

# 化工DCS系统与信息管理系统集成网络方案

范智忠

山西焦化集团有限公司 山西 临汾 041606

**摘要:** 本文聚焦化工DCS与信息管理系统集成网络。首先分析其重要性,指出集成对网络在实时性、安全性、可靠性和数据适配性方面有核心需求。接着阐述核心设计框架,包括采用“控制层-隔离层-管理层”三层架构,从边界、数据、设备防护构建安全策略,以及从传输协议、带宽、数据过滤优化传输。然后说明实施要点,涵盖数据交互接口规范、网络运维保障、性能适配调试。最后强调实施关键注意事项,要保障控制层网络独立、落实网络冗余设计、做好施工与调试风险管控,以保障化工生产稳定运行。

**关键词:** 化工DCS系统;信息管理系统;系统集成;网络方案;安全防护;数据传输

引言:在化工行业智能化发展浪潮下,DCS系统与信息管理系统的集成成为提升生产效能与竞争力的关键。这一集成过程核心在于实现控制层与管理层的数据协同,然而化工生产对实时性、安全性、可靠性及数据适配性要求严苛,传统网络架构难以满足。为攻克这些难题,需构建一套科学完备的集成网络方案,涵盖核心设计框架、实施要点以及关键注意事项等多方面内容。本文将深入剖析这些要点,为化工企业打造高效、稳定、安全的集成网络提供全面指引。

## 1 化工DCS与信息管理系统集成网络的重要性分析

化工DCS系统与信息管理系统的集成,核心在于达成控制层与管理层的数据协同,这一过程对网络提出了多方面关键需求,实时性、安全性、可靠性与数据适配性是其中最为核心的要素。(1)实时性方面,DCS系统承担着化工生产过程实时监控与控制的重任,需将生产中的工艺变量,像温度、压力、流量等,以及设备运行状态信号等数据,及时且准确地上传至信息管理系统,为管理决策提供实时依据。同时,信息管理系统依据生产情况生成的生产调度指令、参数调整命令等,必须无延迟地传达至DCS系统执行层。若传输出现滞后,极易引发生产波动,影响产品质量与生产效率。因此,网络端到端传输延迟需严格控制,且延迟抖动要维持在极小范围内。(2)安全性上,DCS系统直接关联化工生产的核心环节,其运行安全是生产稳定的基础。集成网络必须构建坚固的隔离屏障,防止管理层网络中的异常流量、恶意访问等渗透至控制层,避免对生产控制造成干扰。同时,要保障传输数据的机密性,防止生产工艺参数、控制逻辑等核心数据被窃取或篡改。(3)可靠性层面,化工生产具有连续不间断的特点,集成网络需具备高容错能力。面对链路中断、设备故障等突发状况,要通过冗余设计等手段,确保数据

传输不中断,保障生产控制与管理业务的连续稳定运行。

(4)数据适配性方面,不同厂商的DCS系统与信息管理系统采用的通信协议和数据格式存在差异,集成网络需具备协议转换和数据格式标准化能力,实现异构系统间的数据顺畅交互<sup>[1]</sup>。

## 2 集成网络方案的核心设计框架

### 2.1 网络架构分层设计

基于化工生产控制与管理的分层管控逻辑,集成网络采用“控制层网络-隔离层-管理层网络”的三层架构设计,实现控制与管理的有效隔离与精准衔接。控制层网络聚焦DCS系统内部的数据传输,采用工业以太网架构,适配DCS系统的实时控制需求,保障生产工艺参数、设备状态数据的实时采集与控制指令的快速下达,该层网络采用专用工业交换机与通信链路,确保传输的实时性与稳定性。隔离层作为核心安全屏障,采用工业级防火墙、物理隔离装置等设备,实现控制层与管理层网络的逻辑与物理双重隔离,仅允许经过授权的数据流双向传输,同时对传输数据进行过滤与校验,防范非法数据接入。管理层网络面向信息管理系统,采用通用以太网架构,支撑生产计划、资源调度、数据统计等管理业务的数据传输,该层网络具备较高的带宽与扩展性,满足大量管理数据的整合与交互需求。三层架构通过明确的功能划分与隔离设计,既保障了DCS系统的控制安全性,又实现了与信息管理系统的高效数据协同。

### 2.2 安全防护策略设计

针对化工生产对安全性的高要求,集成网络精心构建了从边界、数据到设备的全方位安全防护策略体系。(1)在边界防护方面,不仅在隔离层部署防火墙与物理隔离装置,形成控制层与管理层间的坚固屏障,还在管理层网络接入外部网络的入口处增设下一代防火墙。

