e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

A STUDY OF THE VARIOUS COMMUNICATION PROTOCOLS USED IN PLC SYSTEMS: MODBUS, PROFIBUS, ETHERNET/IP AND THEIR IMPLEMENTATIONS, EVOLUTION AND COMPARATIVE ANALYSIS

Brijesh Joshi[*1]

[*1]Student, Department Of Electronics And Communication Engineering, Lingaya's Vidyapeeth, Nachauli, Jasana Road, Old Faridabad, Haryana, India.

DOI : https://www.doi.org/10.56726/IRJMETS52882

ABSTRACT

This paper provides an in-depth analysis of the communication protocols commonly employed in Programmable Logic Controller (PLC) systems, including Modbus, Profibus, and Ethernet/IP. The goal of this study is to help engineers and practitioners choose the best protocol for industrial automation applications by examining the development, traits, benefits, drawbacks, features, and applications of different protocols. This research provides an in-depth examination of the existing literature and an analysis of real-world applications to provide valuable insights on the advantages, disadvantages, and applicability of each procedure in various industrial settings. Engineers and practitioners may choose the best protocol, implement it strategically, and optimize the network in PLC-based control systems by being aware of the subtleties of each protocol.

Keywords: Analysis, Investigation, Research

I. INTRODUCTION

The core of industrial automation is comprised of Programmable Logic Controllers (PLCs), which provide the control and observation of a wide range of operations in manufacturing, utility, and other industries. For smooth functioning and coordination within the control system, PLCs and peripheral devices must communicate effectively. Three well-known PLC system communication protocols—Modbus, Profibus, and Ethernet/IP—are examined in this work. This work attempts to offer important insights into the choice and application of communication protocols in industrial automation contexts by following their development, examining important aspects, and weighing relevant factors.

II. METHODOLOGY

EVOLUTION AND OVERVIEW OF COMMUNICATION PROTOCOLS:

2.1 Modbus:

Overview: In industrial automation, Modbus is one of the most used and established communication protocols. Since then, it has evolved into an open standard that is managed by the Modbus Organization, having been created in 1979 by Modicon (now a part of Schneider Electric). Human Machine Interfaces (HMIs) and other peripheral devices, including sensors and actuators, may communicate with PLCs more easily thanks to Modbus.

Key Features:

Master-Slave Architecture: A master device, such a PLC or SCADA system, sends communication requests to one or more slave devices, including sensors, actuators, or more PLCs, in order for Modbus to function.

By periodically querying slave devices for information or sending orders as necessary, the master device in this architecture manages communication.

Serial and Ethernet Communication: Both Ethernet networks (Modbus TCP/IP) and serial connections (RS-232/RS-485) can be used for Modbus communication.

While Modbus TCP/IP allows for quicker data transmission rates and interoperability with contemporary industrial infrastructure, serial communication is frequently utilized for outdated systems and applications in situations where Ethernet connectivity is not available.

Simplicity and Interoperability: Modbus's simplicity and ease of implementation are among its main advantages, since they enable it to be compatible with a broad range of PLC platforms and industrial devices.

Simple function codes that specify the kind of operation (read, write, etc.) and data payloads for transmission make up the Modbus message structure.

Open Standard: Modbus was created by Modicon (now Schneider Electric) as a proprietary protocol in the beginning, but it has subsequently evolved into an open standard that is managed by the Modbus Organization.

Widespread adoption and interoperability across several vendor platforms and industrial applications have been facilitated by this specification.

