Convergence of IoT and Industrial Automation Protocols: Toward Unified Communication Frameworks

ECE 842: Performance Modeling of Communication Networks
Professor Subir Biswas
Michigan State University – Fall 2025
November 30, 2025

Julio Quiroga Galan

***Abstract*—Industrial systems are evolving as the Industrial Internet of Things (IIoT) is added on top of existing automation technologies. Modern factories, warehouses, and vehicles now utilise PLC networks, industrial Ethernet, wireless sensor networks, and other IoT protocols to establish unified communication networks. These technologies require extensive research to be integrated, since each particular technology makes different assumptions about latency, reliability, and integration with higher-level control. In this paper, I review five recent works that study this convergence from different angles: PLC-based automation in warehousing [1], centralised HMI for heterogeneous PLCs [2], embedded sensor networks in industrial settings [3], IoT and cloud-based extensions to automation systems [4], and low-latency communication schemes for time-sensitive industrial applications [5]. Across these papers, I first identify the main problems they report, then summarise the technical approaches proposed and their results. Finally, I highlight common design patterns that appear in several of the works and argue how they point toward more unified communication frameworks for future IIoT and industrial automation deployments.**

I. INTRODUCTION

Over the last decade, low-cost embedded sensing, wireless communication, and cloud services have made it possible to collect much more data from machines and processes and use that data in new ways, for example, for predictive maintenance, remote monitoring, and optimization. The Industrial Internet of Things (IIoT) works toward more developed networks, that include data-driven operation, in which devices, controllers, and complex services are strongly connected.

However, the communication side of this new technology still requires research and development. Many programmable logic controllers (PLCs) protocols are specific to their vendors, while newer IoT devices support a variety of industrial Ethernet protocols such as OPC UA and MQTT. Wireless sensor networks bring in additional stacks, and time-critical applications in motion control, process automation, and effective automation of industry depends on low-latency and highly reliable technologies such as TSN-based Ethernet, EtherCAT, PROFINET IRT, or 5G URLLC. In practice, autonomous industrial systems combine several of these technologies, and engineers must find ways to make them work together without losing efficiency, safety, or security.

This paper reviews five research and industry papers that look at this convergence problem in concrete settings. The selected works cover advanced PLC-based automation for a converging and warehousing facility, a centralized HMI that ties together different PLC platforms using IoT techniques, architectures for embedded sensor networks in industrial environments, IoT-based extensions to industrial automation, and a comparison of low-latency protocols for industrial systems. The goal is not only to summarise each paper, but also to extract the recurring problems and solution patterns that appear across them, and to discuss what these patterns suggest for future unified communication frameworks in IIoT and industrial automation.

II. PROBLEMS ADDRESSED IN THE RESEARCH ARTICLES

A. Advanced PLC-Based Automation for Warehousing Systems

The first paper [1] focuses on a warehouse scenario. The authors argue that the conveyor system has no collision-avoidance logic, so products can jam and bring the line to a stop. Some tasks, like stacking, are mainly done manually, which leads to crooked and misplaced items. This wastes both floor area and space in the racks. Additionally, the inventory is not tracked in a reliable way; therefore, operators have constant problems with under-stacking and over-stacking, which eventually leads to slower order fulfillment. Maintenance is another significant issue; the machines run nonstop until they fail, and motors, sensors, and AGVs are costly to replace. This could be avoided using predictive mechanisms. The final problem proposed is the control layer; the PLCs have not yet been developed to connect with IoT, which makes it hard to coordinate, tune energy usage and efficiency, or expand the system to cover larger or more complex warehouses.