该防火墙具备深度包检测、应用识别等先进功能,可精准管控网络访问行为,有效阻断各类恶意流量与潜在攻击行为。同时,采用VPN技术为远程运维人员搭建安全接入通道,通过身份认证、数据加密等手段,保障远程访问的安全性与可靠性。(2)数据防护层面,对控制层与管理层间传输的关键数据运用加密传输技术,如采用AES等高强度加密算法,确保数据在传输过程中不被窃取或篡改。建立数据完整性校验机制,通过哈希算法等对接收数据进行校验,一旦发现数据异常,立即触发报警机制,并启动数据恢复流程,保障数据的准确性与完整性。(3)设备防护方面,对网络交换机、路由器、防火墙等核心设备进行严格安全配置,关闭不必要的端口与服务,设置强密码与精细访问权限。定期更新设备固件,及时修复安全漏洞,并建立设备运行状态监测机制,实时掌握设备运行状况,快速处理故障与异常,确保设备稳定可靠运行<sup>[2]</sup>。

### 2.3 数据传输优化设计

为切实满足集成网络对实时性与可靠性的严苛要求,数据传输优化设计从传输协议适配、带宽分配以及数据过滤三个关键方面展开精准施策。(1)在传输协议适配上,控制层网络选用适配工业控制场景的实时以太网协议,此类协议专为工业环境打造,具备低延迟、高确定性的特点,可有力保障控制数据在传输过程中的及时性与准确性。同时,在隔离层部署协议转换网关,该网关具备强大的协议解析与转换能力,能实现DCS系统所使用的工业协议与信息管理系统通用的TCP/IP协议之间的无缝对接,确保不同系统间数据交互的顺畅无阻。(2)带宽分配环节,采用服务质量(QoS)技术,依据数据的重要性和实时性对传输数据进行优先级划分。将DCS系统的实时控制数据与指令数据设定为最高优先级,使其在带宽资源竞争中占据主导地位,有效避免因管理数据大量占用带宽而导致的控制数据传输延迟。此外,根据生产过程中高峰期与低谷期的数据流变化情况,动态调整带宽分配策略,实现带宽资源的合理利用与高效分配。(3)数据过滤方面,在隔离层部署专业的数据过滤装置,对传输数据进行严格筛选,仅允许生产控制、调度管理等必要数据通过,过滤掉无效数据与冗余数据,降低网络传输负载,提升整体传输效率。

## 3 集成网络方案的实施要点

### 3.1 数据交互接口规范实施

数据交互接口作为DCS系统与信息管理系统集成的关键枢纽,在实施时必须明确接口规范与适配要求。(1)要采用标准化接口设计,优先选用工业领域广泛应

用的接口协议,如OPC UA等,以及通用的数据格式,以此保障不同系统间的兼容性。对于特殊类型的数据,需制定统一且详细的数据转换规则,将各类异构数据转化为标准格式,实现数据格式的一致性。(2)在接口位置部署专业的数据采集与转发装置,该装置要能精准采集DCS系统的生产工艺参数、设备运行状态等关键数据,并按照既定规范格式,快速、准确地将数据转发至信息管理系统。同时,它还需具备接收信息管理系统调度指令的能力,经过协议转换后,精准无误地将指令下发至DCS系统。(3)建立完善的接口运行监测机制,实时跟踪接口的数据传输状态。一旦出现数据传输中断、延迟超出标准范围或数据异常等情况,立即触发报警,并迅速启动应急处理流程,确保数据交互的连续性与准确性。

### 3.2 网络运维保障实施

为保障集成网络稳定可靠运行,构建完善的网络运维保障机制至关重要。(1)搭建网络状态实时监测系统。该系统需对控制层、隔离层、管理层的网络链路、设备运行状态、数据传输性能等核心指标展开全方位实时监测。借助可视化界面,将网络运行状态以直观清晰的方式呈现,使运维人员能够迅速洞察网络是否存在拥堵、设备有无故障等异常情况,为及时处理问题提供有力依据。(2)制定常态化运维流程。定期对网络设备进行全面巡检与精心维护,清理设备运行缓存,仔细检查链路连接状态,深入排查潜在故障隐患,将问题消灭在萌芽阶段。同时,建立详尽的网络配置档案,详细记录设备配置参数、网络拓扑结构等关键信息,保证配置修改过程可追溯。此外,针对可能出现的突发网络故障,制定科学合理的应急处置预案,明确故障排查流程与恢复措施,最大程度缩短故障处置时间,确保生产业务不受影响,持续稳定运行。

