

# 将物联网与 PLC 系统集成用于智能制造

李瑜媚 李先

(广东省轻工业技师学院, 广东 广州 510310)

**摘要:** 本文探讨将物联网技术 (IoT) 与可编程逻辑控制器 (PLC) 系统集成在智能制造中的优势、挑战和潜在应用。物联网技术可以实现设备之间的通信和数据交换, 而 PLC 系统则用于监控和控制工业设备。将这两者集成可以实现实时数据采集与分析、自动化决策与调度、远程监控与控制等优势。然而, 集成过程中需要解决安全和隐私的问题、标准化和兼容性等问题的挑战, 并考虑系统复杂性和成本等问题。

**关键词:** 智能制造; 物联网; PLC; 实时数据; 自动化决策; 远程监控; 故障预测

智能制造是当今工业领域的重要发展方向, 旨在提高生产效率、降低成本并实现高质量的产品制造。物联网技术和 PLC 系统都是在实现智能制造过程中的关键技术。

## 一、物联网和 PLC 系统的概述

物联网 (Internet of Things, IoT) 是通过物理设备、传感器、专用软件等实现对物品感知、识别、控制, 通过互联网实现数据收集, 分析和处理, 从而提供高智能决策。

PLC 系统 (Programmable Logic Controller, 可编程逻辑控制器) 是一种专门用于自动化控制的计算机系统。它以硬件和软件相结合的形式, 具有可编程性、稳定性、可靠性等特点, 广泛运用于工厂生产线、机械设备、过程控制以及其他自动化领域。

## 二、物联网与 PLC 系统集成的优势

### (一) 实时数据采集和分析

物联网技术可以实时采集各种类型的数据, 数据类型具体取决于应用场景和需求: 如环境参数, 有压力、光照强度、温度、湿度等; 如设备状态, 有电流、电压、功率、振动、噪音等; 如生产数据, 有生产速率、产品质量、物料消耗等; 如健康监测, 有心率、血压、血氧饱和度等数据, 可以实现实时数据的采集, 将准确、及时采集数据传输到云平台进行分析并发送到 PLC 系统进行处理。

实时数据分析可以在数据采集后立即进行, 通过一系列算法和模型处理, 迅速做出决策和采取行动, 可以帮助用户发现潜在问题, 提前预警, 还可以通过监测关键指标数据, 如设备使用率、效率等, 提供洞察力, 支持决策的制定。

### (二) 自动化决策和调度

结合物联网和 PLC 系统, 可以利用物联网中的丰富数据和 PLC 系统的逻辑控制功能, 实现智能化的决策和调度。自动化决策可以涉及设备开关的控制、生产过程的调整、告警和通知等, 将采集到的信息自动安排、优化任务和资源分配, 通过先进的计算方法和模型来达到优化生产计划的目的, 包括设备的启停、物料的运输、人员的调度等, 例如, 在生产线上, 根据实时数据和预设规则, 可以自动调整机器速度、优化生产进度并分配任务, 企业可以实现资源的最优利用、提高生产效率。

### (三) 监控和控制

由于物联网的连接性, 通过手机或电脑等终端设备, 可以实时远程监控、远程诊断和调整。物联网与 PLC 系统的连接让操作者可以随时掌握设备的状态, 进行故障诊断和维护, 无需亲自到场, 这对跨地域、跨时区的监控和控制任务非常有用, 节省时间和成本, 使得生产管理更具有便捷性和灵活性。

### (四) 故障预测和预防

物联网技术结合 PLC 系统通过采集和分析数据来预测可能的

故障, 从而采取预防措施, 降低生产线停机时间。

## 三、物联网与 PLC 系统集成的挑战

### (一) 安全和隐私问题

物联网的使用中产生大量的数据, 数据的传输和共享过程中需保证其隐私和安全。在物联网与 PLC 系统集成中, 需采用适当的措施来保证数据的完整性、可用性和隐私性, 以防止未授权用户的访问和攻击, 我们可以从以下几个方面加强防护。

1. 身份认证与访问控制: 物联网与 PLC 系统集成后, 要确保注册用户才有访问权和控制系统的权限。其认证方式有: 最基本的用户名加密码的身份认证方式; 双因素身份认证, 即除了用户名和密码还需要额外的验证因素, 像手机验证码、指纹识别或硬件令牌等; 由可信的第三方机构颁发的数字证书认证; 也可 API 密钥认证、OAuth 认证、单点登录 (SSO) 等。因此, 用强大的身份认证机制来验证用户身份, 并加以适当的访问控制策略, 是安全保障的一个重要环节。