B. Centralized HMI for Decentralized PLCs Using IoT Technologies

The second paper [2] looks at an industrial lighting management system (LMS). At the BHEL plant, each floor has its own PLC and HMI, from different vendors and generations, and these systems are installed in separate buildings. Operators waste significant time walking long distances to change schedules, adjust zones, and other easy but time-consuming tasks. Because the LMSs are isolated, there is no simple way to change global parameters, monitor all roof lights from one place, or check whether all systems are behaving as expected. On top of that, only some of the PLCs are compatible with IoT communication protocols, while others are older units with limited communication options, so there is no direct efficient way to connect them to a common network with the newer PLCs. According to the authors, using multiple PLC brands with separate HMIs makes coordination between systems difficult. It can cause lighting schedules to drift out of sync and waste energy, and it forces staff to walk the plant to change settings manually instead of spending their time on supervision and analysis.

C. Embedded Sensor Networks for Smart Industrial Automation

The third paper [3] focuses on the role of embedded sensor networks in smart industrial automation and control. The article begins by explaining how moving from traditional wired infrastructure to expanded wireless sensor networks is a complex process. The authors point out that in an industrial environment, sensors must survive vibration, temperature changes, dust, and electromagnetic noise over long periods of time, which can affect their reliability and output incorrect values. Additionally, the sensor nodes can be battery powered, which raises new problems related to the energy consumption and the lifetime of the network. The paper also mentions that once hundreds or thousands of sensors are deployed, scalability becomes a real issue; the network must be managed and coordinated without excessive overhead, and the control system has to work with very large volumes of streaming data. Another set of problems appears around integration and security. Moreover, industrial plants are used for several applications; therefore, multiple sensing devices and wireless protocols (ZigBee, Wi-Fi, Bluetooth) are demanded; these must be implemented in existing industrial architecture without breaking the established requirements. Finally, the authors focus on data privacy and protection concerns because the data travels over shared wireless links, cloud, and or IoT gateways instead of isolated networks.

D. Enhancement of Industrial Automation Using IoT

The fourth paper [4] looks at how existing industrial automation starts to fail when plants try to deal with remote monitoring using only traditional control hardware. The authors describe how there still exist systems where detection of fire, gas leaks, or intrusions is slow or ineffective, requiring human intervention to eradicate the problem, which eventually leads to workers being exposed to unnecessary risks. On top of the mentioned, current infrastructures rely mainly on wired links and stand-alone controllers; this methodology generally fails to get accurate real-time data, analytics in the cloud, or coordinate numerous devices after a detected interference. Current industries require more IoT devices to be added, and as the demand increases so do the problems; different sensors must be integrated into one existing architecture, data needs to be intact from the collection to the reception after going through the cloud, and security becomes a concern due to information traveling over public area networks. Finally, the paper points out that even when IoT hardware is available, there is often no clear way to use it to improve current systems, so the challenge is to design an end-to-end system that can sense hazardous events quickly, move and drive data securely through the cloud, and be fully automated.

E. Low-Latency Protocols for Time-Sensitive Industrial and Autonomous Systems

The fifth paper [5] focuses on finding a solution to the problem of choosing communication protocols for time-sensitive industrial automation, with a focus on reliable low-latency systems. The authors mention that current industrial plants rely on older fieldbuses and Ethernet protocols that lack the development of new technologies that prevent low jitter or guarantee bounded delay. Due to their deficiencies, these plants struggle when the control loops are closed over the network or when numerous nodes must share the same medium. As new applications are developed and integrated, these timing limitations become more apparent. At the same time, there is now a long list of “real-time” industrial protocols available, including TSN-based Ethernet variants, EtherCAT, PROFINET IRT, OPC UA over TSN, and others, each with its own assumptions about scheduling, synchronization, hardware support, and configuration. The paper argues that the lack of clarity when it comes to comparing these options in terms of latency, scalability, and deployment cost makes the protocol selection more complicated. The main solution the authors propose to solve the problem is how to match specific communication protocols to time-sensitive industrial automation scenarios.

III. SOLUTION APPROACHES AND RESULTS

A. Advanced PLC-Based Automation

In [1], the authors propose an automation framework that combines a converging conveyor system, Siemens PLCs, and an automated warehouse, all of which are simulated and tested using Factory I/O. The overall structure is showcased in a block diagram (Figure I), where all the elements of the research are connected to a central PLC. This figure makes it clear that the PLC not only drives motors, but it also coordinates product flow, tracking, and interacts with decision-making logic.

