化工DCS控制系统在复杂工况下的稳定性提升策略

王云芳
山西焦化集团有限公司　山西　临汾　041606

摘　要：本文聚焦于化工DCS控制系统在复杂工况下的稳定性提升策略。首先分析了影响DCS控制系统在复杂工况下稳定性的多方面因素，包括硬件设备的可靠性、软件系统的稳定性、环境因素、网络通信以及人为操作等。随后从硬件优化、软件改进、环境控制、网络强化以及人员管理等多个维度，系统性地提出了提升稳定性的具体策略。通过这些策略的实施，旨在为化工企业在复杂工况下确保DCS控制系统稳定运行提供理论支持和实践指导，保障化工生产的安全、高效与可持续性。

关键词：化工DCS控制系统；复杂工况；稳定性提升策略

1 引言

化工行业作为国民经济的重要支柱产业，其生产过程往往涉及高温、高压、易燃易爆、强腐蚀等复杂工况。在这样的环境下，DCS（Distributed Control System，分散控制系统）控制系统作为化工生产的核心自动化控制手段，承担着对生产过程进行实时监测、控制和优化的重要任务。DCS控制系统的稳定性直接关系到化工生产的安全、产品质量和生产效率。一旦DCS系统出现故障或不稳定，可能导致生产中断、设备损坏甚至引发严重的安全事故，给企业带来巨大的经济损失和社会影响。因此，研究化工DCS控制系统在复杂工况下的稳定性提升策略具有重要的现实意义。

2 影响化工 DCS 控制系统在复杂工况下稳定性的因素分析

2.1 硬件设备可靠性

2.1.1 控制器与I/O模块

如果控制器或I/O模块出现故障，如芯片损坏、接口松动等，将导致控制功能失效或信号传输错误，直接影响系统的稳定性。

2.1.2 电源系统

电源波动、断电或电源模块故障可能导致系统重启、数据丢失或设备损坏。在复杂工况下，由于现场电气设备的频繁启停和电网的不稳定，电源系统更容易受到影响。

2.1.3 现场仪表与执行机构

现场仪表如温度传感器、压力变送器等用于测量工艺参数，其精度和可靠性直接影响到DCS系统获取的数据质量。执行机构如调节阀、变频器等负责根据DCS系统的控制指令调节工艺参数，若执行机构出现故障，如阀门卡涩、电机过载等，将导致控制指令无法正确执行，使系统偏离稳定状态。

2.2 软件系统稳定性

2.2.1 操作系统与控制软件

DCS系统通常运行在特定的操作系统平台上，操作系统的稳定性、安全性和兼容性对DCS系统的运行至关重要。控制软件负责实现各种控制算法、逻辑功能和人机交互界面，软件中的漏洞、错误或算法设计不合理可能导致系统崩溃、控制失灵或操作界面异常[1]。

2.2.2 数据管理与通信软件

DCS系统需要处理大量的实时数据，包括测量数据、控制指令、报警信息等。数据管理软件负责数据的存储、检索和处理，如果数据管理不善，可能导致数据丢失、错误或访问延迟。通信软件则负责DCS系统内部各设备之间以及与外部系统的数据通信，通信故障可能导致信息传递不畅，影响系统的协同工作能力。

2.3 环境因素

2.3.1 温度与湿度

高温会加速电子元件的老化，降低其性能和可靠性；高湿度则可能引起设备内部短路、腐蚀等问题。此外，温度和湿度的剧烈变化还可能导致设备内部结露，进一步影响设备的正常运行。

2.3.2 粉尘与腐蚀性气体

化工生产现场的粉尘和腐蚀性气体容易附着在设备表面，进入设备内部，对电子元件、电路板等造成损害。例如，腐蚀性气体可能会腐蚀金属部件，导致接触不良或电路短路；粉尘堆积可能影响设备的散热，使设备温度升高，降低其使用寿命。

2.3.3 电磁干扰

化工生产现场存在大量的电气设备，如电动机、变压器、变频器等，这些设备在运行过程中会产生电磁辐

射，对DCS系统的信号传输和设备运行造成干扰。电磁干扰可能导致信号失真、误码率增加，甚至使系统出现误动作。

2.4 网络通信

2.4.1 网络拓扑结构

不合理的网络拓扑结构可能导致数据传输延迟、拥塞或单点故障。例如，采用星型拓扑结构时，如果中心节点出现故障，将影响整个网络的通信；而采用环形拓扑结构时，一个节点的故障可能导致整个网络通信中断。

