制审查样表 …… 48
表 E.1　SIL 验证工作表示例 …… 50
表 F.1　SIL 验证质量控制审查样表 …… 52

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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国机械工业联合会提出。

本文件由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本文件起草单位：机械工业仪器仪表综合技术经济研究所、中国石油集团安全环保技术研究院有限公司、国能(连江)港电有限公司、上海燃气工程设计研究有限公司、中国电力工程顾问集团华北电力设计院有限公司、梅思安(中国)安全设备有限公司、中控技术股份有限公司、辽宁美卓伦检测技术有限公司、上海歌略软件科技有限公司。

本文件主要起草人：刘瑶、帅冰、徐德腾、史学玲、黄步余、董秀娟、朱明露、魏振强、唐彬、吕峰、陈小华、范咏峰、施隋靖、俞文光、朱旭营、李秋娟、李旺、王巨洪、孙勇、孙永康、严晓生、孙舒、周卫、张作本、谢亚莲、于世恒、马铁量、李玉明、马云鹏、钱福群、杨敏文、张雪、王晓鹏、曹欣宜、周力、聂中文、马欣欣、赵焱、孙文勇、史威、刁宇、姜志成、吕智嘉、熊文泽、雷柏伟、朱杰、赵俊丹、杜康、魏娟、相桂生、靳江红、姜念琛、孙炜、孟邹清、杨柳、朱弘毅、陈祖志、闫炳均、任军民、陈军松、张益南、刘东、李志勇、杨绍军。

引　言

随着GB/T 20438(所有部分)和GB/T 21109(所有部分)的广泛应用,功能安全概念得到有效普及。在石油、天然气、化工、电力等行业,功能安全研究的是如何确保包括安全仪表系统(SIS)在内的保护层实现足够的风险管控能力。SIS执行安全仪表功能(SIF)的可信性用安全完整性表示,其安全完整性能力用安全完整性等级(SIL)表征。

本文件中提到的危险与风险分析,其目的是全面识别系统中潜在的危险及操作性问题,一般为定性分析,在基本工艺流程设计完成后即可开展。常见的分析方法有:危险与可操作性分析(HAZOP)、故障树分析(FTA)、检查表、失效模式和影响分析(FMEA)。

在工程实践中,对于危险与风险分析中识别出的高风险点和重要控制点一般需开展进一步的半定量分析,以确认设置有足够的保护层,保护层分析(LOPA)即为常用的半定量风险分析方法,在LOPA工作过程中,将针对风险场景识别已设置或应设置的保护层分配降险能力,若涉及SIF,则需为SIF确定相应的SIL要求,此过程即为SIL定级。

SIL验证的目的是通过定量计算及必要时的定性分析,从硬件安全完整性和系统性安全完整性两方面确认SIF配置满足SIL定级提出的SIL要求,常见的SIL验证方法有:可靠性框图法、故障树法、马尔可夫法等。一般在完成SIS设计后开展SIL验证,以确保SIS配置满足安全要求。

在操作和维护阶段需要通过定期的功能安全评估(包括危险与风险分析、SIL定级、SIL验证等)确认SIS执行的SIF可维持相应的SIL能力。

通过本文件的制定,为各行业开展LOPA工作、SIL定级和验证工作提供审查依据,指导企业对LOPA工作、SIL定级和验证过程实现质量控制,提升运行风险管控水平。

保护层分析(LOPA)、安全完整性等级(SIL)定级和验证质量控制导则

1 范围

本文件明确了保护层分析(LOPA)与安全完整性等级(SIL)定级、SIL 验证间的关系,规定了 LOPA 工作、SIL 定级和 SIL 验证的质量控制要素、质量控制要求和质量控制审查要求。

注:本文件中 SIL 定级特指使用 LOPA 方法开展的 SIL 定级工作。

本文件适用于 LOPA、SIL 定级和验证的质量控制。

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(所有部分) 电气/电子/可编程电子安全相关系统的功能安全

GB/T 20438.1—2017 电气/电子/可编程电子安全相关系统的功能安全 第 1 部分:一般要求

GB/T 20438.2—2017 电气/电子/可编程电子安全相关系统的功能安全 第 2 部分:电气/电子/可编程电子安全相关系统的要求

GB/T 21109(所有部分) 过程工业领域安全仪表系统的功能安全

GB/T 21109.1—2022 过程工业领域安全仪表系统的功能安全 第 1 部分:框架、定义、系统、硬件和应用编程要求

GB/T 32857—2016 保护层分析(LOPA)应用指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

场景 scenario

可能导致不期望后果的一种事件或事件序列。

[来源:GB/T 32857—2016,3.1.9]

3.2

初始事件 initial event

使事故序列开始扩展所需的失效或错误的最小组合。

注:一般由一个单独的初始原因、多个原因或有使能条件的初始原因组成。有些情况下初始事件也可能是由同一时间发生的两种不同初始原因构成的。

3.3

中间事件 intermediate event

初始事件发展成后果之前的关键事件。

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

3.4

后果　consequence

事件潜在影响的度量。

注：一个事件可能有一个或多个后果。

3.5

保护层　protection layer

用来防止不期望事件的发生或降低不期望事件后果严重性从而降低过程风险的设备、设施或方案。

[来源：GB/T 32857—2016，3.1.3]

3.6

独立保护层　independent protection layer；IPL

一种设备、系统或行动，有效地防止场景向不期望的后果发展，它与场景的初始事件或其他保护层的行动无关。独立性表示保护层的执行能力不会受到初始事件或其他保护层失效的影响。

注：独立保护层的有效性和独立性可以被审查。

[来源：GB/T 32857—2016，3.1.7，有修改]

3.7

保护层分析　layer of protection analysis；LOPA

对降低不期望事件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过程方法或系统。

[来源：GB/T 32857—2016，3.1.1]

3.8

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

当受保护设备或受保护设备控制系统发出要求时，执行规定安全功能的独立保护层的安全不可用性。

[来源：GB/T 32857—2016，3.1.10]

3.9

风险评估　risk assessment

对不期望事件发生的可能性及其后果进行定性或定量分析，将分析结果与可容忍风险标准进行对比，并进行风险管理决策的过程。

3.10

安全仪表功能　safety instrumented function；SIF

由安全仪表系统(SIS)实现的安全功能。

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

[来源：GB/T 21109.1—2022，3.2.66]

3.11

使能事件或使能条件　enabling event or condition

不直接导致场景后果发生的事件或条件，但是对于场景的后果发生，这些事件或条件是必不可少的。

3.12

安全仪表系统　safety instrumented system；SIS

用来实现一个或多个 SIF 的仪表系统。

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

注 2：SIS 可以包括软件。

注 3：SIS 可以包括人为动作作为 SIF 的一部分。

[来源：GB/T 21109.1—2022，3.2.67]

3.13

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。

3.14

原始风险　initial risk

不考虑任何安全措施作用下的事故剧情的风险。

3.15

残余风险　residual risk

采取防护措施以后仍存在的风险。

[来源:GB/T 20438.4—2017,3.1.8]

3.16

可容忍风险　tolerable risk

根据当前社会发展水平,在给定的范围内能够接受的风险。

[来源:GB/T 20438.4—2017,3.1.7]

3.17

共因失效　common cause failure;CCF

在多通道系统中由一个或多个事件导致的引起两个或多个独立通道同时失效,从而导致系统失效的一种失效。

[来源:GB/T 32857—2016,3.1.14]

3.18

安全完整性　safety integrity

在规定的时间段内和规定的条件下,安全相关系统成功执行规定的安全功能的概率。

[来源:GB/T 20438.4—2017,3.5.4]

3.19

安全完整性等级　safety integrity level;SIL

一种离散的等级(四个可能等级之一),对应安全完整性量值的范围。

注:安全完整性等级 4 是最高的,安全完整性等级 1 是最低的。

[来源:GB/T 20438.4—2017,3.5.8,有修改]

3.20

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

SIF 的运行方式,低要求模式、高要求模式或连续模式。

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

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

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

[来源:GB/T 21109.1—2022,3.2.39]

3.21

条件修正因子　conditional modifiers

在场景风险计算时使用的可能性概率之一,通常在表现为影响后果(例如:人员伤亡、点火概率、致

死率)而不是主要损失事件后果(例如:泄漏、容器破裂)时使用。

3.22

系统性安全完整性　systematic safety integrity

安全相关系统安全完整性中,与危险失效模式下的系统性失效有关的部分。

注:系统性安全完整性通常不能量化(与通常可量化的硬件安全完整性明显不同)。

[来源:GB/T 20438.4—2017,3.5.6]

3.23

硬件安全完整性　hardware safety integrity

安全相关系统安全完整性中,与危险失效模式下的随机硬件失效有关的部分。

注:本术语涉及在危险模式下的失效,即,将削弱其安全完整性的安全相关系统的这类失效。与本术语有关的两个参数是危险失效平均频率和在要求时动作失效的概率。当为保持安全而必须保持连续控制时,使用前一可靠性参数;在安全相关保护系统场合中使用后一可靠性参数。

[来源:GB/T 20438.4—2017,3.5.7]

3.24

故障裕度　fault tolerance

在出现故障或错误的情况下,功能单元继续执行一个要求功能的能力。

[来源:GB/T 20438.4—2017,3.6.3]

3.25

随机硬件失效　random hardware failure

在硬件中,由一种或几种可能的退化机理而产生的,在随机时间出现的失效。

注 1:在各种元件中,存在以不同速率发生的许多退化机理,在这些元件工作不同的时间之后,这些机理可使制造公差引起元件发生故障,从而使包含许多元件的设备将以可预见的速率,但在不可预见的时间(即随机时间)发生失效。

注 2:随机硬件失效和系统性失效的主要区别是由随机硬件失效导致的系统失效率(或其他合适的度量)可以用合理的精度来量化,但系统性失效无法精确预计,因此系统性失效引起的系统失效率则不能精确地用统计法量化。也就是说,由随机硬件失效引起的系统失效率可以用合理的精度来量化,但是由系统性失效引起的系统失效率不能精确地用统计法量化,因为导致系统性失效的这些事件无法简单预测。

[来源:GB/T 20438.4—2017,3.6.5]

3.26

系统性失效　systematic failure

原因确定的失效,只有对设计或制造过程、操作规程、文档或其他相关因素进行修改后,才有可能消除这种失效。

注 1:仅修正性维护而不加修改,通常无法消除失效原因。

注 2:通过模拟失效原因可以引出系统失效。

注 3:系统性失效的原因可包括以下情况中的人为错误:

——安全要求规格书(SRS);

——硬件的设计、制造、安装、运行;

——软件的设计和实现等。

注 4:在本文件中,安全相关系统的失效被分为随机硬件失效和系统性失效。

[来源:GB/T 20438.4—2017,3.6.6]

3.27

安全失效分数　safe failure fraction;SFF

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。公式如下:

$$SFF=(\sum\lambda_{S\,avg}+\sum\lambda_{DD\,avg})/(\sum\lambda_{S\,avg}+\sum\lambda_{DD\,avg}+\sum\lambda_{DU\,avg})$$

如失效率是基于一个常数失效率，则公式简化为：

$$SFF=(\sum\lambda_{S}+\sum\lambda_{DD})/(\sum\lambda_{S}+\sum\lambda_{DD}+\sum\lambda_{DU})$$

[来源：GB/T 20438.4—2017，3.6.15]

3.28

平均恢复时间　mean time to restoration；MTTR

达到恢复的预期时间。

注：MTTR 包括：

——检测失效的时间(a)；和

——开始维修前已过去的时间(b)；和

——维修的有效时间(c)；和

——元件恢复运行前的时间(d)。

(b)的开始时间是(a)的结束时间，(c)的开始时间是(b)的结束时间，(d)的开始时间是(c)的结束时间。

[来源：GB/T 20438.4—2017，3.6.21]

3.29

诊断覆盖率　diagnostic coverage；DC

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。

注 1：危险失效诊断覆盖率是由下式计算的，式中 DC 表示诊断覆盖率，λ_{DD} 表示检测到的危险失效率，λ_{Dtotal} 表示总的危险失效率。

$$DC=\sum\lambda_{DD}/\sum\lambda_{Dtotal}$$

注 2：该定义仅在单个元件失效率为常数时适用。

[来源：GB/T 20438.4—2017，3.8.6]

3.30

复合场景　multi scenario

可能导致同一不期望后果的多个事件或事件序列，此多个事件为互相独立不相关事件。

3.31

风险点　risk point

伴随风险的设备、设施或位置以及在特定设备、设施或位置出现的危险场景的集合。

注：如反应釜压力高为典型的风险点名称。

3.32

安全关键动作　safety critical actions

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

3.33

误停车率　spurious trip rate；STR

未检测到的误停车失效率之和。一种用来衡量安全功能导致误停车的性能参数。

3.34

全可变语言　full variability language；FVL

计算机编程者易于理解，并能提供实现各种各样功能和应用的能力的一种语言。

注 1：使用 FVL 的系统的典型例子是通用型计算机。

注 2：在过程领域，嵌入式软件可能使用 FVL，而应用程序编程则很少使用 FVL。

注 3：FVL 的例子包括：Ada、C、Pascal、指令表、汇编程序语言、C++、Java 和数据库语言(SQL)。

3.35

有限可变语言　limited variability language；LVL

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。

注 1：这种语言用户容易理解，并能提供组合预定义的、应用专用的库函数的能力以实现 SRS。LVL 能提供一种与应用所要求的功能几乎一致的功能。

注 2：GB/T 21109(所有部分)认为实现安全属性必要的约束需综合以下情况：安全手册，应用编程人员定义过程控制算法所需要的功能与语言的契合度，逻辑解算器提供的嵌入到逻辑解算系统程序和逻辑解算器开发环境中的编译和运行时检查，在认证报告和安全手册定义的这些约束需确保满足 GB/T 20438.3—2017 中的相关要求。

注 3：GB/T 21109(所有部分)里提到应用程序时，LVL 是最普遍使用的语言。

4　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)

DC：诊断覆盖率(Diagnostic Coverage)

EUC：受控设备(Equipment Under Control)

FMEA：失效模式和影响分析(Failure Modes and Effects Analysis)

HAZOP：危险与可操作性分析(Hazard and Operability Study)

HFT：硬件故障裕度(Hardware Fault Tolerance)

I/O：输入/输出(Input/Output)

IPL：独立保护层(Independent Protection Layer)

LOPA：保护层分析(Layer of Protection Analysis)

MTTR：平均恢复时间(Mean Time To Restoration)

MRT：平均维修时间(Mean Repair Time)

P&ID：管道和仪表流程图(Piping and Instrumentation Diagram)

PFD：要求时危险失效概率(Probability of Dangerous Failure on Demand)

PFD_{avg}：要求时危险失效平均概率(Average Probability of Dangerous Failure on Demand)

PFH：每小时危险失效平均频率(Average frequency of a dangerous failure per hour)

PTC：检验测试覆盖率(Proof Test Coverage)

RRF：风险降低因子(Risk Reduction Factor)

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)

SRS：安全要求规格书(Safety Requirement Specification)

STR：误停车率(Spurious Trip Rate)