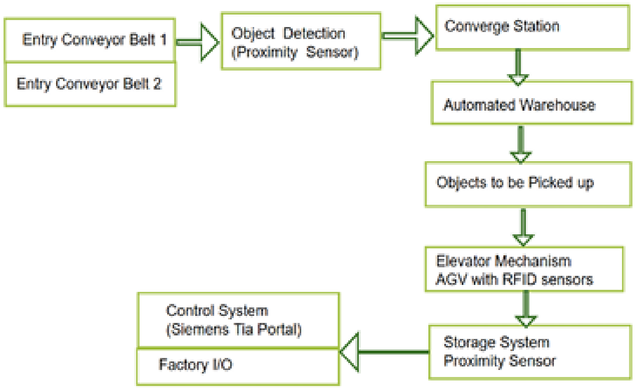


Fig. 1. Block diagram of the converging station and warehouse automation system.

At the PLC programming level, the implementation is based on a function block network developed in TIA Portal (Figure II). This network handles the mapping between physical or simulated I/O and the tags used in the control program. It also manages real-time data exchange with Factory I/O so that the same logic can be applied in the simulation before its transition to actual hardware. This block acts as a bridge between the PLC and the virtual plant communication, an important step towards flexible and testable industrial control.

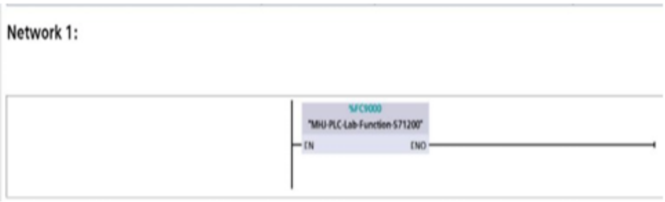


Fig. 2. PLC function block network in TIA Portal used to interface the Siemens PLC with the Factory I/O model.

In the warehouse situation, a similar strategy is applied. The PLC is used to coordinate an AGV and the storage racks with proximity sensors and RFID tags, which are typically used to identify when slots are free or occupied, and if the latter by what elements. The combination of the conveyor logic, with the previously mentioned, creates a fully automated path from the entry to the storage and retrieval.

Finally, the authors describe how all of the sensors and actuators are mapped into the PLC I/O table and then into the Factory I/O model. Each sensor, motor, and indicator is assigned a specific address; these addresses are consistently in the TIA Portal project and the simulation environment. This type of mapping reduces errors in communications and allows the system to be extended for additional devices. The article compares the impact of automation between the original largely used set-ups and the proposed PLC-based system, showcasing how the proposed approach reduces human interaction, fewer collision due to the additional logic, predictive maintenance, and continuous effective tracking.

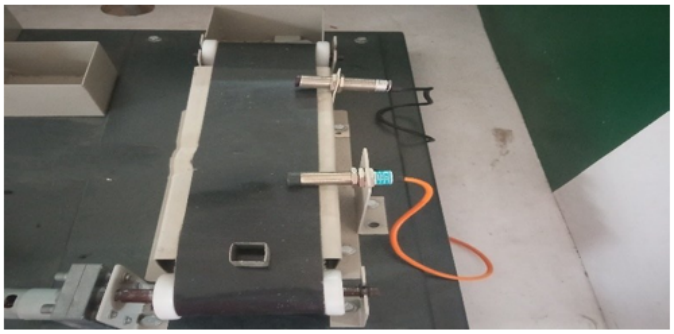


Fig. 3. Screenshots of the converging conveyor station and control panel showing product flow and sensor/drive status.

