Research Inventy: International Journal of Engineering And Science
Vol.15, Issue 9 (September 2025), PP 27-32
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

A Comprehensive Study of Cybersecurity in Fieldbus Protocols

Gordana Ostojic[1],*, Stevan Stankovski[2]

[1]Full professor, Faculty of Technical Sciences, University of Novi Sad, Trg Dositeja Obradovića 6, Centre for Identification Technologies, 21000 Novi Sad, Serbia.
[2] Full professor, Faculty of Technical Sciences, University of Novi Sad, Trg Dositeja Obradovića 6, Centre for Identification Technologies, 21000 Novi Sad, Serbia.
**Corresponding Author*

Abstract:*The increasing integration of industrial automation systems with enterprise networks and cloud-based platforms has elevated the importance of cybersecurity within industrial environments. Communication protocols such as CANopen, Modbus TCP, EtherCAT, PROFINET, and EtherNet/IP form the backbone of industrial control systems, yet many were developed without inherent security features, making them vulnerable to cyber threats including spoofing, denial-of-service, and unauthorized access. This paper analyzes the cybersecurity characteristics of these widely used protocols, highlighting their respective vulnerabilities and the degree to which they support secure communication. The study compares these protocols in terms of encryption, authentication, and resilience against common attack vectors, and provides a set of best practices for securing industrial networks that rely on them. Emphasis is placed on defense-in-depth strategies, including network segmentation, secure gateways, traffic monitoring, and patch management. By addressing both legacy limitations and modern mitigation techniques, the paper aims to provide actionable insights for engineers, system integrators, and cybersecurity professionals involved in protecting industrial systems. The findings underscore the urgent need to retrofit or replace insecure protocols, and to adopt security-by-design principles in future industrial communication architectures.*

Keywords:*Unauthorized Access, Denial-of-Service, Communication Protocols, Ethernet.*

Date of Submission: 08-09-2025 Date of acceptance: 19-09-2025

I. INTRODUCTION

Industrial communication protocols are the foundation of modern automation systems, enabling reliable data exchange between controllers, sensors, actuators, and supervisory systems. These protocols, including CANopen, Modbus TCP, EtherCAT (Ethernet for Control Automation Technology), PROFINET (Process Field Net), and EtherNet/IP, are widely deployed across industries such as manufacturing, energy, transportation, and critical infrastructure. They facilitate real-time control, coordination, and monitoring of industrial processes—functions essential for operational efficiency and system reliability.

However, many of these protocols were originally designed for isolated environments, where security was not a primary concern. At the time of their development, industrial networks were typically closed systems with limited exposure to external threats. Consequently, these protocols often lack fundamental security features such as encryption, authentication, and access control mechanisms. As the industrial landscape evolves toward Industry 4.0 and Industrial Internet of Things (IIoT) paradigms, these protocols are increasingly integrated with IP-based networks and cloud-connected systems [Ostojic & Stankovski, 2024]. This convergence introduces new cybersecurity challenges and significantly expands the potential attack surface.

With the rise of cyberattacks targeting critical infrastructure—ranging from data theft to operational disruption—the security of industrial communication protocols has become a pressing concern [Behera, et al., 2025]. Protocols like Modbus TCP and CANopen, which transmit data in plaintext, are particularly vulnerable to spoofing, tampering, and replay attacks. Even more advanced protocols such as EtherCAT, PROFINET, and EtherNet/IP, though built on Ethernet technologies, often depend on external measures or optional extensions to ensure secure communication.

This paper focuses on the cybersecurity implications and current defense mechanisms associated with five key industrial communication protocols: CANopen, Modbus TCP, EtherCAT, Profinet, and EtherNet/IP. Through technical analysis and comparison, the study explores their inherent vulnerabilities, available mitigation strategies, and best practices for secure deployment in modern industrial environments. Understanding the strengths and weaknesses of these protocols is essential for engineers, integrators, and cybersecurity professionals tasked with protecting industrial control systems from increasingly sophisticated threats.

