仪表自动化系统在化工生产过程中的安全性评估

郑亚斌
山西焦化集团有限公司　山西　临汾　041606
山西德力信电子科技有限公司　山西　临汾　041606

摘　要：随着现代化工产业的快速发展，生产装置日益复杂化、大型化和连续化，对过程控制的安全性、可靠性提出了更高要求。仪表自动化系统（IAS）作为化工生产过程的“神经中枢”，在保障工艺稳定、提升效率的同时，其自身的安全性直接关系到人员、设备和环境的安全。本文系统阐述了仪表自动化系统在化工生产中的核心作用，深入分析了其潜在的安全风险来源，重点探讨了基于功能安全标准（如IEC61511）的安全生命周期管理方法，并详细介绍了危险与可操作性分析（HAZOP）、保护层分析（LOPA）以及安全仪表系统（SIS）验证等关键评估技术。最后，结合当前工业4.0与数字化转型背景，展望了人工智能、数字孪生等新技术在提升仪表自动化系统安全性方面的应用前景，并提出了强化人员培训、完善管理体系等综合建议，旨在为化工企业构建更安全、更可靠的生产环境提供理论支撑与实践指导。

关键词：仪表自动化系统；化工安全；功能安全；IEC61511；HAZOP；LOPA；安全仪表系统（SIS）

引言

化工生产过程通常涉及高温、高压、易燃、易爆、有毒、有害等危险介质，任何一个微小的工艺偏差或设备故障都可能引发灾难性的后果，如火灾、爆炸或大规模泄漏，造成严重的人员伤亡、财产损失和环境污染。历史上，诸如印度博帕尔毒气泄漏、美国德克萨斯城炼油厂爆炸等重大事故，其根本原因之一都指向了过程控制与安全保护系统的失效。在此背景下，仪表自动化系统的重要性日益凸显。它不仅承担着对温度、压力、流量、液位、成分等关键工艺参数的实时监测与精确控制，更是构成化工过程安全保护体系的核心。一个设计合理、运行可靠、维护得当的仪表自动化系统，能够有效预防事故的发生，或在事故发生初期迅速采取措施，将风险降至最低。然而，仪表自动化系统本身并非绝对可靠。传感器漂移、执行器卡涩、控制器逻辑错误、软件缺陷、网络攻击以及人为操作失误等因素，都可能导致系统功能异常，进而削弱甚至完全丧失其安全保障能力。因此，对仪表自动化系统进行系统化、科学化的安全性评估，已成为现代化工企业安全管理不可或缺的关键环节。

1 仪表自动化系统在化工生产中的角色与风险

1.1 核心功能与作用

在现代化工厂中，仪表自动化系统主要由三大层级构成：现场仪表层、过程控制层和操作监控层。（1）现场仪表层：包括各类传感器（如热电偶、压力变送器、流量计）和执行器（如调节阀、开关阀、电机）。它们是系统的“感官”和“手脚”，直接与工艺过程交互，负责采集原始数据和执行控制指令。（2）过程控制层：以分布式控制系统（DCS）或可编程逻辑控制器（PLC）为核心，接收来自现场仪表的数据，根据预设的控制算法（如PID控制）进行运算，并向执行器发出指令，以维持工艺参数在设定的安全、高效范围内。（3）操作监控层：通常由操作员站（HMI/SCADA）组成，为操作人员提供直观的人机界面，用于监视整个生产过程、干预控制回路、处理报警信息以及进行生产调度。除了基本的控制功能外，仪表自动化系统还承担着至关重要的安全保护功能。当工艺过程因设备故障、操作失误或外部干扰等原因偏离正常工况，并可能达到危险状态时，安全仪表系统（SIS）——作为仪表自动化系统的一个独立子系统——会被触发，执行预设的安全动作（如紧急停车、切断物料、泄压等），将过程带入一个安全状态。

1.2 安全风险来源分析

尽管仪表自动化系统是安全的守护者，但其自身也存在多种失效模式，构成了潜在的安全风险源。（1）硬件随机失效：这是由元器件老化、磨损、环境应力（如振动、温度、湿度）等因素引起的不可预测的物理失效。例如，压力变送器的膜片破裂导致读数失真，或电磁阀线圈烧毁导致阀门无法动作[1]。（2）系统性失效：这类失效源于设计、制造、安装、操作或维护过程中的错误，具有可预见性和可预防性。常见原因包括：控制逻辑错误、安全联锁逻辑不完整、未考虑共因失效（CommonCauseFailure,CCF）等。嵌入式软件或应用软件中的逻辑错误、边界条件处理不当、未经过充分测试等。

