文章类型：论文|刊号（ISSN）：2737-4505(P) / 2737-4513(O)

工业控制系统中 PLC 通讯协议的研究与实现

王小宁
安阳钢铁集团有限责任公司
DOI:10.32629/etd.v6i11.17493

[摘　要] 工业控制系统中PLC通讯协议的研究与实现对工业自动化至关重要。研究方法涵盖实验测试法,通过搭建平台测试性能等；理论建模法,构建模型预测性能、诊断故障；专家访谈法,借助专家经验获取见解；仿真模拟法,在虚拟环境评估协议。实现方面包括硬件选型与配置,确保适配稳定；软件编程与开发,保障功能实现；系统集成与联调,达成协同运行；安全保障与优化,提升安全性和性能,为工业控制系统稳定运行提供支撑。
[关键词] 工业控制系统；PLC；通讯协议；实现
中图分类号：TP273　文献标识码：A

Research and Implementation of PLC Communication Protocols in Industrial Control Systems

Xiaoning Wang
Anyang Iron and Steel Group Co., Ltd.

[Abstract] The research and implementation of PLC communication protocols in industrial control systems are crucial for industrial automation. Research methods include experimental testing, which involves building platforms to evaluate performance; theoretical modeling, which constructs models to predict performance and diagnose faults; expert interviews, which leverage expert experience to gain insights; and simulation, which assesses protocols in virtual environments. Implementation aspects encompass hardware selection and configuration to ensure compatibility and stability; software programming and development to guarantee functional realization; system integration and joint debugging to achieve coordinated operation; and security assurance and optimization to enhance safety and performance. These efforts provide robust support for the stable operation of industrial control systems.
[Key words] Industrial Control System; PLC; Communication Protocol; Implementation

引言

在工业4.0和智能制造的时代浪潮下,工业控制系统正朝着自动化、智能化方向飞速发展。PLC作为工业控制系统的核心设备,其通讯协议的重要性日益凸显。它是实现设备间数据交互、协同工作的关键,直接影响着系统的性能、可靠性和兼容性。然而,当前工业场景复杂多样,不同设备、不同应用对通讯协议的要求也不尽相同,现有的PLC通讯协议在实际应用中面临着诸多挑战。因此,深入研究PLC通讯协议,使其更好地适应工业发展需求,具有重大的现实意义。

1 PLC通讯协议概述

在工业自动化蓬勃发展的当下,可编程逻辑控制器(PLC)已成为工业控制系统的核心设备。而PLC通讯协议作为实现设备间数据交换与通讯的规范和标准,在工业自动化领域发挥着举足轻重的作用。首先,它实现了设备间的数据交换,不同设备可通过协议共享数据,实现联动控制和协同工作。例如,传感器将检测到的数据传输给PLC,PLC依据数据对设备进行远程监控和控制。其次,协议保证了通讯的可靠性和稳定性,规定了数据传输的格式、速率和校验方式,防止数据丢失或损坏。此外,它还支持不同厂家设备间的互联互通,使不同品牌、型号的设备能在同一系统中协同工作,提高了工业控制系统的整体效率和可靠性。常见的PLC通讯协议类型多样,Modbus协议是一种开放的通讯协议,基于主从架构,常用于PLC与外部设备(如传感器、执行器)之间的通讯,因其简单、易于实现和应用,在工业领域广泛使用。Profibus协议是一种工业通讯标准,常用于PLC和现场设备之间的通讯,具有传输速度快和可靠性强的特点,适用于复杂工业控制系统。CANOpen协议基于CAN总线,具有通讯速度快、实时性好、数据传输可靠等特点,适用于需要高性能实时通讯的工业控制系统。Ethernet/IP协议基于以太网,支持TCP/IP协议栈,适用于需要高速数据传输和大容量数据处理的工业控制系统。

2 工业控制系统中PLC通讯协议的研究方法

2.1实验测试法

实验测试法是研究工业控制系统中PLC通讯协议的重要手段,能够直观地获取协议在实际应用中的性能表现。(1)搭建实验环境：构建一个接近真实工业场景的实验平台,涵盖PLC、传感器、执行器等设备,模拟不同的工业生产环境,如高温、高湿度、强电磁干扰等,为后续测试提供多样化的条件。(2)进行功能测试：对PLC通讯协议的基本功能进行全面测试,包括数据的发送、接收、存储和处理等。检查协议是否能准确无误地实现设备间的数据交换,确保通讯的准确性和稳定性。(3)开展性能评估：测试协议的关键性能指标,如通讯速率、响应时间、吞吐量等。通过改变网络负载、数据量等因素,评估协议在不同条件下的性能表现,找出其性能瓶颈和优化方向。(4)模拟故障情况：人为设置各种故障场景,如网络中断、设备故障、数据丢失等,观察协议在故障发生时的应对机制和恢复能力,验证其可靠性和容错性。(5)分析测试结果：对实验测试中收集到的数据进行深入分析,总结协议的优点和不足。根据分析结果,提出针对性的改进建议,为协议的优化和应用提供参考。