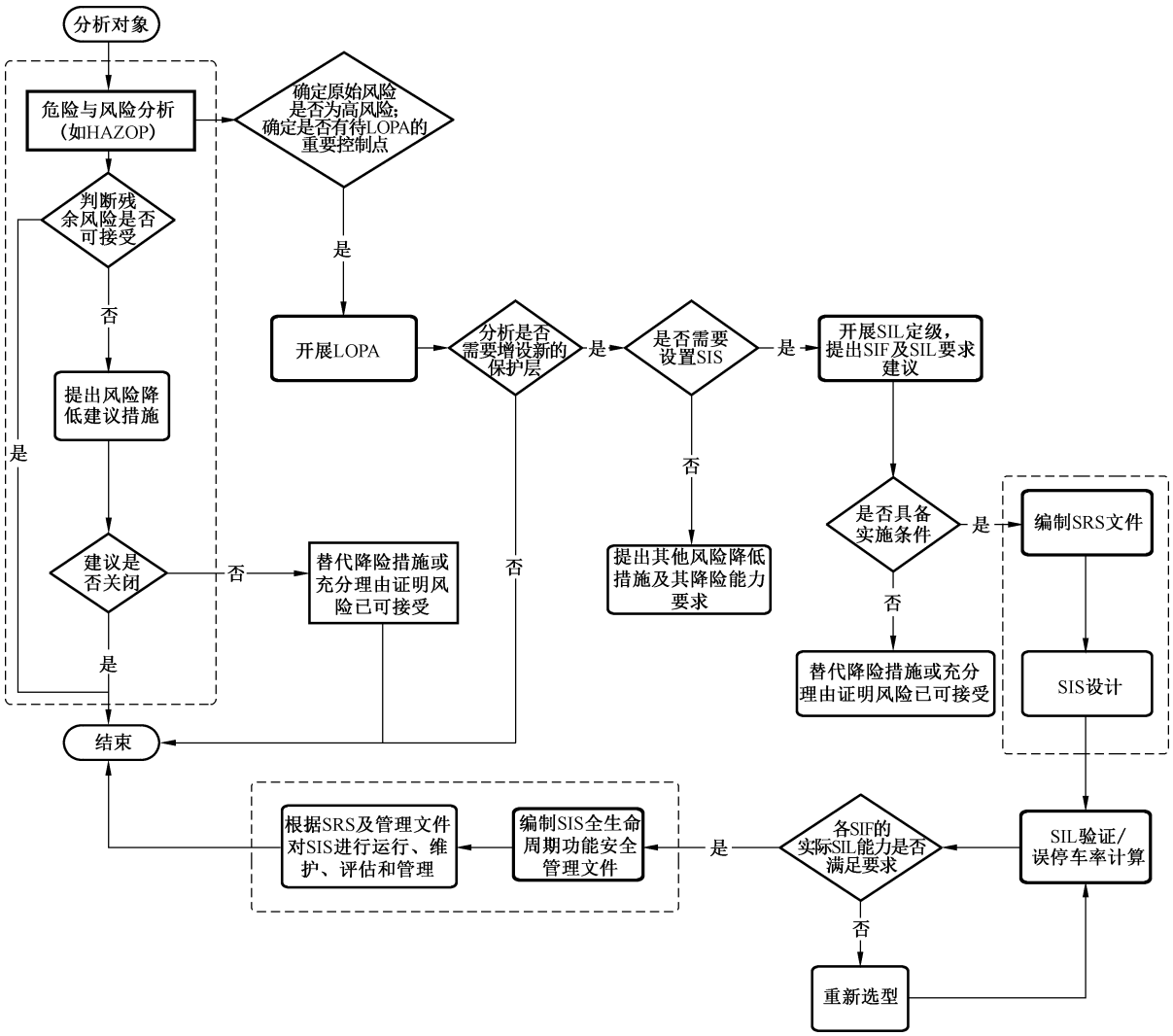
TI：检验测试间隔(Test Interval)

5　质量控制节点

5.1　总体原则

在生命周期各阶段开展的 LOPA 工作、SIL 定级和 SIL 验证如图 1 所示，即根据危险与风险分析

(如 HAZOP)报告识别出需关注的高风险点,同时依据工艺要求、设计说明及相关人员经验识别重要控制点。



注:图中虚框所含内容不在本文件范围之内。

图 1 LOPA 工作、SIL 定级和 SIL 验证的关系

5.2 质量控制节点划分

5.2.1 LOPA 工作质量控制节点

5.2.1.1 控制节点划分

LOPA 工作的质量控制贯穿于整个安全生命周期,在以下阶段执行 LOPA 工作应开展质量控制:

——阶段 1:初步设计(方案设计)阶段;

——阶段 2:详细设计(施工图)阶段,保护层设计之前;

——阶段 3:运行阶段;

——阶段 4:停用和退役阶段。

5.2.1.2 初步设计(方案设计)阶段

在已执行危险与风险分析(如 HAZOP)之后,制定 SRS 之前,应针对原始风险为高风险的场景,通过 LOPA 工作确定保护层设置和各 SIF 的安全要求。

5.2.1.3 详细设计(施工图)阶段

在完成详细设计(施工图)后应开展复审,确认已按照 LOPA 结果设计各保护层,其中对于 SIF 应制定 SRS,并按照 SRS 设计完成 SIS,确认风险已在可接受范围内。

5.2.1.4 运行阶段

5.2.1.4.1 在取得运行经验后,在已执行周期性危险与风险分析(如 HAZOP)之后,应开展 LOPA 工作复审。

5.2.1.4.2 当 LOPA 输入信息发生变更后,应重新开展 LOPA 工作。

注:LOPA 输入信息发生变更的情况包括但不限于:设计变更、现场改造、装置操作和维护模式发生变化、装置所处周边环境发生可能影响危险事件后果的变化。

5.2.1.5 停用和退役阶段

当设备设施停用和退役可能对在役系统带来风险,应对在役系统进行 LOPA 工作。

5.2.2 SIL 定级质量控制节点

SIL 定级质量控制节点划分参照 5.2.1 执行。

5.2.3 SIL 验证质量控制节点

5.2.3.1 控制节点划分

在以下阶段应执行 SIL 验证的质量控制:

——阶段 1:设计阶段完成 SIF 设备选型后;

——阶段 2:运行阶段 SIF 设备变更设计选型后;

——阶段 3:运行阶段 SIF 相关维检修策略发生变化后;

——阶段 4:运行阶段获得现场失效数据后。

5.2.3.2 设计阶段完成 SIF 设备选型后

5.2.3.2.1 在工艺装置设计阶段完成设备选型后应开展 SIL 验证,并根据 SIL 验证结果调整选型,确保 SIF 配置满足 SRS 的要求。

注:此阶段 SRS 已发布,SIF 所使用的设备已完成选型,开展 SIL 验证便于 SIL 验证建议的有效落实。

5.2.3.2.2 施工安装时应确认 SIF 的结构配置与 SRS 保持一致,投运后的维检修策略应按照 SIL 验证采纳的相关参数方案开展,满足相关假设,否则本阶段的 SIL 验证结果将不适用。

5.2.3.3 运行阶段 SIF 设备变更设计选型后

SIF 设备一旦发生变更,例如:配置/表决变化、设备更换型号,在选型后应开展 SIL 验证,确认选型的设备满足 SRS。

5.2.3.4 运行阶段 SIF 相关维检修策略发生变化后

一旦维检修策略发生变化,如检修时间间隔变化、检修方案或 MTTR 变化,SIF 将与 SRS 不一

致，前阶段的 SIL 验证结果不再适用，应根据新的维检修策略重新开展 SIL 验证。

5.2.3.5 运行阶段获得现场失效数据后

运行阶段针对 SIF 设备应建立失效数据收集体系，定期对选型配置时 SIL 验证计算使用的失效率进行校正，并重新开展 SIL 验证。

6 LOPA 工作的质量控制

6.1 控制要素

6.1.1 人员

LOPA 工作应采取讨论会的形式，对识别出的风险点和场景展开讨论，确定保护层有效性。控制要素包括：LOPA 工作小组人员构成、对分析主席的要求、对分析成员的要求，按照 6.2.1 进行质量控制。

6.1.2 资料

LOPA 工作应基于输入资料，包括 P&ID、工艺说明、设计说明、操作手册、法规、标准等，按照 6.2.2 进行质量控制。

6.1.3 流程和内容

LOPA 工作流程和内容按照 6.2.3 进行质量控制。

6.1.4 文档

LOPA 文档包括分析报告、分析记录表等，按照 6.2.4 进行质量控制。

6.2 控制要求

6.2.1 人员控制要求

6.2.1.1 人员构成

LOPA 小组宜由分析主席、分析秘书和分析成员组成。分析主席和秘书应来自分析单位，分析成员宜来自运行单位、分析单位、设计方，必要时还包括承包商。小组成员宜为 6 人～9 人，其中运行单位和设计方宜 4 人～6 人，分析单位宜 2 人～3 人。

注 1：LOPA 分析主席的主要职责包括：

——确认输入资料是否齐全、准确；

——确定工作范围、识别风险点、确定可容忍风险标准，并与小组成员达成一致；

——编制 LOPA 工作计划，组织主持 LOPA 会议，激发小组成员展开讨论，控制讨论内容和进程，保证会议顺利召开；

——总结讨论中心议题，概括分析结果，确保分析结果达成一致，检查记录表确保讨论内容得到准确记录，并确定已落实审查意见的责任方；

——审核并提交 LOPA 报告。

注 2：LOPA 分析成员的主要职责是在 LOPA 分析主席的引导下积极开展分析和讨论，利用自己的知识和经验响应每个步骤的分析内容和要求。

LOPA 分析成员应满足以下要求：

——设计方根据分析需求派出工艺、仪表专业人员，必要时还需派出电气、消防、总图等专业人

员，专业经验不少于3年；

——承包商应派出与项目有关的专业人员；

——运行单位根据分析需求派出工艺、仪表、设备、安全、运行/操作专业人员，必要时还需派出电气、通信、管理等专业人员，专业经验不少于3年。

6.2.1.2 独立等级

LOPA分析主席应是独立的，独立等级应按照GB/T 20438.1—2017中8.2执行。项目设计的人员或项目组其他相关人员配合评估组参与评估活动。

注：分析对象的危险事件后果可能致人员伤亡的需由独立部门执行，后果可能致多人伤亡的需由独立第三方执行。

6.2.1.3 人员能力

6.2.1.3.1 LOPA分析主席能力

LOPA分析主席能力应满足下列要求：

——LOPA分析主席具有LOPA工作主持经验，掌握LOPA工作方法，熟悉工艺流程，了解操作规程，对GB/T 20438(所有部分)、GB/T 21109(所有部分)、GB/T 32857—2016有较为深入的研究，接受过行业权威机构LOPA工作/SIL定级培训，取得培训合格证书；

——LOPA分析主席具有行业认可的功能安全资质，且具有不少于10项LOPA工作项目经验。

注：行业认可的功能安全资质，如国际/国内权威机构。

6.2.1.3.2 LOPA分析成员能力

LOPA分析成员能力应满足下列要求：

——LOPA分析成员了解GB/T 20438(所有部分)、GB/T 21109(所有部分)、GB/T 32857—2016，并经过培训；

——LOPA分析成员具备所分析对象相同或相似领域的经验及相关法律法规知识，以确保评估结果合理可信；

——LOPA分析单位参与项目的高级资质人员不少于2名。

注：高级资质人员指具备功能安全技术能力的高级职称人员；或取得行业权威机构功能安全资质证书的人员，且其所在分析单位具备相关资质的专职分析人员不少于5位，并具有质量体系认证。

6.2.2 资料控制要求

LOPA工作输入资料宜包括：

——危险与风险分析报告(如HAZOP报告)；

——工艺流程图(PFD)、P&ID；

——设计/工艺说明；

——安全联锁功能列表或功能说明；

——安全联锁逻辑因果图；

——管道及材料数据表(承压等级等相关参数)；

——设备数据表(压缩机、冷凝器、蒸发器、贮液器、低压循环桶、安全阀等，包括设计参数)。

注：LOPA工作可能需要的其他输入资料还包括：

——设备标高数据；

——主要容器、塔及反应器的设备结构图；

——设备布置图；

——操作规程；

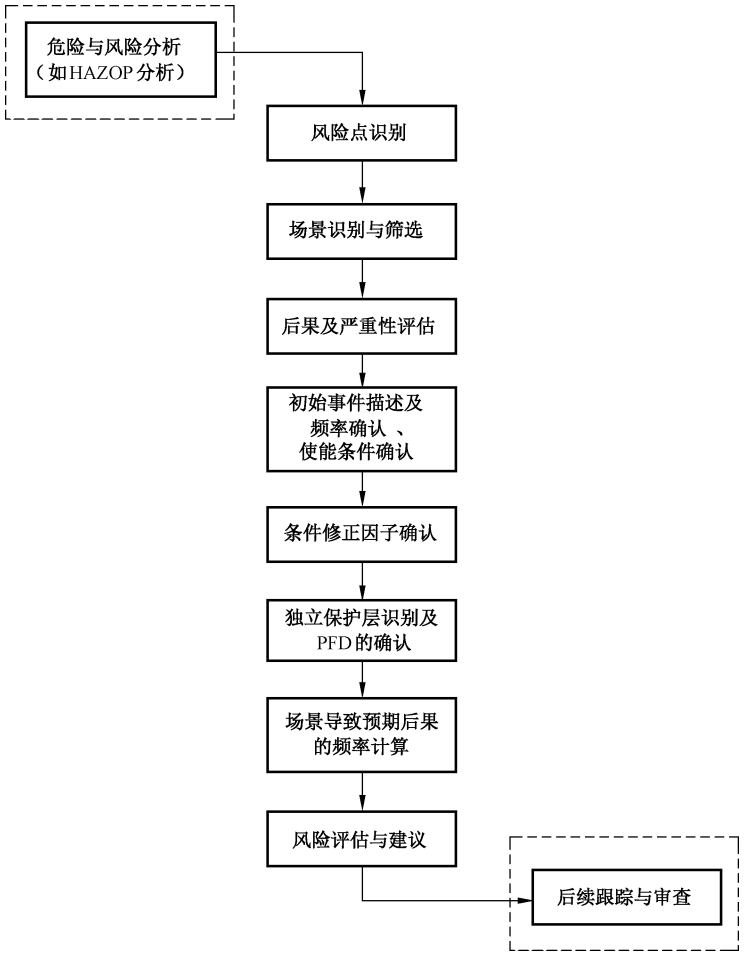
——维检修规程；
——排空放净系统设计原则；
——爆炸危险区域划分图；
——装置区所处区域的气象水文材料；
——设备价值台账；
——周边居民区(人口密度)/水源地分布；
——以前的事故清单、设备故障记录(提供审阅后收回)；
——边界条件表；
——设备、仪器仪表台帐(厂家、型号、投用时间、测量范围，若经过认证，则需提供认证证书和功能安全评估报告)；
——装置变更记录；
——界区外原料储罐设计和操作压力、温度，安全阀定压值和储罐的尺寸，以及输送原料设备的设计数据，如果是离心泵提供泵的特性曲线，如果是压缩机提供压缩机出口安全阀定压值，产品出装置后储罐的设计和操作压力、温度以及安全阀定压值；
——项目前的危险分析或安全评阅结果(如果有)。

6.2.3 流程和内容控制要求

6.2.3.1 LOPA 工作流程

LOPA 工作流程见图 2，主要包括：

a) 风险点识别；
b) 场景识别与筛选；
c) 后果及严重性评估；
d) 初始事件描述及频率确认、使能条件确认；
e) 条件修正因子确认；
f) 独立保护层识别及 PFD 的确认；
g) 场景导致预期后果的频率计算；
h) 风险评估与建议。



注：图中虚框所含内容不在本文件范围之内。

图 2　LOPA 工作流程图

6.2.3.2　分析范围和工作目的

分析范围的描述应保证：

——分析对象的边界已被明确定义；

——分析团队任务明确，分析内容界定在与目标有关的范畴。

分析范围可由以下因素决定：

——危险与风险分析报告（如 HAZOP 报告）；

——当前分析对象已设置的安全联锁功能；

——可获得的设计说明书及图纸的详细程度；

——其他适用于当前分析对象的标准、法规要求。

6.2.3.3　可容忍风险标准确定

分析使用的可容忍风险标准应不低于国家相关法规文件或标准。企业应制定适用的可容忍风险标准。对于个人风险的可容忍标准可参照 GB 36894 制定。

注：可容忍风险一般是指能够被监管部门所接受，且与本地区、本行业社会经济发展水平相适应，并被企业所接受的风险。可容忍风险根据后果种类分别定义，典型的后果种类包括：人员伤亡、财产损失、环境污染、声誉影响等。

6.2.3.4 风险点识别

对于复杂工艺装置开展 LOPA，宜在场景识别前增加风险点及重要控制点识别，即根据危险与风险分析（如 HAZOP）报告识别出需关注的高风险点，同时依据 P&ID、工艺说明及设计人员经验识别重要控制点。

