物联网环境下工业生产过程的智能化监控与管理

李 岷

（金隆铜业有限公司 安徽 铜陵 244021）

摘 要 文中设计并实现了一种能在物联网环境下对工业生产过程进行智能化监控与管理的系统。该系统通过实时数据采集、深度分析和精细处理，优化了生产流程，大幅提高了生产效率，并为企业智能决策提供了支持。同时，文中探讨了物联网中的安全风险，并据此设计了一套多层次的安全通信和认证机制，以确保数据的安全性。经过严格的性能测试和实地验证，该系统在高并发环境下表现出了较好的稳定性和安全性，满足了工业智能化生产的实际需求。

关键词： 工业物联网；智能化监控；物联网安全；加密算法

中图分类号 TP311.5

Intelligent Monitoring and Management of Industrial Production Processes in the Internet of Things Environment

LI Min

（Jinlong Copper Industry Co., Ltd., Tongling, Anhui 244021, China）

Abstract This paper designs and implements a system that can intelligently monitor and manage the industrial production process in the Internet of Things environment. Through real-time data collection, in-depth analysis and fine processing, the system effectively optimizes the production process, greatly improves the production efficiency, and provides support for intelligent decision-making of enterprises. At the same time, this paper discusses the security risks in the Internet of Things, and designs a multi-level security communication and authentication mechanism accordingly to ensure the security of data. After rigorous performance testing and field verification, the system has demonstrated excellent stability and security in a high-concurrency environment, meeting the practical needs of industrial intelligent production.

Key words Industrial Internet of Things, Intelligent monitoring, IoT security, Encryption algorithms

0 引言

智能电气自动化系统集成了现代信息技术、自动化技术、电气工程技术等，能有效提高工业生产效率、降低生产成本、提升产品质量，是实现工业生产现代化的关键[1]。随着物联网技术的不断进步，工业物联网（IIoT）得到了广泛应用，使得海量设备与传感器可以相互连接，实现了实时监控与精细化管理，推动了生产效率和资源利用率的提升。

1 相关技术介绍

1.1 工业物联网

在工业领域，基于物联网（IoT）技术的工业物联网（IIoT）至关重要，其可以对机器设备、感知元件及云端系统进行深度联动，实现工业生产的智能化，实现自动化的管理和远程监控。与传统的工业控制系统相比，IIoT 汇聚了大数据、云计算及人工智能等技术，使得设备可以进行自我监控与维护，降低了故障率。IIoT 的普及提高了生产线的灵活性，为企业提供了更强的市场适应性，增强了企业的市场竞争力。

1.2 物联网技术架构

物联网技术通常由感知层、网络层和应用层组成。感知层汇聚了各种传感器与智能设备，负责采集并初步处理数据；网络层能借助先进的无线通信技术，如 Wi-Fi、5G 等，将感知层获得的数据流畅且快速地传输至云端或其他平台；应用层则可以基于这些数据，催生出远程控制、深度数据分析等一系列服务和应用。在工业环境中，这种技术架构能确保信息从生产现场畅通无阻地传输至企业管理层，推动企业生产方式和管理模式的创新与变革，提高企业的生产效率和灵活性。

1.3 物联网安全

对工业机器人和自动化设备而言，其稳定性和完整性会直接受到物理攻击或破坏的影响。因此，确保工业生产中的人工智能系统（包括监控、访问控制和紧急停机系统）得到适当的物理保护，是保障系统安全性的关键。此外，应

作者简介：李岷（1970—），本科，工程师，研究方向为计算机及电子信息。

用于工业生产的人工智能系统需要符合各种法规和标准，尤其是与数据安全和隐私有关的法规[2]。在复杂的物联网环境中，由于物联网涉及的设备种类繁多且分布广泛，其面临的安全风险也尤为突出，数据泄露、网络攻击等安全威胁层出不穷。为确保物联网的稳定运行，需要采用有效的安全措施。设备认证、加密通信、严格的访问控制和防火墙设置等可以组成一张安全防护网，确保数据传输的机密性、完整性和可用性。在工业物联网领域，安全问题不容忽视。一旦系统遭受攻击，生产流程就会受到严重影响，从而带来经济损失甚至引发安全事故。因此，建立健全的物联网安全机制，是确保物联网能健康、稳定、持续发展的关键。

2 物联网环境下工业生产过程智能化监控与管理系统的设计

2.1 需求分析

在传统制造业中，实时掌握生产状态，有效协调各方资源，持续提升生产效率和产品合格率是生产管理者面临的重大挑战。工业物联网技术的发展为解决这些问题提供了新的思路和工具。通过工业物联网，可以实时监控生产车间的各项数据，包括工单执行情况、人员和设备状态、物料流转、产品质量、环境参数等，从而精准掌握生产状态。物联网技术还可以实现设备间的互联互通，以及部门间业务数据的共享，使得车间协同更加顺畅和高效。通过数字建模和数据分析，管理者能不断优化生产流程和工艺参数，持续提高生产效率和产品合格率，促进企业的可持续发展[3]。

