工业物联网（IIoT）背景下的 PLC 控制系统安全加固方案

蒲国庆[1]，郝 康[2]

[1]衢州纤纳新能源科技有限公司 浙江衢州
[2]深圳市人力资本（集团）有限公司 广东深圳

【摘要】随着工业物联网（IIoT）技术的迅速发展，传统的 PLC 控制系统逐渐面临越来越复杂的安全威胁。PLC 作为工业控制系统的核心，承担着自动化生产、设备监控和实时控制等重要任务。PLC 控制系统通常缺乏有效的安全防护，容易成为黑客攻击和恶意软件侵入的目标。本研究旨在探讨在工业物联网背景下，如何通过多种安全加固措施提升 PLC 控制系统的安全性。通过对现有安全漏洞的分析与评估，提出了一系列安全加固方案，涵盖网络隔离、身份验证、数据加密等措施，旨在构建更为安全的 PLC 控制系统架构，以保障工业生产的稳定性和安全性。

【关键词】工业物联网；PLC 控制系统；安全加固；网络隔离；数据加密
【收稿日期】2025 年 5 月 16 日 【出刊日期】2025 年 6 月 7 日 【DOI】10.12208/j.aics.20250014

Security reinforcement scheme for plc control systems in the context of Industrial Internet of Things (IIoT)

Guoqing Pu[1], Kang Hao[2]

[1]Quzhou Xianna New Energy Technology Co., Ltd. Quzhou, Zhejiang
[2]Shenzhen Human Capital (Group) Co., Ltd. Shenzhen, Guangdong

【**Abstract**】With the rapid development of Industrial Internet of Things (IIoT) technology, traditional PLC control systems are gradually facing increasingly complex security threats. As the core of industrial control systems, PLCs undertake important tasks such as automated production, equipment monitoring, and real-time control. PLC control systems typically lack effective security protection, making them vulnerable targets for hacker attacks and malicious software intrusions. This study aims to explore how to enhance the security of PLC control systems through various security reinforcement measures in the context of IIoT. By analyzing and evaluating existing security vulnerabilities, a series of security reinforcement schemes are proposed, covering measures such as network isolation, authentication, and data encryption. The goal is to construct a more secure PLC control system architecture to ensure the stability and safety of industrial production.

【**Keywords**】Industrial Internet of Things (IIoT); PLC control system; Security reinforcement; Network isolation; Data encryption

引言

随着工业物联网（IIoT）技术在制造业和生产流程中的广泛应用，工业控制系统的安全性问题愈发重要。PLC 控制系统作为核心设备，直接影响着生产过程的自动化与稳定性。然而，传统的 PLC 控制系统在设计时，往往缺乏对网络攻击和系统入侵的防护措施，极易受到外部威胁的侵害。IIoT 的普及使得这些系统不仅面临来自内部的安全隐患，还需要防范来自外部网络的各种安全攻击。针对这一背景，本文提出了在 IIoT 环境下对 PLC 控制系统进行安全加固的必要性与可行性。研究分析了现有安全漏洞，并通过技术手段提出了有效的安全加固方案，旨在为工业生产中的 PLC 控制系统提供更强的安全防护保障。

1 PLC 控制系统安全问题分析与挑战

随着工业物联网（IIoT）技术的快速发展，PLC 控制系统面临的安全问题日益复杂。传统的 PLC 系统在设计时更多关注生产效率和控制稳定性，而忽视了对网络攻击和数据泄露的防护。由于 PLC 设备通常依赖开放的通信协议，如 Modbus、Profinet 等，这使得它们暴露在网络攻击的风险中。攻击者能够通过这些漏洞

远程入侵系统，实施恶意操控或获取敏感数据。这些安全问题不仅威胁到企业的生产安全，还可能导致设备损坏或生产停滞，带来巨大的经济损失。

PLC 控制系统常常缺乏足够的身份验证和访问控制机制，导致内部人员或不法分子通过简单的手段就能接入控制系统。PLC 设备通常运行着重要的工业应用程序，这些程序控制着工厂的生产、监控设备以及关键设备的运行状态。在许多情况下，PLC 系统并未进行加密保护，且没有适当的日志记录与监控机制，这使得恶意行为在系统内部更难以被及时发现，攻击者可以长时间地进行破坏而不被察觉。对于工业控制系统来说，这种缺乏有效监控和响应机制的现状，给信息安全管理带来了极大的挑战。