6.2.3.5 后果及严重性评估

6.2.3.5.1 后果的分析应符合以下要求：

a） 后果分析覆盖可容忍风险标准中的所有后果分类；

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

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

c） 后果分析为假设任何已有的安全措施都失效时导致的最终不利的可信后果。

注 2：可信后果指基于现场实际情况和科学的推导方法确定的最终不利后果。

6.2.3.5.2 后果的记录要求如下：

a） 后果的记录应包括对所有后果分类（如人员伤亡、经济损失、环境影响等）影响的详细描述；

b） 不宜将中间事件当后果，记录最终后果。

6.2.3.5.3 后果严重度评估可采用以下安全分析作为依据：

a） 安评报告；

b） 以往事故借鉴；

c） 同类事故借鉴；

d） 定量风险评价（QRA）、后果模拟等定量方法分析；

e） 工艺实际情况（如：是否属于“两重点一重大”范围）；

f） 地区水文环境等。

6.2.3.5.4 对于精细化工反应热相关的 LOPA 工作，后果严重度评估时，应结合精细化工反应热风险评估结论和现场工况给出评估说明。

6.2.3.6 当前风险点后果发生的可接受频率确定

应基于企业的可容忍风险标准，根据各后果分类的严重性描述确定当前风险点各后果分类的可接受频率。

6.2.3.7 场景识别和筛选

6.2.3.7.1 场景识别应满足以下基本要求。

a） 每个场景至少包括：

- 导致场景发生的初始事件；
- 该事件继续发展过程中的中间事件；
- 该场景所导致的最终后果。

b） 每个场景有唯一的初始事件及其对应后果。

c） 除了初始事件和后果外，一个场景还可能包括：

- 使能事件或使能条件；
- 防护措施失效。

d） 如果使用人员死亡、商业或环境损害作为后果，则场景还可能包括下列部分或全部因素，或条件修正因子：

- 可燃物质被引燃的可能性；

- 人员出现在事件影响区域的概率；
- 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)；
- 其他可能的修正因子。

6.2.3.7.2 场景识别信息主要来源于工艺装置危险与风险分析(如 HAZOP)所识别的原因与后果组成的场景。场景识别信息还可能来源于：

a) 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；
b) 变更；
c) 事故事件；
d) SIF 审查。

6.2.3.7.3 场景筛选方法至少包括以下步骤：

a) 确认待分析风险点；
b) 从危险与风险分析(如 HAZOP)记录中识别当前分析风险点对应的偏差、偏差原因、偏差后果，组成待分析场景；
c) 在 LOPA 工作会议中确认所有已筛选的场景是否适用，并补充未覆盖的场景；
d) 在 SIL 定级时宜使用复合场景计算法开展 LOPA，在场景筛选过程中应确保场景识别完全，且不同场景为独立不相关事件。

6.2.3.8 初始事件及其防护措施确认

6.2.3.8.1 在确定初始事件时，应按照以下要求。

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) 确认已辨识出所有的潜在初始事件，并确保无遗漏。
c) 将每个原因细分为独立的初始事件，以便于识别保护层。
d) 在识别潜在初始事件时，确保已经识别和审查所有的操作模式(如正常运行、启动、停机、低负荷运行等)和设备状态(如待机、维护)下的初始事件。
e) 当人因失效作为初始事件时，制定人员失误频率评估的统一规则并在分析时严格执行。
f) 初始事件主要包括但不限于以下几个方面：
   - 设备设施、仪表等故障；
   - 操作失误；
   - 外部影响；
   - 公用工程失效；
   - 运行条件变更。
g) 以下事件不宜作为初始事件：
   - 操作人员培训不完善；
   - 测试或检查不完善；
   - 保护装置不可用；
   - 其他类似事件。

6.2.3.8.2 初始事件可参考表 1 的类型进行分类。初始事件典型频率值见表 2。

表 1　初始事件分类

类别	外部事件	设备故障	人因失效
分类	a）　地震、海啸、龙卷风、飓风、洪水、泥石流和滑坡等自然灾害； b）　空难； c）　临近工厂的重大事故； d）　破坏或恐怖活动； e）　雷击和外部火灾； f）　其他外部事件	a）　控制系统失效： 1）　硬件失效， 2）　软件失效； b）　仪表设备故障； c）　通讯设备故障； d）　电气设备故障； e）　机械设备故障； f）　辅助系统故障； g）　其他故障	a）　对给出的条件或其他提示未能正确观察或响应； b）　未能按操作规程进行操作； c）　未能按维护规程进行操作； d）　未按管理规定作业； e）　其他行为失误

表 2　初始事件典型频率值

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-100 m-全部断裂	10^{-5}～10^{-6}
管线泄漏(10%截面积)-100 m	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}
锁定、标定(LOTO)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}

6.2.3.8.3　按照 6.2.3.8.1 的要求,根据危险与风险分析(如 HAZOP)报告及现场人员经验确定各风险点的场景以及对应的初始事件,应结合行业经验及现场实际确定初始事件发生频率,频率确定方式包括:

a）　对于现场或企业内发生过的初始事件,应结合实际情况确定发生频率;

b）　对于建立有事件发生频率数据库的企业,可结合数据库数据和现场实际确定发生频率;

c) 已被行业认可的第三方数据库。

注：在分析记录表或报告中需标明初始事件发生频率的确定依据。

6.2.3.8.4 应根据危险与风险分析(如 HAZOP)报告识别出的已有保护措施及现场实际情况确认每项初始事件对应的防护措施，各防护措施应与初始事件相互独立。

注：如某仪表失效，其承担的报警功能不能作为有风险降低能力的防护措施。

6.2.3.9 使能条件确认

使能条件包括以下情况：

——事件序列只有当装置处在某个特定操作场景下时才会发生，以独立于其他事故序列为前提对此事故剧情进行分析是必要且有意义的；

——这种后果只有当装置在使用某种特殊原料、催化剂或加工某个特定的配方时才会发生，以独立于其他事故序列为前提对此事故剧情进行分析是必要且有意义的；

——事件序列能够发生的前提是，初始事件在某个特定的工况(例如环境温度较低或较高)下发生。

注：使能条件会影响 LOPA 工作的结果，如无足够的文件支撑，不建议使用使能条件。

6.2.3.10 条件修正因子确定

6.2.3.10.1 计算后果频率时，在评估人员具有相关经验及数据支持下可使用条件修正。条件修正因子一般包括：

a) 可燃物质点火概率；

b) 人员出现在事件影响区域的概率；

c) 人员致死率(如人员暴露在火灾、爆炸或有毒物质释放影响区内的致死率)；

d) 其他可能的条件修正因子。

6.2.3.10.2 分析对象存在可燃介质时，点火概率取值宜考虑：

a) 介质的组成成分及其燃烧性；

b) 介质泄漏后的最终状态，如液态、气态；

c) 介质泄漏所处环境温度与自燃点的关系；

d) 泄漏形式，是连续还是瞬时释放；

e) 介质所处装置：固定/移动、生产/储存/装卸；

f) 装置区周边点火源情况；

g) 泄漏速率；

h) 现场的安全条件，包括防爆、接地、液体防流散措施、防火安全措施等；

i) 事故历史经验。

6.2.3.10.3 人员出现在事件影响区域的概率取值宜考虑：

a) 人员岗位(包括现场操作、巡检、维检修等)；

b) 人员数量；

c) 在后果影响区内的停留时间。

6.2.3.10.4 人员致死率取值宜考虑：

a) 装置发生事故时的伤亡半径；

b) 燃烧事故的热辐射强度；

c) 爆炸事故的冲击波强度。

6.2.3.11 保护层识别

6.2.3.11.1 保护层由一组设备和/或管理措施组成，具有控制或减轻风险的能力。图 3 为过程工业典

型的保护层模型，揭示了工艺装置运行过程中发生危险事件情况下不同措施实现的保护层的一般启动顺序，它不表示实际的保护层及其独立性分布。

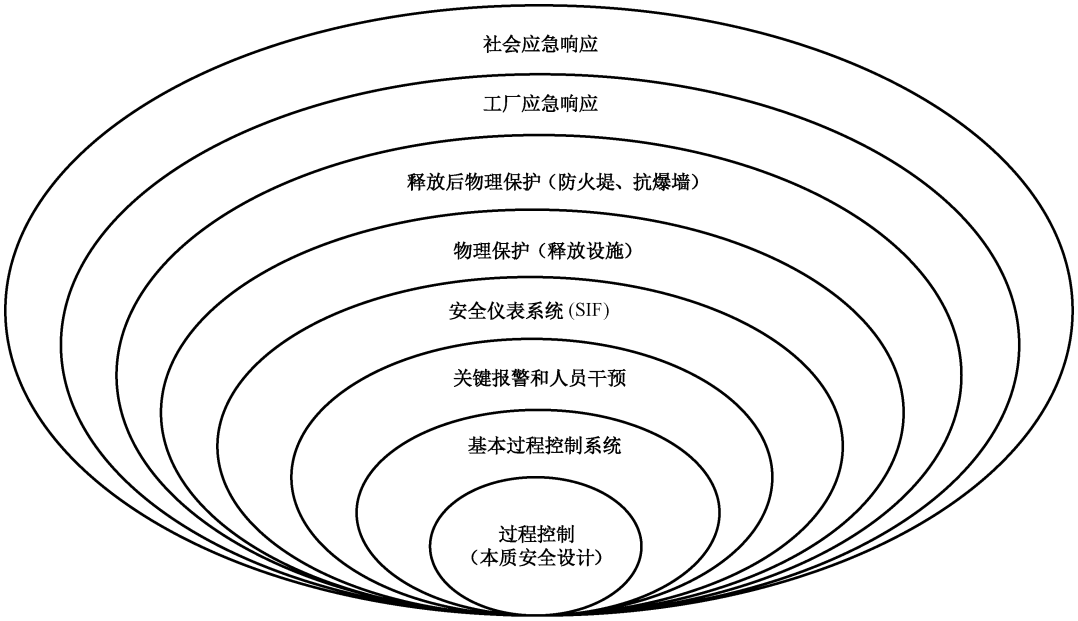


图 3　保护层模型

6.2.3.11.2　在识别保护层时，应对以下内容进行确认。

a）　有效性：按照设计的功能发挥作用，有效地防止后果发生：

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。

b）　独立性：独立于初始事件和任何其他已经被认为是同一场景的保护层。

1）　独立于初始事件的发生及其后果；

2）　独立于同一场景中的其他保护层；

3）　考虑共因失效或共模失效的影响。

c）　可审查性：对于阻止后果的有效性和 PFD 以某种方式（通过记录、审查、测试等）进行验证。通过审查程序确认如果保护层按照设计发生作用，它将有效地阻止后果。

1）　审查确认保护层的设计、安装、功能测试和维护系统的合适性，以取得保护层特定的 PFD；

2）　通过功能测试确认保护层所有的构成元件（传感器、逻辑解算器、最终元件等）运行良好，满足 LOPA 的使用要求；

3）　审查过程中记录了发现的保护层条件、上次审查以来的任何修改以及跟踪所要求的任何改进措施的执行情况。

典型的保护层的描述及相关说明见表 3。

表 3　典型的保护层

保护层	描述	说明
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

表 3　典型的保护层（续）

保护层	描述	说明
BPCS	基本过程控制系统 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
关键报警和人员响应	关键报警和人员响应是操作人员或其他工作人员对报警响应，或在系统常规检查后，采取的防止不良后果的行动	通常认为人员响应的可靠性较低，宜慎重考虑人员行动作为独立保护层的有效性。关键报警应有充分的人员响应时间
SIS	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 SIF 由传感器、逻辑解算器和最终元件组成，具有一定的 SIL	SIF 在功能上独立于 BPCS
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
释放后物理保护（防火堤、抗爆墙）	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	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
工厂和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

保护层满足表 4 条件才能作为独立保护层。

表 4　独立保护层的确定

保护层	描述	作为独立保护层的要求
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、逻辑解算器和最终元件组成	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、逻辑解算器和最终元件； 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，具体评估方法按 GB/T 32857—2016 中的 A.5
SIS	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 SIF 由传感器、逻辑解算器和最终元件组成，具有一定的 SIL	SIF 在功能上独立于 BPCS，是一种独立保护层 SIF 的规格、设计、调试、检验、维护和测试都应按 GB/T 21109(所有部分)的有关规定执行。 SIF 的风险削减性能由其 PFD 所确定，每个 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	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。 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、防爆墙)	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

6.2.3.11.3　以下防护措施不宜作为保护层。

a)　培训和取证：在确定操作人员行动的 PFD 时需要考虑的因素，但不单独作为保护层考虑。

b)　规程：在确定操作人员行动的 PFD 时需要考虑的因素，但不单独作为保护层考虑。

c)　检测：正常的检测将影响某些保护层的 PFD，延长检测周期可能增加保护层的 PFD。

d)　维护：维护活动将影响某些保护层的 PFD。

e)　通信：作为一种基础假设，假设工厂内具有良好的通信。差的通信将影响某些保护层的 PFD。

f) 标识：标识自身不是保护层。标识可能不清晰、模糊、容易被忽略等。标识可能影响某些保护层的 PFD。

6.2.3.12 场景频率计算

6.2.3.12.1 单一场景计算

单一场景后果的频率为初始事件发生频率乘以所有保护层要求时危险失效概率，场景后果的频率可能需要使用下面两种系数进行修正。

a) 假如场景的发生需要使能事件或使能条件，需要乘以使能事件或使能条件的发生概率。

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

- 可燃物质点火概率；
- 人员出现在事件影响区域的概率；
- 火灾、爆炸或有毒物质释放的暴露致死率；
- 其他。

计算见公式(1)：

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

式中：

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

f_n^{I} ——初始事件 n 的发生频率，单位为次每年(次/年)；

P_n^{E} ——使能事件或使能条件发生的概率，假如没有使能事件或使能条件，则取 1；

P_n^{C} ——条件修正因子，假如没有任何条件修正，则取 1；

注：存在多个适用的条件修正因子时，P_n^{C} 为各条件修正因子的乘积。

PFD_{nj} ——初始事件 n 中第 j 个阻止后果 C 的独立保护层要求时危险失效概率(PFD)；

J ——本场景中使用到的独立保护层数量。

6.2.3.12.2 多个/复合场景计算

低要求模式下复合场景分析法后果频率可通过公式(2)计算：

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

式中：

f^{C} ——当前分析风险点产生后果 C 的频率，单位为次每年(次/年)；

N ——当前分析风险点所含场景的个数；

f_n^{I} ——场景 n 的初始事件发生频率，单位为次每年(次/年)；

P_n^{E} ——场景 n 的使能事件或使能条件发生的概率，假如没有使能事件或使能条件，则取 1；

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

注：存在多个适用的条件修正因子时 P_n^{C} 为各条件修正因子的乘积。

PFD_{nj} ——引发场景 n 的初始事件中第 j 个独立保护层要求时危险失效概率(PFD)；

J ——本场景中使用到的独立保护层数量。

也可对各场景均用到的独立保护层和条件修正因子合并同类项，计算见公式(3)：

$$f^{\mathrm{C}} = \left[\sum_{n=1}^{N} \left(f_n^{\mathrm{I}} \times P_n^{\mathrm{E}} \times \prod_{j=1}^{J} \mathrm{PFD}_{nj} \right) \right] \times P_n^{\mathrm{C}} \times \prod_{k=1}^{K} \mathrm{PFD}_k \quad \cdots\cdots(3)$$

