ISSN (e): 2250 – 3005 || Volume, 16 ||Issue, 1||January-2026 ||
International Journal of Computational Engineering Research (IJCER)

AI in Industrial Communication Protocols

Gordana Ostojic[1], Stevan Stankovski[2]
[1]Full professor, Faculty of Technical Sciences, University of Novi Sad, Trg Dositeja Obradovica 6, 21000 Novi Sad, Serbia.
[2] Full professor, Faculty of Technical Sciences, University of Novi Sad, Trg Dositeja Obradovica 6, 21000 Novi Sad, Serbia.
Corresponding Author: Gordana Ostojic

ABSTRACT
The rapid advancement of industrial automation and Industry 4.0 has significantly increased the complexity and volume of data exchanged through industrial communication protocols. Traditional industrial networks such as Modbus, PROFIBUS, CAN, Ethernet/IP, and OPC UA were primarily designed for deterministic communication and reliability, but they face growing challenges related to scalability, latency optimization, fault detection, and cybersecurity. Artificial Intelligence (AI) introduces new possibilities for enhancing the performance, resilience, and security of industrial communication systems.
This paper explores the integration of AI techniques with industrial communication protocols, focusing on applications such as intelligent network monitoring, anomaly detection, predictive maintenance, traffic optimization, and adaptive fault tolerance. Machine learning and deep learning models are analyzed in the context of real-time data streams generated by industrial fieldbuses and industrial Ethernet networks. Special attention is given to AI-driven intrusion detection systems and protocol-aware security mechanisms that address emerging cyber threats in smart factories.
KEYWORDS: *protocols, security, resilience, AI techniques, monitoring*

Date of Submission: 12-01-2026 Date of acceptance: 24-01-2026

I. INTRODUCTION

The rapid digitalisation of industrial systems has fundamentally transformed industrial communication networks. Modern industrial environments rely on a variety of communication protocols to enable the reliable and predictable exchange of data between sensors, actuators, controllers and supervisory systems. Traditionally, industrial communication protocols such as Modbus, PROFIBUS (Process Field Bus), CAN (Controller Area Network), PROFINET, EtherCAT (Ethernet for Control Automation Technology) and OPC UA (Open Platform Communications Unified Architecture) have been designed to meet strict real-time requirements, ensuring high availability and predictable behaviour, which are essential for safe and efficient industrial operation.

However, the increasing interconnection of industrial control systems with enterprise networks, cloud platforms and Industrial Internet of Things (IIoT) infrastructures has significantly increased the vulnerability of industrial networks to cyber threats [1]. Protocols that operated within closed intranet environments are now exposed to cyber threats, including unauthorised access, data manipulation, denial-of-service attacks and advanced persistent threats. At the same time, industrial systems impose strict real-time constraints; even minimal communication delays or packet losses can result in performance degradation, production downtime or safety-critical failures. These characteristics mean that conventional IT security mechanisms are not suitable for industrial communication systems.

Artificial intelligence (AI) has emerged as a promising approach to addressing the growing cybersecurity and real-time performance challenges in industrial communication networks. Leveraging machine learning and data-driven techniques, AI can intelligently monitor network traffic, detect anomalous communication patterns and identify cyber attacks early on, which are difficult to detect using rule-based methods. Unlike traditional security solutions, AI-based approaches can adapt to changing network conditions and evolving attack strategies, all the while maintaining an awareness of protocol-specific behaviours.

Despite its potential, integrating AI into industrial communication protocols poses significant challenges. AI models must operate within strict real-time constraints and with limited computational resources while ensuring deterministic behaviour and high reliability. Furthermore, AI-based security mechanisms must be carefully designed for deployment to avoid introducing additional latency or unpredictability that could

compromise the real-time operation of industrial systems. These challenges emphasise the importance of systematically analysing how AI can be effectively integrated into industrial communication protocols without compromising their fundamental real-time and safety requirements.

This paper examines how AI can enhance the cybersecurity and real-time robustness of industrial communication protocols. It focuses on AI-driven anomaly and intrusion detection and adaptive security mechanisms that consider protocol semantics and real-time constraints. Through the analysis of existing approaches, architectural solutions, and open research challenges, the paper aims to demonstrate the potential of AI to make industrial communication systems more secure, resilient, and intelligent.

II. INDUSTRIAL COMMUNICATION PROTOCOLS

Industrial communication protocols form the backbone of automation systems, enabling the reliable and deterministic exchange of data between distributed industrial devices. Unlike conventional IT communication protocols, industrial protocols are specifically designed to meet strict real-time requirements and ensure high availability and predictable timing behaviour. These characteristics are essential in industrial control systems, as communication delays, jitter or packet loss can directly affect process stability, safety and production efficiency.