2.2 系统总体设计

在物联网驱动的工业生产中，智能化监控与管理系统的总体设计应着眼于实时数据采集与处理，以提高生产效率，提升设备利用率，降低运营成本。该系统可分为感知层、网络层和应用层，如图1所示。

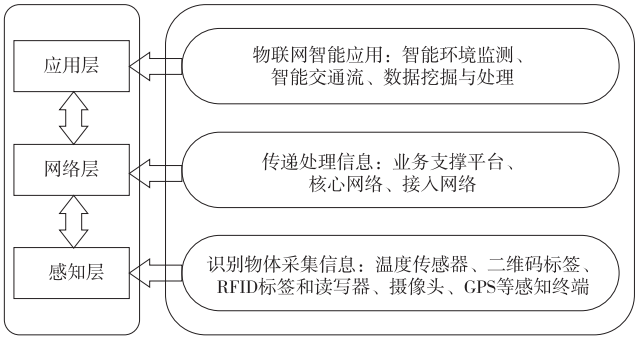

图1 系统总体架构

其中，感知层一般用于捕捉生产设备与环境中的数据；网络层则借助工业以太网、Wi-Fi或5G等通信技术，将数据源源不断地传输至云平台或本地服务器；应用层可对数据进行深度分析与处理，生成直观可视的报告，并提供智能决策支持。该系统设计以模块化、可扩展性与安全性为核心，让企业能依需定制配置，满足不同的生产需求。同时，可利用数据加密和权限管理方法保证信息安全，促进企业的健康发展。

2.3 系统功能模块设计

智能化监控与管理系统的功能模块旨在实现高效、智能的生产流程管理。其中，数据采集模块负责搜集来自传感器、控制器和物联网设备的实时数据，为管理者描绘出生产设备的运行状态；数据分析模块能对数据进行深度挖掘，为生产流程中的优化和异常发现提供依据；报警模块能在发现系统故障或异常时迅速发出警报，并通过短信或电子邮件通知相关人员；设备管理模块则实现了远程的设备控制，使设备管理更便捷；用户界面模块能以人性化的设计确保管理者直观地监控系统状态，快速响应生产过程的变化。

2.4 系统数据库设计

系统数据库设计可用于统一存储和管理各类工业数据。为应对大规模数据的并发处理要求，可以采用分布式架构，确保系统的高效运行。数据库中存储着设备运行状态、生产流程数据、环境监测数据以及报警记录等重要信息，应用了数据加密技术、访问权限控制和备份机制。另外，数据库还支持实时数据与历史数据的查询和分析，以便为智能化决策提供数据支撑。为使用企业不断扩大的生产规模，数据库需具备扩展性，确保系统能长期、稳定地运行。

2.5 系统接口设计

系统接口设计的核心在于打造一个工业生产监控与管理系统与其他外部系统或设备间能高效、安全进行数据交互的通道，其中设备接口、数据接口和用户接口组成了接口体系的核心。设备接口采用标准化协议，如Modbus、OPC等，确保能顺利与各类生产设备与传感器进行连接与通信。数据接口则利用RESTful API或WebSocket等通信协议，使得系统能与外部数据库、云平台或其他信息系统进行数据交换。在用户接口方面，需设计简洁直观的界面，支持PC端控制台访问以及移动设备的APP或网页访问。

2.6 系统功能实现

在设计生产监控与管理系统时，需要协调硬件与软件的功能性。首先，需依赖安装在生产设备上的传感器与控制器等硬件来捕获并传递生产设备的关键数据。其次，软件层需基于数据采集模块接收并处理这些数据流。如此，用户可借助用户界面模块了解生产设备的运行状态，甚至进行远程控制。系统功能还可进一步拓展至故障报警、设备维护计划管理以及生产参数的优化调整。

3 基于加密算法的物联网安全机制设计

3.1 物联网安全风险分析

在物联网领域，设备种类繁多且数量庞大，给管理和安

全保障带来了巨大挑战。每个设备在固件、软件或硬件层面都可能存在潜在的安全隐患，从而被攻击者利用。此外，这些设备通常基于无线网络连接，降低了网络的安全性，使物联网系统易遭受各种恶意攻击，如拒绝服务（DoS）攻击或中间人攻击。在数据传输方面，未经加密的信息在传输过程中会面临被拦截、篡改或泄露的风险[4]。