式中：

f^{C} ——当前分析风险点产生后果 C 的频率，单位为次每年(次/年)；

f_n^{I} ——场景 n 的初始事件发生频率，单位为次每年(次/年)；

P_n^{E} ——场景 n 的使能事件或使能条件发生的概率，假如没有使能事件或使能条件，则取 1；

P_n^{C} ——条件修正因子，假如没有任何条件修正，则取 1；

注：存在多个适用的条件修正因子时，P_n^{C}为各条件修正因子的乘积。

PFD_{nj}——引发场景 n 的初始事件中第 j 个独立保护层要求时危险失效概率(PFD)；

J ——场景 n 中使用到的与其他场景不同的独立保护层数量；

PFD_k ——该风险点各场景均用到的第 k 个独立保护层(IPL)或非 IPL 要求时危险失效概率(PFD)；

K ——各场景均用到的独立保护层数量。

6.2.3.13 风险决策

6.2.3.13.1 通过后果严重性评估确定后果等级，得出对应的可容忍风险频率；通过场景频率计算，得出后果发生频率。

a) 对于单一场景分析法，选择同一风险点不同场景中“采用其他风险降低措施后的后果频率”的最高值与可容忍风险频率比较，若“采用其他风险降低措施后的后果频率”大于可容忍风险频率，则需要增加风险降低措施(如 SIF、安全阀等)，并计算 RRF。其计算见公式(4)：

$$\mathrm{RRF}=\frac{f_n^{\mathrm{C}}}{f_{\mathrm{t}}} \qquad \cdots\cdots(4)$$

式中：

f_{t} ——可容忍风险频率；

f_n^{C} ——后果发生频率。

b) 对于复合场景分析法，直接使用计算得出的“采用其他风险降低措施后的后果频率”与可容忍风险频率比较，若“采用其他风险降低措施后的后果频率”大于可容忍风险频率，则需要增加风险降低措施(如 SIF、安全阀等)，并计算 RRF。其计算见公式(5)：

$$\mathrm{RRF}=\frac{f^{\mathrm{C}}}{f_{\mathrm{t}}} \qquad \cdots\cdots(5)$$

式中：

f_{t} ——可容忍风险频率；

f^{C} ——后果发生频率。

6.2.3.13.2 若建议增加的风险降低措施为 SIF，则按照第 7 章的要求开展 SIL 定级工作。

6.2.4 文档控制要求

6.2.4.1 LOPA 记录表

LOPA 记录表宜包括以下内容。

a) 后果描述：包括风险矩阵中的后果分类，以便确定可容忍风险频率。

b) 可容忍风险标准：记录表中选取的可容忍风险标准应和后果分类一致，可容忍风险标准的频率值应符合公司可容忍风险标准值。

c) 初始事件：记录表中清晰记录场景初始事件，同时给出初始事件频率。

d) 防护措施：记录表中记录针对初始事件的防护措施描述及其失效概率。

e) 使能事件或使能条件：对初始事件的使能事件或使能条件进行描述，并给出使能事件发生的概率。

f) 条件修正：描述条件修正因子取值说明。

注：一般需标明这些假定值的参考依据，且对标准值的任何修改需说明理由并记录在案。

g) 中间事件频率：初始事件频率和所有使能事件或使能条件发生概率以及条件修正因子的乘积。

h) 独立保护层：写出所有现有的及建议的独立保护层，包括每个独立保护层失效概率。如果独立保护层的失效概率不同于企业内采用的标准值，则需阐明调整理由。

i) 后果频率：考虑已有防护措施和 IPL 后的后果频率。

j) 是否满足可容忍风险标准：使用考虑已有防护措施和 IPL 后的后果频率与采用的可容忍风险标准进行比较，假如后果频率小于对应后果分类的可容忍风险标准，则当前风险在可容忍范围内，否则为不满足。

k) 仍需完成的降险能力 PFD：假如存在后果频率大于可容忍风险标准的情况，需计算各后果分类仍需完成的降险能力 PFD。

l) 满足可容忍风险标准所要求采取的行动：

- 描述未将风险降低至可容忍标准内还需采取的行动内容；
- 假如后果频率大于可容忍风险标准，但企业目前无法采取其他行动，因此不得不接受这样的风险，这种特殊情况可能需要高级管理人员的签字，并附在分析文档中。

m) 备注：包括所有背景资料，或记录与场景或采取行动相关的此类信息。

n) 参考资料：任何有关的工艺流程图、P&ID、SIF 描述或联锁逻辑图、仪表清单、设备清单、操作规程、测试程序等参考资料，从而完整地记录分析的依据，以协助审查或执行分析的结果。

6.2.4.2 LOPA 报告

在 LOPA 工作会议后，LOPA 分析主席和秘书应将会议记录进行整理、汇总，形成 LOPA 报告文件，报告模版见附录 A。报告宜包括以下内容：

——项目基本概况；

——LOPA 工作方法及流程：包括分析目的、LOPA 工作程序、详细步骤等；

——LOPA 工作实施：包括日程安排、参与人员、参考资料等；

——工作成果汇总：包括分析结果和所提建议；

——LOPA 记录表；

——分析依据的可容忍风险标准；

——LOPA 工作参与人员签到表。

6.3 审查要求

应对 LOPA 工作的人员、资料、流程和文档 4 个方面进行审查，质量控制审查样表见附录 B。

——否决项：LOPA 工作报告质量控制的关键要素，若未满足相关审查要求，则本次审查不予通过。

——非否决项：LOPA 工作报告质量控制的一般要素，若发现不符合项，后续需进行整改或优化。审查人员可根据实际情况综合研判，得出审查结论。

注：对于非否决项，若不符合项超过 5 项，推荐为审查不通过。

7 SIL 定级的质量控制

7.1 控制要素

7.1.1 人员

SIL 定级人员按照 7.2.1 进行质量控制。

7.1.2 资料

SIL 定级资料按照 7.2.2 进行质量控制。

7.1.3 流程和内容

SIL 定级工作流程和内容按照 7.2.3 进行质量控制。

7.1.4 文档

SIL 定级文档按照 7.2.4 进行质量控制。

7.2 控制要求

7.2.1 人员控制要求

人员控制要求按照 6.2.1 执行。

7.2.2 资料控制要求

资料控制要求按照 6.2.2 执行。

7.2.3 流程和内容控制要求

7.2.3.1 SIL 定级工作流程

SIL 定级的主要工作流程包括：

a) LOPA(其具体工作流程见图 2)；

b) SIF 分配；

c) 确定 SIF 的 SIL。

7.2.3.2 开展 LOPA

按照 6.2.3 要求执行。

7.2.3.3 SIF 分配

开展 LOPA 后，考虑已设置和建议设置的待 SIL 定级的 SIF 以外的其他风险降低措施后，对于仍存在的残余风险合理分配需要设置的 SIF。

7.2.3.4 确定 SIF 的 SIL

7.2.3.4.1 按照 6.2.3.13 计算 SIF 的 RRF，与表 5 中的 RRF 进行比对，确定 SIF 的 SIL 要求。对于连续运行模式或高要求运行模式，应按照表 6 确定 SIF 的 SIL 要求。

表 5 低要求运行模式下的 SIL 要求(GB/T 21109.1—2022 中表 4)

要求运行模式		
SIL	PFD_{avg}	要求的风险降低
4	10^{-5}～$<10^{-4}$	>10 000～100 000
3	10^{-4}～$<10^{-3}$	>1 000～10 000

表 5　低要求运行模式下的 SIL 要求(GB/T 21109.1—2022 中表 4)(续)

要求运行模式		
SIL	PFD_{avg}	要求的风险降低
2	10^{-3}～$<10^{-2}$	>100～1 000
1	10^{-2}～$<10^{-1}$	>10～100

表 6　连续运行模式或高要求运行模式下的 SIL 要求(GB/T 21109.1—2022 中表 5)

连续运行模式或高要求运行模式	
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}～$<10^{-5}$

7.2.3.4.2　当分析过程中涉及多个 SIF 预防同一危险事件时,对共享或共用硬件、嵌入式软件或应用程序实现的 SIL 能力应提出高于当前分析 SIF 的 SIL 能力要求。

示例:以某储罐高高液位联锁保护为例,其 SIL 要求为 SIL2,在高液位还设置了具有 SIL1 要求的其他联锁保护,若两者共用 SIS 控制器和最终执行元件,高液位联锁保护执行单元失效将导致高高液位联锁保护同时失效,则共用的 SIS 控制器和最终执行元件及相关软件或应用程序需实现高于 SIL2 的能力。

7.2.4　文档控制要求

7.2.4.1　SIL 定级记录表

SIL 定级记录表宜包括以下内容。

a)　后果描述:包括风险矩阵中的后果分类,以便确定可容忍风险频率。

b)　可容忍风险标准:记录表中选取的可容忍风险标准应和后果分类一致,可容忍风险标准的频率值应符合公司可容忍风险标准值。

c)　初始事件:记录表中清晰记录场景初始事件,同时给出初始事件频率。

d)　防护措施:记录表中记录针对初始事件的防护措施描述及其失效概率。

e)　使能事件或使能条件:对初始事件的使能事件或使能条件进行描述,并给出使能事件或使能条件发生的概率。

f)　条件修正:描述条件修正因子取值说明。

注:一般需标明这些假定值的参考依据,且对标准值的任何修改需说明理由并记录在案。

g)　中间事件频率:是初始事件频率和所有使能事件或使能条件发生概率以及条件修正因子的乘积。

h)　独立保护层:写出所有现有的及建议的独立保护层,包括每个独立保护层失效概率。如果独立保护层的失效概率不同于企业内采用的标准值,则需阐明调整理由。

i)　后果频率:考虑已有防护措施和 IPL 后的后果频率。

j)　是否满足可容忍风险标准:使用考虑已有防护措施和 IPL 后的后果频率与采用的可容忍风险标准进行比较,假如后果频率小于对应后果分类的可容忍风险标准,则当前风险在可容忍范

围内，否则为不满足。

k） 本 SIF 仍需完成的降险能力 PFD/RRF：假如存在后果频率大于可容忍风险标准的情况，需计算各后果分类仍需完成的降险能力 PFD/RRF。

l） 满足可容忍风险标准所要求采取的行动：

- 描述未将风险降低至可容忍标准内还需采取的行动内容；
- 假如后果频率大于可容忍风险标准，但企业目前无法采取其他行动，因此不得不接受这样的风险，这种特殊情况可能需要高级管理人员的签字，并附在分析文档中。

m） 备注：包括所有背景资料，或记录与场景或采取行动相关的此类信息。

n） 参考资料：任何有关的工艺流程图、P&ID、SIF 描述或联锁逻辑图、仪表清单、设备清单、操作规程、测试程序等参考资料，从而完整地记录分析的依据，以协助审查或执行分析的结果。

7.2.4.2 SIL 定级报告

在 SIL 定级分析会议后，由分析主席和秘书将会议记录进行整理、汇总，形成 SIL 定级分析报告文件，报告模版见附录 C。报告宜包括以下内容：

——项目基本概况；

——SIL 定级分析方法及流程：包括分析目的、SIL 定级工作程序、详细步骤等；

——SIL 定级分析实施：包括日程安排、参与人员、参考资料等；

——工作成果汇总：包括分析结果和所提建议；

——SIL 定级分析记录表（记录表模版见附录 C）；

——分析依据的可容忍风险标准；

——SIL 定级分析工作参与人员签到表。

7.3 审查要求

应对 SIL 定级的人员、资料、流程和文档 4 个方面进行审查，质量控制审查样表见附录 D：

——否决项：SIL 定级报告质量控制的关键要素，若未满足相关审查要求，则本次审查不予通过；

——非否决项：SIL 定级报告质量控制的一般要素，若发现不符合项，后续需进行整改或优化。审查人员可根据实际情况综合研判，得出审查结论。

注：对于非否决项，若不符合项超过 5 项，推荐为审查不通过。

8 SIL 验证的质量控制

8.1 控制要素

8.1.1 人员

SIL 验证人员按照 8.2.1 进行质量控制。

8.1.2 资料

SIL 验证资料按照 8.2.2 进行质量控制。

8.1.3 流程和内容

SIL 验证流程和内容按照 8.2.3 进行质量控制。

8.1.4 文档

SIL 验证文档按照 8.2.4 进行质量控制。

8.2 控制要求

8.2.1 人员控制要求

8.2.1.1 人员构成

SIL 验证小组由主席、秘书、参与人员组成。SIL 验证主席和秘书来自验证单位，参与人员来自运行单位、验证单位、设计方，必要时还包括承包商。

注 1：SIL 验证主席需具有 SIL 验证经验，在调研过程中一般通过访谈、核查等方法获取各安全功能回路真实的配置和维护信息。SIL 验证主席的主要职责包括：

——确认输入资料是否齐全、准确；

——确定工作范围、确定待验证回路、确定 SIL 定级结果，并与小组成员达成一致；

——编制 SIL 验证工作计划，主持调研，组织参与人员提供真实的配置和维护信息，保证调研顺利开展；

——检查调研记录表，确保所有调研内容准确记录；

——组织开展 SIL 验证分析计算，对未实现 SIL 要求的回路提出配置/维护建议；

——审核并提交 SIL 验证报告。

注 2：SIL 验证参与人员的主要职责是在 SIL 验证主席的引导下积极回答访谈问题，配合完成核查，提供真实的安全功能回路配置和维护信息。

8.2.1.2 独立等级

SIL 验证主席应是独立的，独立等级应按照 GB/T 20438.1—2017 中 8.2 执行。项目设计的人员或项目组其他相关人员配合评估组参与评估活动。

注：分析对象的危险事件后果可能致人员伤亡的宜由独立部门执行，后果可能致多人伤亡的宜由独立第三方执行。

8.2.1.3 人员能力

8.2.1.3.1 SIL 验证主席能力

SIL 验证主席能力应满足下列要求：

——SIL 验证主席具有 SIL 验证经验，能熟练使用计算软件和数据库；

——SIL 验证主席掌握 SIL 验证方法，熟悉仪器仪表，对 GB/T 20438(所有部分)、GB/T 21109(所有部分)有深入研究，接受过行业权威机构 SIL 验证、GB/T 20438(所有部分)、GB/T 21109(所有部分)标准技术培训，取得培训合格证书；

——SIL 验证主席具有行业认可的功能安全资质，且具有不少于 10 项 SIL 验证项目经验。

8.2.1.3.2 SIL 验证参与人员能力

SIL 验证参与人员能力应满足下列要求：

——SIL 验证组成员了解 GB/T 20438(所有部分)、GB/T 21109(所有部分)，并经过培训；

——SIL 验证组成员具备所分析对象相同或相似领域 SIL 验证项目经验，以确保验证结果合理可信；

——SIL 验证单位参与项目的高级资质人员不少于 2 名。

8.2.2 资料控制要求

SIL 验证的输入资料宜包括：

——SIL 定级报告(需明确 SIL 等级和 PFD/RRF 值)；

——运行模式说明；

——P&ID；
——SRS；
——安全联锁功能列表、功能描述、设定点、回路结构；
——安全联锁逻辑图或因果表；
——SIF 组成仪表设备的厂家、型号、仪表类型/原理、投用时间、量程等信息；
——经过认证的仪表设备需提供合规的 SIL 证书、评估报告及安全手册等认证材料；
——维检修规程；
——功能性测试报告；
——以前的设备故障记录(提供审阅后收回)；
——其他所需资料。

8.2.3 流程和内容控制要求

8.2.3.1 SIL 验证工作流程

8.2.3.1.1 SIL 验证原理

硬件安全完整性验证应通过分析和定量计算的方式确认 SIF 是否满足 SIL 要求，系统性安全完整性验证应通过定性分析的方式确认是否满足要求。

注 1：安全完整性定义为在规定的条件下、规定的时间内，安全相关系统成功实现所要求的安全功能的概率。安全完整性关系到安全相关系统执行安全功能的性能(执行的安全功能将在 SRS 中规定)。

注 2：硬件安全完整性：与在危险失效模式下的随机硬件失效有关，一般以一个合理的精确度水平对安全相关的硬件安全完整性达到的规定等级进行估计。硬件安全完整性通过架构约束和随机硬件失效概率计算。在计算硬件安全完整性时，需考虑导致非安全状态的所有失效因素。