Early industrial communication protocols such as Modbus, PROFIBUS and CAN were developed for closed environments. The primary design goals of these protocols were simplicity, determinism and robustness rather than cybersecurity. Consequently, many of these protocols lack native security mechanisms such as authentication, encryption, and access control. While this design choice was acceptable for traditional industrial networks, it has significant security risks in today's interconnected industrial environments.

As industrial Ethernet technologies have evolved, protocols such as Modbus, PROFINET, EtherCAT and Ethernet/IP have become dominant in real-time industrial communication [2-4]. These protocols utilise standard Ethernet physical layers while introducing specialised mechanisms to achieve deterministic behaviour, low latency and precise synchronisation. Techniques such as time-slotted communication, prioritised traffic scheduling and hardware-based frame processing enable these protocols to meet real-time constraints. However, adopting Ethernet also introduces vulnerabilities inherited from standard networking technologies, increasing exposure to cyber-attacks such as spoofing, man-in-the-middle attacks and denial-of-service scenarios.

Service- and IIoT-oriented protocols such as OPC UA and MQTT (Message Queuing Telemetry Transport) represent an evolution towards greater interoperability and flexible data exchange across the different layers of industrial systems [5]. OPC UA, in particular, offers built-in security features such as encryption, authentication and role-based access control, making it better suited to secure industrial communication. However, the complexity of these protocols and their deployment across heterogeneous systems can create new attack vectors, particularly in the event of misconfigurations or insecure implementations. Furthermore, the adoption of publish–subscribe communication models and cloud connectivity poses challenges in terms of latency predictability and real-time performance.

Real-time control requirements are a critical aspect of industrial communication protocols. Many industrial applications operate under strict real-time constraints; delayed or lost messages can result in unsafe states or system failures. Therefore, security mechanisms introduced at the communication level must be carefully designed to avoid introducing non-deterministic delays or excessive computational overhead. Achieving the right balance between security and real-time performance remains one of the central challenges in designing industrial communication systems.

The increasing number of connected devices means that industrial communication networks are becoming more heterogeneous. This makes traditional static configuration and rule-based monitoring insufficient for ensuring secure and reliable operation. The behaviours, timing characteristics and traffic patterns of different industrial networks and applications vary significantly due to their protocol-specific nature. This creates an opportunity for AI-based approaches that can learn normal communication behaviour, identify real-time deviations and enhance security and operational robustness, all without compromising deterministic performance.

III. ARTIFICIAL INTELLIGENCE IN INDUSTRIAL COMMUNICATION SYSTEMS

As industrial communication networks grow in size and diversity and become more interconnected, AI is emerging not only as a supporting technology, but also as a key enabler of intelligent, adaptive industrial communication systems.

AI-based analysis of industrial communication traffic relies on the ability to model normal operational behaviour with great accuracy. Industrial protocols exhibit highly structured communication patterns, including cyclic message exchanges, deterministic timing and well-defined state transitions [6]. Machine learning models can leverage these characteristics to identify temporal and spatial patterns in network traffic, such as inter-packet timing, message sequence consistency and protocol-specific field usage. Once trained, these models can

detect deviations that may indicate cyber-attacks, device malfunctions or configuration errors, often at an early stage, before system performance is visibly affected.

One of the most significant applications of AI in industrial communication systems is the detection of anomalies and intrusions. AI-driven intrusion detection systems analyse behavioural features to identify both known and previously unseen attacks, rather than relying on predefined signatures. This is particularly important in industrial environments, where attackers often exploit legitimate protocol functions to avoid detection. AI models that understand the expected temporal and logical behaviour of industrial protocols and can identify timing-based attacks, replay attacks, and manipulation of control messages [7]. These protocol detection mechanisms can significantly enhance cybersecurity while minimising the number of false positives that could disrupt industrial operations.

Real-time constraints are crucial in the development of AI applications within industrial communication networks. Security mechanisms must operate within tight latency bounds and exhibit predictable execution behaviour. To meet these requirements, AI-based solutions are increasingly being deployed at the edge of the network, for example in programmable logic controllers, industrial gateways or dedicated monitoring devices. Edge-based AI enables real-time traffic analysis and an immediate response to detected threats, thereby reducing reliance on centralised cloud processing and minimising communication delays. Lightweight machine learning models and streaming data processing techniques are particularly well suited to these scenarios as they strike a balance between detection accuracy and computational efficiency.

AI can support adaptive and autonomous responses to security incidents and communication anomalies, going beyond mere detection. By correlating information across different network layers and timescales, AI systems can help with dynamic traffic prioritisation, isolating compromised devices and reconfiguring communication paths to maintain system stability. In real-time industrial environments, however, such adaptive responses must be carefully controlled to avoid introducing non-deterministic behaviour. Therefore, AI-driven decision-making is often combined with predefined safety rules and control policies to ensure critical real-time communication remains unaffected.