B. *IoT-Enabled Centralized HMI for Heterogeneous PLCs*

The solution in the second paper [2] is built around a web-based centralized HMI that can talk to all five LMS PLCs at the BHEL plant, even though they come from different vendors and generations. The authors split the implementation into two cases. For the IoT-ready Siemens S7-1214C PLCs in buildings B107 and B108 (grouped as PLC-A), the PLC is used not only as a controller but also as a small web server. The authors use a basic Ethernet network, and each PLC is assigned a fixed IP address. The central HMI uses PROFINET to communicate with the PLCs, and using HTTP or HTTPS, the operator can open the configuration pages. As shown in Figure IV, the PLC also behaves as a web server and delivers HTML pages to any client machine on the plant network. Within the TIA Portal project, the built-in web server is enabled and custom HTML pages are defined, with input fields reserved for the lighting timing and zone parameters. The authors then generate a dedicated data block that stores the web content and link it to a web-server function block in the main program. The web interface for the B107 LMS lets the operator adjust on/off times and holiday schedules, saving time from walking to the central HMI to execute any overrides.

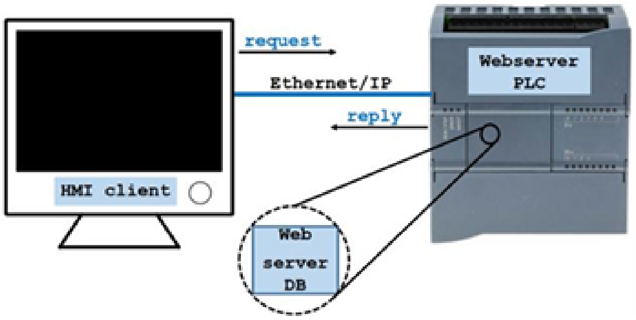


Fig. 4. Web-server-based centralized HMI architecture for the IoT-ready PLC-A lighting management systems.

The PLCs in building B117, B119, and B123 (PLC-B) are bridged to the central HMI using an ESP32 microcontroller because the mentioned PLCs can not use modern IoT communication protocols. In this second method, illustrated in Figure V, the ESP32 runs its own web server and connects wirelessly to the same LAN through a WiFi router. In this setup, the centralized HMI sends HTTP requests to the ESP32. The microcontroller takes the updated parameters, converts them into binary-coded digital signals, and applies them to the input channels of the legacy PLC. A set of switching relays is used between the ESP32 and the PLC I/O to adapt the voltage levels so that both sides can interface safely. This approach closely mirrors the layout used for the IoT-ready PLCs so that operators see a consistent HMI regardless of which shop floor they are controlling.

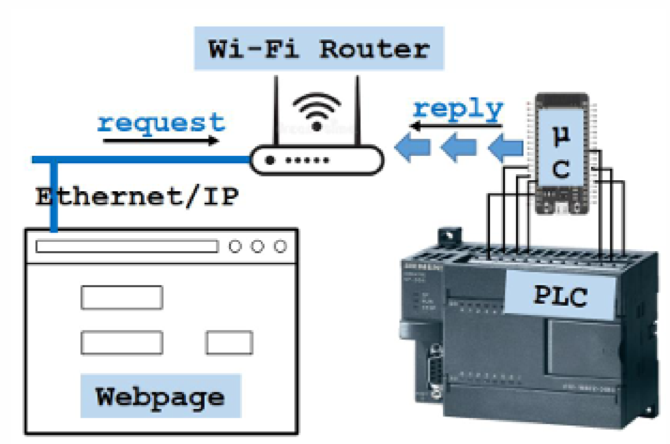


Fig. 5. ESP32-based web-server bridge used to integrate legacy PLC-B units into the centralized HMI architecture.

In the result section of the paper, the authors report that all five LMS PLCs are now connected to a centralized HMI and therefore, a lot of time will be saved in the future from unnecessary configuration or patrol walks around the industrial plant. By updating the web-server parameters, they can keep deviations within five minutes, which is important given the large installed lighting load. Instead of getting rid of the local HMIs, they remain available as a backup in case of connectivity failure, so the old PLCs are still accessible in emergencies. The authors mention that using the web server adds some delay to the system, but it does not affect operation in any noticeable way. Overall, adding the HMI on the newer PLCs and adding ESP32 bridges for the old ones fixes the communication issues and lets the plant move to a centralized control structure without needing a full hardware replacement.

