化工过程自动化控制系统的本质安全设计与容错能力提升

黄云飞
泛华保险公估股份有限公司河北分公司，河北 石家庄 050000

[摘要]化学工业作为国民经济重要支柱产业,与经济社会发展和人民生活息息相关。化工生产原辅料种类繁多、生产工艺复杂，涉及高温高压、易燃易爆、有毒有害等诸多危险因素，一旦失控发生安全事故，往往造成重大人员伤亡和财产损失，引发严重环境污染和社会影响。本质安全设计通过从源头消除或降低风险，容错能力提升则实现系统在故障工况下的风险可控，二者共同构成化工过程自动化控制系统安全保障体系的核心。文章基于本质安全理论与容错控制原理，对化工过程自动化控制系统的本质安全设计内涵与核心原则进行阐述，从故障检测与诊断、冗余配置优化、容错控制策略构建三个维度搭建容错能力提升的技术路径，以供参考。

[关键词]化工过程；自动化控制系统；本质安全设计；容错能力；风险管控
DOI：10.33142/ect.v3i12.18604 中图分类号：TQ086 文献标识码：A

Inherent Safety Design and Fault Tolerance Enhancement of Chemical Process Automation Control System

HUANG Yunfei
Hebei Branch of Fanhua Inc., Shijiazhuang, Hebei, 050000, China

Abstract: As an important pillar industry of the national economy, the chemical industry is closely related to economic and social development and people's lives. There are various types of raw materials and complex production processes in chemical production, involving many dangerous factors such as high temperature and high pressure, flammability and explosiveness, toxicity and harm. Once out of control, safety accidents often occur, causing significant casualties and property losses, leading to serious environmental pollution and social impact. Intrinsic safety design eliminates or reduces risks from the source, while improving fault tolerance enables the system to control risks under fault conditions. The two together form the core of the safety assurance system for chemical process automation control systems. Based on the theory of intrinsic safety and the principle of fault-tolerant control, this article elaborates on the connotation and core principles of intrinsic safety design for chemical process automation control systems. It constructs a technical path for improving fault-tolerant capabilities from three dimensions: fault detection and diagnosis, redundant configuration optimization, and fault-tolerant control strategy construction, for reference.

Keywords: chemical process; automated control system; inherent safety design; fault tolerance capability; risk control

引言

化工行业是国民经济的支柱产业，但其生产过程涉及大量危险化学品和极端工艺条件,具有事故发生率高、后果严重等特点。据统计，全球化工行业重大安全事故中，约 45%与自动化控制系统故障或设计缺陷相关。化工生产本质在于通过一系列化学反应和物理过程，将原料转化为具有特定性质的目标产品，同一产品往往存在多种工艺路线可供选择，不同工艺路线在原料组成、反应条件、生产流程等方面存在较大差异，从而影响化工装置固有安全水平。随着工业 4.0 技术的深度融合，化工过程自动化控制系统朝着集成化、智能化、复杂化方向发展，其安全设计的核心已从“被动防护”转向“主动预防”,本质安全设计与容错能力提升成为解决化工过程安全问题的关键突破口。本质安全理念起源于 20 世纪 60 年代的工业安全领域，核心思想是通过设计消除或减少危险源，使系统在本质上具备安全属性，即使发生人为失误或设备故障，也不会导致事故发生。将该理念应用于化工过程自动化控制系统，需在系统设计阶段充分考量化工过程的风险特性，通过硬件选型、软件架构设计、控制逻辑优化等手段，从源头降低系统故障概率与故障后果严重程度。容错能力作为本质安全设计的延伸与补充，聚焦于系统发生故障后的风险管控，通过一系列技术措施使系统在局部故障工况下仍能维持核心功能正常运行，避免故障扩大化。

目前,关于化工过程自动化控制系统安全的研究多集中于故障诊断算法优化、单一设备的安全设计等局部领域,缺乏对本质安全设计与容错能力提升的系统性整合分析。本文立足化工过程的全流程风险特性,构建本质安全设计与容错能力提升的一体化分析框架,先明确本质安全设计的核心要素与实现路径,再针对性提出容错能力提升的技术方案,旨在为提升化工过程自动化控制系统的全生命周期安全性能提供理论指导。

1 化工过程自动化控制系统的本质安全设计内涵与核心原则

化工过程自动化控制系统本质安全设计，是在系统规划至研发阶段，识别化工危险源（如物料状态、生产工艺参数偏差等），结合系统特性（传感器等组件），用技术从源头消除危险源或降低风险。其核心是“源头规避、过程抑制、风险可控可防”。通过精准的选型以及系统架构优化，从源头上消除潜在的设计缺陷，采用冗余控制逻辑，增强系统运行的稳定性与容错能力，合理选用传感器，从硬件层面确保系统的安全。在系统运行的过程中，通过借助自适应算法动态调整各个参数以满足不同工况下的运行实际需求。在风险可控层面，当系统出现异常时可以自动切换至安全模式，同时具备故障隔离功能，保障人员与设备安全。化工过程自动化控制系统的本质安全设计应该严格遵循最小风险、简化性、兼容性、可追溯性的核心原则。