2.2理论建模法

理论建模法是深入研究工业控制系统中PLC通讯协议内在规律和性能表现的有效途径。(1)构建基础模型：依据PLC通讯协议的工作原理、数据传输规则以及协议状态转换机制,构建起能够准确描述协议运行过程的基础数学模型。此模型要涵盖数据帧格式、传输流程、错误处理等关键要素,为后续研究奠定基础。(2)参数关联分析：确定与协议性能密切相关的参数,如波特率、数据位、停止位等,并分析这些参数之间的相互关系及其对协议性能的影响。通过建立参数与性能指标之间的函数关系,深入理解协议的运行机制。(3)性能预测建模：基于已构建的基础模型和参数分析结果,建立性能预测模型。该模型可根据输入的不同参数值,预测协议在各种工况下的性能表现,如通讯速率、数据传输准确性等,为协议的优化提供依据。(4)故障诊断建模：运用数据分析和机器学习算法,开发故障诊断模型。该模型能够对协议运行过程中出现的故障进行快速、准确的诊断和定位,通过对故障特征的学习和分析,提高故障诊断的效率和准确性。(5)模型验证优化：利用实验测试数据对构建的各种模型进行验证和优化。不断调整模型参数,改进模型结构,使模型能够更精确地反映协议的实际运行情况,提高模型的可靠性和实用性。

2.3实地调研法

实地调研法对工业控制系统中PLC通讯协议的研究意义重大。走访应用PLC通讯协议的企业和工厂,能与现场技术骨干和管理人员直接对话。技术骨干熟悉设备操作与协议应用细节,会分享协议在不同工况下的数据传输稳定性问题,像在强电磁干扰环境中通讯中断的情况;管理人员着眼生产全局,能反馈协议对生产流程和成本控制的影响,比如协议故障导致的生产停滞损失。在工厂车间实地观察PLC通讯系统运行,可直观了解其工作状态。记录系统运行参数、通讯周期内的数据流量变化,以及故障发生瞬间的表现,如指示灯闪烁规律等。这些现场观察到的细节,是理论研究中难以触及的,能为协议优化提供关键线索。同时,广泛收集工作人员对现有协议的反馈。他们在日常操作中积累了丰富经验,其提出的改进意见和期望,如简化协议配置流程、增强协议兼容性等,能让研究更贴合工业实际需求,确保研究成果可有效应用于工业控制系统。

2.4仿真模拟法

仿真模拟法是研究工业控制系统中PLC通讯协议的有效途径,能够在虚拟环境中对协议进行全面、深入的研究。第一,搭建仿真环境。利用专业的仿真软件,构建出高度逼真的工业控制系统场景,涵盖PLC、传感器、执行器等设备,以及不同的网络拓扑结构和通讯链路,尽可能模拟真实工业环境中的各种工况和干扰因素。第二,开展协议模拟运行是深入了解PLC通讯协议性能的有效途径。在仿真环境里,运行不同的PLC通讯协议,精心设置各类参数与条件。密切观察协议在数据传输时的流畅性,以及设备交互中的协调性。详细记录运行过程中的关键数据,像通讯延迟能反映协议的实时性,数据包丢失率则体现其可靠性。通过模拟运行和数据记录,为评估和优化协议提供有力依据,助力工业控制系统稳定运行。第三,进行性能评估分析。根据记录的数据,对协议的性能进行评估,分析其在不同条件下的优缺点。通过改变仿真参数,研究协议的适应性和稳定性,找出影响协议性能的关键因素。第四,开展故障模拟测试。

3 工业控制系统中PLC通讯协议的实现

3.1硬件选型与配置

硬件选型与配置是实现工业控制系统中PLC通讯协议的基础,直接影响着系统的性能和稳定性。(1)PLC核心选择：依据工业控制系统的规模、功能需求和复杂程度,挑选合适的PLC型号。要考虑其处理能力、存储容量、输入输出点数等关键指标,确保能满足系统的实时控制和数据处理要求。(2)通讯模块适配：根据所选的通讯协议,选择与之匹配的通讯模块。不同的通讯协议对模块的要求不同,如Modbus协议可能需要串口通讯模块,而Ethernet/IP协议则需要以太网通讯模块,要保证模块的兼容性和稳定性。目前10#锅炉,11#锅炉以及AV100更新了PLC施耐德M580,由原来的同轴电缆更换成网线接口,网络故障大大降低。(3)接口设备搭配:搭配合适的接口设备,如RS-232/RS-485转换器、光纤收发器等,以实现不同设备之间的连接和通讯。注意接口设备的电气特性和传输距离,确保数据传输的准确性和可靠性。(4)电源系统保障：设计稳定可靠的电源系统,为PLC和通讯模块提供干净、稳定的电源。考虑电源的冗余性和抗干扰能力,防止电源波动对设备造成损坏,影响通讯协议的正常运行。如现场配电柜进线和UPS都采用了双切换方式能有效保障所有PLC电系统供电正常(5)硬件布局规划：合理规划硬件设备的布局,遵循电磁兼容性原则,减少设备之间的电磁干扰。确保设备的散热良好,避免因温度过高影响设备性能,同时方便设备的安装、维护和管理。

