浅谈安全仪表系统的安全完整性评估方法

李鹏

洛阳智达石化工程有限公司

摘要：介绍了安全仪表系统在过程工业应用中的安全完整性评估方法，重点阐述了安全完整性等级的定级和验证方法，为安全仪表系统的完整性评估提供依据。

关键词：安全仪表功能；安全完整性等级；失效概率；保护层分析

近年来，随着社会经济的发展、安全意识的提高以及国家相关法律法规的出台，安全仪表系统（SIS）被提出，并广泛应用于石化行业内。安全仪表系统（SIS）在降低事故风险发生概率、维持工艺过程处于安全状态发挥了重要作用。

安全仪表系统（SIS）在装置生产正常时处于休眠或静止状态，一旦生产装置或设施出现可能导致安全事故的情况时，能够瞬间准确动作，使生产过程安全停止运行或自动导入预定的安全状态，如果安全仪表系统（SIS）失效，往往会导致严重的安全事故[1]。

应急管理部（原国家安全监管总局监督监管三司）在2014年发布了关于加强化工安全仪表系统管理的指导意见的116号文件，文件对加强化工安全仪表系统管理、预防和减轻石油化工企业危险事故的发生提出了明确要求和相关指导意见，并且要求各使用化工企业积极推进安全仪表系统的评估工作。

1　安全仪表系统的相关概念

原国家安监总局三司在2014年发布了关于加强化工安全仪表系统管理的指导意见的116号文中指出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、可燃气体及火灾检测保护系统等[1]。

GB/T21109《过程工业领域安全仪表系统的功能安全》第一部分中将安全仪表系统的定义为：用于执行一个或多个安全仪表功能（SIF）的仪表系统。SIF针对特定的危险事件（人员伤害、财产损失、环境影响或声誉影响），意图使工艺过程达到或保持在安全状态，SIF应取得所需的安全完整性等级（SIL）[2]。

安全完整性等级（SIL）是指在规定时间、条件下，安全仪表系统成功执行所要求的安全功能的概率[3]。安全仪表功能(SIF)是通过安全仪表系统(SIS)执行的、具有特定安全完整性等级(SIL)的安全功能，将被控工艺对象置于或保持在安全状态[3]。要求时的失效概率（PFD）是指系统要求独立保护层（IPL）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]。

为有效地防止事故场景向不期望的后果发展，需要一种保护措施，并且该保护措施与该事故场景发生的原因或其他保护措施无关，该保护措施可以是一种设备、系统或者行动，该保护措施称之为独立保护层（IPL）。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[3]。

安全仪表功能（SIF）的操作模式分为：低要求模式、高要求模式和连续模式。石化行业的安全仪表功能（SIF）的操作模式一般为低要求模式。安全功能仅在要求时执行动作，以便将工艺过程置于特定的安全状态[4]。

为在识别出石油化工装置工艺系统中潜在的危害和操作性问题，一般采用一种结构化和系统化的检查技术，即危险与可操作性分析（HAZOP），这是一种工艺灾害识别方法（PHA）。通过这种分析可以有效地识别出石油化工装置工艺系统中存在的中高风险项。

基于危险与可操作性分析(HAZOP)的分析结果，进一步采用保护层分析（LOPA）方法来评估事故场景的发生的风险，以确定现有保护措施的风险降低是否在可接受的范围内，是否需要增加其他的保护措施来降低现有的事故风险。这一分析过程称之为安全完整性定级。

安全仪表系统的安全完整性评估不仅仅是安全仪表完整性定级，同时还包含安全仪表完整性验算。下文将重点介绍安全仪表完整性定级和安全仪表完

整性验算的方法。

2　安全完整性等级定级方法

2.1　平均失效概率与安全完整性等级的关系

安全完整性等级（SIL）定级可分为 SIL1、SIL2、SIL3、SIL4 四级。石油化工行业中安全仪表功能（SIF）的安全仪表完整性等级最高为 SIL3 级。SIL 等级越高意味着安全仪表功能的失效率越低。其对应关系见表 1。

表 1　安全完整性等级（摘自 GB/T50770）[4]

安全完整性等级	低要求模式下的平均失效概率
1	$10^{-2} \leqslant PFDavg < 10^{-1}$
2	$10^{-3} \leqslant PFDavg < 10^{-2}$
2	$10^{-4} \leqslant PFDavg < 10^{-3}$

2.2　定级方法介绍

IEC-61511-3 提供的安全仪表完整性等级的定级方法主要有：矩阵法、风险图法、保护层分析法和定量风险分析法。目前通常依据 AQ/T—3054—2015《保护层分析（LOPA）方法应用导则》和 GB/T—32857—2016《保护层分析 (LOPA) 应用指南》进行保护层分析方法（LOPA）来确定安全仪表完整性等级定级。

