基于本质安全的化工工艺联锁系统设计与可靠性分析

肖　佳

天津葆光工程科技有限公司 天津 300100

【摘　要】：化工生产风险高，本质安全理念指引工艺联锁系统设计。本文结合本质安全与工艺联锁耦合逻辑，明确系统设计核心原则及危险参数界定方法，搭建独立型 SIS/ESD 系统与 DCS 协同架构，分析冗余容错、安装环境、仪表性能及人为管理对联锁系统可靠性的作用，给出功能测试、稳定性考核、量化评价及本质安全综合评价的验证方法。科学联锁设计、规范安装调试与完善管理体系，可提升系统可靠性与本质安全水平，保障化工装置长周期安全运行。

【关键词】：本质安全；化工工艺；联锁系统；SIS/ESD；可靠性评价

DOI:10.12417/2705-0998.26.08.060

引言

化工生产涉及易燃易爆、有毒有害物料，温度、压力等参数波动及设备故障易引发安全事故，工艺联锁系统作为核心安全保障手段，设计合理性直接决定装置运行安全性。本质安全理念强调从源头降低风险，与化工工艺联锁融合是实现安全生产的关键路径。部分化工企业联锁系统存在设计冗余、逻辑繁琐、可靠性不足等问题，易导致联锁误动或拒动。本文结合工程实例，系统研究本质安全理念下化工工艺联锁系统的设计、可靠性影响因素及验证评价方法，为化工企业联锁系统优化升级提供理论支撑与实践参考。

1 本质安全理念下化工工艺联锁系统设计基础

1.1 本质安全与工艺联锁的耦合逻辑

本质安全与化工工艺联锁的耦合核心，是将源头减危、故障安全、失误安全融入联锁全生命周期，使联锁从被动防护升级为工艺固有安全属性[1]。化工生产中温度、压力、液位、流量等参数越限、设备故障、操作误动作等风险，需通过联锁的强制约束将装置导向安全状态，形成控制逻辑与硬件配置的双重安全屏障。DCS 承担常规工艺控制，SIS/ESD 专职安全联锁与紧急停车，二者物理隔离、功能分立，是本质安全“控制与安全分离”的工程落地。山东东明石化曾因极端天气导致全厂停电，独立设置的 SIS 系统快速启动紧急泄压与安全停车，避免反应系统超温超压引发爆炸，验证了分离架构在极端工况下的本质安全保障能力。

1.2 化工工艺联锁系统本质安全设计原则

化工工艺联锁系统本质安全设计遵循故障安全、独立保护层、冗余容错、逻辑最简、参数精准匹配五大原则。故障安全要求系统在断电、断气、元件失效时自动进入安全状态，紧急切断阀采用失气关闭设计即为典型应用。独立保护层强调 SIS/ESD 与 DCS 完全独立，不共用传感器、控制器与执行机构，阻断控制层故障向安全层传导。冗余容错针对关键回路采用多重冗余与表决机制，消除单点失效风险。逻辑最简杜绝冗余判断与非必要延时，某石化重整装置压缩机振动高高联锁曾增设延时与负荷调节逻辑，虽降低误停车率却大幅提升事故风险，违背本质安全即时保护初衷。参数匹配要求联锁设定值严格贴合工艺危险临界条件，兼顾保护有效性与生产连续性。

1.3 工艺危险参数与联锁触发条件界定

工艺危险参数与联锁触发条件以 HAZOP、LOPA 分析为依据，结合物料特性、操作工况与事故后果分级确定。危险参数覆盖温度、压力、液位、流量、组分、振动等关键指标，触发条件分为报警预警、联锁动作、紧急停车三级。江苏某石化反应釜以设计压力 90%为高报、100%为高高联锁，超限后 0.8 秒内触发紧急停车与泄压，成功阻断爆炸风险[2]。界定过程需明确测量点位置、检测元件类型、信号传输路径、动作执行对象与时序，形成完整联锁逻辑表。天津南港乙烯项目国产 SIS 系统精准界定裂解炉、反应器等单元危险参数与触发条件，实现系统可用率 100%，满足百万吨级乙烯装置本质安全控制要求。