AI applications in industrial communication systems also enhance system resilience and fault tolerance. Communication anomalies are not always caused by malicious activity, but may result from hardware degradation, electromagnetic interference or configuration inconsistencies. AI models trained on operational data can distinguish between normal process variations and abnormal conditions, enabling more accurate fault diagnosis and predictive maintenance of communication infrastructure. This capability is particularly valuable in large-scale industrial installations where manual monitoring is impractical and communication failures can propagate rapidly through interconnected systems.

Despite their advantages, AI-based applications in industrial communication systems face significant challenges regarding trust, explainability, and validation. In safety-critical and real-time environments, it is essential to understand why a communication occurrence has been classified as anomalous or malicious. Therefore, explainable AI techniques and hybrid approaches combining data-driven models with protocol-specific rules are becoming increasingly important. Furthermore, AI models must be validated under realistic operational conditions to ensure stable performance when network loads and timing constraints vary.

Integrating AI into industrial communication systems enables advanced cybersecurity capabilities and improved real-time robustness. AI provides intelligent monitoring, protocol-aware intrusion detection and adaptive response mechanisms, enhancing the security and resilience of industrial communication protocols while respecting their strict real-time requirements. The convergence of AI, cybersecurity and real-time communication is a critical step towards developing autonomous and trustworthy industrial networks.

IV. SYSTEM ARCHITECTURES AND CHALLENGES FOR AI INTEGRATION IN INDUSTRIAL COMMUNICATION

Effective integration of artificial intelligence into industrial communication systems requires system architectures that are carefully designed to respect the strict real-time, reliability and safety constraints of industrial environments. Unlike conventional IT systems, industrial networks must guarantee deterministic behaviour and predictable communication timing, even when security monitoring and adaptive control mechanisms are in place. Consequently, AI integration cannot be treated as an additional component, but must be embedded into the communication architecture in such a way as to preserve real-time performance while enhancing cybersecurity and system resilience.

Industrial communication architectures are increasingly adopting a hierarchical structure spanning edge, fog and cloud layers. At the edge level, AI components are deployed close to industrial devices and communication endpoints. This enables real-time traffic monitoring and the immediate detection of anomalies. Edge-based AI is particularly well suited to latency-sensitive applications as it minimises communication delays and enables security-related decisions to be made locally. However, the limited computational resources of edge

devices impose constraints on the complexity of AI models that can be deployed. This necessitates the use of lightweight models, optimised inference engines, all of which are tailored to specific industrial protocols.

Fog and gateway-level architectures provide an intermediate layer that balances real-time responsiveness with enhanced computational power. Industrial gateways can aggregate communication data from multiple devices and protocols, enabling more comprehensive, AI-based analysis while maintaining acceptable latency. This architectural layer is ideal for protocol-aware intrusion detection, event correlation across different network segments and coordinated response strategies. However, the introduction of AI processing at this level must be carefully managed to prevent bottlenecks and non-deterministic delays that could impact time-critical communication flows.

Cloud-based architectures offer powerful computing resources and long-term data storage, making them ideal for training models, analysing global networks, and integrating threat intelligence. However, their use in real-time industrial communication is limited by network latency, bandwidth constraints and concerns over availability. Consequently, cloud-based AI is generally employed in a supplementary capacity, facilitating offline analysis, model refinement, and system-wide optimisation rather than real-time decision-making. Separating training and inference across different architectural layers is a common approach to balancing performance and real-time requirements.

Despite the architectural flexibility offered by edge–fog–cloud paradigms, integrating AI into industrial communication systems has several fundamental challenges. One of the most critical of these is ensuring deterministic behaviour in the presence of AI-based processing. Many AI models, particularly those based on deep learning, exhibit variable execution times and data-dependent behaviour, which can conflict with real-time constraints. Therefore, it is essential to ensure predictable inference latency and limited execution times for the deployment of AI in safety-critical industrial environments.

Another major challenge lies in the availability and quality of training data. Industrial communication data is often proprietary, sensitive and highly specific to the application in question. This restricts the availability of representative datasets for training and validation purposes. Furthermore, as industrial networks typically operate under stable conditions for extended periods, abnormal or attack-related events are rare, resulting in imbalanced datasets. This makes it difficult to develop robust AI models and increases the risk of false positives or undetected attacks.

Cybersecurity requirements introduce additional complexity as the AI components themselves can become targets of attack. Adversarial attacks that manipulate machine learning models and model poisoning where malicious data is injected into an AI model's training data, pose significant risks to AI-based security mechanisms. In industrial environments, where trust and reliability are of greatest importance, safeguarding AI models and ensuring their integrity is as crucial as identifying external cyber threats. Therefore, secure deployment, model authentication and continuous validation are essential elements of AI-enabled industrial communication architectures.