工业物联网的普及使得 PLC 控制系统与外部世界的连接性大大增强，但这种扩展也带来了更多的安全风险。通过网络连接的 PLC 系统往往要面临来自互联网的攻击，包括 DDoS 攻击、恶意软件传播等问题。尤其是当控制系统与云计算平台、大数据平台以及其他业务系统的接口没有进行严格保护时，外部攻击者就能通过这些接口突破防线，甚至在系统中植入病毒或勒索软件[1]。面对这些挑战，传统的防火墙和杀毒软件往往无法有效应对工业环境中的独特安全威胁，导致现有的 PLC 控制系统在工业物联网环境中极易受到攻击和入侵。

2 工业物联网环境下的 PLC 控制系统安全需求

在工业物联网环境下，PLC 控制系统的安全需求变得愈加复杂和迫切。随着设备和系统的互联互通，PLC 不再是孤立的单元，而是与各种传感器、执行器以及更高层次的生产管理系统相连接。这样的高度集成使得 PLC 控制系统暴露于更广泛的攻击面，迫切需要采取更加严密的安全措施，确保系统的完整性、保密性和可用性。PLC 系统不仅需要抵御外部的网络攻击，还必须防范来自内网的潜在威胁。这就要求在设计时，必须考虑到全面的身份验证、访问控制以及数据加密措施，确保只有经过授权的用户或系统才能访问和操作 PLC。

在这样的背景下，数据的安全传输成为一个至关重要的需求。PLC 控制系统通常需要通过网络与其他设备或云平台进行通信。为了防止数据在传输过程中被篡改或泄露，通信协议和数据传输过程必须采用高强度的加密措施。随着 IIoT 的广泛应用，越来越多的外部设备和终端接入到 PLC 控制系统，增加了系统的复杂性。为了应对这一挑战，控制系统的安全需求不仅仅是防止恶意攻击和数据泄露，更需要考虑到如何在保证系统安全的前提下，保证其在复杂环境中的正常运行。PLC 系统必须具备强大的实时监控能力和自动响应机制，能够在系统受到攻击或出现异常时，迅速做出反应，避免重大事故的发生。

随着工业环境中智能化和自动化的不断推进，PLC 控制系统的安全需求也涵盖了对安全漏洞的实时监测和修复。为了保证系统长期安全运行，定期的安全审计和漏洞扫描成为必不可少的环节[2-6]。通过部署多层次的安全防护措施，如防火墙、入侵检测系统、行为分析等，及时发现潜在的安全威胁并进行响应，是保障 PLC 控制系统免受攻击的必要条件。随着工业物联网技术的不断进步，PLC 控制系统的安全性不仅依赖于传统的防护手段，还需要结合人工智能、大数据分析等技术，提升对复杂攻击模式的识别能力，从而确保工业生产的高效、安全和稳定。

3 PLC 控制系统安全加固技术方案

为了提高 PLC 控制系统在工业物联网环境中的安全性，必须采取一系列切实可行的安全加固技术。一个关键的加固技术是网络隔离。通过将 PLC 控制系统与外部网络进行物理或逻辑隔离，能够有效阻止外部网络攻击或恶意软件的侵入。此方法通过设立防火墙、使用虚拟局域网（VLAN）以及网络访问控制（NAC）来限制 PLC 系统与其他系统或设备之间的直接通信。这种隔离技术不仅能够降低被攻击的风险，还能够限制恶意行为的蔓延，确保重要工业控制系统的独立性和安全性。

增强身份验证和访问控制机制是提升 PLC 控制系统安全性的重要手段，能够有效防范未经授权的访问和恶意操作。多因素身份验证（MFA）不仅要求用户提供传统的密码，还能结合指纹、面部识别或安全令牌等生物识别技术或硬件设备，以确保用户身份的真实性和唯一性。角色基础访问控制（RBAC）则根据用户的职责和角色设置不同的访问权限，确保不同层级的人员只能访问其职责范围内的系统资源。这种方法不仅防止了外部黑客的入侵风险，也能有效遏制内部人员的不当操作或恶意行为，减少系统滥用和数据泄露的可能，增强整体系统的防护水平。

加密技术也是 PLC 控制系统安全加固方案中的重要组成部分。由于 PLC 系统需要进行大量的数据传输，尤其是在工业物联网环境下，数据的安全传输尤为关键。通过采用强加密协议，如 AES（高级加密标准）或 TLS（传输层安全协议），可以确保 PLC 控制系统