II. FIELDBUS COMMUNICATION PROTOCOLS

Communication protocols form the backbone of industrial control systems, yet many were developed without inherent security features, making them vulnerable to cyber threats including spoofing, denial-of-service, and unauthorized access. An analysis of mostly used industry protocols like: CANopen, Modbus TCP, EtherCAT, PROFINET, and EtherNet/IP, with their characteristics (Table 1.) and vulnerabilities are represented.

CANopen has a complete communication architecture that includes device profiles, communication services, and application layers. This makes it much easier to develop interoperable and reliable systems.

One of the key features of CANopen is its communication model, which includes several types of messages optimized for different purposes. Process Data Objects (PDOs) are used for real-time data exchange. These are short, time-critical messages (up to 8 bytes) that can be sent cyclically, based on events, or synchronized to a common time base. For configuration, diagnostics, and other less time-sensitive tasks, Service Data Objects (SDOs) are used. These allow devices to read from or write to one another's memory using a client-server model. Additional message types include emergency messages (EMCY), used to signal critical faults, and synchronization messages (SYNC), which coordinate the timing of PDO transmissions [Barbosa, et al., 2003].

Each CANopen device contains an internal data structure known as the Object Dictionary. This is a standardized list of all the device's parameters, such as configuration settings, process variables, and status indicators. The Object Dictionary provides a consistent way for other devices or control systems to interact with a device, regardless of its specific function or manufacturer. Parameters are accessed by their 16-bit index and subindex, making the system both organized and highly flexible [CiA, 2025].

CANopen has many advantages. It is lightweight and efficient, which is especially important in systems with limited computing resources. It supports real-time communication, making it suitable for motion control and other time-sensitive applications. It is also very reliable, with built-in error handling and diagnostic capabilities, including heartbeat messages, node guarding, and emergency messages. Furthermore, CANopen is scalable, allowing networks to range from just a few nodes to several dozen, and its flexibility in topology and device configuration means it can be adapted to a wide range of use cases.

However, CANopen is not without limitations. The maximum payload of 8 bytes per message can be restrictive for data-heavy applications, and the maximum communication speed of 1 Mbps may be insufficient for high-bandwidth needs. In addition, the physical characteristics of the CAN bus limit network length, especially at higher speeds—for instance, at 1 Mbps, the recommended bus length is around 40 meters. For these reasons, newer Ethernet-based protocols like EtherCAT and PROFINET are becoming more common in applications that require high data throughput and long distances.

Modbus TCP (also known as Modbus TCP/IP) is a network protocol used in industrial automation systems for communication over Ethernet. Modbus TCP operates over standard Ethernet networks using the TCP/IP protocol stack. This makes it a modern and flexible solution for integrating field devices, controllers, Supervisory Control and Data Acquisition (SCADA) systems, and human-machine interfaces (HMIs) into IP-based networks.

Modbus TCP follows the client-server model (equivalent to the master-slave model in Modbus RTU), where the client (often a Programmable Logic Controller (PLC), SCADA, or HMI) initiates requests and the server (a field device such as a sensor, actuator, or I/O (input/output) module) responds. What makes Modbus TCP particularly appealing is that it retains the core structure and function codes of the original Modbus protocol, which ensures compatibility and ease of migration from serial to Ethernet-based systems.

Modbus TCP uses Transmission Control Protocol (TCP) port 502 for communication and encapsulates Modbus frames within a standard TCP/IP packet. The Modbus Application Data Unit (ADU) consists of two parts: MBAP (Modbus Application Protocol) Header that contains transaction ID (identification), protocol ID, length, and unit ID (replacing the slave address in RTU), and PDU (Protocol Data Unit) that contains the function code and associated data (same as in Modbus RTU) [Machaka, et al., 2025].

Because Modbus TCP uses the full Ethernet stack, it can be integrated into existing Local Area Networks (LAN) and Wide Area Networks (WAN). Devices can be connected via switches, routers, and even wireless access points, allowing for easy scalability and remote access capabilities.

Modbus TCP benefits from using standard Ethernet networks, allowing easy integration with existing infrastructure and eliminating the need for special converters. It offers higher communication speeds compared to serial Modbus, enabling faster data exchange and better scalability across large or distributed systems. Its simplicity and wide vendor support make it easy to implement, and remote access capabilities facilitate monitoring and control from anywhere.

