Proceedings of the 3rd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/2025.22249

Convergence of IoT and PLC in Industrial Automation: A Systematic Review of Emerging Trends, Technical Challenges, and Prospects

Jinhua Wei

University of Science and Technology Beijing, Beijing, China
1102300979@qq.com

Abstract: Integrating PLCs with emerging IoT technologies for industrial automation has transformed the manufacturing ecosystems towards a smarter and data-driven one. This systematic review explores the synergistic potential of IoT's connectivity and PLCs' reliability in modern industrial settings. It analyses trends such as edge computing, AI-driven analytics and digital twins for technical challenges and proposes future directions using blockchain integration and 5G-enabled automation to support them. This review synthesizes academic literature, industry case studies and technological frameworks to outline a roadmap for resilient, efficient and adaptable industrial systems.

Keywords: Industrial Automation, IoT, PLC, Edge Computing, Cybersecurity

1. Introduction

The technologies in PLC and IoT have greatly revolutionized industrial automation. The traditional backbone of automation PLCs, PLCs are now augmented by the IoT's capability to exchange real-time data, monitor remotely, and predict maintenance. The purpose of this convergence is to overcome scalability and flexibility constraints as well as enhance the ability of businesses and enterprises to make decisions. Nevertheless, integrating legacy PLC systems with IoT architectures brings in technical and operational complexities. In this paper, the state-of-the-art integration between IoT, linked with multiple data fusion and deep data processing abilities, and PLC, which can control motors, valves, sensors, etc., is systematically reviewed, the challenges are evaluated, and a future direction of advancement is forecasted.

2. Background

2.1. Role of PLCs in Industrial Automation

Dominated in industrial control systems since the 1970s, PLCs have guaranteed deterministic performances for things like assembly line control and machinery synchronization. However, they are necessary due to their robustness in harsh environments and their ability to process in real time.

© 2025 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2025.22249

2.2. IoT's Impact on Industrial Systems

Ubiquitous connectivity is introduced by IoT communicating via MQTT, CoAP and other protocols. Sensor networks and cloud analytics are driven by applications such as smart grids and predictive maintenance. While the IoT brings operational technology and information technology together to leverage data-driven optimization.

2.3. Convergence Motivations

PLCs are integrated with IoT technologies to overcome the limitations in traditional industrial automation systems and enable new capabilities in modern manufacturing and process control.

2.3.1. Enhanced Visibility and Real-Time Monitoring

Traditional PLCs are usually isolated in the silo and do not have the granularity of data collection and remote oversight. IoT enables real-time monitoring of distributed industrial assets, embedding sensors, wireless connectivity and cloud-based dashboards [1]. For example, IoT-enabled PLCs can send key operational parameters like temperature, vibration and energy consumption to the centralized platform from which operators can see performance metrics of entire operations. This visibility enables proactive interventions, including adjusting production line speeds according to live throughput or identifying bottlenecks in the supply chains. Industries achieve a unified view of physical and digital workflows by merging PLCs' deterministic control with IoT's pervasive sensing.

2.3.2. Predictive Capabilities Through Data-Driven Analytics

Fusing PLCs with IoT facilitates the transition from reactive maintenance to predictive optimization. Machine learning models trained on historical and real-time IoT data streams can predict equipment degradation or failure modes with high accuracy at farther points [2]. For instance, vibration data sent in IoT sensors linked to PLC-regulated motors can be processed to discover hints of bearing wear, permitting maintenance staff to permit repairments before catastrophic failures take place. In addition, anomaly detection algorithms utilize process data that is generated by the PLC to detect abnormal operating conditions. The predictive capabilities contribute to reducing unplanned downtime, increasing asset lifespan and optimizing resources, leading to cost savings as well as operational efficiency.

2.3.3. Scalability via Cloud-Edge Architectures

Some limitations of legacy PLCs associated with centralized control architecture are that they lack agility in the changing demands of modern industrial ecosystems. This brings IoT an edge to the scalable cloud edge frameworks that decentralize decision-making. Edge nodes deployed at the edge of the systems near PLCs are responsible for the execution of real-time tasks while non-critical data is offloaded to the cloud for long-term analytics and storage. The hybrid nature of this approach allows factories to scale operations, for example, adding a new IoT-enabled production unit without having to upgrade from legacy PLC infrastructure. Furthermore, edge-based processing is latency and bandwidth-efficient, which enables high-speed execution without any significant degradation in massive deployment cases, including smart grid and multi-plant manufacturing networks.