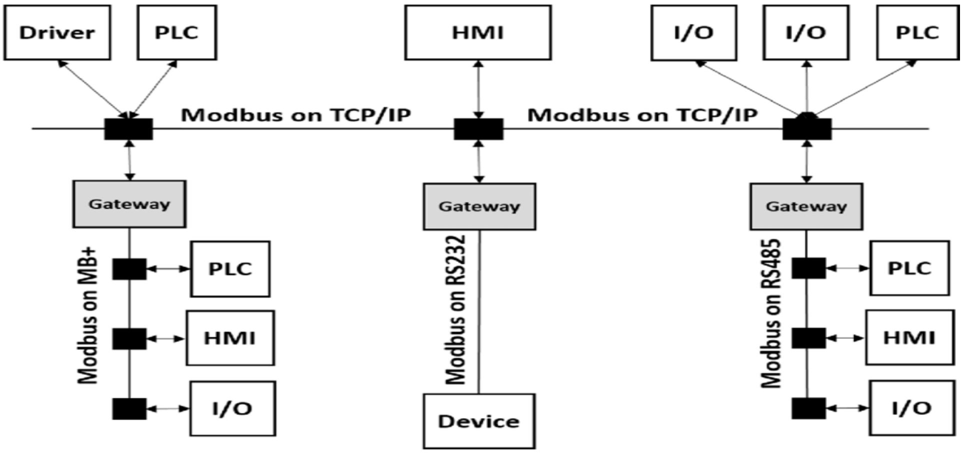


Figure 1: Modbus Protocol Overview Diagram

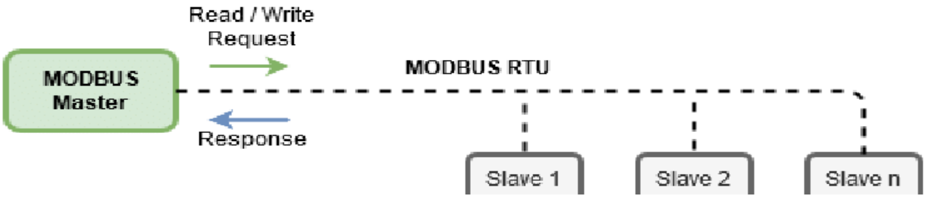


Figure 2: Modbus RTU Communication Diagram

Early Versions: Initially, Modbus operated primarily over serial connections (RS-232/RS-485), offering simple master-slave communication with limited data transfer rates.

Evolution: Over the years, Modbus has evolved to adapt to changing industrial needs. The introduction of Modbus TCP/IP extended its capabilities to Ethernet networks, facilitating faster data exchange and compatibility with modern industrial infrastructure.

Standardization: Although Modbus originated as a proprietary protocol, it has since become an open standard maintained by the Modbus Organization. This standardization has contributed to its widespread adoption across diverse PLC platforms and industrial applications.

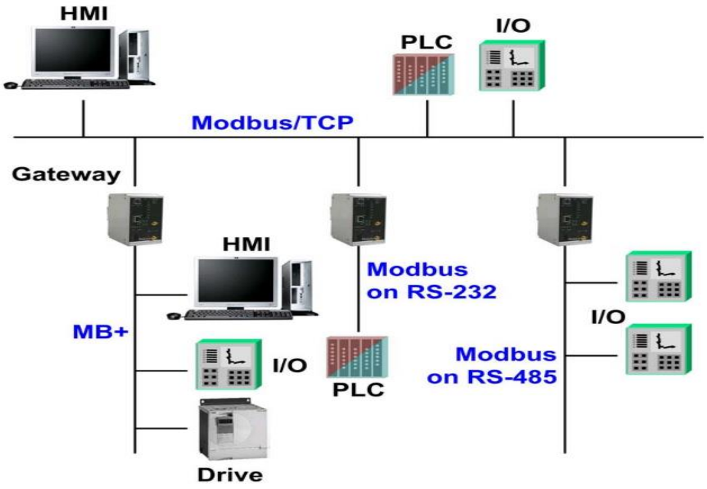


Figure 3: Modbus Implementation in PLC Systems

Advantages:

Compatibility: Modbus is supported by numerous PLC manufacturers and industrial devices, ensuring compatibility and ease of integration.

It is a widely adopted protocol in various industries, making it easy to find Modbus-compatible devices and components.

Simplicity: The straightforward communication model and message structure of Modbus make it relatively easy to implement and troubleshoot.

This simplicity reduces development time and costs associated with PLC programming and system integration.

Versatility: With support for both serial and Ethernet communication, Modbus can be deployed in diverse industrial environments, ranging from legacy systems to modern automation networks.

Limitations:

Limited Security Features: Modbus lacks built-in security mechanisms, making it vulnerable to cyber threats such as unauthorized access and data interception.

This limitation necessitates additional security measures, such as firewall configurations or VPN tunnels, to protect Modbus communication in industrial networks.