EtherCAT is a high-performance industrial Ethernet protocol standardized under IEC 61158. It is widely recognized for its exceptional real-time capabilities, deterministic behavior, and scalability, making it ideal for applications requiring fast cycle times and precise synchronization, such as motion control, robotics, and high-speed manufacturing systems.

At the core of EtherCAT's performance is its unique "on-the-fly" processing mechanism. Unlike conventional Ethernet protocols, where each node receives, interprets, and forwards frames individually, EtherCAT frames are processed as they pass through each slave device. Devices extract and insert data into the frame without delaying its propagation, resulting in extremely low latency and jitter. This process allows EtherCAT to achieve cycle times of less than 100 microseconds and synchronization accuracy better than 1 microsecond [He, et al., 2021].

EtherCAT uses standard IEEE 802.3 Ethernet frames and operates primarily over Fast Ethernet physical layers, although it is also compatible with fiber optics and other media. It employs a master-slave topology, where a single master communicates with up to thousands of slave devices in a ring or line configuration. The use of full-duplex communication and distributed clocks ensures precise timing and robust operation even in complex topologies [Lind, et. al., 2016].

One of EtherCAT's strengths is its flexibility in data handling. It supports various protocols (CoE (CAN application protocol over EtherCAT), SoE (Servo Profile over EtherCAT), FoE (File over EtherCAT), AoE) for communication with different types of devices and applications. For example, CoE is commonly used to communicate with devices using CANopen profiles, allowing interoperability with existing systems. Additionally, EtherCAT supports hot-connect functionality and cable redundancy, enhancing reliability in mission-critical environments.

PROFINET is a widely used industrial Ethernet communication protocol. As the Ethernet-based successor to Profibus, PROFINET combines the advantages of traditional fieldbus systems with the speed and flexibility of Ethernet, making it a powerful solution for industrial automation applications.

PROFINET is based on standard IEEE 802.3 Ethernet and supports real-time and non-real-time communication, enabling it to handle both deterministic control traffic and general data transmission over the same infrastructure. It follows a client-server model (also called controller-device), where the central controller (e.g., PLC) communicates with distributed field devices (sensors, actuators, drives) [Jasperneite, 2005].

Devices in a PROFINET network are typically addressed by IP addresses and device names, allowing integration into broader IT systems while still supporting deterministic industrial communication.

PROFINET offers a wide array of features that make it one of the most versatile and efficient industrial communication protocols available today. One of its key strengths lies in its scalability and flexibility, allowing it to be used across a broad range of applications—from simple I/O devices to complex, distributed automation systems. PROFINET supports various network topologies, including line, star, ring, and tree structures, making it adaptable to different plant layouts and system architectures.

Another major benefit is its real-time communication capability. Through different communication classes—Real-Time (RT), Isochronous Real-Time (IRT), and Non-Real-Time (NRT), PROFINET enables both time-critical process control and non-critical data exchange within a single network [Dias, et al., 2021]. This duality reduces the need for separate communication layers and simplifies system integration.

PROFINET also excels in interoperability, as it is backward-compatible with PROFIBUS and supports integration with other protocols using gateways and proxies. This ensures a smooth transition for industries migrating from older systems while maintaining compatibility with a wide ecosystem of devices.

Ease of installation and maintenance is another important advantage. The use of GSDML (Generic Station Description Markup Language) files simplifies device integration, configuration, and diagnostics. Engineers can quickly deploy devices and access detailed device information through engineering tools, reducing commissioning time and minimizing the risk of configuration errors.

In terms of reliability and availability, PROFINET supports redundancy mechanisms such as Media Redundancy Protocol (MRP) and system redundancy classes (S1, S2, R1, R2), which are crucial for high-availability applications. These features ensure continuous operation even in the event of cable or device failures, making PROFINET suitable for mission-critical systems.

Additionally, PROFINET provides comprehensive diagnostic capabilities, allowing real-time monitoring and fault detection down to the individual device or channel level. These diagnostics are integrated into the system architecture and can be accessed without additional tools, facilitating predictive maintenance and reducing downtime.