2 基于本质安全的化工工艺联锁系统架构设计

2.1 独立型安全联锁（SIS/ESD）系统设计

独立型 SIS/ESD 系统依据 IEC 61511 标准构建，采用独立传感器、独立逻辑控制器、独立执行器三层架构，逻辑控制器选用故障安全型 CPU，配置冗余电源与冗余通信网络。关键测量回路采用二取一、三取二表决机制，系统响应时间控制在毫秒级。该系统全程静态值守、无需人工干预，权限高于 DCS，仅在危险状态触发动作。内蒙古君正化工电石装置 SIS 系统针对炉温超温、料位异常、可燃气体泄漏等场景，独立执行紧急停炉、切断进料、氮气置换等操作，与 DCS 控制回路完全隔离。环丁砜生产装置 SIS 系统通过多重冗余与故障安全设计，满足 SIL 等级要求，有效提升高风险工艺的本质安全水平。

2.2 DCS 与安全联锁系统的协同配置

DCS 与安全联锁系统协同配置遵循“控制与安全分离、功能互补、单向通信”原则。DCS 负责工艺参数监测、常规调节、顺序控制与操作管理，不参与联锁逻辑运算与执行；SIS/ESD 专职安全联锁与紧急停车，不介入常规控制。二者不共用 I/O

模块、控制电缆与供电回路，仅通过单向通信将 SIS/ESD 状态信息上传至 DCS。DCS 设联锁状态显示、分级报警、权限管理与操作记录，严禁修改联锁逻辑与定值；SIS/ESD 向 DCS 发送动作、故障等信号，形成监控—保护—反馈闭环。青海盐湖工业化肥装置采用该协同架构，既实现工艺精准控制，又通过独立联锁降低安全风险，为化工装置安全管控提供示范（见图 1）。

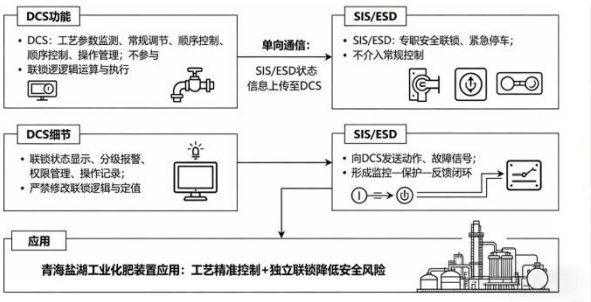

图 1 DCS 与安全联锁系统的协同配置

2.3 联锁逻辑与控制回路本质安全化设计

联锁逻辑与控制回路本质安全化设计遵循故障安全、单向执行、时序严谨、无扰动切换准则。逻辑设计采用最简路径，取消非必要延时、判断与手动复位环节，明确执行机构失电、失气、失信号安全状态，紧急切断阀失气关闭、调节阀失气保持原位均符合要求[3]。控制回路采用对称设计，测量元件与执行元件一一匹配，优化信号传输路径以减少干扰与误差。关键联锁回路采用冗余配置，避免单一元件失效影响整体功能。某大型炼化装置加氢单元通过逻辑优化与回路对称设计，消除信号延迟与误动作隐患，联锁动作准确率与响应速度均达到本质安全标准。

2.4 硬件设施本质安全匹配设计

硬件设施本质安全匹配围绕系统环境、I/O 配置、控制站、操作站、供电、通信等维度展开。DCS 与 SIS 控制室需满足抗干扰、接地、供电、温湿度要求，为系统稳定运行筑牢基础。I/O 点配置预留 10%—15%备用量，明确热备用与冷备用区分，控制站主控单元、内部网络、I/O 卡件、电源均采用冗余配置，机柜预留 10%备用空间。操作站按工段与人员分工配置，至少设置两台主操作站，报警与报表打印机分开部署。通信系统网卡、网线、交换机等关键部件实施冗余配置，保障信号稳定传输。UPS 容量需超出系统需求 40%，电网停电后持续供电不低于 30 分钟，危险场所严格按规范选用安全栅。备品备件储备需满足两年用量，确保硬件设施长期可靠运行。