Data Transfer Speed: Compared to newer protocols designed for Ethernet communication, Modbus may exhibit limitations in data transfer speed, especially over serial connections.

This can impact system performance in applications requiring high-speed data exchange or real-time control.

Scalability: Modbus networks may face challenges in scalability and network management, particularly in large-scale installations with complex topologies.

As the number of devices and communication nodes increases, the overhead associated with polling and addressing devices may degrade network performance.

2.2 Profibus:

Overview: Profibus (Process Field Bus) is a widely used fieldbus communication protocol in industrial automation. It was developed in the 1990s by Siemens and has since become an open standard (IEC 61158). Profibus is designed to provide high-speed, deterministic communication for factory automation and process control applications.

Key Features:

High-Speed Communication: Profibus offers high-speed data transmission, enabling real-time control and monitoring of industrial processes.

It is designed to meet the demanding requirements of factory automation and process control applications, where precise timing and synchronization are essential.

Variants: Profibus encompasses multiple variants to address different application requirements and industrial environments.

Profibus DP (Decentralized Periphery) is optimized for factory automation and discrete manufacturing processes, while Profibus PA (Process Automation) caters to process industries with intrinsic safety requirements.

Token Passing Mechanism: Profibus uses a token passing mechanism for deterministic communication, ensuring reliable data exchange in industrial networks.

In this mechanism, a token is passed sequentially among network devices, granting them permission to transmit data in a controlled and predictable manner.

Interoperability: Profibus devices from different manufacturers can communicate seamlessly within the same network, thanks to standardization efforts and compliance with IEC standards.

This interoperability promotes flexibility and modularity in industrial automation systems, allowing users to mix and match devices from various vendors.

Development: Initially developed by Siemens, Profibus evolved through collaboration with other industrial automation leaders to establish it as an open standard (IEC 61158).

Variants: Profibus encompasses multiple variants to accommodate different application requirements. Profibus DP (Decentralized Periphery) is optimized for fast, cyclic data exchange in factory automation, while Profibus PA (Process Automation) caters to process industries with intrinsic safety and hazardous area requirements.

Advancements: Advancements in Profibus technology have focused on enhancing data transfer rates, network diagnostics, and interoperability with other industrial communication standards.

Advantages:

Deterministic Communication: Profibus provides deterministic communication, making it suitable for applications that require precise timing and synchronization.

This deterministic behavior ensures consistent performance in time-critical processes and enhances overall system reliability.

High Data Transfer Rates: Profibus offers high-speed data transmission, supporting demanding industrial automation tasks such as motion control, machine vision, and process monitoring.

This enables rapid exchange of information between PLCs, HMIs, and other industrial devices, improving system responsiveness and efficiency.

Standardization: As an open standard maintained by the International Electrotechnical Commission (IEC), Profibus promotes interoperability and compatibility across diverse PLC platforms and industrial devices.

This standardization simplifies system integration and reduces the risk of vendor lock-in, allowing users to choose from a wide range of Profibus-compatible products.

Limitations:

Network Configuration Complexity: Profibus networks may require careful configuration and setup, particularly in large-scale installations with complex topologies.

Proper network design, addressing schemes, and termination techniques are essential to ensure reliable communication and minimize signal degradation.

Susceptibility to Interference: Profibus networks may be susceptible to electromagnetic interference (EMI) and noise in harsh industrial environments, impacting communication reliability.

Shielded cables, proper grounding, and noise suppression techniques are necessary to mitigate the effects of interference and maintain signal integrity in Profibus networks.

Limited Support for Ethernet: While Profibus is primarily designed for fieldbus communication, it may face challenges in integrating with Ethernet-based networks without additional gateways or converters.

This limitation may require users to invest in additional hardware or software solutions to bridge the gap between Profibus and Ethernet systems, adding complexity and cost to the implementation.

2.3 Ethernet/IP:

Overview: Ethernet/IP is an industrial Ethernet protocol based on standard TCP/IP technology. It emerged in the late 1990s as industrial automation began adopting Ethernet technology for its inherent speed, reliability, and widespread availability. Ethernet/IP combines the benefits of standard Ethernet networking with industrial automation requirements, offering high-speed communication, scalability, and interoperability.