保护层分析是在确定初始事件概率及后果危险性等级的基础上，进一步对事故场景的风险进行半定量化的分析，识别现有的已设置的合理保护措施，并通过分析现有保护措施中的独立保护层，并确认独立保护层可降低的风险倍数，进一步判断该事故场景发生的概率能否满足企业要求的可容许风险标准，并根据分析结果确定是否需要增加其他的保护措施，其目的是把事故风险发生的概率尽可能合理地降低至风险标准所要求的可容许概率。通过保护层分析可以计算出每个安全仪表功能所对应的安全完整性等级要求。

2.3　保护层分析法分析流程

LOPA 分析前首要需要确定风险矩阵及风险可接受标准（一般在 HAZOP 分析前应确定）。风险可接受标准的选择尤为重要，采用过低的风险接受标准可能导致评估结果不满足规范要求，采用过高的风险接受标准评估结果虽然满足国家要求，但是评估结果对于 SIF 回路的子系统配置要求更为苛刻。因此采用合理的风险可接受标准是 LOPA 分析的重要一步。其次根据 HAZOP 分析并从中挑取初始风险为高及以上的事故场景，并确定该场景的初始事件及相应频率。再次分析出此事故场景的独立保护层、条件修正因子以及使能条件，同时需分析出相应的 PFD。然后根据风险矩阵及风险可接受标准确定在此事故场景下最终可接受频率。最后将叠加保护层、条件修正因子以及使能条件后的后果发生频率与最终可接受频率进行比较，确定是否需要配置额外的 SIF 回路以及相应回路所要求的 SIL 等级。保护层分析流程如图 1 所示。

在 LOPA 分析过程中，需要重点关注初始事件（IE）、使能事件、条件修正因子、独立保护层（IPL）频率的确定，因为这些都会影响定级的最终结果。

初始事件频率、独立保护层（IPL）频率的来源可以参考《保护层分析（LOPA）方法应用导则》AQ/T 3054—2015，也可以参考其他公开数据等来确定事件发生频率。通常情况下企业的经验数据往往可以更好地反映企业实际情况，但目前很少企业能做到这种统计性分析，所以这部分数据还无法应用到实际的定级过程中。

因此 LOPA 分析会议时需要企业的工艺、仪表、设备及安全人员参与对相关数据进行确认或修正，以便评估结果更能反映企业实际情况。

2.4　独立保护层的评估

独立保护层（IPL）是一种防止事故场景向不期望后果发展的设备、系统或行动。每个独立保护层都必须具备独立性、有效性、安全性及可审查性的特性。

石化企业典型的保护层有：本质安全设计、BPCS 系统、设置报警同时操作人员有相关响应、安全仪表功能、物理保护措施以及事故发生后的保护设施。

独立保护层（IPL）必须有防止随意的或未经授权批准的变更的预防措施，变更管理需要执行比其他变更更为严格的变更程序，同时应有足够且详细的设计文件、调试记录、测试记录和运行记录等文件。

2.5　事故场景发生频率定量计算

事故场景的发生频率一般按式（1）计算：

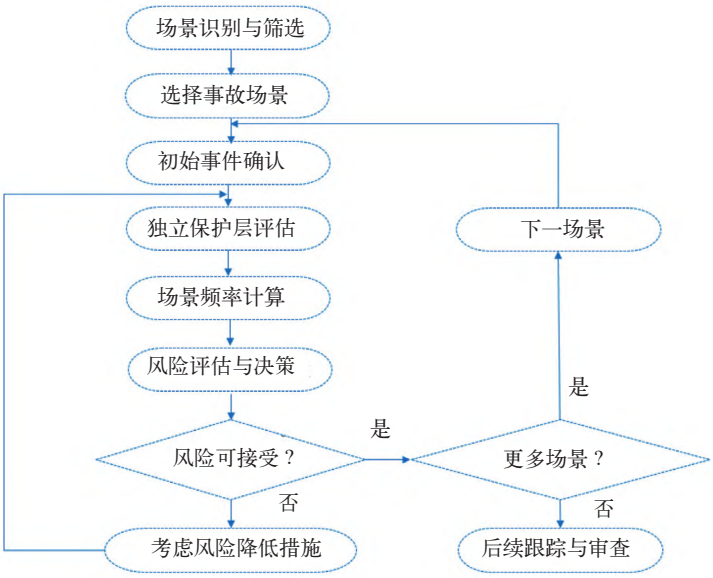

图 1　LOPA 分析流程

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

式中 f_i^c——初始事件或原因 i 所导致后果 C 的发生频率，单位为 / 年；

f_i^I——初始事件或原因 i 的发生频率，单位为 / 年；

PFD_{ij}——初始事件或原因 i 中第 j 个阻止后果 C 发生的 IPL 的失效概率。

在根据需要对事故场景进行修正时，事故场景的发生频率一般按式（2）和式（3）计算。

a）存在使能条件时：

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

式中 f_i^E——使能条件发生概率，单位为 / 年；

2）采用点火概率、人员暴露概率和死亡概率对后果频率进行修正：

$$f_i^c = f_i^I \times f_i^E \times P_{ig} \times P_{ex} \times P_d \times \prod_{j=1}^{J} PFD_{ij f_i^I} \quad (3)$$