### 3.3 性能适配调试实施

集成网络方案落地实施后,开展全面且细致的性能适配调试工作必不可少,以此确保网络性能切实满足化工生产控制与管理需求。(1)调试内容涵盖多个关键方面。实时性测试方面,精心模拟生产场景下的数据流传输,精准测量控制数据与管理数据的传输延迟以及延迟波动范围,严格对照设计要求,保证各项延迟指标达标。安全性测试环节,通过模拟网络攻击、数据篡改等真实威胁场景,全面验证网络安全防护策略的实际有效性。可靠性测试中,模拟设备突发故障、链路意外中断等状况,着重测试网络的故障自愈能力以及数据传输的连续性。兼容性测试则聚焦于验证不同厂商设备、不

同通信协议之间的适配程度,保障数据交互顺畅无阻。

(2)依据详细的调试结果,对网络配置参数、带宽分配方案、安全防护策略等进行针对性优化调整,经过反复测试与完善,直至网络性能完全适配实际生产需求,为化工生产稳定运行提供坚实网络支撑<sup>[1]</sup>。

#### 4 集成网络方案实施的关键注意事项

##### 4.1 控制层网络独立性保障

在集成网络实施阶段,保障DCS控制层网络的独立性至关重要,这能有效避免集成操作对生产控制功能产生干扰。(1)必须严格禁止控制层网络与管理层网络直接连通,二者间的数据交互只能借助隔离层的专用隔离设备来实现。这些隔离设备具备强大的安全防护与数据过滤功能,可有效阻挡管理层网络中的异常流量与潜在威胁,防止其对控制层网络造成影响。(2)控制层网络的设备与链路应保持专用性,严禁接入非控制类设备。非控制类设备的接入会占用控制层网络的带宽与资源,影响数据传输的及时性与准确性,进而干扰生产控制功能。

##### 4.2 网络冗余设计落地

为切实增强集成网络的可靠性,冗余设计需全面融入方案实施的各个环节。(1)在链路冗余上,控制层和隔离层之间、隔离层与管理层之间,均采用双链路部署策略。这两条链路相互独立又互为备份,一旦主链路出现诸如物理损坏、信号干扰等故障,系统能够迅速且自动地切换至备用链路,从而保障数据传输的连续性,避免因链路中断导致生产控制或管理业务停滞。(2)对于核心网络设备,像工业交换机、防火墙等,采用双机热备模式。精心配置主备设备的自动切换机制,当主设备发生故障,如硬件故障、软件崩溃时,备用设备可立即接管工作,防止单一设备故障引发整个网络瘫痪。

##### 4.3 施工与调试的风险管控

化工生产现场环境错综复杂,高温、高压、易燃易爆等风险因素交织,集成网络的施工与调试必须高度重

视风险管控。(1)施工前,要对现场环境展开全方位排查,精准界定危险区域范围,依据排查结果制定详细且具有针对性的安全施工规范。施工人员必须配备专业的安全防护装备,如防爆服、安全帽、防护手套等,并严格遵循现场作业安全要求,杜绝违规操作。(2)调试过程中,要谨防对DCS系统的生产控制功能造成误触发。对于涉及控制指令传输的调试操作,需提前与生产运维团队充分沟通,采用模拟信号或离线测试的方式开展。同时,实时监测网络运行状态与DCS系统运行参数,一旦发现异常,立即停止调试,迅速启动应急措施,将潜在的生产安全风险扼杀在萌芽状态,确保化工生产安全稳定运行。

#### 结束语

化工DCS与信息管理系统集成网络对于化工生产意义重大,其重要性体现在满足实时性、安全性、可靠性与数据适配性等关键需求上。核心设计框架从网络架构、安全防护、数据传输优化多维度构建,为集成网络奠定坚实基础。实施要点涵盖接口规范、运维保障、性能适配调试等方面,确保集成网络顺利落地。而实施中的关键注意事项,如保障控制层网络独立、落实冗余设计、管控施工调试风险等,进一步保障了集成网络稳定运行。只有全面考量并落实这些要点与注意事项,才能打造出适配化工生产需求的集成网络,推动化工行业智能化、高效化发展。

#### 参考文献

- [1]李焕宇.基于DCS的水电厂电气二次控制设备集成与应用[J].机电信息,2024(20):74-77.
- [2]赵鹏,王勇,陈山.基于PLC和DCS的柔性生产线集成与优化[J].石油石化物资采购,2024(7):230-232.
- [3]黄恒儒,陈玲,葛集庆,徐彬彬.数智化工地综合监控系统的建设[J].城市轨道交通研究,2024,27(1):239-243+247.