2.4.2 网络设备与协议

如果网络设备出现故障或性能不足，可能导致数据传输速度慢、丢包率增加。此外，网络通信协议的选择和配置不当也可能导致通信不稳定，如协议不兼容、参数设置错误等。

2.5 人为操作

2.5.1 操作人员技能水平

如果操作人员对系统不熟悉，操作不熟练，可能导致误操作，如错误设置控制参数、误发控制指令等，从而影响系统的稳定性。

2.5.2 维护与管理不当

如果维护人员未能按照规定的周期和方法对系统进行维护，如未及时清理设备灰尘、未对硬件设备进行检测和更换等，可能导致设备故障隐患积累。同时，缺乏完善的管理制度和应急预案，在系统出现故障时可能无法及时、有效地进行处理，进一步扩大故障影响。

3 化工 DCS 控制系统在复杂工况下稳定性提升策略

3.1 硬件优化策略

在DCS系统选型和建设过程中，应优先选择具有高可靠性、良好抗干扰性能和宽工作温度范围的硬件设备。例如，采用工业级的控制器、I/O模块、电源模块等，这些设备经过特殊设计和严格测试，能够在恶劣环境下稳定运行。对于现场仪表和执行机构，应选择质量可靠、精度高、稳定性好的产品，并根据现场工况采取相应的防护措施，如安装防护罩、采用防腐材料等。

为提高系统的可靠性，可采用硬件冗余设计。例如，对关键设备如控制器、电源模块、通信模块等采用双冗余配置，当一个设备出现故障时，冗余设备能够自动切换投入运行，确保系统不间断运行[2]。对于I/O模块，可采用通道冗余设计，即对重要的测量信号和控制指令采用多个通道采集和输出，当其中一个通道出现故障时，系统能够自动切换到其他正常通道，保证数据的准确性和控制的有效性。

3.2 软件改进策略

选择稳定、安全、兼容性好的操作系统作为DCS系统的运行平台，并及时对操作系统进行更新和补丁安装，以修复系统漏洞，提高系统的安全性和稳定性。在控制软件开发过程中，应采用先进的软件开发技术和方法，进行严格的软件测试和验证，确保软件功能正确、性能稳定。例如，采用模块化设计思想，将控制软件划分为多个功能模块，便于软件的维护和升级；对控制算法进行优化，提高算法的精度和响应速度；对软件进行压力测试、容错测试等，模拟各种复杂工况下的运行情况，发现并解决软件中存在的问题。

采用高效、可靠的数据管理技术，确保DCS系统中的数据安全、完整和可访问性。例如，采用数据库管理系统对实时数据和历史数据进行存储和管理，定期对数据库进行备份和维护，防止数据丢失。在通信软件方面，选择合适的通信协议，如以太网通信协议、现场总线通信协议等，并根据实际需求进行合理配置。同时，采用数据加密、校验等技术手段，提高数据传输的安全性和可靠性。此外，建立通信故障监测和预警机制，实时监测网络通信状态，一旦发现通信异常，能够及时发出警报并采取相应的处理措施。

在软件设计中融入容错与自恢复机制，提高系统在面对软件故障时的稳定性和可靠性。例如，采用异常处理技术，对软件运行过程中可能出现的各种异常情况进行捕获和处理，避免因异常导致系统崩溃。同时，设计软件自恢复功能，当系统出现故障后，能够自动检测故障原因，并尝试恢复到正常运行状态。例如，通过设置软件看门狗，定期检测软件的运行状态，如果软件出现死锁或无响应情况，看门狗能够自动重启软件，使系统恢复正常运行。

3.3 环境控制策略

在DCS控制室和现场机柜间的建设过程中，应充分考虑环境因素对设备的影响，采取有效的环境控制措施。例如，控制室和机柜间应具备良好的通风、空调和除湿设备，将室内温度、湿度控制在适宜的范围内，一般温度应保持在18-25℃，相对湿度应保持在40%-60%。同时，应做好室内的防尘、防静电措施，如铺设防静电地板、安装空气过滤装置等，减少灰尘和静电对设备的影响。

对于安装在现场的仪表和执行机构，应根据现场工况采取相应的防护措施。例如，对于处于高温环境下的设备，可采用散热片、风扇、水冷等方式进行散热；对于处于粉尘和腐蚀性气体环境下的设备，可采用密封良好的防护罩进行保护，并定期对防护罩进行清理和检查，确保其防护效果[3]。此外，对于一些关键设备，还可

采用正压防爆柜等特殊防护设备，进一步提高设备的安全性和可靠性。

在DCS系统的设计和建设过程中，应充分考虑电磁兼容性问题，采取有效的电磁屏蔽、接地和滤波等措施，减少电磁干扰对系统的影响。例如，对控制室和机柜间进行电磁屏蔽设计，采用金属屏蔽网或屏蔽材料对房间进行包裹，防止外部电磁辐射进入室内；对设备进行良好的接地处理，确保设备外壳与大地之间的电气连接良好，将电磁干扰引入大地；在电源线和信号线上安装滤波器，滤除高频干扰信号，提高信号传输的质量。