注 3：系统性安全完整性：与在危险失效模式下的系统性失效有关，一般无法定量计算，能采用定性分析。

8.2.3.1.2 SIL 验证基本工作流程

SIL 验证方法包括：可靠性框图法、马尔可夫模型、故障树法等。图 4 为常用的 SIL 验证基本工作流程。

注：可靠性框图法、马尔可夫模型、故障树法仅建模方式不一样，验证过程中数据的输入、选择、结构划分相关质量控制要求一致。

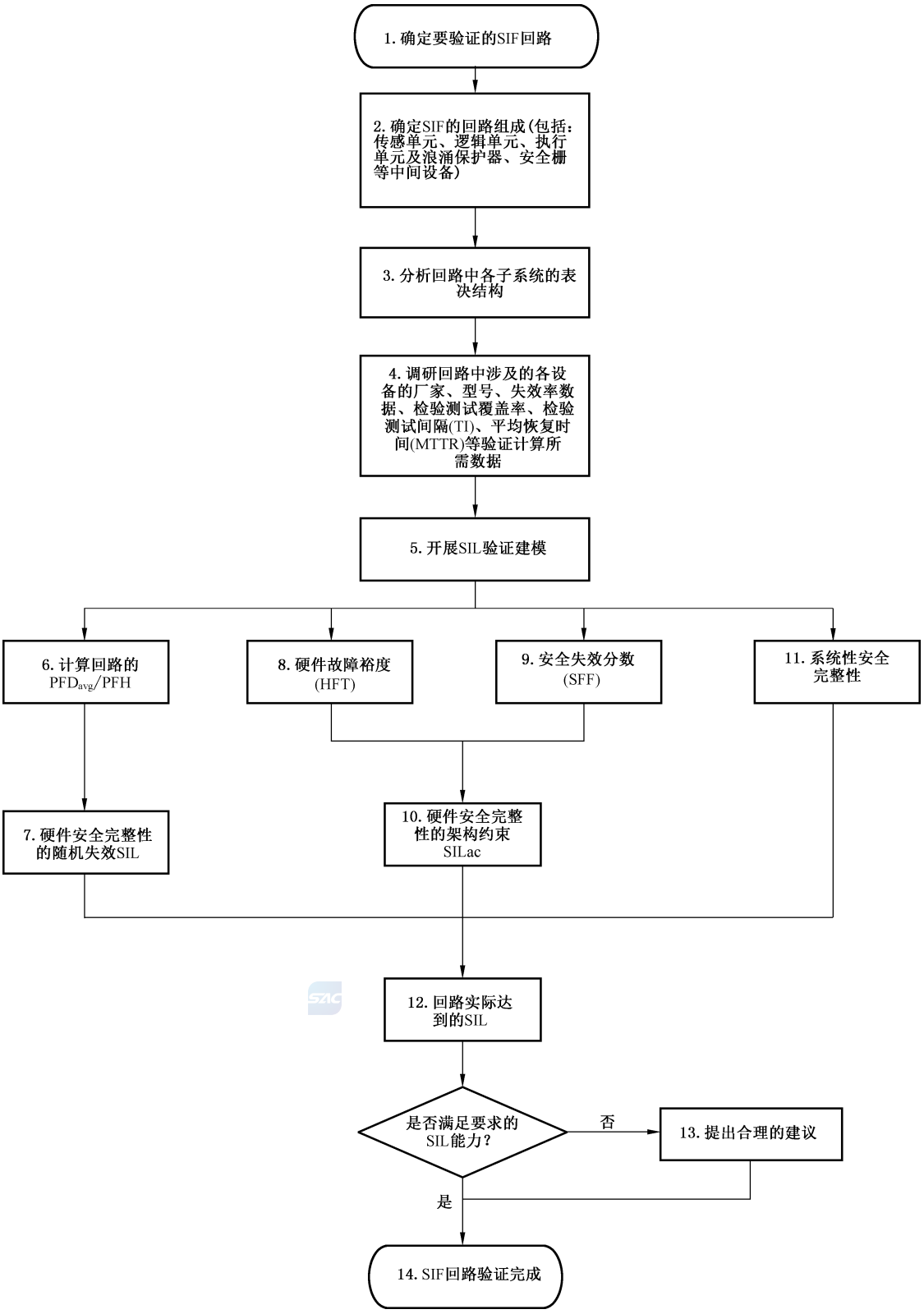


图 4　SIL 验证基本工作流程

注：当 SRS 中明确有 STR 要求时，或在役阶段用户对于装置可用性有要求时，在 SIL 验证阶段增加 STR 计算。

8.2.3.2 验证对象确定

依据 SRS、SIL 定级报告、安全联锁功能列表、安全联锁逻辑图或因果表辨识出待验证的 SIF。

8.2.3.3 回路结构分析

应明确参与 SIF 的仪表设备、安全关键动作及其逻辑/冗余关系，包括回路执行到哪一步即可进入安全状态，安全状态的定义只针对当前 SIF 所保护场景的降险需求，出于维护或装置再启动等相关安全或便捷考虑的执行动作不宜纳入 SIL 验证计算。

注 1：例如，停机回路到继电器还是到执行器。

注 2：例如：煤浆气化炉超温联锁停机执行单元只需考虑氧气进料切断，煤浆给料阀等其他动作一般不纳入 SIL 验证计算。

8.2.3.4 SIL 验证现场调研

SIL 验证工作通常采取现场调研的形式，对 SIF 进行梳理，获取 SIF 的完整信息，包括每一条 SIF 的传感（输入）子系统、逻辑子系统到执行（输出）子系统的完整信息。

验证调研人员应准确记录调研信息。SIL 验证调研记录表宜包括如下信息：

——SIF 编号；

——SIF 名称；

——SIF 功能描述、运行模式；

——SIF 回路传感器位号、设备厂家、型号、类型/原理、投用时间、运行条件、表决机制、诊断设置、共用性情况等数据；

——SIF 回路逻辑解算器设备厂家、型号、投用时间、运行条件、表决机制、诊断设置、共用性情况等数据；

——SIF 回路执行器位号、设备厂家、型号、类型/原理、投用时间、运行条件、表决机制、诊断设置、共用性情况等数据；

——SIF 回路其他单元（如浪涌保护器、安全栅、信号分配器、继电器等）设备厂家、型号、投用时间、运行条件、表决机制、诊断设置、共用性情况等数据；

——MTTR/MRT，设备的备品备件情况；

——SIF 设备检验测试方案（以确认 PTC）以及 TI。

8.2.3.5 调研内容分析

8.2.3.5.1 根据调研确认 SIF 运行模式。

8.2.3.5.2 根据调研确认每一条 SIF 回路结构信息，包括传感单元、逻辑单元、执行单元、安全栅、浪涌保护器、信号分配器、输入输出卡件、继电器、端子排接线方式等。

8.2.3.5.3 根据现场调研确认 SIF 组成设备的完整信息，确定符合现场实际的各设备 λ_{DD}、λ_{DU}、λ_{SD}、λ_{SU}，确定方式包括：

——采用认证数据作为验证输入：应将符合 GB/T 20438（所有部分）要求的认证证书和功能安全评估报告及安全手册作为数据来源，并确认现场使用环境和条件与安全手册要求一致；

——采用失效模式、影响及其诊断分析（FMEDA）方法基于数据库或以往使用数据开展失效率分配；

——采用可信数据库作为数据来源。

8.2.3.5.4 根据 GB/T 20438（所有部分）要求计算 SFF 或 DC。

8.2.3.5.5 根据调研确认 TI。

8.2.3.5.6 根据调研确认检验测试方案以估计 PTC。

8.2.3.5.7 根据调研确认设备 MTTR 及 MRT。

8.2.3.5.8 根据调研确认 SIF 回路传感单元、逻辑单元以及执行单元的冗余情况，确定各单元的 HFT。

8.2.3.6 硬件安全完整性

8.2.3.6.1 SIL 验证分析建模

根据 SIF 的回路构成，确定各单元的表决结构，完成 SIL 验证分析建模。

8.2.3.6.2 硬件安全完整性的架构约束

架构约束的安全完整性由以下因素决定：

——HFT，即容错能力，例如：HFT＝1，意味着发生一个危险故障不会导致安全功能丧失；

——SFF，它是对危险故障预发现能力的度量，由安全失效和可被诊断测试检测到的危险失效共同决定。应根据 GB/T 20438(所有部分)、GB/T 21109(所有部分)确定硬件安全完整性的架构约束。

SIS 或者 SIS 子系统的最小 HFT 要求按照以下任一种方式确定：

——GB/T 21109.1—2022 中的 11.4.5～11.4.9；

注：在依据表 7 确定要求的最小 HFT 时，还需同时满足以下内容：

——FVL 和 LVL 可编程装置的诊断覆盖率不小于 60%；

——失效量计算中使用的可靠性数据由不小于 70%的统计上界置信区间确定。

表 7 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

——GB/T 20438.2—2017 中的 7.4.4.2(路线 1_H)；

注：如果是 A 类组件，按照表 8 确定子系统可声明的最高 SIL；如果是 B 类组件，按照表 9 确定子系统可声明的最高 SIL。

表 8 A 类安全相关组件或子系统执行安全功能时的最大允许 SIL

组件的 SFF	HFT		
	0	1	2
＜ 60%	SIL 1	SIL 2	SIL 3
60%～＜ 90%	SIL 2	SIL 3	SIL 4
90%～＜ 99%	SIL 3	SIL 4	SIL 4

表 8　A 类安全相关组件或子系统执行安全功能时的最大允许 SIL（续）

组件的 SFF	HFT		
	0	1	2
≥ 99%	SIL 3	SIL 4	SIL 4

注：如果要实现安全功能的元器件满足下列全部条件，则组件一般视为 A 类：

a）　所有组成元器件的失效模式都被明确定义；

b）　故障状况下组件的行为能够完全确定；

c）　有充足而可靠的失效数据，能显示出满足所声明的检测到的和未检测到的危险失效的失效率。

表 9　B 类安全相关组件或子系统执行安全功能时的最大允许 SIL

组件的 SFF	HFT		
	0	1	2
<60%	不允许	SIL 1	SIL 2
60%～< 90%	SIL 1	SIL 2	SIL 3
90%～< 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

注：如果要实现安全功能的元器件满足下列条件之一，则组件一般视为 B 类：

a）　至少一个组成元器件的失效模式未被明确定义；

b）　故障状况下组件的行为不能完全确定；

c）　没有充足而可靠的失效数据，能显示出满足所声明的检测到的和未检测到的危险失效的失效率。

——GB/T 20438.2—2017 中的 7.4.4.3（路线 2_H）。

8.2.3.6.3　PFD_{avg}/PFH 计算方法的质量控制

PFD_{avg}/PFH 计算方法的质量控制要求如下。

a）　PFD_{avg}/PFH 计算应基于以下假设：

- 在低要求模式下，要求时系统出现失效的平均概率低于 10^{-1}；
- 在系统寿命内元器件失效率为常量；
- 传感器（输入）子系统包含实际的传感器、其他元器件、接线；
- 逻辑子系统包括 I/O 卡件和控制器；
- 最终元件（输出）子系统包括用来处理来自逻辑子系统的最终信号的所有部件和连线，还包括最终执行元器件；
- 作为计算输入和表格中的硬件失效率是子系统的单通道失效率；
- 在一个表决组中所有通道具有相同的失效率和诊断覆盖率；
- 子系统中一个通道的硬件总失效率为此通道危险失效率和安全失效率的总和（假设两者是相同的）；
- 检验测试间隔至少要比平均维修时间（MRT）大一个数量级（适用于低要求模式）；
- 对于每个子系统都有自身的检验测试间隔以及 MRT（适用于低要求模式）；

- 对于所有子系统的1oo2、1oo2D、1oo3、2oo3表决组，诊断覆盖率规定的失效部分，在平均恢复时间内被检测和修复，平均恢复时间决定硬件安全完整性的需求；
- 当电源失效不能对失电安全型SIF提供电力时，系统联锁停车进入安全状态，此时电源不会对SIF要求的危险失效平均概率产生影响；如果SIF为得电安全型，或者电源的失效模式能引起SIF不安全工作，电源需包括在评价内容之中；
- 当使用“通道”这个术语时，它只限于所讨论的那部分系统，通常指传感器子系统、逻辑子系统或最终元件子系统。

b) 验证计算使用参数至少包括表10中的内容。

表10 验证计算使用参数及其范围

参数	描述	单位
TI	检验测试间隔	h
MTTR	平均恢复时间	h
MRT	平均修理时间	h
β	具有共同原因的、没有被检测到的失效分数（在公式中用一个分数或者百分比表示）	—
β_D	具有共同原因的，已被诊断测试检测到的失效分数（在公式中表示成一个分数或者百分比）	—
PFD_G	表决通道组在要求时的平均失效概率（如果传感器子系统、逻辑子系统或最终元件子系统分别对应一个表决组，则PFD_G分别等于PFD_S、PFD_L或PFD_{FE}）	—
PFD_S	传感器子系统在要求时的平均失效概率	—
PFD_L	逻辑子系统在要求时的平均失效概率	—
PFD_{FE}	最终元件子系统在要求时的平均失效概率	—
PFH_G	表决通道组的平均危险失效频率（如果传感器、逻辑或最终元件子系统分别对应一个表决组，则PFH_G分别等于PFH_S、PFH_L或PFH_{FE}）	—
PFH_S	传感器子系统的平均危险失效频率	—
PFH_L	逻辑子系统的平均危险失效频率	—
PFH_{FE}	最终元件子系统的平均危险失效频率	—
λ_{DD}	子系统中一个通道被检测到的危险失效率（它是子系统中该通道所有被检测到的危险失效率的总和）	h^{-1}
λ_{DU}	子系统中一个通道未检测到的危险失效率（它是子系统中该通道所有未检测到的危险失效率的总和）	h^{-1}
λ_{SD}	子系统中一个通道被检测到的安全失效率（它是子系统中该通道所有被检测到的安全失效率的总和）	h^{-1}
λ_{SU}	子系统中一个通道未被检测到的安全失效率（它是子系统中该通道所有未检测到的安全失效率的总和）	h^{-1}
t_{CE}	1oo1、1oo2、2oo2、2oo3结构中通道的等效平均不工作时间（它是子系统通道中所有部件的组合不工作时间）	h
t_{GE}	1oo2、2oo3结构中表决组的等效平均不工作时间（它是表决组中所有通道的组合不工作时间）	h
t'_{CE}	1oo2D结构中通道的等效平均不工作时间（它是子系统通道中所有部件的组合不工作时间）	h

表 10　验证计算使用参数及其范围（续）

参数	描述	单位
t'_{GE}	1oo2D 结构中表决组的等效平均不工作时间(它是表决组中所有通道的组合不工作时间)	h
T_d	要求之间的时间间隔	h
PTC	检验测试覆盖率	—

c）　基于 a)中的假设和 b)中的参数，各表决结构的 PFD_{avg}/PFH 计算过程见 GB/T 20438.6—2017 中附录 B。

8.2.3.6.4　硬件随机失效的 SIL 要求

应根据 GB/T 20438(所有部分)、GB/T 21109(所有部分)计算 SIF 的 PFD_{avg} 或 PFH，依据表 5 和表 6 确定硬件随机失效的 SIL。

8.2.3.6.5　硬件安全完整性的 SIL

SIF 硬件安全完整性的 SIL 取架构约束的 SIL 与硬件随机失效的 SIL 中的低值。

8.2.3.6.6　SIL 验证计算工具

若使用 SIL 验证计算工具，应采用权威机构认可的数据库和软件。

8.2.3.7　系统性安全完整性

8.2.3.7.1　对各 SIF 回路包含设备的系统性失效、检测到故障时的系统行为等方面宜采用工作表形式进行分析，分析内容包括：

——对控制系统性故障的分析(依据 GB/T 20438.2—2017 中的 7.4.7)；

——应用程序的符合性分析(依据 GB/T 21109.1—2022 中的第 12 章)；

——对设计和集成过程中可能存在的失效分析(依据 GB/T 20438.2—2017 中的 7.4.6)；

——检测到故障时的系统行为分析(依据 GB/T 20438.2—2017 中的 7.4.8，GB/T 21109.1—2022 中的 11.3)。

8.2.3.7.2　采用认证证书作为验证输入时，可采信 SIF 设备经认证的系统性能力。

8.2.3.7.3　SIF 设备发生故障时的系统行为分析时，应根据 SIL 验证调研确认 SIF 回路及其所包含设备的故障检测/诊断措施，分析其响应机制：

——若响应方式为将系统导入安全状态，则需确认响应时间、安全状态、超驰/旁路设置等是否满足要求；

——若响应方式为报警，则需确认人员响应是否有操作规程要求并确保人员在过程安全时间内及时采取动作；

——对于对动力源(如电源、空气、液动源或气动源)中断而不进入安全状态的所有 SIS 设备，应确认已对共用动力源丢失和 SIS 电路完整性设置有检测和报警措施(如线路终端监视、供压测量、液压或气压检测)并根据 GB/T 21109.1—2022 中的 11.3 采取行动。