C. *Embedded Sensor Networks in Industrial Automation*

In the third paper [3], the authors move from the general idea of wireless sensor networks to a concrete architecture for smart industrial automation. Their solution is based on an embedded sensor network that ties together many low-cost sensor nodes, a central hub, an IoT gateway, and a cloud back end. The basic layout is sketched in Figure VI. Individual WSN nodes measure temperature, pressure, vibration, and other local variables to then wirelessly send the data to a close hub. After this process, an IoT gateway adds any additional readings and these are uploaded to a cloud server for processing and storage; finally, the users can observe the outputs.

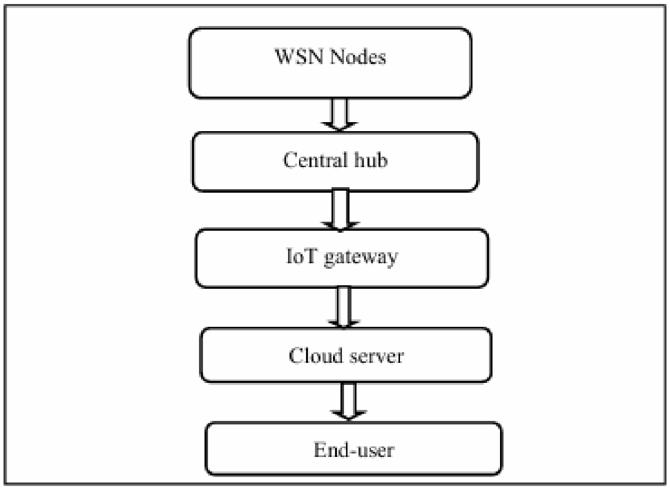
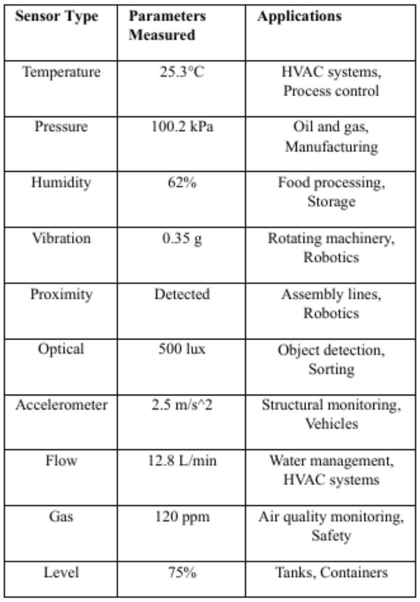


Fig. 6. Overall embedded sensor network model with WSN nodes, central hub, IoT gateway, cloud server, and end user.

On the data side, the paper proposes a simple processing pipeline that runs partly at the edge and partly in the cloud. At the gateway, in order to get rid of duplicated packets, out-of-range values, and any type of distinguishable noise, cleaning and filtering methods are used to ensure the data is ready to be sent. Once the data is ready, it passes through specialized machine learning algorithms to detect and predict possible future errors and ensure energy efficiency. For example, rotating machine vibration and temperature data can be monitored to prevent the wear of bearings. When a threshold is crossed, the cloud application automatically generates an alert, as an SMS message that is sent to a supervisor's phone when the system detects an abnormal condition. The authors also give a small example data set, Figure VII, that lists typical values for different sensor types, which helps show how the system would behave under normal operation.



Sensor Type	Parameters Measured	Applications
Temperature	25.3°C	HVAC systems, Process control
Pressure	100.2 kPa	Oil and gas, Manufacturing
Humidity	62%	Food processing, Storage
Vibration	0.35 g	Rotating machinery, Robotics
Proximity	Detected	Assembly lines, Robotics
Optical	500 lux	Object detection, Sorting
Accelerometer	2.5 m/s^2	Structural monitoring, Vehicles
Flow	12.8 L/min	Water management, HVAC systems
Gas	120 ppm	Air quality monitoring, Safety
Level	75%	Tanks, Containers

Fig. 7. Sensor types, parameters measured, and applications in the embedded sensor network.