2. 网络安全: 物联网与 PLC 系统集成是通过网络进行通信。这增加了网络攻击的风险, 例如黑客入侵、拒绝服务攻击等。为了确保网络安全, 必须采取安全的通信协议、加密技术和防火墙等措施来保护通信过程中的数据安全。

3. 数据隐私: 物联网与 PLC 系统集成在运行过程中会产生大量的数据, 这些数据可能包含敏感信息, 不加以妥善保护, 可能导致隐私泄露。因此, 需要采取数据加密、数据去标识化和数据访问控制等措施, 确保数据的隐私性。

4. 设备安全: 在物联网与 PLC 系统集成中的设备可能存在安全漏洞, 受到恶意攻击。为了提高设备的安全性, 可定期更新设备的个别固件和软件, 使用可信的供应链, 加强设备的物理安全等。

5. 系统监控与响应: 物联网与 PLC 系统集成的使用, 需要建立有效的监控机制, 及时检测异常活动、未经授权的访问、恶意的攻击等, 并及时生成警报。同时, 还需要建立相应的响应机制, 快速响应和隔离受影响系统和设备, 以减小潜在的损失, 定期备份物联网和 PLC 系统中的重要数据, 测试恢复机制, 确保在被攻击或出现故障时能够快速恢复运行。

6. 人员培训与意识: 安全与隐私问题不仅仅依赖于技术措施, 也需要关注人员的意识和技能的培训。为系统管理员和用户提供免费安全培训, 了解最佳的安全实践, 并保持对安全威胁的警惕。

### (二) 数据格式和标准化

物联网设备和 PLC 系统能生成和处理不同的数据格式。数据可以采用多种格式进行表示, 如文本、数字、时间、布尔值等。为了确保数据的一致性和互操作性, 需要定义统一的数据格式。常见的数据格式包括 JSON (JavaScript Object Notation)、XML (eXtensible Markup Language) 和 CSV (Comma Separated Values)

等,而 PLC 系统使用的是二进制格式。在集成过程中,需要确定合适的格式,并确保数据在传输和处理过程中保持一致。

实现设备之间的通信和数据交换,需要定义统一的数据协议。常见的数据协议有 MQTT (Message Queuing Telemetry Transport) 消息队列遥测传输协议、CoAP (Constrained Application Protocol) 受限应用程序协议、OPC UA (Open Platform Communications Unified Architecture) 用于实现工业自动化系统中的设备和应用程序之间的通信等。这些协议提供了在不同设备之间可靠、安全和高效通信的机制。

为了推动物联网与 PLC 系统集成的数据格式和标准化,有一些组织致力于制定相关标准和指南。例如,国际标准化组织 (ISO) 制定了一系列与物联网和工业自动化相关的标准,如 ISO/IEC 27000 系列关于信息安全管理系统的标准,ISO/IEC 30141 关于物联网参考架构的标准等。此外,还有各行业的标准组织,如 OPC Foundation 致力于开放式工业自动化标准,IEEE (Institute of Electrical and Electronics Engineers) 致力于电子和电气工程标准等。

物联网与 PLC 系统集成涉及到不同的领域和行业,每个领域都可能有其特定的数据格式和标准。例如,在智能家居领域,可以使用 Zigbee、Z-Wave 等无线通信协议;在工业自动化领域,可以使用 Modbus、Profibus 等通信协议。因此,根据具体的应用场景和行业要求,需要遵循特定的领域标准。

### (三) 通信协议兼容性

物联网设备和 PLC 系统通常使用不同的通信协议。物联网设备使用基于 IP 的协议,如 MQTT 或 HTTP,而 PLC 系统通常使用专有的实时通信协议,如 Modbus 或 Profibus。因此,为了实现无缝集成和通信,需要制定统一的标准和协议,并确保不同设备能够相互兼容和协作。

在选择通信协议时,应考虑 PLC 系统和物联网设备所支持的协议。如果两者之间的通信协议不兼容,就需要使用网关或中间件来进行协议转换。物联网设备和 PLC 系统通常通过不同的硬件接口进行连接,如以太网、串口、无线通信等。在集成过程中,需要确保物联网设备和 PLC 系统之间的硬件接口兼容,并且能够正确地传输数据。