注 1：通过使用辅助动力源(如备用电池、不间断电源、储气罐、液压蓄能器、第二气源)来提高动力源完整性。

注 2：动力源中断可能影响多个 SIF，甚至多个 SIS。因此需考虑多个 SIF 的共因失效。

8.2.3.8　SIL 验证建议

针对验证结果显示不能满足 SIL 要求的安全功能回路应进行分析，确认是传感单元、逻辑单元还

是执行单元的随机失效或架构约束不满足 SIL 要求，分析其架构及 PFD_{avg}/PFH 分布，给出合理的建议，使回路的安全完整性达到要求。

在役装置 SIL 评估建议措施应当及时关闭，不能及时落实或者关闭的，应落实替代的风险控制措施，确保风险受控。

注 1：当 SIF 的 SIL 定级结果发生变化或者实际的回路配置发生变化时，需及时进行 SIL 验证复核，确保变更后的 SIF 的 SIL 满足要求。

注 2：建议包括缩短检验测试间隔到多长时间，如何调整检修方案，推荐的诊断设置方案，推荐的设备结构配置，推荐的设备选型等。

8.2.4 文档控制要求

8.2.4.1 SIL 验证工作表

根据 SIL 验证调研表的信息，确定回路配置信息和维护信息，应建立 SIL 验证工作表，完成 SIL 验证分析计算，给出 SIL 验证结论。SIL 验证工作表至少包括以下内容：

——项目名称；

——SIF 编号、SIF 名称、SIF 描述；

——回路中各设备的名称、位号、厂家型号、表决结构、MTTR、MRT、TI 等；

——回路中各设备的 λ_{DD}、λ_{DU}、λ_{SD}、λ_{SU} 或 PFD_{avg} 数据，以及共因失效因子 β、β_D；

——绘制的可靠性框图/故障树/马尔可夫状态转移图；

——经分析计算得出的回路传感、逻辑、执行各部分的 PFD_{avg}/PFH 值、架构约束的 SIL；

——经分析计算得出的回路 PFD_{avg}/PFH 值、随机失效的 SIL、架构约束的 SIL；

——回路实际的 SIL 能力与要求的 SIL；

——SIL 验证建议。

8.2.4.2 SIL 验证报告

在 SIL 验证分析完成后，验证人员将调研表、SIL 验证工作表进行整理、汇总，形成 SIL 验证报告文件，报告模版见附录 E。报告宜包括以下内容：

——验证概况；

——SIL 验证方法及流程、验证假设等相关说明；

——验证实施：包括参与人员、输入资料及实施计划安排等；

——验证结果汇总：包括计算结果和所提建议，必要时可包括企业相应的整改计划；

——验证工作表；

——验证使用数据及来源；

——验证调研工作参与人员签到表；

——SIL 验证主席的简历和资质信息。

8.3 审查要求

应对 SIL 验证的人员、资料、流程和文档 4 个方面进行审查，质量控制审查样表见附录 F。

——否决项：SIL 验证报告质量控制的关键要素，若未满足相关审查要求，则本次审查不予通过。

——非否决项：SIL 验证报告质量控制的一般要素，若发现不符合项，后续需进行整改或优化。审查人员可根据实际情况综合研判，得出审查结论。

注：对于非否决项，若不符合项超过 5 项，推荐为审查不通过。

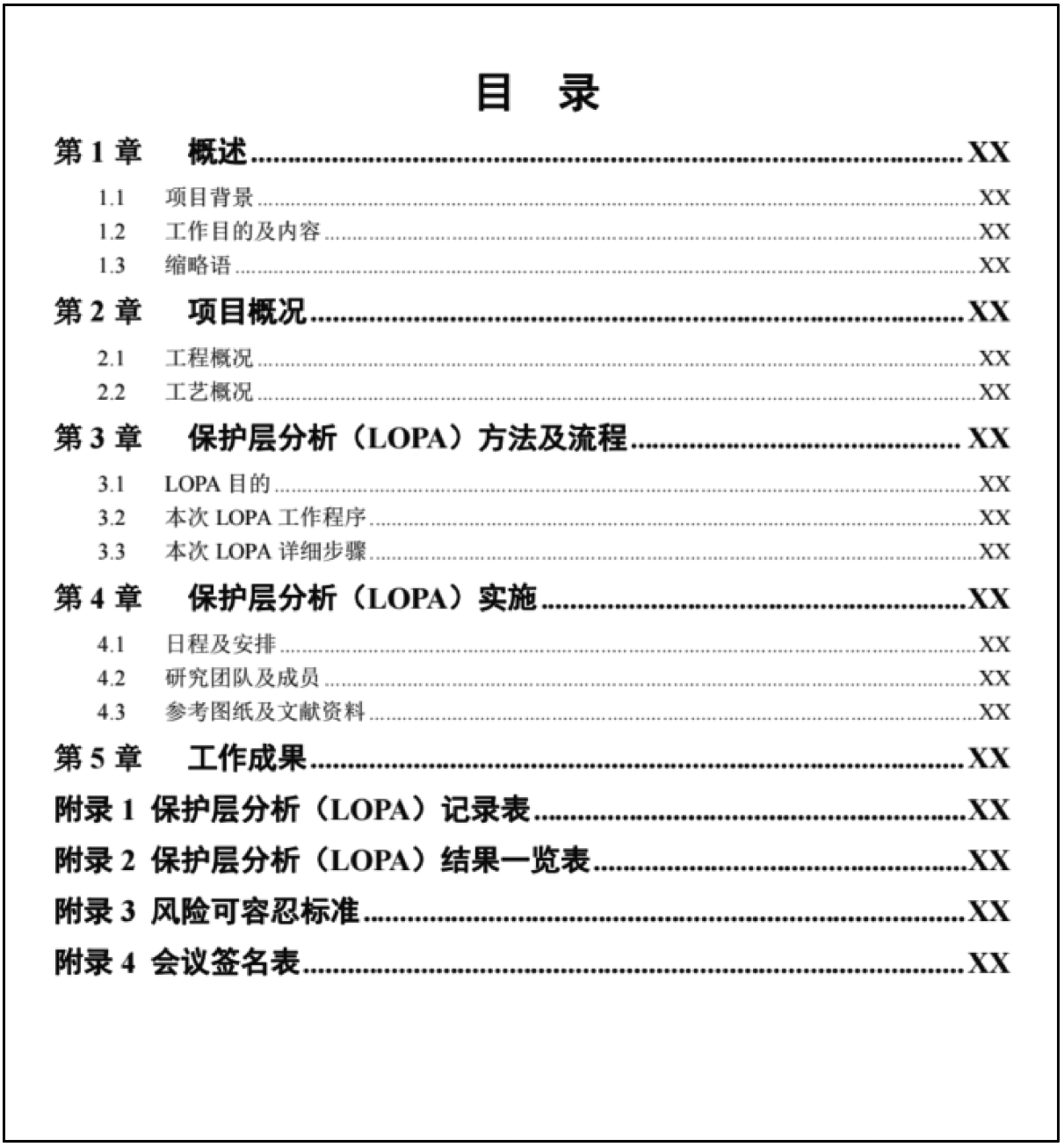
附 录 A
（资料性）
LOPA 记录表与报告示例

LOPA 记录表示例见表 A.1。

表 A.1 LOPA 记录表示例

LOPA 分析记录表				
风险点编号				
风险点名称				
风险点描述				
所在区域				
运行模式				
分析项目	描述	概率/频率	后果频率	备注
后果描述				
后果严重性等级				
风险可容忍标准	人员：			
	财产：			
	环境：			
	声誉：			
场景 1				
初始事件 1				
防护措施 1				
使能事件 1				
场景 2				
初始事件 2				
防护措施 2				
使能事件 2				
中间事件频率				
条件修正（如果适用）	点火事件			
	人在影响区内			
	致死			
	其他			
“中间事件及后果”IPL				
后果频率	人员			
	财产			
	环境			
	声誉			
是否满足风险可容忍标准(是/否)				
仍需完成的降险能力 PFD	人员			
	财产			
	环境			
	声誉			
满足风险可容忍标准所要求采取的行动				
备注				

LOPA 工作报告可参考图 A.1。



目　录

第 1 章　概述 XX
1.1　项目背景 XX
1.2　工作目的及内容 XX
1.3　缩略语 XX
第 2 章　项目概况 XX
2.1　工程概况 XX
2.2　工艺概况 XX
第 3 章　保护层分析（LOPA）方法及流程 XX
3.1　LOPA 目的 XX
3.2　本次 LOPA 工作程序 XX
3.3　本次 LOPA 详细步骤 XX
第 4 章　保护层分析（LOPA）实施 XX
4.1　日程及安排 XX
4.2　研究团队及成员 XX
4.3　参考图纸及文献资料 XX
第 5 章　工作成果 XX
附录 1　保护层分析（LOPA）记录表 XX
附录 2　保护层分析（LOPA）结果一览表 XX
附录 3　风险可容忍标准 XX
附录 4　会议签名表 XX

图 A.1　LOPA 工作报告示例

附 录 B
（资料性）
LOPA 工作质量控制审查样表

LOPA 工作质量控制审查样表，见表 B.1。

表 B.1 LOPA 工作质量控制审查样表

LOPA 工作质量控制审查样表						
审查：对 LOPA 工作的人员、资料、流程和内容、文档 4 个方面进行审查。 **否决项**：LOPA 工作报告质量控制的关键要素，若未满足相关审查要求，则本次审查不予通过。 **非否决项**：LOPA 工作报告质量控制的一般要素，若发现不符合项，后续需进行整改或优化，审查人员根据实际情况综合研判，得出审查结论。对于非否决项，若不符合项超过 5 项，推荐为审查不通过。						
序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
1	人员	人员构成	LOPA 小组宜由分析主席、分析秘书和分析成员组成。分析主席和秘书应来自分析单位，分析成员宜来自运行单位、分析单位、设计方，必要时还包括承包商。小组成员宜为 6 人～9 人，其中运行单位和设计方宜 4 人～6 人，分析单位宜 2 人～3 人	否		
2			LOPA 分析成员应满足以下要求： 1)设计方根据分析需求派出工艺、仪表专业人员，必要时还需派出电气、消防、总图等专业人员，专业经验不少于 3 年； 2)承包商应派出与项目有关的专业人员； 3)运行单位根据分析需求派出工艺、仪表、设备、安全、运行/操作专业人员，必要时还需派出电气、通信、管理等相关专业人员，专业经验不少于 3 年	是		
3		独立性	LOPA 分析主席应是独立的，独立等级应按照 GB/T 20438.1—2017 中 8.2 执行，项目设计的人员或项目组其他相关人员配合评估组参与评估活动。 分析对象的危险事件后果可能致人员伤亡的宜由独立部门执行，后果可能致多人伤亡的宜由独立第三方执行	是		
4		人员能力	LOPA 分析主席能力应满足下列要求： 1)LOPA 分析主席具有 LOPA 工作主持经验，掌握 LOPA 工作方法，熟悉工艺流程，了解操作规程，对 GB/T 20438(所有部分)、GB/T 21109(所有部分)、GB/T 32857—2016 有较为深入的研究，接受过行业权威机构 LOPA 工作/SIL 定级培训，取得培训合格证书； 2)LOPA 分析主席具有行业认可的功能安全资质，且具有不少于 10 项 LOPA 工作项目经验	是		

表 B.1　LOPA 工作质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
5	人员	人员能力	LOPA 分析成员能力应满足下列要求： 1）LOPA 分析成员了解 GB/T 20438（所有部分）、GB/T 21109（所有部分）、GB/T 32857—2016，并经过培训； 2）LOPA 分析成员具备所分析对象相同或相似领域的经验及相关法律法规知识，以确保评估结果合理可信； 3）LOPA 工作单位参与项目的高级资质人员不少于 2 名	是		
6	资料	LOPA 工作输入资料	LOPA 工作依据的图纸是否为与当前装置符合的 PFD、P&ID	是		
7			LOPA 工作输入资料宜包括： 1）危险与风险分析报告（如 HAZOP 报告）； 2）设计/工艺说明； 3）安全联锁功能列表、功能描述、设定点、回路结构； 4）安全联锁逻辑因果图； 5）管道及材料数据表（承压等级等相关参数）； 6）设备数据表（压缩机、冷凝器、蒸发器、贮液器、低压循环桶、安全阀等，包括设计参数）。 LOPA 工作可能需要的其他输入资料还包括： 1）设备标高数据； 2）主要容器、塔及反应器的设备结构图； 3）设备布置图； 4）操作规程； 5）维检修规程； 6）排空放净系统设计原则； 7）爆炸危险区域划分图； 8）装置区所处区域的气象水文材料； 9）设备价值台账； 10）周边居民区（人口密度）/水源地分布； 11）以前的事故清单、设备故障记录（提供审阅后收回）； 12）边界条件表； 13）设备、仪器仪表台帐（厂家、型号、投用时间、测量范围，若经过认证，则需提供认证证书和功能安全评估报告）； 14）装置变更记录； 15）界区外原料储罐设计和操作压力、温度，安全阀定压值和储罐的尺寸，以及输送原料设备的设计数据，如果是离心泵提供泵的特性曲线，如果是压缩机提供压缩机出口安全阀定压值，产品出装置后储罐的设计和操作压力、温度以及安全阀定压值； 16）项目前的危险分析或安全评阅结果（如果有）	否		

表 B.1　LOPA 工作质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
8	流程和内容	LOPA 分析工作流程	LOPA 工作流程主要包括： 1）风险点识别； 2）场景识别与筛选； 3）后果及严重性评估； 4）初始事件及使能条件确认； 5）条件修正因子确认； 6）独立保护层识别及 PFD 的确认； 7）场景导致预期后果的频率计算； 8）风险评估与建议	否		
9		分析范围和工作目的	是否明确了分析范围和工作目的，且相关描述应保证以下两点： 1）分析对象的边界已被明确定义； 2）分析团队任务明确，分析内容界定在与目标有关的范畴	否		
10		可容忍风险标准确定	是否设置可容忍风险标准，并且不低于国家相关法规文件或标准。企业应制定适用的可容忍风险标准。对于个人风险的可容忍标准可参照 GB 36894 制定	是		
11		风险点识别	若为复杂工艺装置开展 LOPA，宜在场景识别前增加风险点及重要控制点识别，报告中应明确识别规则（如原始风险等级高于几级，或原始风险后果高于几级，或被评估方提供的重要控制点），同时依据 P&ID、工艺说明及设计人员经验识别重要控制点	否		
12		后果及严重性评估	对于每个风险点，后果分析应符合以下要求： 1）后果分析覆盖可容忍风险标准中的所有后果分类； 2）分析至最终后果，并描述所有后果分类（如人员伤亡、经济损失、环境影响等）的严重性情况； **注 1**：例如，若后果仅描述为“安全阀动作”或“压缩机停机”等，均不是最终后果，不符合要求。 3）后果分析时假设任何已有的安全措施都失效时导致的最终不利的可信后果。 **注 2**：可信后果指基于现场实际情况和科学的推导方法确定的最终不利后果。	否		
13			后果的记录要求如下： 1）后果的记录应包括对所有后果分类（如人员伤亡、经济损失、环境影响等）影响的详细描述； 2）不宜将中间事件当后果，记录最终后果	否		
14			后果严重度评估可采用以下安全分析作为依据： 1）安评报告； 2）以往事故借鉴； 3）同类事故借鉴； 4）QRA、后果模拟等定量方法分析； 5）工艺实际情况（如：是否属于“两重点一重大”范围）； 6）地区水文环境等	否		