3 化工过程自动化控制系统关键组成部分的本质安全设计

3.1 传感器的本质安全设计

在化工控制系统中，传感器主要负责采集化工过程中的压力、温度等各个参数。其可靠性与精确度与系统的安全性能与控制效果有着直接的影响。以化工过程的危险等级为依据，合理选择传感器，从源头上保障监测的安全性与可靠性，与此同时选择本质安全型信号电缆进行电信号传输。对于远距离的信号传输建议采用数字化传输方式，确保在长距离传输过程中信号不衰减，并且配置过压、过流保护装置为整个传输系统的稳定运行提出保障。值得注意的是，传感器的安装位置要严格避开高压高温强腐蚀等危险区域，以防影响传感器的性能，缩短其使用寿命。

3.2 执行器的本质安全设计

执行器主要是根据控制器的指令对工艺参数进行调整，其可靠性与精确性对化工过程的稳定性有着直接的影响。实际运行过程中，执行器面临着诸多的潜在风险，会造成严重的化工生产事故。基于此，应该充分考虑本质安全型驱动装置，建立采用气动执行器，从源头上降低事故的发生风险。为了确保执行器的动作精准性，运用定位器进行优化，采用模块化设计理念对执行器进行设计，以便在出现故障时能够第一时间进行更换或维修。同时要关注执行器的密封性能，应该根据实际工况情况合理选择密封材料。

3.3 控制器的本质安全设计

控制器负责接收传感器的测量信号、执行控制算法、向执行器发出控制指令，为了确保控制器能够适应各种复杂工况采用冗余设计理念选用工业级高可靠性硬件组件进行构建设置多重保护装置。在控制算法方面选用经过大量实践验证的可算方法，以此确保系统的精准控制。在软件层面融入先进的故障检测报警逻辑实时捕捉系统运行过程中的异常情况发出警报，软件编程采用模块化设计方法。人机界面简洁直观，操作权限实施分级管理，实时显示关键参数与运行状态。

3.4 通信链路的本质安全设计

通信链路是自动化控制系统信息传输的桥梁，优先选本质安全型通信介质（如光纤、本质安全型电缆），远距离通信采用光纤替代电缆；合理选规格型号以适应化工极端环境。选择符合工业安全标准的通信协议（如 IEC 61158、IEC 61784），用加密技术（如 AES 加密）处理数据，协议中加强数据校验机制。采用分布式网络架构，设通信冗余链路，主链路故障自动切换，设置防火墙与入侵检测系统，防止出现通信故障。

4 化工过程自动化控制系统容错能力提升路径

4.1 故障检测与诊断技术优化

在化工过程自动化控制领域过程中，通过对系统故障类型故障的程度进行精准识别对于实现高效的容错控制具有重要意义。鉴于化工生产过程的复杂与多变性，或采用单一参数进行检测，容易出现漏判或误判的情况，对故障处理的有效性与及时性有严重影响。尽于此，引入智能算法构建故障诊断模型，基于强大的数据处理能力，精准定位故障发生的具体位置并对故障的严重程度进行评估。

4.2 冗余配置优化

冗余配置作为提升系统容错能力的重要手段，通过部署备用组件或冗余链路，构建起多层次的故障防御体系，在运行过程中出现故障时系统能够通过备用组件维持核心功能的正常稳定运行。在关键工艺参数监测环节采用多传感器冗余配置方式对关键工艺参数进行多点测量，借助先进的数据融合算法综合处理多元测量的数据，提高测量数据的精准性与可靠性。在控制层架构设计中采用多机冗余配置或双机热备份的方式，主控制器与备用控制器通过高速数据总线实时同步运行数据构建起镜像化的控制体系，当主控制器突发故障时备用控制器能够依托预先同步的运行数据能够在毫秒级时间内无缝切换，以此确保控制过程的连续性，确保工艺过程的平稳进行。

4.3 容错控制策略构建

容错控制策略作为提高系统容错性能的主要核心手段，通过设计的控制算法以及逻辑结构可以确保系统在故障工作下自动调整控制策略的能力，从而确保系统的稳定运行。当系统检测到传感器发生故障时，主动容错控制策略以故障诊断模块输出的精准结果为依据对故障传感器的具体类型以及故障严重程度进行精准的判定。随后，该策略可以充分利用其他正常传感器的实时测量数据以及系统预先构建的精准模型生成全新的控制指令，维持核心功能正常运行。主动容错控制策略的实施主要依赖于精确的系统模型，对故障诊断的精准性提出了较为严格的要求。混合容错控制策略融合了被动容错控制与主动容错控制的优势形成了一套更为完备的故障应对机制，基于故障的

类型，合理选择容错控制方式。对于在工况中较为常见的故障，为了可以提高响应速度，建议采用被动容错控制策略。反之，对于发生率较低、成因复杂的罕见故障，建议采用主动容错控制方式，提高容错能力，线路故障的有效隔离，快速恢复系统的性能。