与其他设备、管理系统之间的通信不被第三方窃取或篡改。加密不仅适用于数据的传输过程，还应涵盖存储的数据，防止数据在静态状态下受到攻击[7]。为了提升系统的响应能力，PLC 控制系统需要集成实时安全监控和入侵检测系统。通过对 PLC 网络和设备进行持续监控，可以及时发现异常行为，并采取相应的防护措施，如自动隔离受影响区域或触发警报。这些技术手段能有效预防潜在攻击，增强系统的自愈能力，确保生产过程的安全性与稳定性。

4 加固方案实施与效果评估

在实施 PLC 控制系统的安全加固方案时，首先需要对现有的系统架构进行全面的评估与分析。通过识别和分析现有安全漏洞、潜在威胁以及系统中存在的薄弱环节，可以为加固措施的实施提供科学依据。实施网络隔离措施时，工程师需要对系统的网络拓扑进行优化，确保 PLC 系统与其他网络之间实现物理或逻辑隔离。这一过程通常涉及到防火墙的配置、VLAN 的划分及网络访问控制策略的制定，以确保不允许未经授权的外部网络访问 PLC 控制系统。在实施这些加固技术时，还必须确保系统的实时性和响应速度不受影响，避免加固措施带来不必要的生产延误。

实施多层次的身份验证与访问控制措施时，需要对现有用户权限进行严格审核。每个用户或设备的访问权限应当基于其实际工作需要来设定，而不应过度授权。角色基础访问控制（RBAC）通过严格区分操作权限，确保只有经过授权的人员可以进行敏感操作。结合多因素身份验证（MFA）可以显著提高系统的安全性。实施这些措施时，企业需要对现有操作人员进行相关培训，确保他们能够正确理解和执行新的访问控制政策。只有在员工对新安全措施有充分认识和理解的基础上，系统的安全性才能得到有效保障。

在加固方案实施后，效果评估是关键步骤。通过监控和分析系统的运行状况，能够及时发现加固措施的有效性及其可能存在的问题。为了全面评估安全加固措施的效果，可以通过定期的安全审计、漏洞扫描和压力测试来验证系统的抗攻击能力。入侵检测系统（IDS）和实时监控系统的部署能够实时检测到潜在的安全事件，并及时响应[8]。通过对比加固前后的系统稳定性、攻击防御能力以及操作效率，能够全面评估加固措施是否达到了预期效果。对于潜在的漏洞和系统配置缺陷，还应进行持续地修复和优化，确保 PLC 控制系统在面对不断变化的安全威胁时，能够保持高效稳定地运行。

5 结语

PLC 控制系统在工业物联网环境中的安全性至关重要。随着网络攻击和安全威胁的日益增加，传统的 PLC 系统面临巨大的安全挑战。通过采取有效的安全加固措施，如网络隔离、身份验证、数据加密和实时监控，可以显著提升 PLC 系统的防护能力，减少潜在的安全风险。实施这些加固方案不仅能够保障系统的稳定运行，还能提高生产效率和安全性。在实施过程中，持续的效果评估和漏洞修复同样至关重要，确保系统在动态威胁环境中始终处于安全状态。最终，通过全面的安全加固，工业控制系统可以更好地应对未来的挑战，确保工业物联网的长期健康发展。

参考文献

[1] 王晔,施颖,夏天乐,等.面向工业物联网的时延感知半同步联邦学习客户端资源联合调度方案[J/OL].物联网学报,1-15[2025-06-24].

[2] 艾墨轩,马雪芮.基于 5G 工业物联网的造纸设备运行数据实时采集监控研究[J/OL].造纸科学与技术,1-5[2025-06-24].

[3] 陈恒云,庞勇.干式变压器工业物联网温度实时在线监测技术分析[J].电器工业,2025,(06):70-75.

[4] 周小明,刘微,张文波.一种面向工业物联网的轻量级共识机制[J].沈阳理工大学学报,2025,44(04):21-29.

[5] 张自强,杨云吉.工业物联网驱动的设备数据资产分类与预测性维护系统研究与实践[J].中国信息界,2025,(05):162-164.

[6] 吉顺平.工业物联网的智能交互模型的研究[J].自动化应用,2024,65(24):156-159.

[7] 陈振伟,黄艳华,黄慰忠,等.基于工业物联网的市政隧道智能监控系统技术浅析[J].中国市政工程,2024,(06):97-101+164.

[8] 顾成远.工业物联网场景中无线信道建模研究[D].江南大学,2024.

版权声明：©2025 作者与开放获取期刊研究中心（OAJRC）所有。本文章按照知识共享署名许可条款发表。
http://creativecommons.org/licenses/by/4.0/

OPEN ACCESS