表 B.1　LOPA 工作质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
15	流程和内容		若为精细化工反应热相关的 LOPA 工作，在后果严重度评估时，应结合精细化工反应热风险评估结论和现场工况给出评估说明	否		
16		当前风险点后果发生的可接受频率确定	应基于企业的可容忍风险标准，根据各后果分类的严重性描述确定当前风险点各后果分类的可接受频率	否		
17		场景识别和筛选	对于每个风险点，审查场景识别来源是否全面及合理，来源一般包括： 1）危险与风险分析（如 HAZOP）报告； 2）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； 3）变更； 4）事故事件； 5）SIF 审查。 场景识别还需完成以下工作。 1）从危险与风险分析（如 HAZOP）记录中识别当前分析风险点对应的偏差、偏差原因、偏差后果，组成待分析场景。 2）在 LOPA 工作会议中确认所有已筛选的场景是否适用，并补充未覆盖的场景。 3）在 SIL 定级时宜使用复合场景计算法开展 LOPA。在场景筛选过程中应确保场景识别完全，且不同场景为独立不相关事件	否		
18			每个场景描述应至少包括： 1）导致场景发生的初始事件； 2）该事件继续发展过程中的中间事件； 3）该场景所导致的最终后果	否		
19			每个场景应有唯一的初始事件及其对应后果。除了初始事件和后果外，一个场景还可能包括： 1）使能事件或使能条件； 2）防护措施失效。 如果使用人员死亡、商业或环境损害作为后果，则场景还可能包括下列部分或全部因素，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	否		

表 B.1　LOPA 工作质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
20	流程和内容	初始事件及其防护措施确认	在确定各场景初始事件时，审查应确认： 1)已辨识出所有的潜在初始事件，并确保无遗漏，且各初始事件互为不相关； 2)该初始事件为有效初始事件； 3)在识别潜在初始事件时，确保已经识别和审查所有的操作模式(如正常运行、启动、停机、低负荷运行等)和设备状态(如待机、维护)下的初始事件； 4)当人的失效作为初始事件时，制定人员失误频率评估的统一规则并在分析时严格执行	否		
21			初始事件分类可分为外部事件、设备故障和人的故障几大类，可包括但不限于以下几个方面： 1)设备设施、仪表等故障； 2)操作失误； 3)外部影响； 4)公用工程失效； 5)运行条件变更。 以下事件不宜作为初始事件： 1)操作人员培训不完善； 2)测试或检查不完善； 3)保护装置不可用； 4)其他类似事件	否		
22			应为每项初始事件估计合理的发生频率，并明确频率确定的依据。频率确定方式包括： 1)对于现场或企业内发生过的初始事件，应结合实际情况确定发生频率； 2)对于建立有事件发生频率数据库的企业，可结合数据库数据和现场实际确定发生频率； 3)已被行业认可的第三方数据库	否		
23			应根据危险与风险分析(如 HAZOP)报告识别出的已有保护措施及现场实际情况确认每项初始事件对应的防护措施。各防护措施应与初始事件相互独立	否		
24		使能条件确认	如无足够的文件支撑，不应使用使能条件。若使用使能条件，其描述应能体现： 1)事件序列只有当装置处在此特定操作场景下才会发生，以独立于其他事故序列为前提对此事故剧情进行分析是必要且有意义的； 2)这种后果只有当装置在使用某种特殊原料、催化剂或加工某个特定的配方时才会发生，以独立于其他事故序列为前提对此事故剧情进行分析是必要且有意义的； 3)事件序列能够发生的前提是，初始事件在某个特定的工况(例如环境温度较低或较高)下发生	否		

表 B.1　LOPA 工作质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
25	流程和内容	条件修正因子确定	条件修正因子应合理修正不同的后果分类。如点火概率，应结合实际确认是否能对人员、经济、环境等形成有效修正	否		
26			在确定点火概率时应明确确定依据。宜考虑： 1)介质的组成成分及其燃烧性； 2)介质泄漏后的最终状态，如液态、气态； 3)介质泄漏所处环境温度与自燃点的关系； 4)泄漏形式，是连续还是瞬时释放； 5)介质所处装置：固定/移动、生产/储存/装卸； 6)装置区周边点火源情况； 7)泄漏速率； 8)现场的安全条件，包括防爆、接地、液体防流散措施、防火安全措施等； 9)事故历史经验	否		
27			人员出现在事件影响区域的概率应明确确定依据。宜考虑： 1)人员岗位(包括现场操作、巡检、维检修等)； 2)人员数量； 3)在后果影响区内的停留时间	否		
28			人员致死率应明确确定依据。宜考虑： 1)装置发生事故时的伤亡半径；或 2)燃烧事故的热辐射强度；或 3)爆炸事故的冲击波强度	否		
29		保护层识别	应对保护层识别过程进行审查，确定各保护层。 a)具有有效性：按照设计的功能发挥作用，有效地防止后果发生，确认该保护层： 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。 b)具有独立性：独立于初始事件和任何其他已经被认为是同一场景的保护层： 1)独立于初始事件的发生及其后果； 2)独立于同一场景中的其他保护层； 3)考虑共因失效或共模失效的影响； c)具有可审查性：对于阻止后果的有效性和 PFD 应以某种方式(通过记录、审查、测试等)进行验证。通过审查程序确认如果保护层按照设计发生作用，它将有效地阻止后果： 1)审查确认保护层的设计、安装、功能测试和维护系统的合适性，以取得保护层特定的 PFD； 2)通过功能测试确认保护层所有的构成元件(传感器、逻辑解算器、最终元件等)运行良好，满足 LOPA 的使用要求； 3)审查过程中记录了发现的保护层条件、上次审查以来的任何修改以及跟踪所要求的任何改进措施的执行情况。 **注**：如安全阀，需在分析过程中确认其设计工况。	否		

表 B.1　LOPA 工作质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
30	流程和内容	保护层识别	以下防护措施不宜作为保护层： 1)培训和取证：在确定操作人员行动的 PFD 时需要考虑的因素，但不单独作为保护层考虑； 2)规程：在确定操作人员行动的 PFD 时需要考虑的因素，但不单独作为保护层考虑； 3)检测：正常的检测将影响某些保护层的 PFD，延长检测周期可能增加保护层的 PFD； 4)维护：维护活动将影响某些保护层的 PFD； 5)通信：作为一种基础假设，假设工厂内具有良好的通信。差的通信将影响某些保护层的 PFD； 6)标识：标识自身不是保护层。标识可能不清晰、模糊、容易被忽略等。标识可能影响某些保护层的 PFD	否		
31		场景频率计算	单一场景计算： 单一场景后果的频率为初始事件发生频率乘以所有保护层要求时危险失效概率，场景后果的频率可能需要使用下面的两种系数进行修正： 1)假如场景的发生需要使能事件或使能条件时，需要乘以使能事件或使能条件的发生概率； 2)假如需要计算危险物质释放后的后续后果发生频率时，需要乘以条件修正因子，常见的条件修正因子如下：可燃物质点火概率、人员出现在事件影响区域的概率、火灾/爆炸或有毒物质释放的暴露致死率或其他	是		
32			多个/复合场景计算： 对于复合场景后果发生频率计算，应分析当前风险点同一后果相关的所有场景、初始事件及其对应的个性防护措施，将其频率相加得复合场景频率，再与条件修正及共用的保护层、非独立保护层相乘，得出该风险点后果的发生频率	是		
33		风险决策	对于单一场景分析法，选择同一风险点不同场景中“采用其他风险降低措施后的后果频率”的最高值与可容忍风险频率比较，若“采用其他风险降低措施后的后果频率”大于可容忍风险频率，则需要增加风险降低措施（如 SIF、安全阀等），并按照 6.2.3.13.1 计算 RRF	否		
34			对于复合场景分析法，直接使用计算得出的“采用其他风险降低措施后的后果频率”与可容忍风险频率比较，若“采用其他风险降低措施后的后果频率”大于可容忍风险频率，则需要增加风险降低措施（如 SIF、安全阀等），并按照 6.2.3.13.1 计算 RRF	否		
35			若建议增加的风险降低措施为 SIF，则按照 SIL 定级质量控制要求开展 SIL 定级工作	否		

表 B.1　LOPA 工作质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
36	文档	LOPA 记录表	LOPA 记录表宜包括以下内容。 1)后果描述：包括风险矩阵中的后果分类，以便确定可容忍风险频率。 2)可容忍风险标准：记录表中选取的可容忍风险标准需和后果分类一致，可容忍风险标准的频率值需符合公司可容忍风险标准值。 3)初始事件：记录表中清晰记录场景初始事件，同时给出初始事件频率。 4)防护措施：记录表中记录针对初始事件的防护措施描述及其失效概率。 5)使能事件或使能条件：对初始事件的使能事件或使能条件进行描述，并给出使能事件发生的概率。 6)条件修正：描述条件修正因子取值说明。一般需标明这些假定值的参考依据，且对标准值的任何修改需说明理由并记录在案。 7)中间事件频率：初始事件频率和所有使能事件或使能条件发生概率以及条件修正因子的乘积。 8)独立保护层：写出所有现有的及建议的独立保护层，包括每个独立保护层失效概率。如果独立保护层的失效概率不同于企业内采用的标准值，则需阐明调整理由。 9)后果频率：为考虑已有防护措施和 IPL 后的后果频率。 10)是否满足可容忍风险标准：使用考虑已有防护措施和 IPL 后的后果频率与采用的可容忍风险标准进行比较，假如后果频率小于对应后果分类的可容忍风险标准，则当前风险在可容忍范围内，否则为不满足。 11)仍需完成的降险能力 PFD：假如存在后果频率大于可容忍风险标准的情况，需计算各后果分类仍需完成的降险能力 PFD。 12)满足可容忍风险标准所要求采取的行动：描述未将风险降低至可容忍标准内还需采取的行动内容；假如后果频率大于可容忍风险标准，但企业目前无法采取其他行动，因此不得不接受这样的风险，这种特殊情况可能需要高级管理人员的签字，并附在分析文档中。 13)备注：包括所有背景资料，或记录与场景或采取行动相关的此类信息。 14)参考资料：任何有关的工艺流程图、P&ID、SIF 描述或联锁逻辑图、仪表清单、设备清单、操作规程、测试程序等参考资料，从而完整地记录分析的依据，以便协助审查或执行分析的结果	否		

表 B.1　LOPA 工作质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
37	文档	LOPA 报告要求	在 LOPA 工作会议后，由 LOPA 分析主席和秘书将会议记录进行整理、汇总，形成 LOPA 报告文件，报告宜包括以下内容： 1)项目基本概况； 2)LOPA 工作方法及流程：包括分析目的、LOPA 工作程序、详细步骤等； 3)LOPA 工作实施：包括日程安排、参与人员、参考资料等； 4)工作成果汇总：包括分析结果和所提建议； 5)LOPA 记录表； 6)分析依据的可容忍风险标准； 7)LOPA 工作参与人员签到表	否		

附 录 C
（资料性）
SIL 定级分析记录表与报告示例

SIL 定级分析记录表示例见表 C.1。

表 C.1 SIL 定级分析记录表示例

SIL 定级分析记录表				
SIF 编号				
SIF 名称				
SIF 描述				
所在区域				
运行模式				
分析项目	描述	概率/频率	后果频率	备注
后果描述				
等级				
风险可容忍标准				
场景 1				
初始事件 1				
防护措施 1				
使能事件 1				
场景 2				
初始事件 2				
防护措施 2				
使能事件 2				
中间事件频率				
条件修正（如果适用）	点火事件			
	人在影响区内			
	致死			
	其他			
“中间事件及后果”IPL				
后果频率	人员			
	财产			
	环境			
	声誉			
是否满足风险可容忍标准(是/否)				
本 SIF 需完成的降险能力 PFD/RRF	人员			
	财产			
	环境			
	声誉			
满足风险可容忍标准所要求采取的行动				
备注				

SIL 定级分析报告可参考图 C.1。

目　录

第 1 章　概述 XX

1.1　项目背景 XX
1.2　工作目的及内容 XX
1.3　缩略语 XX

第 2 章　项目概况 XX

2.1　工艺概况 XX
2.2　主要设备及技术参数 XX

第 3 章　保护层分析（LOPA）方法及流程 XX

3.1　LOPA 目的 XX
3.2　本次 LOPA 工作程序 XX
3.3　本次 LOPA 详细步骤 XX

第 4 章　SIL 定级实施 XX

4.1　日程及安排 XX
4.2　研究团队及成员 XX
4.3　参考图纸及文献资料 XX

第 5 章　工作成果 XX

附录 1　SIL 定级分析记录表 XX
附录 2　风险可容忍标准 XX
附录 3　SIL 定级分析会议签名表 XX
附录 4　分析所依据图纸等资料 XX

图 C.1　SIL 定级报告示例

附 录 D
（资料性）
SIL 定级质量控制审查样表

SIL 定级质量控制审查样表，见表 D.1。

表 D.1 SIL 定级质量控制审查样表

SIL 定级质量控制审查样表						
审查：对 SIL 定级的人员、资料、流程和内容、文档 4 个方面进行审查。 **否决项**：SIL 定级报告质量控制的关键要素，若未满足相关审查要求，则本次审查不予通过。 **非否决项**：SIL 定级报告质量控制的一般要素，若发现不符合项，后续需进行整改或优化，审查人员根据实际情况综合研判，得出审查结论。对于非否决项，若不符合项超过 5 项，推荐为审查不通过。						
序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
1	人员、资料、部分流程	LOPA 工作	可按照附录 B“LOPA 工作质量控制审查样表”开展审查	是		
2	流程和内容	确定 SIF 的 SIL	对于低要求运行模式应按照表 5 确定 SIF 的 SIL 要求。对于连续运行模式或高要求模式，应按照表 6 确定 SIF 的 SIL 要求	是		
3			当分析过程中涉及多个 SIF 预防同一危险事件时，对共享或共用硬件、嵌入式软件或应用程序实现的 SIL 能力应提出高于当前分析 SIF 的 SIL 能力要求。 示例：以某储罐高高液位联锁保护为例，其 SIL 要求为 SIL2，在高液位还设置了具有 SIL1 要求的其他联锁保护，两者共用 SIS 控制器和最终执行元件，高液位联锁保护执行单元失效将导致高高液位联锁保护同时失效，则共用的 SIS 控制器和最终执行元件及相关软件或应用程序应实现高于 SIL2 的能力	是		
4	文档	SIL 定级记录表	LOPA 记录表宜包括以下内容。 1）后果描述：包括风险矩阵中的后果分类，以便确定可容忍风险频率。 2）可容忍风险标准：记录表中选取的可容忍风险标准应和后果分类一致，可容忍风险标准的频率值应符合公司可容忍风险标准值。 3）初始事件：记录表中清晰记录场景初始事件，同时给出初始事件频率。 4）防护措施：记录表中记录针对初始事件的防护措施描述及其失效概率。 5）使能事件或使能条件：对初始事件的使能事件或使能条件进行描述，并给出使能事件发生的概率。 6）条件修正：描述条件修正因子取值说明。一般需标明这些假定值的参考依据，且对标准值的任何修改需说明理由并记录在案。	否		