3 化工工艺联锁系统可靠性影响因素分析

3.1 系统冗余冗错对可靠性的作用

冗余容错是提升联锁系统可靠性的核心手段，通过储备备用单元抵消单点失效影响。冗余按工作状态分为热备用与冷备用，按范围涵盖元件级、部件级、子系统级与系统级，按程度分为二重、三重与多重冗余。控制站、电源、通信网络、关键 I/O 卡件采用热备用冗余，故障时无扰动切换，保障参数监测与控制不中断。三重冗余 CPU 搭配三取二表决机制，能有效规避单一元件故障引发的联锁拒动或误动。冗余设计可延长系统平均无故障时间，降低失效概率，某大型甲醇装置联锁系统经冗余优化后，系统可用性提升至 99.99%，满足长周期安全运行需求。

3.2 安装调试与运行环境的可靠性影响

安装质量、调试规范度与运行环境直接决定联锁系统可靠性。系统安装涵盖台柜就位、设备固定、卡件安装、线缆连接、接地与供电施工，隐蔽工程需全程记录，冬季施工需控制温度梯度避免设备损伤[4]。调试包含单机调试、系统调试、现场联调，按检测、调节、报警、联锁、冗余、I/O、回路逐项验证，逻辑功能通过编程器测试确认，ESD 逻辑对照梯形图与逻辑图核对。运行环境需满足温湿度、防尘、抗干扰、接地要求，环境不达标易引发信号漂移、卡件故障、通信中断。某精细化工企业因控制室温湿度超标，导致 DCS 卡件频繁故障，联锁系统误动作率上升，环境整改后恢复稳定运行。

3.3 仪表与执行机构失效对联锁可靠性的影响

仪表与执行机构是联锁系统的现场终端，其可靠性直接决定保护功能能否实现。传感器损坏、零点漂移、管路泄漏会导致测量失真，执行机构卡涩、气源中断、电磁阀故障会造成联锁拒动。关键仪表需“三证”齐全，定期校验，重要开关量仪表整定后投用时间不超过两个月，配备充足备品备件。仪表技术资料需完整，包含仪表卡片、说明书、校验记录、控制流程图、接线图等。在线仪表故障时系统应及时报警，必要时启动联锁。某石化企业加热炉因流量仪表指示失灵未及时处理，导致炉管结焦破裂引发火灾，暴露仪表失效对联锁可靠性的致命影响。

3.4 人为因素与管理体系对联锁可靠性的作用

人为误操作与管理缺陷是联锁系统失效的重要诱因。操作人员不熟悉联锁逻辑、误碰接点、误动仪表、带电作业、违规解除联锁，均会引发非计划停车或事故。管理缺失体现在联锁变更未审批、校验未记录、培训不到位、应急演练缺失。人员培训覆盖系统工程师、组态工程师、维护人员与操作人员，确保掌握操作、组态、维护与应急处置技能。某装置开工时违规解除联锁，导致反应器氧气超量突发爆炸，证明人为因素与管理体系直接影响联锁可靠性。完善管理制度、强化培训、严格权限管理，可有效降低人为风险。

4 化工工艺联锁系统可靠性验证与评价

4.1 联锁系统功能测试与逻辑验证

联锁系统功能测试与逻辑验证是可靠性确认的关键环节。

检测系统在现场输入模拟信号，核对 CRT 显示值与系统误差，带报警点回路同步验证报警值与动作响应[5]。调节系统在手动状态输出 4—20mA 信号，检查执行机构全行程与回讯动作。报警系统按设计定值设定，逐点输入信号验证声光报警与画面显示。联锁保护系统通过单机、联机、冗余容错试验确认功能有效。网络通信与 I/O 卡件冗余试验验证切换无扰动。逻辑验证借助编程器测试功能，对照逻辑图核对输入输出关系，ESD 逻辑逐项核对手动开关与报警响应，确保逻辑运算与设计要求一致。