2.3.4. Interoperability and Adaptive Automation

Additionally, besides these main motivations, the convergence of PLC with IoT meets the ever-increasing need for interoperability among heterogeneous industrial systems. The tools that serve as

DOI: 10.54254/2755-2721/2025.22249

bridges between the legacy PLC protocols and the modern IoT communication standards are called IoT middleware solutions, say OPC Unified Architecture. This interoperability allows for the coexistence of legacy and newer IoT devices and allows for a gradual updating of the industrial infrastructure. Furthermore, adaptive automation frameworks use IoT data to adaptively reconfigure PLC logic to do things such as modify robotic assembly paths based on the results of real-time IoT vision systems quality inspection results.

3. Emerging Trends

3.1. Edge Computing and Fog Architectures: Redefining Data Processing Hierarchies

However, as cloud systems become ever more centralized, they lack the latency that is required to thrive in today's industrial environment, which requires the shift to edge computing and fog architectures. However, in edge computing, data processing has been decentralized and is occurring close to PLCs and IoT devices to compute resources, allowing decisions in real-time, like in robotic control or anomaly or production of unexpected values detection [3].

This paradigm is extended by fog architectures that create an intermediate layer between edge devices and the cloud to provide collaborative processing. Fog nodes in automotive manufacturing collect data from IoT vision systems and PLC-controlled robotic arms and perform localized quality inspections. A hybrid model was created that includes balancing computational load, assigning time-sensitive tasks to the edge layer and any non-critical data, such as long-term performance logs, to the cloud. Though there are still challenges managing distributed security policies and seamless failover in the event of a disruption to the network, standards such as the Open Fog Consortium's reference architecture are driving interoperability.

3.2. AI-Driven Analytics and Digital Twins: From Reactive to Proactive Automation

By integrating AI-driven analytics into PLC systems, industrial operations are being transformed to predict and prescribe capabilities [4]. Now, machine learning models are trained against IoT-generated datasets that help to identify patterns associated with equipment wear or process inefficiencies.

This trend is further amplified by digital twins: virtual replicas of physical systems. By simulating real-world scenarios, digital twins enable "what-if" analyses for optimizing PLC logic. GE's digital twin of a wind turbine in the energy sector, which is built on IoT sensors' data and combines them with PLC control algorithms, simulates a blade's stress, which is subjected to varying wind conditions, and cuts the maintenance by 25%. Platforms like ANSYS Twin Builder bring advanced physics-based modelling combined with this real-time IoT data so that operators can try out recommended PLC code updates in a virtual risk-free environment before real deployment. Challenges are to ensure fidelity of the models and to manage the computational overhead associated with high fidelity simulations.

3.3. Hybrid PLC-IoT Communication Protocols and Cybersecurity Innovations

These legacy PLC systems need to converge with IoT by using hybrid communication protocols to bridge the gap between deterministic industrial networks and flexible IoT frameworks. The cornerstone of said concept has been formed by OPC Unified Architecture over Time Sensitive Networking, which ensures secure, real-time data exchange between PLCs and IoT devices. OPC UA's publisher-subscriber model, combined with TSN's IEEE 802.1AS timing synchronization, ensures microsecond-level precision for tasks like synchronized motor control in assembly lines.

DOI: 10.54254/2755-2721/2025.22249

Using OPC UA TSN, for instance, Bosch Rexroth's PLCs help to coordinate IoT-weaned hydraulic systems between a smart factory's PLCs, allowing accuracy within 99.999%.

This connectivity, however, creates attack surfaces that need to be secured. Blockchain technology is being experimented with for securing PLC-IoT networks—Shell's blockchain pilot in offshore drilling rigs uses smart contracts to authenticate PLC commands so that an unauthorized person would not change them. Even in these resource-constrained edge devices, lightweight encryption protocols, like AES-128-GCM, are being swept up to secure data-in-transit without compromising on latency.