The results are reported mainly in a qualitative way. The authors argue that once this architecture is in place, operators gain continuous visibility into process variables and can react earlier to unsafe or inefficient situations. They also mention how keeping sensory data in the cloud makes predictive maintenance possible by detecting trends and other anomalies, which leads to faster action and cheaper maintenance costs. On the other hand, the paper is honest about how large deployments raise issues about scalability, power efficiency, and security concerns over large data streams using cloud servers. Overall, the proposed embedded sensor network works as an early prototype that can be modified and improved in areas such as protocol choices, energy management, and data security for future integration in industry.

D. IoT-Based Enhancement of Industrial Automation

In the fourth paper [4], the authors build a prototype aimed at handling dangerous situations in an industrial setting. Their idea is to combine local sensing on a small mobile robot with cloud-based processing and decision making. The high-level architecture, shown in Figure VIII, starts with physical equipment and processes on the shop floor, where sensors measure quantities such as temperature, gas concentration, and energy usage. These signals collected from the embedded devices before reaching the cloud back end pass through IoT connectivity; from there, the data is used to trigger actions or send alerts to the plant.

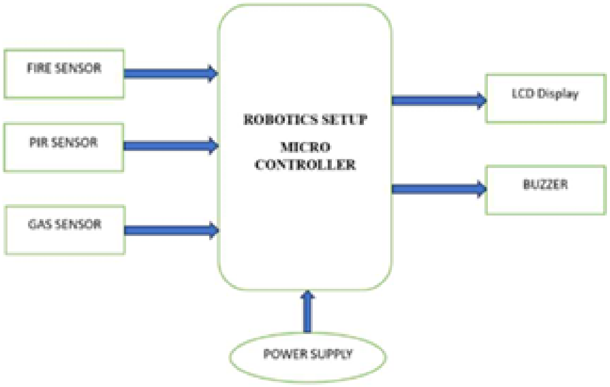


Fig. 8. Overall IoT-based system for hazardous-event monitoring and response.

The hardware section of the paper describes the individual components in more detail. A flame sensor (KY-026) uses radiation in the 760-1100 nm range to detect any open flames, while the gas sensor (MQ2) measures smoke and combustible gases, like propane or butane. In their prototype, an L298N H-bridge is used to drive the DC motors. All of the components are then fixed on a simple robot base with two wheels, plus an ultrasonic sensor, so the robot can move towards the source of the event.

On the software side, the control logic is written in the Arduino IDE; after initialization, the microcontroller reads the flame and gas sensors and checks if the outputs cross the thresholds. If a flame or high gas level is detected, the code switches the robot into rescue mode; the robot moves towards the source, and a buzzer is activated to indicate an alarm. At the same time, the IoT modem is used to forward information about the event to a remote application built with PHP, so that an operator can see that a fire, gas leak, or intrusion has been detected. The authors also outline a simple algorithm for structuring the program into steps such as designing the circuit, writing and uploading code, testing the sensor readings, and integrating the robot movement with the hazard-detection logic.

To evaluate the system, the paper presents an experimental graph with three iterations, which is reproduced in Figure IX. In the experiments, each iteration is plotted with time on the horizontal axis (in minutes) and a “speed” or throughput value on the vertical axis, and the table records the time taken to sense a hazardous condition, the communication speed, and whether the robot’s response is classified as fast or slow. Although the absolute numbers and units are not always consistent, the main point is that higher communication speeds and better integration reduce the delay between the start of a hazardous event and the robot’s reaction. Overall, the results support the claim that adding IoT connectivity and mobile sensing can improve response time and can become essential in industrial safety applications.