Interoperability and standardisation also present significant challenges. Industrial communication systems comprise a wide variety of protocols, vendors and legacy devices, each with specific security characteristics. Integrating AI solutions across such heterogeneous environments requires standardised interfaces, protocol-aware feature representations, and compatibility with existing industrial standards. Without this alignment, AI-based solutions risk becoming isolated components that are difficult to deploy and maintain on a large scale.

Regulatory and safety imperatives establish stringent requirements for the verification, validation, and interpretability of AI systems. Within safety-critical industrial domains, it is essential that decisions generated by AI components remain transparent and demonstrably justifiable to operators, engineers, and certification authorities. Addressing these demands necessitates the integration of explainable AI methodologies alongside hybrid frameworks that combine data-driven models with deterministic rules and established domain expertise.

V. CONCLUSION

In-depth examination of the integration of AI into industrial communication protocols, with particular emphasis on cybersecurity and real-time operational requirements is represented in this paper. Industrial communication protocols constitute the foundational infrastructure of modern automation systems; however, many were originally conceived for deployment within isolated and inherently trusted environments. The progressive interconnection of industrial networks has rendered these protocols increasingly susceptible to diverse cyber threats, while simultaneously accentuating the necessity for deterministic and predictable communication behavior. AI has emerged as a transformative instrument for augmenting both the security and resilience of industrial communication systems.

The analysis presented in this paper demonstrates that AI-driven approaches enable advanced monitoring, protocol-aware anomaly detection, and intelligent intrusion detection mechanisms that transcend the limitations of static rules or predefined attack signatures. By modeling normative communication patterns and

timing characteristics, AI systems are capable of discerning subtle deviations indicative of cyber attacks, system faults, or configuration anomalies. When integrated into industrial architectures—particularly at edge and gateway levels—these mechanisms can operate within stringent real-time constraints, thereby ensuring timely and effective responses to emergent threats.

At the same time, the study underscores that the adoption of AI in industrial communication systems is accompanied by significant challenges. Ensuring deterministic behavior, explainability, and trustworthiness of AI-based decisions remains imperative, particularly in safety-critical environments. Moreover, resource constraints, limited data availability, and interoperability concerns further complicate deployment, thereby highlighting the necessity for lightweight models, protocol-aware designs, and hybrid approaches that combine AI with established engineering methodologies.

Looking ahead, industrial communication systems are anticipated to evolve toward AI-native and security-by-design architectures. The integration of AI with time-sensitive networking technologies, next-generation industrial Ethernet, and private 5G and 6G infrastructures will facilitate more flexible yet deterministic communication paradigms. In parallel, digital twin technologies are expected to assume a pivotal role in the development and validation of AI-based monitoring and security mechanisms, offering safe environments for experimentation and optimization.

Future research will prioritize explainable and resilient AI solutions that can be certified and trusted within industrial contexts. Safeguarding AI components against adversarial attacks and ensuring their long-term reliability will constitute essential dimensions of industrial cybersecurity strategies. Ultimately, the convergence of AI, industrial communication protocols, and real-time cybersecurity represents a critical enabler for the next generation of intelligent, robust, and secure industrial automation systems.

ACKNOWLEDGMENT

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 inženjerskog menadžmenta.”

REFERENCES

[1]. G. Ostojić, and S. Stankovski, IoT Protocols and Cybersecurity Threats, *Journal of Mechatronics, Automation and Identification Technology – JMAIT*, Vol. 9, (2024), No. (1), pp. 1-4.

[2]. C. Urrea, C. Morales, and R. Muñoz, Design and implementation of an error detection and correction method compatible with MODBUS-RTU by means of systematic codes, *Measurement*, Vol. 91, (2016), pp. 266-275.

[3]. L.F. Marques da Luz, P. Freitas de Araujo-Filho, D.R. Campelo, Multi-stage deep learning-based intrusion detection system for automotive Ethernet networks, *Ad Hoc Networks*, Vol. 162, (2024), 103548.

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

[5]. L. Freitas, M. Silva, G. Vale, C. Avram, H. Lopes, F. Pereira, N. Leal and J. Machado, OPC UA and MQTT performance analysis within a unified namespace context, *Internet of Things*, Vol. 33, (2025), 101734.

[6]. K. Saleem, L. Wang and S. Bharany, Survey of AI-driven routing protocols in underwater acoustic networks for enhanced communication efficiency, *Ocean Engineering*, Vol. 314, (2024), Part 1, 119606.

[7]. H. Ahmad, M.M. Gulzar, S. Aziz, S. Habib and I. Ahmed, AI-based anomaly identification techniques for vehicles communication protocol systems: Comprehensive investigation, research opportunities and challenges, *Internet of Things*, Vol. 27, (2024), 101245.