5 本质安全设计与容错能力提升的协同优化

在化工过程自动化控制系统的安全保障体系中，本质安全设计与容错能力的提升尤为关键，两者相互补充，能够从源头上预防故障的发生风险，从而提高化工过程自动化控制系统的安全性能，确保化工生产稳定安全进行。

该系统的设计阶段应该充分考量本质安全设计与容错能力提升的需求进行统筹考量与综合规划，在本质安全设计方案中融入容错能力使两者形成一个有机的整体。另外采用风险矩阵法、事件树分析法（ETA）、故障树分析法（FTA）等风险评估方法准确识别潜在的风险点，并找出故障的根本原因与关键点，为后续的优化改进方案提供有力支持。在系统的运行过程中，应该借助先进的监测设备与传感器实时监测与采集系统运行过程中的各项参数，对本质安全设计的实际有效性进行评估，同时深入分析系统的运行状况。采取针对性的措施，不断完善设计方案，例如增加冗余配置、更换性能更优的设备原器件等，全方位提高系统的安全性能。在系统的维护阶段制定科学合理的检查计划方案，检查电器的性能，通信的连接，加强完善维护记录与故障档案，全面记录冗余组件的维护历史和故障情况，以便为后续的故障排障以及维护决策方案的制定提供有力的参考。全生命周期的协同优化贯穿于整个流程阶段形成一个闭环的管理体系，可以能够确保系统的安全性能适应化工过程的工况变化，能够有效应对各种故障和风险。

6 化工过程自动化控制系统的保障措施

化工过程自动化控制系统要以工艺危害分析和风险评估为基础，科学确定安全功能和安全完整性等级，选用高可靠性、故障安全的仪表设备，合理设计安全功能逻辑和动作时序，确保安全功能的可靠执行。一要与基础控制系统和紧急停车系统实现功能协调、逻辑清晰的联动，避免逻辑错误和功能遗漏。二要建立完善的安全状态监测和故障诊断机制，实时掌控化工过程自动化控制系统的健康状况，及时发现和排除潜在隐患。三要加强化工过程自动化控制系统的功能测试和性能评估，定期开展安全完整性等级复核，持续提升系统的安全性和可靠性。四要完善化工过程自动化控制系统的管理制度和操作规程，加强人员培训和应急演练，确保化工过程自动化控制系统优化成果落地见效。

7 结论与展望

7.1 结论

化工过程自动化控制系统在化工生产领域中可以确保生产的连续性、产品的质量、人员安全。本质安全设计作为一种预防性前瞻性的安全利益，在设计过程中应该严格遵循一系列科学的原则，充分考量深度融合系统设计过程中的每一环节，将故障风险控制在最小化。容错能力提升是在本质安全设计的基础上增强系统应对事故的能力，通过实施冗余配置优化、容错控制策略构建等能够实现故障过程中的风险可控以及系统安全稳定运行。本质安全设计与容错能力提升的协同优化源头上降低故障的发生风险，能够最大化提升系统的安全性能，推动化工行业向高效、安全的方向发展。

7.2 展望

但随着智能化技术的持续发展与深度扩展，在化工过程自动化控制体系的设计过程中融入智能化技术，充分利用大数据、人工智能等智能技术推进本质安全设计的智能化与自动化。借助先进的机器学习算法，深度挖掘化工过程中的海量数据，并进行分析，对潜在的风险点精准识别，同时可优化安全设计策略，可实现化工过程自动化控制系统的本质安全水平，而且可以提高设计的效率。同时在后续研究中开发具备自适应能力强的容错控制算法，以实际工况变化为依据合理调整。三是数字化孪生方向，构建化工过程自动化控制系统的数字化孪生模型，通过虚拟仿真验证本质安全设计的有效性与容错能力的可靠性，降低实际系统的测试成本与风险。在研究工作中应该紧密围绕上述方向进行开展，持续探索创新，进一步增强化工过程自动化控制系统的安全性，推动化工行业的安全、绿色、高效发展。

[参考文献]

[1]赵学刚,唐世慧.优化化工安全设计在预防事故中的作用与建议[J].劳动保护,2024(7):98-100.
[2]陈红.化工安全设计在预防化工事故发生中的作用[J].当代化工研究,2024(10):185-187.
[3]付新星,程森.化工安全设计在预防事故中的作用探讨[J].化工安全与环境,2023(6):31-33.
[4]张刚.关于化工安全设计在预防化工事故中的重要作用[J].轻工科技,2023(2):85-87.
[5]沈雷雷,曾伟.化工安全设计在预防化工事故发生中的作用及实施策略[J].化工管理,2022,11(32):87-89.
[6]刘晋,任晋楠,蒋晋晋,等.化工工艺安全评价指标体系的灰色关联度分析模型优化[J].安全与环境工程,2024,31(2):44-50.
[7]赵新梅,冯金,潘婷娟.化工工艺的风险识别与安全评价研究[J].石油石化物资采购,2024(9):46-48.

作者简介：黄云飞（1982.6—），毕业院校：河北科技大学，所学专业：药学，当前就职单位：泛华保险公估股份有限公司河北分公司，职务：安全工程师，职称级别：中级注册安全工程师。