Key Features:

Standard Ethernet Infrastructure: Ethernet/IP leverages standard Ethernet hardware and infrastructure, simplifying deployment and maintenance in industrial environments.

It uses standard Ethernet cables, switches, and routers, making it compatible with existing IT infrastructure and reducing the need for specialized hardware.

Real-Time Communication: Ethernet/IP supports both implicit messaging (I/O data) and explicit messaging (explicit communication), enabling real-time control and data exchange in industrial automation systems.

Implicit messaging is used for cyclic data exchange, such as process control and monitoring, while explicit messaging allows for on-demand communication between devices.

Scalability: Ethernet/IP offers scalability to accommodate large-scale industrial installations, supporting thousands of devices within a single network.

This scalability enables the expansion of automation systems to meet growing production demands without compromising performance or reliability.

Security Features: Ethernet/IP incorporates robust security measures to protect against cyber threats and ensure the integrity and confidentiality of industrial data.

Security features include device authentication, data encryption, network segmentation, and access control mechanisms to safeguard industrial networks from unauthorized access and malicious attacks.

Emergence: Ethernet/IP emerged in the late 1990s as industrial automation began adopting Ethernet technology for its inherent speed, reliability, and widespread availability.

Convergence: Ethernet/IP represents a convergence of standard Ethernet networking with industrial automation protocols, leveraging TCP/IP technology for real-time data exchange.

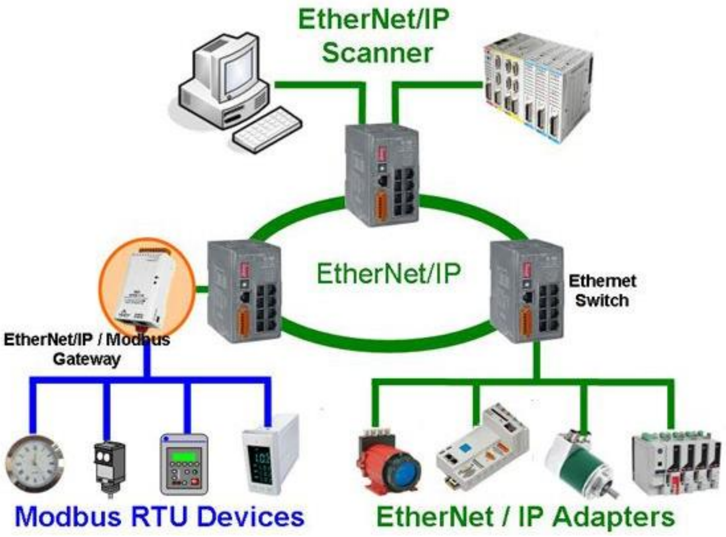


Figure 4: Ethernet/IP Network Architecture Diagram

Advantages:

High-Speed Communication: Ethernet/IP provides high-speed data transmission, facilitating rapid exchange of information between PLCs, HMIs, and other industrial devices.

This high-speed communication enhances system responsiveness, enabling real-time monitoring, control, and decision-making in industrial automation applications.

Interoperability: Ethernet/IP promotes interoperability and compatibility across different vendor platforms, thanks to standardization efforts and adherence to open standards.

This interoperability allows users to integrate devices from various manufacturers seamlessly, enabling flexibility and modularity in automation systems.

Integration with Enterprise Networks: Ethernet/IP seamlessly integrates with enterprise IT systems, enabling data sharing and communication between the factory floor and higher-level business systems.

This integration facilitates data-driven decision-making, process optimization, and resource allocation across the entire organization, improving overall operational efficiency and productivity.

Robust Security: Ethernet/IP incorporates robust security measures to protect against cyber threats and ensure the integrity and confidentiality of industrial data.

Security features such as device authentication, data encryption, network segmentation, and access control mechanisms mitigate the risk of unauthorized access, data breaches, and system vulnerabilities.

Limitations:

Complexity: Ethernet/IP networks may require more sophisticated configuration and setup compared to traditional fieldbus protocols, leading to increased complexity in deployment and maintenance.

Proper network design, VLAN configurations, and security policies are essential to ensure optimal performance, reliability, and cybersecurity in Ethernet/IP networks.

Cost: While Ethernet/IP offers numerous benefits, the initial investment in Ethernet-compatible hardware and infrastructure may be higher compared to legacy communication protocols.