式中 P_{ig}——点火概率；

P_{ex}——人员暴露概率；

P_d——人员受伤或死亡概率。

注：对于毒性介质造成的事故影响，不需要考虑点火概率。

3 安全完整性等级验证方法

进行安全仪表完整性等级验证的目的是检验设计的 SIF 回路的实际可达到的安全完整性等级是否满足安全仪表系统的安全完整性等级（SIL）定级的要求。SIL 等级的验证仅需要验证 SIL 等级大于等于 1 的 SIF 回路。

通常采用的验证方法主要有故障树、可靠性方块图以及马尔科夫模型。

3.1 验算流程

安全仪表完整性等级验证的主要步骤如图 2 所示。

3.2 平均失效概率量化

安全仪表系统的 SIF 回路各子系统的平均失效概率之和构成回路的平均失效概率：

$$PFD_{SIS}=PFD_S+PFD_L+PFD_{FE} \quad (4)$$

式中 PFD_{SIS} —— 安全仪表系统的平均失效概率；

PFD_S——检测单元的平均失效概率；

PFD_L ——逻辑控制单元的平均失效概率；

PFD_{FE} —— 执行单元的平均失效概率。

根据检测单元、逻辑控制单元以及执行单元的不同配置，采用不同的方法进行 PFD 计算。根据检测单元、逻辑控制单元以及执行单元的选型，选择相应的可靠性数据进行每一部分的 PFD 计算。SIF 回路的 PFD 是检测单元、逻辑控制单元以及执行单元的 PFD 之和，根据回路 PFD 大小判断其是否满足所需 SIL 等级要求。如果回路计算所得的 PFD 不大于所需的 PFD，则说明现有的 SIF 回路配置可以满足 SIL 等级要求；如果回路计算所得的 PFD 大于所需的 PFD，则说明现有的 SIF 回路配置不满足所需 SIL 等级的要求，需要对回路的配置进行调整。

3.3 结构约束及系统能力

基于 IEC—61508 路径 1 认证的各类子系统的结构性约束见表 2。

硬件子系统的失效分为可检测的安全失效、可检测的危险失效、不可检测的安全失效以及不可检测的危险失效。可检测的危险失效可以是子系统转入安全状态，等同于安全失效。安全失效分数是安全失效概率与总失效概率之比。

硬件故障裕度是指子系统在出现故障或偏差的情况下，功能单元可以按照要求继续执行所要求功能的能力，代表了子系统对硬件危险的容忍度。例如二取一的子系统，其硬件故障裕度为 1。

子系统的类型一般有 A 型和 B 型

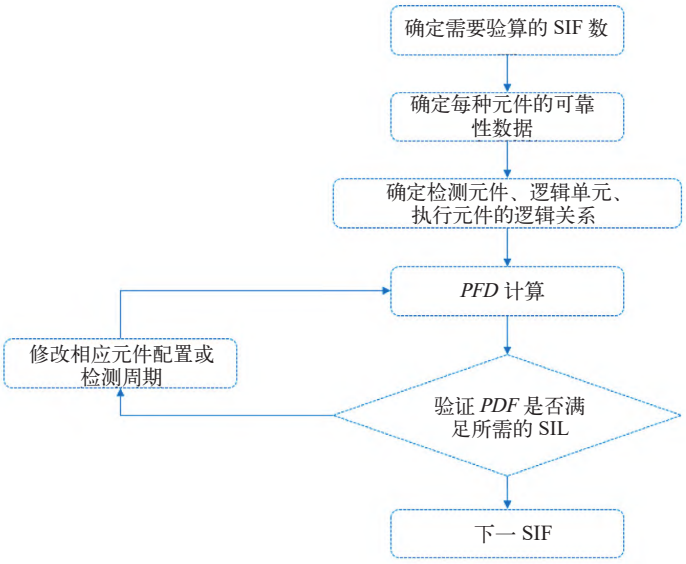

图 2 安全仪表完整性验证流程

表 2 结构约束

安全失效分数	A 型子系统			B 型子系统		
	硬件故障裕度			硬件故障裕度		
	0	1	2	0	1	2
< 60%	SIL1	SIL2	SIL3	NA	SIL1	SIL2
60% ~ 90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
90% ~ 99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4