表 D.1　SIL 定级质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
4	文档	SIL 定级记录表	7)中间事件频率:初始事件频率和所有使能事件或使能条件发生概率以及条件修正因子的乘积。 8)独立保护层:写出所有现有的及建议的独立保护层,包括每个独立保护层失效概率。如果独立保护层的失效概率不同于企业内采用的标准值,则需阐明调整理由。 9)后果频率:为考虑已有防护措施和 IPL 后的后果频率。 10)是否满足可容忍风险标准:使用考虑已有防护措施和 IPL 后的后果频率与采用的可容忍风险标准进行比较,假如后果频率小于对应后果分类的可容忍风险标准,则当前风险在可容忍范围内,否则为不满足。 11)本 SIF 仍需完成的降险能力 PFD/RRF:假如存在后果频率大于可容忍风险标准的情况,需计算各后果分类仍需完成的降险能力 PFD/RRF。 12)满足可容忍风险标准所要求采取的行动:描述未将风险降低至可容忍标准内还需采取的行动内容;假如后果频率大于可容忍风险标准,但企业目前无法采取其他行动,因此不得不接受这样的风险,这种特殊情况可能需要高级管理人员的签字,并附在分析文档中。 13)备注:包括所有背景资料,或记录与场景或采取行动相关的此类信息。 14)参考资料:任何有关的工艺流程图、P&ID、SIF 描述或联锁逻辑图、仪表清单、设备清单、操作规程、测试程序等参考资料,从而完整地记录分析的依据,以便协助审查或执行分析的结果	否		
5		SIL 定级报告	在 SIL 定级会议后,由分析主席和秘书将会议记录进行整理、汇总,形成 SIL 定级报告文件,报告宜包括以下内容: 1)项目基本概况; 2)SIL 定级方法及流程:包括分析目的、SIL 定级工作程序、详细步骤等; 3)SIL 定级实施:包括日程安排、参与人员、参考资料等; 4)工作成果汇总:包括分析结果和所提建议; 5)SIL 定级记录表; 6)分析依据的可容忍风险标准; 7)SIL 定级工作参与人员签到表	否		

附 录 E
（资料性）
SIL 验证工作表与报告示例

SIL 验证工作表示例见表 E.1。

表 E.1 SIL 验证工作表示例

SIL 验证工作表								
SIF 编号								
SIF 名称								
SIF 描述								
所在区域								
运行模式								
回路构成								
设备名称	设备位号	厂家型号	表决结构	MTTR/h	TI/h	PTC	T_d/h	MRT/h
数据分析								
厂家型号			λ_{DD}	λ_{DU}	λ_{SD}	λ_{SU}	β	β_D
可靠性框图/故障树/马尔可夫状态转移图								
分析计算结论								
回路 PFD_{avg}/PFH 值			随机失效 SIL	架构约束 SIL	实际 SIL	实际 RRF	要求 SIL	要求 RRF
随机失效			PFD_{avg}/PFH		MTTF		SIL_{pfd}	
传感单元								
逻辑单元								
执行单元								
架构约束			SILac					
传感单元								
逻辑单元								
执行单元								
PFD/PFH 分布图					MTTF 分布图			
建议								

SIL 验证报告可参考图 E.1。

目　录

第 1 章　验证概况 XX
1.1　项目背景 XX
1.2　工作目的及内容 XX
1.3　缩略语 XX
第 2 章　SIL 验证原理及流程 XX
2.1　硬件安全完整性的架构约束 XX
2.2　硬件随机失效的安全完整性等级要求 XX
2.3　SIL 验证方法流程 XX
2.4　验证说明 XX
第 3 章　SIL 验证实施 XX
3.1　研究团队及成员 XX
3.2　参考图纸及文献资料 XX
第 4 章　工作成果 XX
4.1　SIL 验证结果汇总 XX
附录 1　SIL 验证工作表 XX
附录 2　SIL 验证用数据 XX

图 E.1　SIL 验证报告示例

附 录 F
（资料性）
SIL 验证质量控制审查样表

SIL 验证质量控制审查样表，见表 F.1。

表 F.1 SIL 验证质量控制审查样表

SIL 验证质量控制审查样表						
审查：对 SIL 验证的人员、资料、流程和内容、文档 4 个方面进行审查。 **否决项**：SIL 验证报告质量控制的关键要素，若未满足相关审查要求，则本次审查不予通过。 **非否决项**：SIL 验证报告质量控制的一般要素，若发现不符合项，后续需进行整改或优化，审查人员根据实际情况综合研判，得出审查结论。对于非否决项，若不符合项超过 5 项，推荐为审查不通过。						
序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
1	人员	人员构成	SIL 验证小组由主席、秘书、参与人员组成。SIL 验证主席和秘书来自验证单位，参与人员来自运行单位、验证单位、设计方，必要时还包括承包商	否		
2		独立性	SIL 验证主席应是独立的，独立等级应按照 GB/T 20438.1—2017 中 8.2 执行，项目设计的人员或项目组其他相关人员配合评估组参与评估活动。 分析对象的危险事件后果可能致人员伤亡的宜由独立部门执行，后果可能致多人伤亡的宜由独立第三方执行	是		
3		人员能力	SIL 验证主席能力应满足下列要求： 1)SIL 验证主席具有 SIL 验证经验，能熟练使用计算软件和数据库； 2)SIL 验证主席应掌握 SIL 验证方法，熟悉仪器仪表，对 GB/T 20438(所有部分)、GB/T 21109(所有部分)有深入研究，接受过行业权威机构 SIL 验证、GB/T 20438(所有部分)、GB/T 21109(所有部分)标准技术培训，取得培训合格证书。 3)SIL 验证主席具有行业认可的功能安全资质，且具有不少于 10 项 SIL 验证项目经验	是		
4			SIL 验证参与人员能力应满足下列要求： 1)SIL 验证组成员了解 GB/T 20438(所有部分)、GB/T 21109(所有部分)，并经过培训； 2)SIL 验证组成员应具备所分析对象相同或相似领域 SIL 验证项目经验，以确保验证结果的合理可信； 3)SIL 验证单位参与项目的高级资质人员不应少于 2 名	否		

表 F.1　SIL 验证质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
5	资料	SIL 验证输入资料	SIL 验证的输入资料宜包括： 1)SIL 定级报告(需明确 SIL 等级和 PFD_{avg}/RRF 值)； 2)运行模式说明； 3)P&ID； 4)SRS； 5)安全联锁功能列表、功能描述、设定点、回路结构； 6)安全联锁逻辑图或因果表； 7)SIF 组成仪表设备的厂家、型号、仪表类型/原理、投用时间、量程等信息； 8)经过认证的仪表设备需提供合规的 SIL 证书、评估报告及安全手册等认证材料； 9)维检修规程； 10)功能性测试报告； 11)以前的设备故障记录(提供审阅后收回)； 12)其他所需资料	否		
6	流程和内容	SIL 验证原理	如果是硬件安全完整性验证应通过分析和定量计算的方式确认 SIF 是否满足 SIL 要求；如果是系统性安全完整性验证应通过定性分析的方式确认是否满足要求；若开展的是回路综合的 SIL 验证，则应包含硬件安全完整性验证和系统性安全完整性验证	否		
7		SIL 验证方法	应在报告中明确本次 SIL 验证采用的方法和相关说明	否		
8		验证对象确定	依据 SRS、SIL 定级报告、安全联锁功能列表、安全联锁逻辑图或因果表辨识出待验证的 SIF	是		
9		回路结构定义	应明确参与 SIF 的仪表设备、安全关键动作及其逻辑/冗余关系，包括回路执行到哪一步即可进入安全状态，安全状态的定义只针对当前 SIF 所保护场景的降险需求，出于维护或装置再启动等相关安全或便捷考虑的执行动作不宜纳入 SIL 验证计算。 **注 1**：例如，停机回路到继电器还是到执行器。 **注 2**：例如：煤浆气化炉超温联锁停机执行单元只需考虑氧气进料切断，煤浆给料阀等其他动作一般不纳入 SIL 验证计算。	否		
10		SIL 验证现场调研	SIL 验证工作通常采取现场调研的形式，对 SIF 进行梳理，获取 SIF 的完整信息，包括每一条 SIF 的传感(输入)子系统、逻辑子系统到执行(输出)子系统的完整信息	否		

表 F.1　SIL 验证质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
11	流程和内容	SIL 验证现场调研	验证调研人员应准确记录调研信息。SIL 验证调研工作记录表宜包括如下信息： 1)SIF 编号； 2)SIF 名称； 3)SIF 功能描述、运行模式； 4)SIF 回路传感器位号、设备厂家、型号、类型/原理、投用时间、运行条件、表决机制、诊断设置、共用性情况等数据； 5)SIF 回路逻辑解算器设备厂家、型号、投用时间、运行条件、表决机制、诊断设置、共用性情况等数据； 6)SIF 回路执行器位号、设备厂家、型号、类型/原理、投用时间、运行条件、表决机制、诊断设置、共用性情况等数据； 7)SIF 回路其他单元(如浪涌保护器、安全栅、信号分配器、继电器等)设备厂家、型号、投用时间、运行条件、表决机制、诊断设置、共用性情况等数据； 8)MTTR/MRT,设备的备品备件情况； 9)SIF 设备检验测试方案(以确认 PTC)以及 TI	否		
12		调研内容分析	根据调研确认 SIF 运行模式	否		
13			根据调研确认每一条 SIF 回路结构信息,包括传感单元、逻辑单元、执行单元、安全栅、浪涌保护器、信号分配器、输入输出卡件、继电器、端子排接线方式等	否		
14			根据现场调研确认 SIF 组成设备的完整信息,确定符合现场实际的各设备 λ_{DD}、λ_{DU}、λ_{SD}、λ_{SU},确定方式包括： 1)采用认证数据作为验证输入：应将认证证书和功能安全评估报告及安全手册作为数据来源,并确认现场使用环境和条件与认证证书和功能安全评估报告或安全手册要求一致； 2)采用 FMEDA 方法基于数据库或以往使用数据开展失效率分配； 3)采用可信数据库作为数据来源	否		
15			根据 GB/T 20438(所有部分)要求计算 SFF 或 DC	否		
16			根据调研确认 TI	否		
17			根据调研确认检验测试方案以估计 PTC	否		
18			根据调研确认设备 MTTR 及 MRT	否		
19			根据调研确认 SIF 回路传感单元、逻辑单元以及执行单元的冗余情况,确定各单元的 HFT	否		

表 F.1　SIL 验证质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
20	流程和内容	硬件安全完整性	根据 SIF 的回路构成，确定各单元的表决结构，完成 SIL 验证分析建模	是		
21			根据 GB/T 20438（所有部分）、GB/T 21109（所有部分）确定硬件安全完整性的架构约束。 SIS 或者 SIS 子系统的最小 HFT 要求按照以下任一种方式确定： 1）GB/T 21109.1—2022 中的 11.4.5～11.4.9； **注**：在依据表 7 确定要求的最小 HFT 时，还需同时满足以下内容： • FVL 和 LVL 可编程装置的诊断覆盖率不小于 60%； • 失效量计算中使用的可靠性数据应由不小于 70%的统计上界置信区间确定。 2）GB/T 20438.2—2017 中的 7.4.4.2（路线 1_H）； 3）GB/T 20438.2—2017 中的 7.4.4.3（路线 2_H）	是		
22			应在报告中明确 PFD_{avg}/PFH 计算基于的假设	是		
23			应根据 GB/T 20438.6—2017 中附录 B 计算 SIF 的 PFD_{avg} 或 PFH，依据表 5 和表 6 确定硬件随机失效的 SIL	是		
24			SIF 硬件安全完整性的 SIL 取架构约束的 SIL 与硬件随机失效的 SIL 中的低值	是		
25			若使用 SIL 验证计算工具，应采用权威机构认可的数据库和软件	是		
26		系统性安全完整性	对各 SIF 回路包含设备的系统性失效、检测到故障时的系统行为等方面宜采用工作表形式进行分析，分析内容包括： 1）对控制系统性故障的分析（依据 GB/T 20438.2—2017 中的 7.4.7）； 2）应用程序的符合性分析（依据 GB/T 21109.1—2017 中的第 12 章）； 3）对设计和集成过程中可能存在的失效分析（依据 GB/T 20438.2—2017 中的 7.4.6）； 4）检测到故障时的系统行为分析（依据 GB/T 20438.2—2017 中的 7.4.8，GB/T 21109.1—2022 中的 11.3）	否		
27			采用认证证书作为验证输入时，可采信 SIF 设备经认证的系统性能力			

表 F.1　SIL 验证质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
28	流程和内容	系统性安全完整性	SIF 设备发生故障时的系统行为分析时，应根据 SIL 验证调研确认 SIF 回路及其所包含设备的故障检测/诊断措施，分析其响应机制： 1)若响应方式为将系统导入安全状态，则需确认响应时间、安全状态、超驰/旁路设置等是否满足要求； 2)若响应方式为报警，则需确认人员响应是否有操作规程要求并确保人员在过程安全时间内及时采取动作。 3)对于对动力源（如电源、空气、液动源或气动源）中断而不进入安全状态的所有 SIS 设备，应确认已对共用动力源丢失和 SIS 电路完整性设置有检测和报警措施（如线路终端监视、供压测量、液压或气压检测）并根据 GB/T 21109.1—2022 中的 11.3 采取行动。 **注 1**：通过使用辅助动力源（如备用电池、不间断电源、储气罐、液压蓄能器、第二气源）来提高动力源完整性。 **注 2**：动力源中断可能影响多个 SIF，甚至多个 SIS。因此需考虑多个 SIF 的共因失效。	否		
29		SIL 验证建议	针对验证结果显示不能满足 SIL 要求的安全功能回路应进行分析，确认是传感单元、逻辑单元还是执行单元的随机失效或架构约束不满足 SIL 要求，分析其架构及 PFD_{avg}/PFH 分布，给出合理的建议，使回路的安全完整性达到要求	否		
30			在役装置 SIL 评估建议措施应当及时关闭，不能及时落实或者关闭的，应落实替代的风险控制措施，确保风险受控。 **注 1**：当 SIF 的 SIL 定级结果发生变化或者实际的回路配置发生变化时，需及时进行 SIL 验证复核，确保变更后的 SIF 的 SIL 满足要求。 **注 2**：建议包括缩短检验测试间隔到多长时间，如何调整检修方案，推荐的诊断设置方案，推荐的设备结构配置，推荐的设备选型等。	否		

表 F.1　SIL 验证质量控制审查样表（续）

序号	控制要素	控制要求	审查内容及要求	是否为否决项	是否满足要求	存在问题描述
31	文档	SIL 验证工作表	根据 SIL 验证调研表的信息，确定回路配置信息和维护信息，应建立 SIL 验证工作表，完成 SIL 验证分析计算，给出 SIL 验证结论。SIL 验证工作表至少包括以下内容： 1）项目名称； 2）SIF 编号、SIF 名称、SIF 描述； 3）回路中各设备的名称、位号、厂家型号、表决结构、MTTR、MRT、TI 等； 4）回路中各设备的 λ_{DD}、λ_{DU}、λ_{SD}、λ_{SU} 或 PFD_{avg}/PFH 数据，以及共因失效因子 β、β_D； 5）绘制的可靠性框图/故障树/马尔可夫状态转移图； 6）经分析计算得出的回路传感、逻辑、执行各部分的 PFD_{avg}/PFH 值、架构约束的 SIL； 7）经分析计算得出的回路 PFD_{avg}/PFH 值、随机失效的 SIL、架构约束的 SIL； 8）回路实际的 SIL 能力与要求的 SIL； 9）SIL 验证建议	否		
32		SIL 验证报告	在 SIL 验证分析完成后，验证人员将调研表、SIL 验证工作表进行整理、汇总，形成 SIL 验证报告文件。编制 SIL 验证的最终报告，报告宜包括以下内容： 1）验证概况； 2）SIL 验证方法及流程、验证假设等相关说明； 3）验证实施：包括参与人员、输入资料及实施计划安排等； 4）验证结果汇总：包括计算结果和所提建议，必要时可包括企业相应的整改计划； 5）验证工作表； 6）验证使用数据及来源； 7）验证调研工作参与人员签到表； 8）SIL 验证主席的简历和资质信息	否		

参 考 文 献

[1] GB/T 20438.3—2017 电气/电子/可编程电子安全相关系统的功能安全 第3部分:软件要求

[2] GB/T 20438.4—2017 电气/电子/可编程电子安全相关系统的功能安全 第4部分:定义和缩略语

[3] GB/T 20438.6—2017 电气/电子/可编程电子安全相关系统的功能安全 第6部分:GB/T 20438.2 和 GB/T 20438.3 的应用指南

[4] GB 36894 危险化学品生产装置和储存设施风险基准