Lastly, PROFINET integrates seamlessly with PROFIsafe, enabling the safe transmission of safety-related signals over the same communication infrastructure. This unification simplifies system design, reduces wiring complexity, and ensures compliance with international safety standards.

Altogether, these features make PROFINET a powerful solution for modern industrial environments, offering high performance, reliability, and maintainability in one unified communication platform.

EtherNet/IP builds upon standard Ethernet and the Common Industrial Protocol (CIP) to provide a scalable and robust solution for real-time industrial communication. Its openness, interoperability, and integration with standard IT infrastructure have made it a preferred choice in industries ranging from manufacturing to energy and transportation.

At its core, EtherNet/IP uses the CIP protocol to define the structure and behavior of data exchange, extending it over Ethernet using TCP/IP and UDP/IP for transport. Unlike traditional fieldbus protocols that require dedicated physical layers and proprietary stacks, EtherNet/IP leverages standard Ethernet components and IEEE 802.3 technologies, allowing it to coexist with office and enterprise systems on the same network infrastructure [Barrios-Avilés, et al., 2017].

Devices are addressed using IP addresses, and the protocol supports client-server (scanner-adapter) and peer-to-peer communication models. EtherNet/IP is highly flexible and supports a wide range of topologies, including line, star, ring, and mesh, as well as device-level ring (DLR) redundancy for fault-tolerant communication.

Table1Fieldbus protocol characteristics

Protocol	Data Rate	Topology	Deterministic	Real-time Support	Typical Application Areas
CANopen	Up to 1 Mbps	Bus	Yes	Good	Embedded systems, robotics, mobile machinery
Modbus TCP	Ethernet (10/100 Mbps)	Star (Ethernet)	No	Poor	Industrial Ethernet devices
EtherCAT	100 Mbps (full-duplex)	Daisy-chain	Yes (cycle time <100 µs)	Excellent	High-performance motion, PLC, I/O systems
PROFINET	100 Mbps – 1 Gbps	Star, Line	Yes (RT/IRT)	Very good to excellent	Factory automation, motion control
EtherNet/IP	100 Mbps	Star (Ethernet)	Yes (CIP Sync)	Good to very good	Discrete and process automation

III. ANALYSIS AND DISCUSSION OF CYBERSECURITY

Cybersecurity in Fieldbus protocols is a critical concern in modern industrial automation systems. These protocols—such as CANopen, Modbus TCP, EtherCAT, PROFINET, EtherNet/IP—were originally designed for efficiency, real-time control, and robustness in industrial environments, not with cybersecurity in mind. As industries move toward Industry 4.0 and IIoT (Industrial Internet of Things), the exposure of these protocols to networked environments has made them vulnerable to cyber threats (Table 2., summarizes fieldbus protocol cybersecurity characteristics).

CANopen was primarily designed for robustness and real-time performance, not for secure communication. CANopen lacks basic security mechanisms such as encryption, authentication, or message integrity verification. As a result, it is vulnerable to message spoofing, replay attacks, and denial-of-service (DoS) through bus flooding. Any malicious node connected to the network can potentially inject unauthorized commands or disrupt communication.

To secure CANopen networks, physical access to the bus must be strictly controlled, and network segmentation should be enforced to prevent unauthorized devices from connecting. However, since security features are not native to the protocol, external measures such as secure gateways or protocol wrappers must be used for enhanced protection.

Modbus TCP suffers from serious security flaws. Communication is carried out in plaintext, without encryption or authentication. Any attacker with network access can intercept, modify, or inject messages, potentially changing critical process values or issuing unauthorized commands.

Although Modbus Security variants exist, which include Transport Layer Security (TLS) encryption and device authentication, they are not widely implemented in legacy systems. In most industrial environments, Modbus TCP continues to be deployed without protective measures. To mitigate these risks, organizations should use Virtual Private Network (VPN) or encrypted tunnels to protect Modbus TCP traffic, implement strict firewall rules, and isolate the industrial network from external systems.