This cost consideration includes Ethernet switches, routers, cables, and network infrastructure upgrades necessary to support Ethernet/IP communication in industrial automation systems.

Compatibility with Legacy Systems: Integrating Ethernet/IP with legacy PLC systems or devices that do not support Ethernet may require additional hardware or protocol converters.

This compatibility challenge adds complexity and cost to the implementation, particularly in retrofitting existing automation systems with Ethernet/IP capabilities.

Standardization: Ethernet/IP is an open standard managed by the Open DeviceNet Vendor Association (ODVA), ensuring compatibility and interoperability across different vendors and devices.

Security: With the increasing emphasis on cybersecurity in industrial networks, Ethernet/IP incorporates security features such as device authentication, data encryption, and network segmentation to safeguard against cyber threats.

2.4 Evolutionary Trends:

Integration: One of the overarching trends in the evolution of PLC communication protocols is the integration of industrial automation with enterprise IT systems. Protocols like Ethernet/IP facilitate seamless connectivity between the factory floor and higher-level business systems, enabling data-driven decision-making and process optimization.

Interoperability: Standardization efforts and advancements in protocol technology have improved interoperability between PLCs, devices, and software platforms from different vendors. This interoperability fosters flexibility and modularity in industrial automation systems.

Cybersecurity: With the proliferation of interconnected industrial networks, cybersecurity has become a critical concern. Modern protocols like Ethernet/IP incorporate robust security measures to protect against cyber threats and ensure the integrity and confidentiality of industrial data.