之分，主要区别如下：A 型子系统是结构简单的子系统，其失效模式可以完整定义，失效行为可以完全确定，并且能够获取足够的失效概率数据。石油化工行业内常见的 A 型子系统有：热电偶、热电阻、机械开关型仪表、电磁阀、阀门、继电器等。B 型子系统是结构复杂的子系统，其失效模式无法完整定义、失效行为无法完全确定、无法获取足够的失效概率数据。石油化工行业内常见的 B 型子系统有：智能变送器、可编程控制器等。系统能力是系统安全完整性的度量，用 SC1 到 SC4 表示。一个 SILn 的子系统的系统能力为 SCn。

3.4 验算结果的确定

SIF 回路的 SIL 等级最终能否满足回路定级的要求，需要 3 方面条件同时满足才能确定。首先系统结构约束必须达到相应的 SIL 等级要求，其次回路要求的失效概率要在所需的失效概率范围之内，再次各子系统的系统能力必须达到 SC N[5]。

4 结论

综上所述，安全仪表系统的评估对于安全仪表系统正确地执行安全功能至关重要。目前，安全仪表系统在设计、安装、调试和维护等生命周期各阶段，还存在着风险分析不完全、设计选型不严谨、结构设置不理想、使用维护管理不健全等问题，因此需要加强和规范安全仪表系统管理、完善安全仪表系统的评估，通过安全仪表系统的安全完整性评估使得安全仪表系统在风险分析、设计选型、结构设计等方面更合理、更完善，从而将石油化工装置的潜在风险发生的可能性降到最低，保障人民生命和财产的安全。

参考文献：

[1] 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 [A/OL]. (2014-11-05) . http://www.mem.gov.cn/.

[2] 过程工业领域安全仪表系统的功能安全 : GB/T 21109—2007[S]. 北京 : 中国标准出版社 , 2007.

[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[S]. 北京 : 中国标准出版社 , 2017.

[4] 石油化工安全仪表系统设计规范 : GB/T 50770—2013 [S]. 北京 : 中国标准出版社 , 2013.

[5] 张建国 . 安全仪表系统在过程工业中的应用 [M]. 北京 : 中国电力出版社 , 2010.

（上接83页）

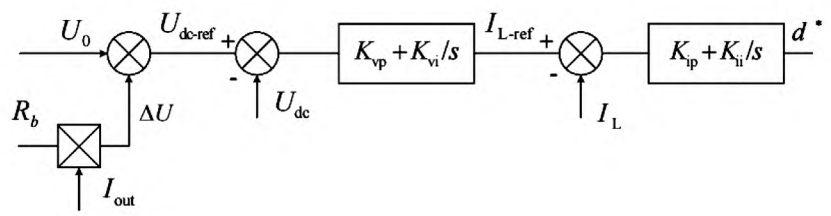

图 5 传统下垂控制框图

调控制性能和运行可靠性。

4）超级电容器的自抗扰控制策略。超级电容器作为微网系统中短时间高功率输出的关键储能单元，其控制策略需兼顾动态响应与鲁棒性。本文引入线性自抗扰控制（LADRC）替代传统 PI 控制，通过构建包含跟踪微分器、扩张状态观测器（LESO）及误差反馈控制器的控制架构，实现对母线电压的快速稳压控制。LADRC 无需依赖精确系统模型，能够实时估算系统扰动并动态补偿，使系统对光伏波动或负载突变具备更强的响应能力。相比于传统 PI 控制，LADRC 在母线电压控制方面表现出更低的超调率和更短的响应时间，有效保障了微网系统的动态稳定性和抗干扰能力，提升了超级电容器在复杂运行条件下的控制性能。

4 结论

本文基于光伏发电 - 制氢 - 混合储能智能微网构架，系统分析了电压变换、能量调控及控制策略设计，提出了多种优化方法，并通过仿真验证其稳定性与高效性。研究表明：模糊 MPPT 提升了发电效率，PI 制氢控制保障了电解稳定运行，改进下垂控制和 LADRC 显著增强了储能系统的动态响应与母线电压稳定性。

参考文献：

[1] 席嫣娜 , 鞠力 , 丁瑜 , 等 . 离网光储氢微网储能配置优化的混合构网型控制策略 [J]. 电力自动化设备 , 2025,45(1):1-13.

[2] 胡启明 . 硫酸铁高效催化氢化镁水解制氢研究 [J]. 工业催化 ,2025, 33(1):58-63.

[3] 李欣 , 韦古强 , 强同波 , 等 . 压缩空气储能与氢能耦合系统的研究进展 [J]. 发电技术 ,2025, 45(1):1-17.

[4] 荆捷 , 董砚 , 杨富荃 . 孤岛风电制氢系统日前及实时能量管理 [J]. 科学技术与工程 ,2025,25(1):210-218.

[5] 孔令国 , 范乃文 , 石振宇 , 等 . 风 - 储 - 氢 - 燃机协同平抑功率波动运行配置策略 [J]. 高电压技术 , 2025,45(1):1-14.