EtherCAT is a high-speed, real-time Ethernet-based protocol designed for motion control and precision automation. It achieves superior performance by using a “processing-on-the-fly” method that reduces latency. However, security was not a priority in its original specification. EtherCAT does not include built-in support for encryption or authentication, making it vulnerable to frame injection, replay attacks, and manipulation of synchronization messages.

While efforts are underway to develop more secure extensions (such as EtherCAT G), most deployed systems remain unprotected. Since EtherCAT frames are not standard Ethernet frames, they may evade traditional security tools. Therefore, securing EtherCAT networks requires isolation, trusted devices, and the use of managed switches with port security.

PROFINET is a flexible industrial Ethernet. Unlike older protocols, PROFINET includes some security mechanisms in its specification through defined Security Classes (1, 2, and 3). These classes address various aspects of cybersecurity such as message integrity, device authentication, and secure booting. However, in practice, many PROFINET systems still operate without full implementation of these security features due to backward compatibility requirements or lack of awareness.

PROFINET networks can be susceptible to network scanning, device spoofing, or denial-of-service (DoS) attacks if not properly configured. To enhance security, organizations should ensure that PROFINET Security Class 3 features are supported and enabled where possible. Additional measures such as traffic filtering, Virtual LAN (VLAN) separation, and endpoint authentication further reduce the attack surface.

EtherNet/IP is another Ethernet-based protocol, widely used in industrial automation. It is built on the CIP and allows both real-time control and data exchange over standard Ethernet. One of its major advantages is the support for CIP Security, which introduces features like TLS encryption, mutual device authentication, and secure session key exchange.

Despite these advancements, many EtherNet/IP installations still rely on unprotected configurations due to legacy devices or misconfiguration. Without CIP Security enabled, EtherNet/IP is susceptible to traffic sniffing, replay attacks, and malicious message injection. It is critical that organizations deploying EtherNet/IP ensure the use of secure firmware, validate configurations, and apply CIP Security wherever supported.

Table 2 Fieldbus protocol cybersecurity characteristics

Protocol	**Native Security**	**Encryption**	**Authentication**	**Secure Extension Available**
CANopen	No	No	No	No
Modbus TCP	Minimal	No	No	Yes (Modbus Security)
EtherCAT	No	No	No	In development (EtherCAT G)
PROFINET	Partial	Partial	Partial	Yes (Security Class 3)
EtherNet/IP	Yes (CIP Sec)	Yes	Yes	Yes

IV. MITIGATION STRATEGIES AND BEST PRACTICES

Given the increasing exposure of industrial communication protocols to cyber threats, especially in environments integrating legacy Fieldbus systems and modern Ethernet-based technologies, it is essential to adopt comprehensive mitigation strategies. Since many of these protocols—such as CANopen, Modbus TCP, EtherCAT, PROFINET, and EtherNet/IP—lack native security features, protection must be implemented through external methods and good cybersecurity practices.

One of the most effective strategies is network segmentation, where the operational technology (OT) network is physically and logically separated from the corporate IT network. This reduces the chances of lateral movement from compromised systems in the business network to critical industrial assets. Segmenting networks using VLANs and placing sensitive devices in isolated zones behind firewalls or within demilitarized zones (DMZs) helps contain potential attacks and limit access to critical equipment.

In addition, access control is fundamental. This includes applying strict policies such as Media Access Control (MAC) address filtering, IP whitelisting, and enforcing authentication mechanisms at entry points into the control network. These measures ensure that only authorized devices and users can communicate with industrial equipment. Where possible, user role-based access and multi-factor authentication should be employed to prevent unauthorized control commands or configuration changes.

Since many industrial protocols do not support encryption or secure authentication, secure gateways and protocol proxies should be used to wrap insecure communication within encrypted tunnels such as TLS or VPNs. These gateways can enforce authentication, encrypt data, and even perform packet inspection to identify abnormal behavior. Particularly for protocols like Modbus TCP or CANopen, where data is transmitted in plaintext, tunneling traffic through a secure channel is essential when operating over shared or public networks.

Traffic monitoring and anomaly detection are also crucial in industrial cybersecurity. Deploying Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) that are tailored to industrial protocols can help identify unusual traffic patterns, unauthorized message types, or attempts at replay attacks. These tools can alert operators or automatically block traffic to prevent escalation of a potential incident.