III. RESULTS AND DISCUSSION

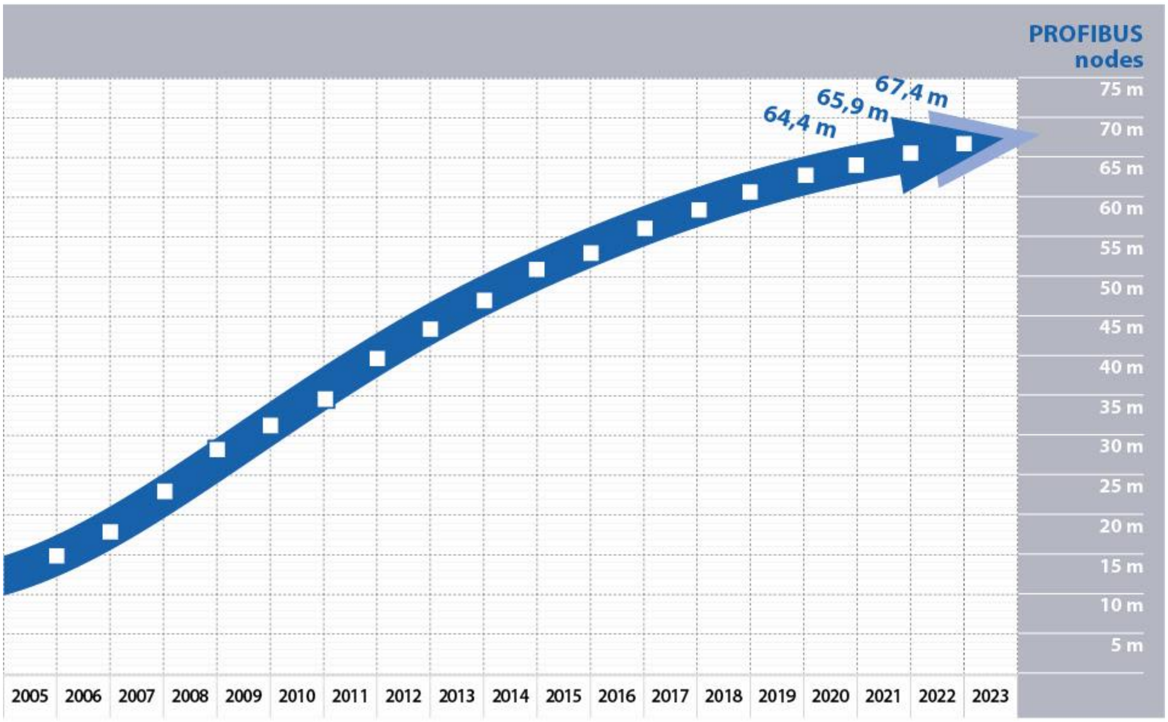


Figure 5: Usage of Profibus in world yearly

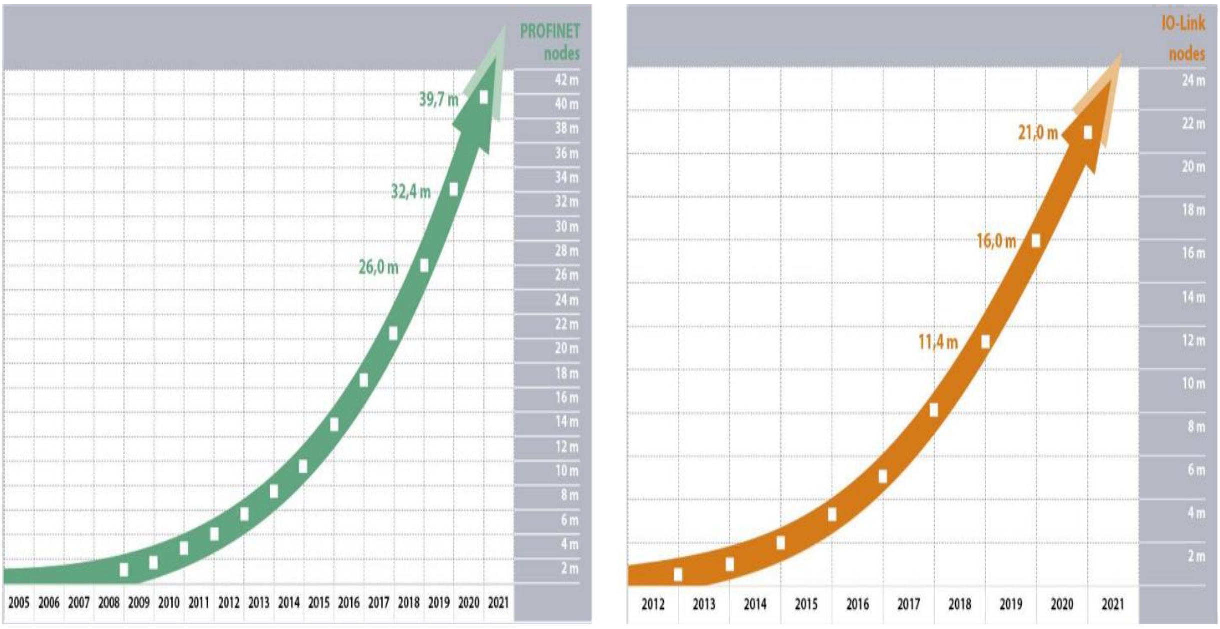


Figure 6: Usage of Profinet in world yearly

Even in a year marked by coronavirus-related issues, PROFINET was able to achieve significant growth, with the installed base exceeding 40 million. IO-Link continues to flourish in 2020, supplying a record-breaking 5 million new IO-Link devices in a single year.