4. Technical Challenges

4.1. Interoperability and Standardization Barriers

However, a gap exists on various key aspects for the integration of IoT with legacy PLC systems, such as compatibility difficulties of communication protocols and lack of common standards. As many of today's legacy PLCs are ancient, they were designed decades ago and thus utilize proprietary protocols such as Modbus or Profibus, which have no native support for modern IoT frameworks like MQTT, HTTP/2, etc. This gap can be bridged with middleware, aka. protocol converters, which incur complexity, cost and potential failure points.

Making matters worse, this is interlaced by a fragmented standardization landscape. However, adoption remains slow even for Industrial initiatives such as the Industrial Internet Consortium and OPC Unified Architecture that are trying to unify Industrial communication. Many of the manufacturers are not willing to overhaul the existing system for fear of downtime or financial constraints. This reluctance is keeping things status quo where PLCs run alongside IoT devices in a siloed manner without being able to easily work together. The inefficiencies that result impose scalability problems, especially in multi-vendor environments like smart factories or energy grids where one must harmonies multiple systems to achieve holistic automation [5].

4.2. Cybersecurity Vulnerabilities in Converged Networks

IoT convergence with PLCs leads to exponential expansion of attack surfaces, exposing industrial systems to cyber threats of great sophistication. Unfortunately, legacy PLCs were designed with isolated networks in mind and don't offer built-in security features such as encryption or authentication. But, when connected to IoT ecosystems, they become susceptible to ransomware, data manipulation, as well as unauthorized access. The Mirai botnet attack on insecure IoT devices to disrupt some critical infrastructures in 2019 shows the catastrophic potential of such vulnerabilities.

Data Interception is a weak point concerning the security of IoT-PLC networks. If PLCs and IoT devices communicate unencrypted, then communication between these devices can be intercepted and malicious actors can change machine commands or steal your proprietary data.

Device spoofing is particularly serious for IoT-PLC networks. Also, they can impersonate authorized IoT nodes to inject false sensor readings, which might result in bad PLC decisions.

In the case of IoT-PLC networks, supply chain risk may be the greatest risk. PLC systems can be introduced with backdoors inside them by third-party IoT components with unvetted firmware.

To address these risks, a multi-layered security framework provides hardware-based root of trust mechanisms, lightweight encryption protocols for resource-constrained devices and zero trust architecture that constantly validates user and device identity.

4.3. Latency, Data Management, and System Reliability

The fusion of IoT and PLCs results in performance bottlenecks with respect to real-time responsiveness and data handling. For sub-millisecond latency and deterministic behavior, mission-

DOI: 10.54254/2755-2721/2025.22249

critical applications like robotic assembly lines and chemical process control require this. Since edge computing delays data processing near the PLCs, there are still problems in cases when synchronized actions must be made between distributed nodes. For example, autonomous guided vehicles in a smart warehouse require real-time coordination with PLCs and IoT sensors, with PLCs controlling actuators IoT sensors controlling the sensing and PLCs being responsible for the coordination of the actuators and the sensing; in the case of a network congestion or packet loss, time is disrupted which results in collisions or the halting of the workflow.

Furthermore, IoT's data deluge floods legacy PLCs with data that legacy PLCs do not have the computational resources to process [6]. Hence, these streams can be viewed as high velocity. Sending unfiltered data to central servers creates network overload, latency, storage costs, and more. Edge-based data filtration and federated learning are one way to reduce bandwidth consumption.

Another factor that degrades reliability is the inherent instability of the wireless IoT network. Global Communication sensors are used in harsh industrial environments, where electromagnetic interference or physical obstruction may degrade signal integrity and thereby compromise time-sensitive PLC operations. While hybrid wired–wireless architectures and redundant communication pathways are being used as mitigative strategies, these strategies need to be exhaustively tested to guarantee fail safe performance.

5. Prospects

5.1. Next-Generation Connectivity and Computational Power

However, it will be the evolution of communication technologies and computational paradigms that will bring about transformative advancements in the integration of IoT PLC over the horizon [7]. Taking the form of ubiquitous, ultra-reliable, low-latency communication and massive machine-type communication, the 5G network will facilitate the real-time coordination among the PLCs and IoT devices at scales hitherto unforeseen. For example, 5G is expected to support autonomous guided vehicles in smart factories to synchronize movement with PLC controlled conveyors with sub milliseconds latency to reduce the chance of collision and improve material flow. When we talk about beyond the fifth generation, quantum computing is going to play a part because it can address problems that encrypt and optimize now. On the other hand, quantum-resistant algorithms can protect IoT – PLC networks from future cyber threats, and quantum annealing can solve in milliseconds typical complex resource allocation problems like dynamic rerouting of the production workflow in case of a supply chain disruption.