3.2软件编程与开发

软件编程与开发是工业控制系统中实现PLC通讯协议的关键环节,关乎着整个系统能否高效、稳定运行。通讯程序架构设计,依据选定的PLC通讯协议,设计科学合理的通讯程序架构。明确数据的发送、接收、处理流程,规划好各个功能模块的职责,确保程序结构清晰、易于维护。数据处理算法编写,开发高效的数据处理算法,对通讯过程中采集到的数据进行预处理。比如进行滤波操作以去除噪声干扰,开展数据转换使数据格式符合系统要求,实施数据分析挖掘数据背后的价值,为后续的控制决策提供有力支持。错误处理机制构建,在程序里构建完善的错误处理机制,以应对通讯过程中可能出现的各类异常情况。当发生数据丢失、校验错误、网络中断等问题时,程序能够迅速做出响应,采取重传数据、报警提示等措施,保障通讯的可靠性。程序测试与优化,对编写完成的通讯程序进行全面测试,包括功能测试、性能测试、兼容性测试等。

3.3系统集成与联调

系统集成与联调是工业控制系统中PLC通讯协议实现的重要阶段,它确保各个组件协同工作,使整个系统稳定运行。(1)设备整合连接：将PLC、传感器、执行器等各类设备按照设计要求进行物理连接,确保连接的稳定性和正确性。遵循电气规范进行布线,减少信号干扰,为数据的可靠传输奠定基础。(2)协议适配优化：对不同设备所采用的通讯协议进行适配,依据协议特点和设备性能进行参数调整与优化。确保设备之间能够准确无误地进行数据交换,实现无缝通讯。例如采集第三方环保数据时我们利用NT6000双通道Modbus RTU通讯模件,同过RS485接口采集数据,起到低速,短距离,无干扰的性能。(3)数据交互测试：开展全面的数据交互测试,验证设备之间的数据传输是否准确、及时。模拟各种工况,检查数据的完整性和一致性,发现并解决可能存在的数据传输问题。(4)功能协同验证：对系统的各项功能进行协同验证,确保设备之间能够按照预定的逻辑协同工作。测试系统在不同工作模式下的运行情况,检查功能的实现是否符合设计要求。(5)问题排查解决：在联调过程中,密切关注系统的运行状态,及时发现并排查出现的问题。针对通讯故障、设备异常等问题,进行深入分析,采取有效的解决措施,确保系统能够稳定、可靠地运行。

3.4安全保障与优化

在工业控制系统中,实现PLC通讯协议时,安全保障与优化至关重要,关乎系统的稳定运行和数据安全。建立访问控制机制,设置严格的用户权限,防止未经授权的访问。采用数据加密技术,对传输和存储的数据进行加密处理,避免数据在传输过程中被窃取或篡改。同时,建立身份认证体系,确保通讯双方身份的真实性。部署防火墙,对网络流量进行监控和过滤,阻止外部非法入侵。安装入侵检测系统,实时监测系统的异常行为,一旦发现入侵迹象及时发出警报。定期更新安全补丁,修复系统漏洞,增强系统的抗攻击能力。对通讯协议的参数进行优化调整,如调整通讯速率、重传间隔等,以提高数据传输效率。优化数据处理算法,减少数据处理时间,提高系统的响应速度。同时,合理分配系统资源,避免资源浪费和瓶颈问题。持续监控与维护是保障系统安全稳定的长效机制,建立实时监控系统,对通讯协议的运行状态进行全面监控,及时发现潜在的安全隐患和性能问题。定期对系统进行维护和检查,对设备进行保养和升级,确保系统始终处于最佳运行状态。

4 结语

未来,工业自动化持续推进,PLC通讯协议也将不断演进。必须持续关注技术发展,紧跟工业4.0、物联网、人工智能等新兴技术趋势,把握技术发展方向,以便及时将新技术融入协议优化中。不断优化协议性能,如提高通讯速率、降低延迟、增强数据处理能力等,满足工业控制系统日益增长的需求。同时,着重增强协议的安全性与兼容性,抵御网络攻击,实现不同设备、系统间的无缝对接。如此,方能为工业控制系统的高效、智能运行提供更坚实有力的支撑。

[参考文献]

[1]张晓锐,马世超,刘卫国.基于PLC的智能工业机器人控制系统研究[J].现代制造技术与装备,2025,61(1):192-194.

[2]李博涵,曹浩.基于PLC的工业机器人控制系统设计分析[J].计算机应用文摘,2025,41(12):123-125.

[3]李婷婷.PLC控制的工业机器人系统的研究与实现分析[J].今日自动化,2020(7):32-34.