3.2 物联网通信安全问题分析

在数据传输过程中，若缺乏足够的加密保护，信息就可能被恶意的中间人拦截或篡改，导致敏感数据的泄露。另外，当未经充分验证的设备接入网络时，也可能带来未经授权的访问风险。攻击者也可能会伪装成合法设备来窃取系统的敏感信息或控制权。网络层攻击的另一形式为拒绝服务（DoS）攻击，即通过大量的恶意请求来瘫痪网络，让设备间的正常通信受阻。

3.3 物联网认证机制

在物联网生态系统中，各种设备和用户需被赋予明确的身份，并经过严格的验证，以确保系统的稳定性与安全性，使得只有经过认证的设备和用户才能在网络中进行数据交互。为应对物联网设备资源受限的挑战，认证机制需追求轻量化和安全性。这需要在设计认证机制时考虑设备的性能，确保信息的安全传输。常见的认证方法包括数字签名、公共密钥基础设施（PKI）、对称加密等。只有当设备通过认证服务器的严格检验，确认其身份合法性后，该设备才能获得接入网络的权限。

3.4 物联网安全通信机制

保护数据在设备与网络间的安全传输是物联网安全通信机制的核心目标。为确保数据不被窃取或篡改，需要采用多种加密技术和协议。对称加密（如AES）在实时性要求较高的场景下表现出色，能实现对数据的有效保护。非对称加密（如RSA）更适用于需要进行身份验证的通信，可通过公钥和私钥的配合确保进行身份验证。此外，TLS和DTLS等安全通信协议在物联网设备间的通信中十分重要，这些协议可以利用先进的加密技术和机制保护信息的机密性、完整性和不可否认性，来降低数据泄露和中间人攻击的风险[5]。

4 效果评估

4.1 系统运行环境

在工业生产过程中，智能化监控与管理系统的运行环境至关重要[6-7]，该系统集成了硬件与软件两个层面。在硬件层面，其借助高精度的传感器、工业控制器、网络设备和服务器，确保了数据采集和传输的稳定性。在软件层面，其能基于云平台架构，应用分布式数据库和大数据处理框架，实现多终端的实时访问和控制。借助工业以太网和5G网络，系统呈现出高带宽、低延迟的卓越性能。同时，需严格保护网络安全，实施加密通信和访问控制策略，保障工业数据的安全传输和设备的稳定运行。

4.2 系统性能测试与验证

为验证系统性能，本文进行了多项测试。（1）数据采集与处理能力的负载测试，以确保系统能在高并发环境下保持稳定。（2）响应速度测试，以评估系统面对突发故障和生产异常的反应速率。该测试全面涵盖了数据处理能力、响应速度、稳定性和安全性，测试结果如表1所列。可以看到，在高负载情况下系统能维持稳定的数据处理与响应，满足了工业生产的严苛要求。

表1 关键测试结果的数据

测试项目	测试条件	结果/s	标准值/s	通过与否
数据采集延迟	高负载下300设备并发	1.2	≤1.5	通过
响应时间	设备异常报警	2.3	≤2.5	通过
数据传输安全	模拟攻击情况下	无数据泄露	无泄露	通过

4.3 结果分析

该智能化监控与管理系统表现出色，不仅能进行高并发数据采集任务，且在面对生产异常时具备较高的响应速度。系统在数据采集延迟和设备异常响应时间的测试中均超越了行业标准，展现出较高的运行效率。此外，经过模拟攻击测试，该系统的网络安全机制成功守护了数据安全，验证了其可靠性。

5 结语

本文设计并实现了一种适用于物联网环境下的工业生产的智能监控与管理系统，同时建立了安全通信和认证机制。该系统不仅提高了生产效率和管理水平，还提高了数据传输的安全性。经过测试，该系统具备较强的稳定性和有效性，为工业企业提供了强有力的技术支持，能帮助企业更好地适应智能化生产需求，提升竞争力。

参考文献

[1] 严登梅，阚新星.智能电气自动化系统在工业生产中的应用研究[J].造纸装备及材料，2024，53(7)：47-49.
[2] 刘潇.人工智能技术应用于工业生产的研究[J].信息记录材料，2024，25(6)：164-166.
[3] 马丽丽，刘源.基于工业物联网的数字化生产车间设计[J].中国信息化，2024(4)：68-70.
[4] 蔡红斌.物联网通信在工业监控系统中的应用[J].信息记录材料，2024，25(2)：96-98.
[5] 申晓波.基于物联网数字工厂与智能工厂的整合[J].中国新通信，2024，26(1)：38-40.
[6] 柴天佑.工业人工智能与工业互联网协同实现生产过程智能化及其未来展望[J].控制工程，2023，30(8)：1378-1388.
[7] 班雯.工业经济智能化发展的五个关键[J].信息化建设，2021(7)：37-38.