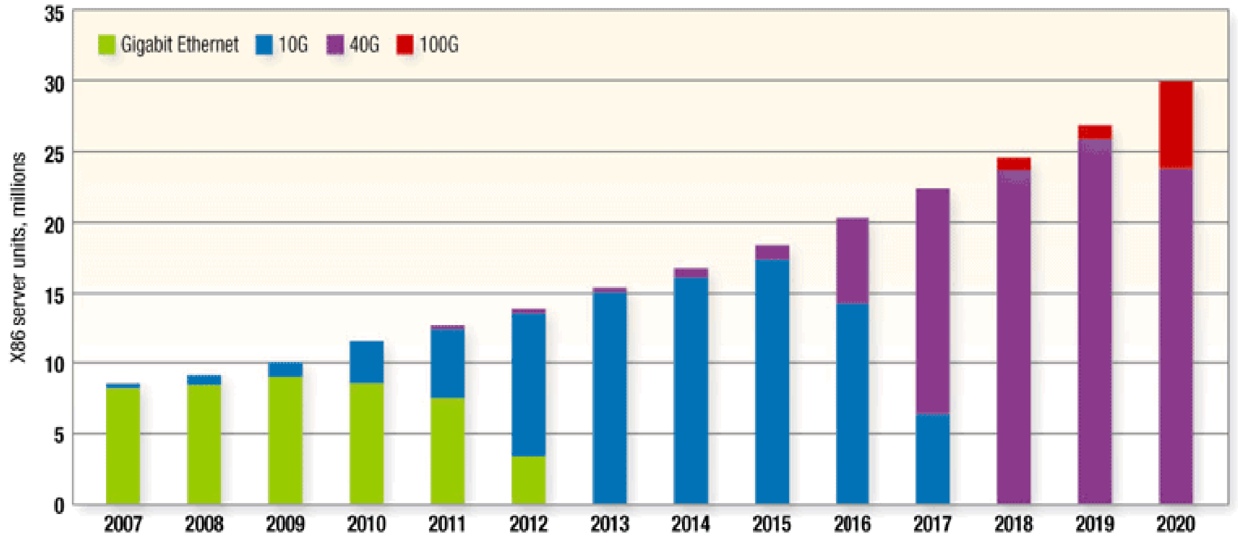
An impartial third party conducts the count. He requests device manufacturers, who anonymously respond with their company's node count. If the corporation does not react, their count is set to zero. (That, in my opinion, is the incorrect approach, as we know they manufactured some. So we undercounted our nodes. Only the aggregate figure is submitted to PI.

The numbers are PROFINET. Now at 16,400,000, up 3,600,000 from 2016. A 28% rise year over year.

PROFIBUS. Now valued at 56,100,000. In 2016, 2,400,000 were added. A modest decrease from 2015. Everyone was surprised by the long-anticipated decrease.

PROFIsafe. In 2016, the most often installed functional safety bus reached about 7,000,000 units.

IO-Link. This fieldbus-independent communications technology is still expanding at a rapid pace. There are already 5,300,000 total installations, including 1,700,000 in 2016 alone.



Source: Intel, Broadcom

Figure 7: Ethernet/IP growth in world

The graphic depicts the projected adoption of higher-speed Ethernet server interconnects as bandwidth demand drives current 10G Ethernet deployment and accelerates acceptance of forthcoming 40G and 100G Ethernet solutions.

Ethernet is the obvious choice for integrated SAN and LAN communication due to its scalability, performance, and cheap cost. The flow standard, which is now supported by most Ethernet switch makers, offers the network visibility required for operating data centers in this continuously changing environment.

IV. CONCLUSION

This research paper has provided a comprehensive analysis of the evolution, characteristics, advantages, and limitations of communication protocols in PLC systems, focusing on Modbus, Profibus, and Ethernet/IP. By understanding the historical development, key features, and practical considerations of these protocols, engineers and practitioners can make informed decisions regarding protocol selection, deployment strategies, and network optimization in industrial automation environments. As industrial automation continues to evolve, communication protocols will play a pivotal role in enabling connectivity, interoperability, and cybersecurity in the smart factories of the future.

V. REFERENCES

[1] Open DeviceNet Vendor Association (ODVA). (n.d.) . The ODVA Ethernet/IP Technology. https://www.odva.org/Technologies/EtherNetIP.

[2] Rinaldi, J.S.(2001). Industrial Ethernet https://www.rtaautomation.com/technologies/ethernetip/how-much-will-it-cost/.

[3] Hirst, B., & Martell, M. (2008). Profibus: A Pocket Guide. The Profibus Group.

[4] Linse, D., & Schneider, A. (2002). PROFIBUS – The Fieldbus for Industrial Automation. Springer Science & Business Media

[5] Leong, L. (2015). Emerging Technology Analysis: Ethernet/IP. Gartner Research.

[6] Franklin, T., & P., S. (2010). Industrial Ethernet: How to Plan, Install, and Maintain TCP/IP Networks: The Basic Reference Guide for Automation and Process Control Engineers. ISA - The Instrumentation, Systems, and Automation Society.

[7] Rinaldi, J. (2019). The Basics of Modbus - Specifications. Retrieved from https://www.rtautomation.com/technologies/modbus/.

[8] Data from internet https://us.profinet.com/profinet-profibus-growth/

[9] Data from Profinet and Profibus company https://blog.sflow.com/2009/09/ethernet-growth.html