4.2 系统稳定性运行考核

系统稳定性运行考核以连续稳定运行为核心指标，通常选取工艺正常运行阶段开展 72 小时考核。考核指标涵盖计算机模件开工率不低于 99.95%，DCS 系统开工率不低于 99.99%，通过运行记录统计事故时间与开工率。考核期间监测参数显示、控制输出、报警响应、联锁动作、通信状态、冗余切换等功能，详细记录异常情况与故障处理过程。连续稳定运行无异常、故障及时消除、冗余切换正常，即视为稳定性合格。某乙烯装置 SIS 与 DCS 系统经 72 小时考核，开工率全部达标，无联锁误动与拒动现象，顺利通过可靠性验证。

4.3 可靠性量化评价指标与方法

联锁系统可靠性量化评价采用可用性、平均无故障时间、平均修复时间、失效概率、安全完整性等级等指标。可用性为系统正常运行时间与总时间比值，关键联锁系统可用性不低于 99.99%。平均无故障时间反映系统固有可靠性，平均修复时间体现维护便捷性。失效概率分为安全失效与危险失效，危险失效概率需满足 SIL 等级要求。评价方法结合硬件失效率数据、冗余配置、测试周期、维护记录，采用可靠性框图与故障树分析，计算系统整体可靠性指标。某炼化装置联锁系统通过量化评价，识别薄弱环节并优化，危险失效概率显著降低。

4.4 本质安全有效性综合评价

本质安全有效性综合评价从设计、硬件、软件、安装、调试、运行、维护、人员、管理全维度开展。评价内容涵盖工艺参数设计合理性、软件功能符合性、硬件匹配性、安装可靠性、调试规范性、运行稳定性、冗余容错能力、故障处理能力、人员技能水平、管理体系有效性。结合功能测试、稳定性考核、量化指标与现场核查，判定联锁系统是否实现源头控制、故障安全、独立保护、可靠动作。评价结论明确系统本质安全水平、薄弱环节与整改要求，形成闭环管理。经综合评价，系统满足设计标准与安全规范，能在危险工况下可靠实现安全保护，即视为本质安全有效。

5 结语

本质安全理念下，化工工艺联锁系统的设计与可靠性管控是防范化工安全事故的核心环节。本文从设计基础、架构构建、可靠性影响因素及验证评价四个维度，系统梳理联锁系统的设计要点与管控方法，明确故障安全、独立保护、冗余容错等核心原则的实践路径，结合多个石化企业工程实例验证了设计与评价方法的有效性。未来需进一步结合智能化技术，优化联锁逻辑设计与故障预警机制，强化人员培训与管理体系建设，持续提升联锁系统的本质安全水平，为化工行业安全生产筑牢技术屏障。

参考文献：

[1] 沙帅,王猛,王绪梅,等.化工工艺的风险识别与安全评价研究[J].山西化工,2025,45(08):198-200.

[2] 田佳.化工工艺设计与安全评价对化工安全生产的影响分析[J].中国石油和化工标准与质量,2025,45(14):25-27.

[3] 王栋.化工工艺安全设计中的危险因素及防范措施[J].当代化工研究,2025,(08):152-154.

[4] 王建平.化工工艺安全风险预警体系构建与本质安全提升策略[C]//重庆市大数据和人工智能产业协会.人工智能与经济工程发展学术研讨会论文集（三）.湖州衡一检测有限公司;,2025:864-867.

[5] 远亚群,仝育婷.化工工艺危险特性及其安全控制技术研究[J].化工设计通讯,2024,50(11):53-55+61.