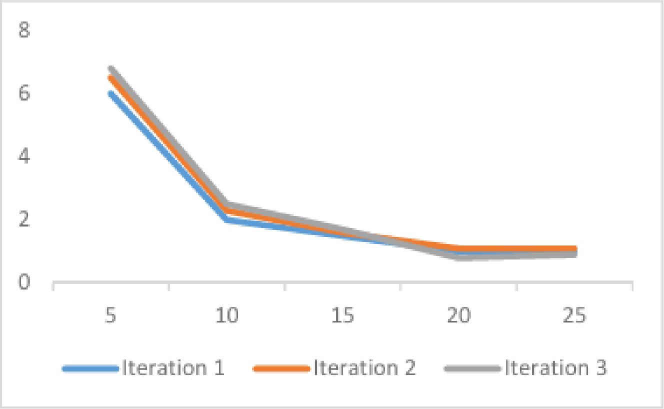


Fig. 9. Graphical comparison between the existing system and the proposed IoT-based system.

E. Low-Latency Protocols for Time-Sensitive Industrial Automation

In the fifth paper [5], the authors organize the existing options for time-sensitive industrial automation. They look at standard protocols, such as TSN, EtherCAT, PROFINET IRT, CC-Link IE, POWERLINK, Modbus TCP, BACnet/IP, DeviceNet, and FOUNDATION Fieldbus. In order to classify them, the authors use a comparison table (Figure X) that lists each protocol with an approximate latency range, expected reliability, scalability, and typical use cases. This helps separate protocols used specifically for real-time motion control from those that are more effective in slower monitoring and supervisory tasks.

PROTOCOL	LATENCY	RELIABILITY	SCALABILITY	USE CASE	STRENGTHS	CHALLENGES
TIME-SENSITIVE NETWORK	Microsecond-level	High	High	Real-time control in industrial robots, machines	Deterministic, low-latency communication	Complex configuration and implementation
ETHERCAT	100 μs	High	High	High-speed motion control, CNC machines, robotics	Low-latency, high synchronization accuracy	Difficult to configure in complex networks
PROFINET	1ms (IRT mode)	High	High	Factory automation, process control	Isochronous real-time communication	Complex setup for optimal real-time performance
OPC UA WITH TSN	Low, deterministic	High	High	Smart factories, IIoT, machine-to-machine communication	Platform-independent, real-time communication	Complex integration with legacy systems
MODBUS TCP	Moderate	Moderate	Low to moderate	Basic control and sensor data acquisition	Easy to implement, widely supported	Lacks advanced real-time and deterministic features
BACNET/IP	Moderate	Moderate	High	Building automation, HVAC control	Interoperable, energy-efficient	Limited real-time capabilities
DEVICENET	10ms	Moderate	Low to Moderate	Device-level industrial communication	Cost-effective, simple architecture	Limited scalability
CC-LINK IE	1ms	High	High	High-speed motion and machine control	Real-time deterministic Ethernet-based network	Limited vendor support outside Asia
FOUNDATION FIELDBUS	Low (1ms or less)	High	Moderate	Process automation in hazardous environments	Deterministic field-level communication	Complex setup and high cost
POWERLINK	1ms	High	High	Real-time motion control robotics	Open-source deterministic Ethernet	Dependency on network configuration

Fig. 10. Summary of performance indicators for industrial automation protocols

The paper then groups the protocols into two broad families. TSN, EtherCAT, PROFINET IRT, OPC UA with TSN, CC-Link IE, and POWERLINK are placed in the "very low latency" category and are suggested for applications like synchronised drives and high-speed control loops. On the other hand, Modbus TCP, BACnet/IP, DeviceNet, and some fieldbuses are described as reliable and widely used, but with looser timing and no guarantees on jitter. In the latency plot, Figure XI, the newer deterministic Ethernet protocols all end up on the side with the smallest delays, while the more traditional options appear further along the axis, and the more traditional protocols towards the higher end.