不同的通信协议使用不同的数据格式和结构。在物联网与 PLC 系统集成中,需要进行数据格式的转换,以确保不同设备之间能够正确地解析和处理数据。例如,使用中间件或数据网关进行数据格式转换,将从物联网设备接收到的数据转换为 PLC 系统能够理解的格式。在物联网与 PLC 系统集成完成后,应进行兼容性测试以验证通信协议的兼容性。通过模拟实际环境中的通信和数据传输,可以确保物联网设备能够正确地与 PLC 系统进行通信,并且数据能够准确地传输和分析。

### (四) 复杂性和可靠性

物联网与 PLC 系统集成可能涉及到多个设备、传感器和网络的联接,这增加了系统的复杂性,可能导致在集成、部署和维护过程中出现问题,所以要确保系统的可靠性和稳定性,以及建立适当的错误处理和故障恢复机制。

物联网中的设备类型多样,这些设备通过各种不同的通信协议进行通信。PLC 系统也有不同的型号和品牌,它们使用的通信协议和数据格式也可能不同。因此,将不同类型的物联网设备与 PLC 系统集成需要处理多样性的设备和协议。物联网设备会产生大量的数据,这些数据需要被捕获、处理和传输到 PLC 系统进行进一步的操作和控制。确保数据的准确性、完整性和实时性是非常重要的,同时还需要考虑数据存储和数据安全。

将物联网与 PLC 系统集成需要设计和实施适当的系统架构。这涉及到连接和通信的配置、数据流的管理以及各个组件之间的集成。同时,还需考虑到系统的可扩展性和灵活性,以便在需要时能够添加、更新或替换设备或组件。在网络上进行通信时,网络通信的可靠性是确保数据和指令能够准确、及时地传输的关键因素。对于实时控制应用,如工业自动化,延迟或中断的网络连接可能会导致系统故障或损失。

物联网设备和传感器是数据采集和控制的关键组成部分,这些设备需要具备较高可靠性,以确保其正常运行和准确的数据采集。设备的故障可能导致数据丢失、错误的操作或导致系统停机。由于物联网设备和 PLC 系统都容易成为网络攻击的目标,必须采取适当的安全措施来保护系统免受未经授权的访问、数据泄漏或其他潜在威胁。

### (五) 数据管理和分析

确保有效地管理和分析物联网设备和 PLC 系统产生的大量数据,以便提取有价值的信息、优化生产过程并做出正确的决策,至关重要。为此,建立适当的数据管理和分析策略。

物联网设备收集各种类型的数据,PLC 系统可以生成控制命令和状态反馈的数据。在集成过程中,这些需要被采集和存储的数据需要保证其准确、完整和实时性。将采集到的数据可以使用数据库、云存储或边缘计算设备等方式进行存储,以便后续分析和应用。

为实现有效的数据存储和分析,可以采取以下措施:

1. 确定数据采集需求和存储方案,包括数据类型、频率和存储容量的规划。
2. 使用合适的清洗和预处理技术,如异常检测、插值或滤波等,以确保数据质量。
3. 选择适当的数据分析工具和算法,如实时监测算法、故障诊断方法或机器学习模型。
4. 将数据可视化展示,如图表、仪表或报告等,使数据更易于理解和应用。
5. 加强数据安全和隐私保护,确保只有授权人员才能访问和使用数据。

### 五、结论

将物联网技术与 PLC 系统集成是实现智能制造的一种重要途径。该集成可以提供实时数据采集与分析、自动化决策与调度、远程监控与控制等优势。然而,在实施过程中需要克服安全和隐私问题、标准化和互操作性的挑战,同时考虑系统的复杂性和成本。尽管如此,物联网与 PLC 系统集成在智能制造领域具有广泛的潜在应用,可以推动工业生产的转型升级,提高生产效率和产品质量。

### 参考文献:

- [1] 杨永泉. 物联网技术在智能制造中的应用 [J]. 现代制造技术与装备, 2022, 58 (10): 121-123.
- [2] 张超, 周光辉, 李晶晶, et al. 新一代信息技术赋能的数字孪生制造单元系统关键技术及应用研究 [J]. 机械工程学报, 2022, 58 (16): 15.
- [3] 鹿晓丹. 从物联网到人工智能. 上 [M]. 浙江大学出版社, 2020.
- [4] 邹尚恩, 刘开鑫, 孙晓辰, 等. 智慧景观背景下物联网技术研究进展与展望 [J]. 风景园林, 2023, 30 (8): 64-71.