操作员误操作（如错误地旁路安全联锁）、维护人员错误的校准或组态修改。随着工业控制系统（ICS）与企业信息网络的融合，系统面临来自外部的网络攻击风险，如恶意软件、拒绝服务攻击（DoS）或数据篡改，可能导致系统失控。（3）环境与外部因素：雷击、电网波动、电磁干扰（EMI）等外部事件也可能干扰仪表自动化系统的正常运行，导致信号失真或设备损坏。

对这些风险来源的清晰认知，是开展有效安全性评估的前提。

2 功能安全理念与标准框架

2.1 功能安全的定义与核心

功能安全（FunctionalSafety）是指与受控设备（EUC）及其控制系统相关的整体安全的一部分，其目标是确保安全相关系统在发生随机硬件失效、系统性失效或操作指令时，能够以足够高的置信度正确地执行其安全功能。简言之，功能安全关注的是“系统在需要时能否正确地执行安全动作”。功能安全的核心思想是风险降低。它承认风险无法完全消除，但可以通过实施一系列保护层（LayersofProtection）来将其降低到社会可接受的水平（AsLowAsReasonablyPracticable,ALARP）。

2.2 IEC61511标准体系

在过程工业领域，国际电工委员会（IEC）发布的IEC61511系列标准是指导仪表自动化系统（特别是SIS）实现功能安全的权威性框架。该标准基于更通用的IEC61508（电气/电子/可编程电子安全相关系统的功能安全），并针对化工、石油、天然气等流程工业的特点进行了具体化。IEC61511的核心是安全生命周期（SafetyLifecycle）概念。它将从概念设计到最终退役的整个过程划分为16个阶段，涵盖了管理、技术、验证和文档等各个方面，强调在整个生命周期内对安全相关系统进行系统化的管理。安全生命周期主要分为三个宏观阶段：（1）分析阶段：识别危险、分析风险、确定安全需求[2]。（2）实现阶段：根据安全需求进行设计、集成、安装和调试。（3）运行与维护阶段：确保系统在运行期间持续满足安全要求，并在生命周期结束时妥善处理。遵循安全生命周期方法，可以确保功能安全工作有章可循，避免遗漏关键环节。

2.3 安全完整性等级（SIL）

安全完整性等级（SIL）是IEC61511中用于量化安全功能所需风险降低程度的离散等级。SIL等级分为1到4级，SIL4代表最高的安全完整性要求，即需要最大的风险降低。确定一个安全仪表功能（SIF）所需的SIL等级，是安全生命周期中承上启下的关键步骤。它直接决定了后续设计、选型、验证等环节的严格程度。SIL等级的确定必须基于对特定危险场景的风险评估。

3 安全性评估的关键技术与方法

3.1 危险与可操作性分析（HAZOP）

HAZOP（HazardandOperabilityStudy）是化工行业应用最广泛、最有效的定性风险识别工具。它通过一个由多专业人员（工艺、仪表、操作、安全等）组成的团队，系统地、结构化地审查工艺流程图（P&ID），使用引导词（如“无”、“多”、“少”、“反向”等）对每个工艺参数（如流量、压力）进行偏差分析。对于每个识别出的偏差，团队会分析其可能的原因、后果以及现有的保护措施（包括DCS的报警和控制、SIS、物理保护、应急响应等）[3]。如果现有保护措施不足以将风险降至可接受水平，则会提出建议措施，其中最常见的建议之一就是增设或修改一个SIF。HAZOP是识别需要SIS介入的危险场景的起点。

3.2 保护层分析（LOPA）

LOPA是一种半定量的风险评估方法，用于对HAZOP等定性分析中识别出的高风险场景进行更精确的风险量化，并最终确定所需的SIL等级。LOPA的基本原理是：初始事件（如泵故障、阀门内漏）的发生频率乘以所有独立保护层（IPLs）的失效概率，得到该场景下不期望事件（如火灾、爆炸）的最终发生频率。这个最终频率需要与企业的风险可接受标准（RiskToleranceCriteria）进行比较。LOPA中的保护层必须满足独立性、有效性、可审查性等严格标准。典型的IPLs包括：（1）基本过程控制系统（BPCS）中的控制回路；（2）报警及操作员干预；（3）安全仪表系统（SIS）；（4）物理保护（如爆破片、安全阀）；（5）工厂应急响应；（6）社区应急响应。通过计算，如果现有IPLs提供的风险降低不足，就需要增加一个新的IPL（通常是SIS），并计算出该SIS需要达到的平均要求失效概率（PFDavg），从而对应到具体的SIL等级。