3.4 网络强化策略

根据DCS系统的规模和实际需求，选择合理的网络拓扑结构。对于小型DCS系统，可采用星型拓扑结构，其结构简单、易于管理和维护；对于大型DCS系统，可采用冗余环形拓扑结构或双星型拓扑结构，提高网络的可靠性和容错能力。在网络设计过程中，应合理规划网络节点的布局和连接方式，避免出现网络瓶颈和单点故障。同时，采用网络分段技术，将整个网络划分为多个子网，减少广播风暴的影响，提高网络性能。

选择具有高带宽、低延迟、高可靠性的网络设备，如工业以太网交换机、路由器等。这些设备应具备良好的抗干扰性能和工业级防护等级，能够适应化工生产现场恶劣的环境条件。在网络协议方面，应选择成熟、稳定、通用性强的通信协议，如Modbus TCP、Profinet等，并根据实际需求进行合理配置。同时，采用网络管理软件对网络设备进行实时监控和管理，及时发现并解决网络故障。

随着DCS系统与企业管理信息系统的集成度不断提高，网络安全问题日益突出。为防止网络攻击和非法入侵对DCS系统造成影响，应采取一系列网络安全防护措施。例如，在网络边界部署防火墙，对进出网络的数据流量进行过滤和监控，阻止非法访问；采用入侵检测系统（IDS）和入侵防御系统（IPS），实时监测网络中的异常行为和攻击行为，并及时采取相应的防范措施；对网络设备进行访问控制，设置强密码和用户权限，防止未经授权的访问和操作；定期对网络进行安全评估和漏洞扫描，及时发现并修复网络安全漏洞。

3.5 人员管理策略

定期组织操作人员参加DCS系统操作培训，提高操作人员的专业知识和技能水平。培训内容应包括DCS系统的基本原理、操作界面、控制算法、故障处理等方面。通过理论教学、模拟操作和实际操作相结合的方式，使操作人员熟练掌握系统的操作方法和技巧，能够准确、快速地处理各种异常情况。同时，鼓励操作人员不断学习和积累经验，提高自身的应急处理能力和问题解决能力。

建立健全DCS系统维护管理制度，明确维护人员的职责和工作流程。制定详细的维护计划，包括日常巡检、定期维护、预防性维护等内容，并严格按照计划执行。在维护过程中，应做好详细的维护记录，记录设备的运行状态、维护内容、更换的零部件等信息，为设备的后续维护和管理提供依据[4]。此外，建立设备故障报告和处理机制，要求维护人员在发现设备故障后及时报告，并按照规定的流程进行处理，确保故障能够得到及时、有效的解决。

针对DCS系统可能出现的各种故障和事故情况，制定完善的应急预案。应急预案应包括故障现象描述、应急处理措施、人员分工、联系方式等内容，确保在故障发生时能够迅速、有序地进行处理。定期组织应急演练，模拟各种故障场景，检验应急预案的可行性和有效性，提高维护人员和操作人员的应急响应能力和协同配合能力。通过演练，及时发现应急预案中存在的问题和不足之处，并进行修订和完善。

结语

化工DCS控制系统在复杂工况下的稳定性对于化工生产的安全、高效运行至关重要。通过深入分析影响DCS控制系统稳定性的多方面因素，我们可以从硬件优化、软件改进、环境控制、网络强化以及人员管理等多个维度采取针对性的提升策略。在实际应用中，化工企业应根据自身的生产工艺、设备状况和环境特点，综合运用这些策略，不断优化和完善DCS控制系统，提高系统在复杂工况下的稳定性和可靠性。同时，随着信息技术的不断发展和化工行业的持续进步，DCS控制系统也将面临新的挑战和机遇，我们需要不断探索和创新，推动DCS控制系统技术的进一步发展，为化工行业的可持续发展提供有力保障。

参考文献

[1]闫淑娟,赵小鸽,孔进.DCS系统在硫酸工序中稳定性提升的研究及应用[C]//河南省企业服务活动办公室,河南省有色金属行业协会,中国有色金属工业协会扩大铝应用办公室.第三届中原国际铝加工新技术应用及发展论坛论文集.河南豫光锌业有限公司,2021:169-174.

[2]学晓春.提高DCS系统稳定可靠性的措施探讨[J].机电信息,2016,(36):48-50.

[3]王杰.DCS控制系统在精细化工中的应用研究[J].石化技术,2025,32(02):16-18.

[4]刘成,叶长波.化工安全生产中DCS控制系统的升级改造研究[J].石化技术,2024,31(09):53-55.