5.2. Decentralized Trust and Sustainable Automation

Decentralized technologies and Blockchain technologies will go a long way in providing the necessary assurance of security, transparency, and sustainability among industrial ecosystems. Other similar are blockchain-based smart contracts that can automate PLC operations in auditable and tamper-proof ways. For example, in energy grids, smart contracts could serve to facilitate self-executing agreements between PLC-controlled renewable energy sources and IoT-powered storage systems that minimize the use of intervening parties and optimize energy distribution.

At the same time, IoT-PLC systems will focus on sustainable automation based on AI resource optimization. Real-time IoT sensor data-powered dynamic energy management algorithms could either automatically bring the PLC-controlled machinery to operate during off-peak hours or to go to low power modes. Companies like Hitachi are already pioneering "green manufacturing" initiatives, where IoT-PLC networks reduce carbon footprints by 30–40% through adaptive load balancing and waste minimization.

DOI: 10.54254/2755-2721/2025.22249

5.3. Augmented Human-Machine Collaboration

For Industrial Automation, the symbiotic interaction of intelligent machines and human operators will be the future. IoT-PLC systems coupled with augmented reality and virtual reality interfaces will essentially make workers see things in a contextual and real-time-based view. AR head-up displays could, for example, overlay PLC diagnostic data on top of physical equipment, allowing technicians to troubleshoot faults without shutting down production.

Adaptive PLCs and IoT feedback to the sensor systems will further push the boundaries of the collaborative robotic roles of humans and machines. Broader democratization of access to complicated automation tools and closing skill gaps within an ageing workforce will be made possible via these advancements that will not only improve productivity [8].

6. Conclusion

With IoT and PLCs converging, industrial automation is being transformed to serve more innovative and more efficient purposes of operations with real-time sharing of data and prediction analytics. However, using IoT to expand the attack surface of legacy PLC presents cybersecurity risks, including ransomware. By their nature, traditional PLC protocols and modern IoT standards have interoperability issues that make integration challenging and costly, with expensive middleware in many cases. A collaboration among academia, industry, and policymakers is needed to address these challenges. Academia should develop lightweight, secure protocols, while industry leaders should purchase hybrid architectures. Standardization of IoT PLC ecosystems can be driven by policymakers.

Future advancements in 5G, blockchain, and AI will further enhance IoT-PLC integration. 5G's ultra-reliable low-latency communication will enable real-time coordination of autonomous systems, while blockchain will secure PLC operations, as seen in Shell's energy grids. Finally, IoT-PLC convergence provides a lot of room for innovation. By addressing the challenges and utilizing emerging technologies, industries can construct resilient, adaptive, and sustainable ecosystems for the future.

References

[1] *Folgado, F. J., Calderón, D., González, I., & Calderón, A. J. (2024). Review of Industry 4.0 from the perspective of automation and supervision systems: Definitions, architectures and recent trends. Electronics, 13(4), 782.*

[2] *Xu, H., Yu, W., Griffith, D., & Golmie, N. (2018). A survey on industrial Internet of Things: A cyber-physical systems perspective. Ieee access, 6, 78238-78259.*

[3] *Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. IEEE access, 8, 23022-23040.*

[4] *Dotoli, M., Fay, A., Miśkowicz, M., & Seatzu, C. (2019). An overview of current technologies and emerging trends in factory automation. International Journal of Production Research, 57(15-16), 5047-5067.*

[5] *Babayigit, B., & Abubaker, M. (2023). Industrial internet of things: A review of improvements over traditional scada systems for industrial automation. IEEE Systems Journal, 18(1), 120-133.*

[6] *Chataut, R., Phoummalayvane, A., & Akl, R. (2023). Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0. Sensors, 23(16), 7194.*

[7] *Nechibvute, A., & Mafukidze, H. D. (2024). Integration of scada and industrial iot: Opportunities and challenges. IETE Technical Review, 41(3), 312-325.*

[8] *Dhameliya, N. (2023). Revolutionizing PLC Systems with AI: A New Era of Industrial Automation. American Digits: Journal of Computing and Digital Technologies, 1(1), 33-48.*