Another important practice is implementing encryption, especially in cases where the protocol itself does not support it natively. Even in real-time systems where full encryption might introduce latency, partial encryption of configuration channels or administrative access can significantly enhance security. For protocols that do offer secure versions—like CIP Security in EtherNet/IP or PROFINET Security Class 3—those features should be enabled and properly configured.

Finally, patch management and device hardening complete the security strategy. Industrial devices should be regularly updated with the latest firmware patches provided by manufacturers, especially when vulnerabilities are disclosed. Additionally, unused ports, services, and protocols should be disabled to reduce the attack surface. Devices should be configured according to best practices and locked down against changes, either physically or through software protections.

Altogether, these mitigation strategies form a defense-in-depth approach, which is essential in today's converged industrial networks. As the line between IT and OT continues to blur, robust cybersecurity practices are no longer optional—they are a fundamental requirement for protecting critical infrastructure and ensuring the safety, reliability, and continuity of industrial operations.

V. CONCLUSION

Industrial communication protocols are the backbone of automated systems, but many were not designed with cybersecurity in mind. As these protocols become exposed to wider networks, their vulnerabilities pose serious risks to system integrity and operational continuity. Protocols like CANopen, Modbus TCP, and EtherCAT remain vulnerable without external security layers. On the other hand, newer protocols such as PROFINET and EtherNet/IP have started to incorporate security features, but proper configuration and implementation are critical.

Ultimately, securing industrial communication networks requires more than just protocol upgrades. A comprehensive defense-in-depth strategy—combining segmentation, encryption, monitoring, and policy enforcement—is essential for protecting industrial systems from modern cyber threats. The transition toward secure-by-design protocols and adherence to international standards such as IEC 62443 will further strengthen the cybersecurity posture of industrial environments.

Conflict of interest

There is no conflict to disclose.

ACKNOWLEDGEMENT

The research for this paper was funded by the project „Unapređenje kvaliteta nastave na sudijskim programima Departmana kroz implementaciju rezultata naučno-istraživačkog rada u oblasti Industrijskog inženjerstva i menadžmenta “.

REFERENCES

[1]. Barbosa, M., Farsi, M., Allen, C. & Carvalho, A.S., 2003. Formal validation of the CANopen communication protocol. IFAC Proceedings Volumes, 36(13), 225-230.

[2]. Barrios-Avilés, J., Rosado-Muñoz, A., Iakymchuk, T. & García-Chulbi, M., 2017. POWERLINK and Ethernet/IP Comparison as Robust Industrial Ethernet Protocols. IFAC-PapersOnLine, 50(1), 363-368.

[3]. CiA. 2025. CAN: From physical layer to application layer and beyond https://www.can-cia.org/can-knowledge

[4]. Dias, A.L., Turcato, A.C., Sestito, G.S., Brandao, D. & Nicoletti, R., 2021. A cloud-based condition monitoring system for fault detection in rotating machines using PROFINET process data. Computers in Industry, 126, 103394.

[5]. He, S., Huang, L., Chen, X. Wang, Z., Wang, G., Zuo, Y. & Zhang, X., 2021. Remote monitoring system for ITER PF converter system based on EtherCAT. Fusion Engineering and Design, 164, 112182.

[6]. Jasperneite, J., 2005. Fieldbus Integration to the Realtime Ethernet Standard PROFINET, IFAC Proceedings Volumes, 38(1), 25-29.

[7]. Lind, M., Morset, E. & Bredeli, M., 2016. EtherCAT-integrated Processing Machine with Full Local Task Redundancy. Procedia CIRP, 54, 204-209.

[8]. Machaka, V., Figueroa-Lorenzo, S., Arrizabalaga, S., Elduayen-Echave, B. & Hernantes, J., 2025. Assessing the impact of Modbus/TCP protocol attacks on critical infrastructure: WWTP case study. Computers and Electrical Engineering, 126, 110485.

[9]. Ostojić, G. & Stankovski, S., 2024. IoT Protocols and Cybersecurity Threats. Journal of Mechatronics, Automation and Identification Technology – JMAIT, 9(1), 1-4.