3.3 安全仪表系统（SIS）的验证与确认

在SIS按照SIL要求设计、选型和安装完成后，必须对其进行严格的验证（Verification）与确认（Validation），以证明其能够满足预定的安全要求。（1）SIL验证：主要验证SIS的硬件架构是否能达到目标SIL等级所要求的PFDavg。这通常通过可靠性建模（如马尔可夫模型、故障树分析FTA）来完成，需要考虑设备的失效率、诊断覆盖率、冗余结构、共因失效等因素。验证结果必须证明计算出的PFDavg小于或等于该SIL等级所允许的最大PFDavg[4]。（2）工厂验收测试（FAT）与现场验收测试（SAT）：在系统集成商工厂和最终用户现场分别进行的功能测试，确保所有SIF在各种预设场景下都能正确、及

时地动作。（3）定期的功能安全评估（FSA）：在安全生命周期的不同阶段（如概念设计、详细设计、安装调试、运行维护后），由独立的评估员对功能安全活动的符合性进行审查，确保整个过程符合IEC61511的要求。

4 新技术发展对安全性评估的影响

随着工业4.0和智能制造的推进，仪表自动化系统正经历深刻的变革，这对安全性评估也提出了新的挑战与机遇。

4.1 人工智能（AI）与机器学习（ML）

AI/ML技术可用于对海量的历史运行数据进行分析，实现对设备健康状态的预测性维护，提前发现传感器或执行器的潜在故障趋势，从而变被动维护为主动维护，降低硬件随机失效的风险。此外，AI还可以用于优化控制策略，减少过程波动，间接提升安全性。然而，AI模型的“黑箱”特性也带来了新的系统性失效风险，其决策过程的可解释性和可靠性是安全性评估必须面对的新课题。

4.2 数字孪生（DigitalTwin）

数字孪生技术通过构建物理工厂的高保真虚拟映射，为安全性评估提供了强大的仿真平台。可以在数字孪生体上进行虚拟的HAZOP/LOPA分析、SIF逻辑测试、应急演练等，无需中断实际生产，极大地提高了评估的效率和安全性。同时，数字孪生可以实时同步物理工厂的状态，为在线风险监控和动态SIL评估提供可能。

4.3 网络安全一体化

未来的安全性评估必须将网络安全（CyberSecurity）与功能安全（FunctionalSafety）深度融合。需要采用如IEC62443等工业网络安全标准，对仪表自动化系统进行威胁建模、脆弱性评估和渗透测试，确保其在面对网络攻击时仍能保持基本的安全功能。

5 结语

仪表自动化系统是化工生产安全的基石，其安全性评估是一项复杂而系统的工程。本文通过梳理其风险来源，引入以IEC61511为核心的功能安全标准框架，并详细阐述了HAZOP、LOPA和SIS验证等关键技术，构建了一个从风险识别、量化到验证确认的完整评估链条。为有效提升仪表自动化系统的安全性，本文提出以下建议：企业应将功能安全管理融入项目管理和日常运营的全过程，确保每个阶段的活动都得到有效执行和记录。培养和引进兼具工艺、仪表、安全和IT知识的复合型人才，确保HAZOP、LOPA等分析活动的质量。积极利用AI、数字孪生等新技术赋能安全管理，但同时要对其引入的新风险进行充分评估，并建立相应的验证和审计机制。加强操作员和维护人员的培训，特别是对安全联锁逻辑的理解和应急处置能力的训练，减少人为失误。定期回顾和更新风险评估结果，分析运行期间发生的未遂事件和小事故，不断优化仪表自动化系统的设计和管理。

参考文献

[1]连建奎.某化工过程自动化安全仪表系统设计与应用[J].生物化工,2025,11(04):154-156+163.

[2]林泽群.基于化工仪表的自动化控制与安全防护[J].广州化工,2025,53(15):140-142.

[3]高日伟.初探化工电气自动化仪表安装检修与改造安全技术[J].四川建材,2021,47(02):125-126.

[4]焦兴.化工企业电气仪表自动化控制技术的运用[J].中国石油和化工标准与质量,2025,45(17):170-172.