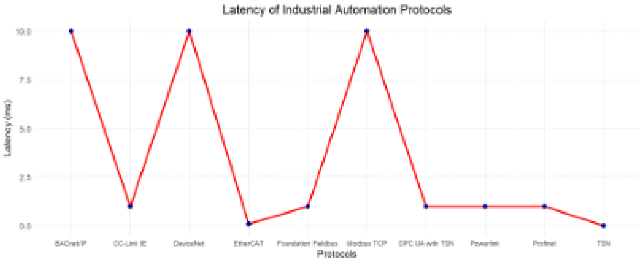


Fig. 11. Latency comparison of industrial communication protocols such as TSN, EtherCAT, PROFINET, OPC UA with TSN, Modbus TCP, BACnet/IP, DeviceNet, CC-Link IE, FOUNDATION Fieldbus, and POWERLINK.

Finally, the authors comment on scalability and reliability, Figure XII. The newer deterministic Ethernet protocols are presented as both scalable and robust, but they also come with higher configuration effort and integration cost, especially when mixed with legacy devices. As long as the system allows for a few milliseconds of delay, the simpler protocols are favorable in smaller systems. Overall, the paper gives a practical overview that helps engineers choose the appropriate family protocol that matches the timing and complexity of a given industrial automation project.

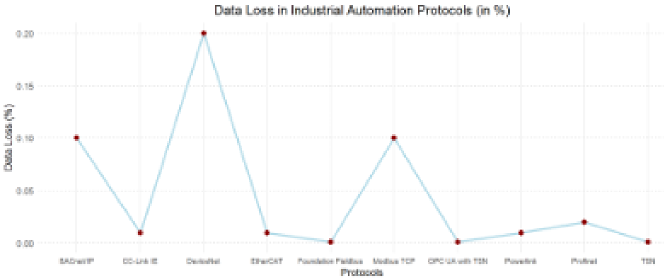


Fig. 12. Qualitative comparison of industrial protocols in terms of reliability.

IV. Summary and Conclusions

To sum up, the five papers reviewed show how difficult it is to merge automation with newer IIoT technologies, while pointing to some ways toward the goal. The warehousing case and the centralized HMI project both use the PLCs as the control layer, and both projects also use the web-servers, gateways, or microcontrollers to expose the controllers through the IP networks while keeping the existing hardware. The embedded sensor network and the IoT-robot prototype show how traditional systems can be extended with monitoring, predictive maintenance, and faster response. The survey of low-latency industrial protocols highlights when deterministic Ethernet solutions such as TSN, EtherCAT, or PROFINET IRT are needed, and shows when simpler protocols, like Modbus TCP or BACnet/IP are still acceptable. The papers suggest that unified communication frameworks will likely combine the legacy PLC and fieldbus networks, deterministic Ethernet, on the factory floor, and the application-layer standards, with the data moving toward cloud platforms. The papers also coincide that security, configuration work, and long-term scaling are still not solved. Unified communication frameworks still require advanced research to arrive at efficient scalability. Finally, the articles agree that there is still a need for practical tools and common standards that can hide most of the protocol differences from the application side, while keeping delay, reliability, and safety within the limits required in industrial plants.

References

[1] S. Vijayachitra, K. Prabhu, S. Agilan, M. A. Salih, and S. Madhumitha, "Advanced PLC-based automation for converging system and warehousing," *2025 5th International Conference on Trends in Material Science and Inventive Materials (ICTMIM)*, pp. 386–395, 2025.

[2] M. Jagannathan, S. P. Simon, M. E. R., K. A. Kumar, and S. K., "Centralized HMI for decentralized PLCs in industrial lighting management using IoT technologies," *2024 International Conference on System, Computation, Automation and Networking (ICSCAN)*, pp. 1–5, 2024.

[3] R. Raman and R. Halam, "Embedded sensor networks for smart industrial automation and control systems," *2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 1016–1021, 2023.

[4] A. Sheeba, C. A. Subasini, K. P. A. S., and M. V. S., "Enhancement of industrial automation using Internet of Things," *2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS)*, pp. 1–6, 2024.

[5] G. Jain, R. Das, D. Raj, and H. Mohapatra, "Exploring low-latency communication protocols for time-sensitive industrial automation and autonomous vehicle systems," *2025 International Conference on Computing, Intelligence, and Application (CIACON)*, pp. 1–7, 2025.