UDC 004.722

INTERACTION MODELS OF INTELLIGENT SENSOR NETWORKS IN INDUSTRIAL INTERNET OF THINGS

Norkusheva D.M.
bachelor's degree, L.N. Gumilyov Eurasian national university (Astana, Kazakhstan)

МОДЕЛИ ВЗАИМОДЕЙСТВИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СЕНСОРНЫХ СЕТЕЙ В ПРОМЫШЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ

Норкушева Д.М.
бакалавр, Евразийский национальный университет имени Л.Н. Гумилёва (Астана, Казахстан)

Abstract

Interaction models in intelligent sensor networks (ISNs) form the basis for autonomous communication and coordination in industrial internet of things (IIoT) systems. The analysis focuses on topological structures, hierarchical communication layers, synchronization strategies, and decentralized behavior control. Core challenges related to interoperability, temporal consistency, and field-level integration are discussed alongside technical patterns for achieving scalable and resilient performance. The findings contribute to the development of robust ISN infrastructures capable of operating under the complexity of modern industrial environments.

Keywords: intelligent sensor networks, IIoT, decentralized coordination, interaction models, synchronization, interoperability, industrial protocols, distributed sensing.

Аннотация

Модели взаимодействия интеллектуальных сенсорных сетей (ИСН) служат основой для автономной коммуникации и согласованных действий в системах промышленного Интернета вещей (IIoT). Представлены ключевые подходы к построению топологий, организации многоуровневой передачи данных, синхронизации во времени и децентрализованному управлению поведением узлов. Особое внимание уделено совместимости, устойчивости к сбоям и особенностям применения в условиях реального промышленного производства. Предложенные выводы ориентированы на создание масштабируемых и надёжных ИСН-решений для сложных распределённых систем.

Ключевые слова: интеллектуальные сенсорные сети, IIoT, децентрализованная координация, модели взаимодействия, синхронизация, совместимость, промышленные протоколы, распределённые сенсоры.

Introduction

The rapid development of industrial automation and cyber-physical infrastructure has intensified the deployment of distributed sensing systems across manufacturing, energy, logistics, and resource management sectors. These systems rely on sensor networks capable of capturing environmental parameters, process states, and operational metrics in real time. As the scale and complexity of such networks increase, the emphasis shifts from simple data acquisition toward intelligent behavior and coordinated interaction among sensing units. This transition marks the evolution toward intelligent sensor networks, where autonomous sensing, processing, and communication capabilities enable adaptive, context-aware functionality.

The integration of ISNs within the framework of the industrial internet of things brings new challenges and opportunities. IIoT, defined as a distributed ecosystem of devices, communication protocols, and edge-computing systems applied in industrial settings, demands robust interaction models to ensure efficient, scalable, and resilient operations. In this context, interaction refers not only to data exchange but also to collaborative sensing, event-driven decision-making, and cooperative task execution. The behavior of ISNs is governed by a combination of decentralized logic, embedded intelligence, and networked coordination mechanisms that operate across heterogeneous physical and digital infrastructures.

This paper aims to investigate the conceptual and practical models of interaction among ISNs in IIoT environments. The focus lies on structural principles, communication topologies, decision protocols, and the role of local autonomy in global system behavior. Special attention is given to the design patterns that support synchronization, fault tolerance, and scalability, as well as to the constraints imposed by resource-limited devices and dynamic industrial environments. The objective is to provide a systematic overview of interaction models that form the basis for developing resilient, intelligent, and interoperable sensor networks in industrial domains.

Main part

Interaction within intelligent sensor networks deployed in IIoT environments extends far beyond traditional data polling or broadcasting. Modern systems are expected to exhibit autonomous behavior, which includes local decision-making, adaptive sampling, and collaborative filtering. These features are implemented through decentralized algorithms that operate under constrained power, memory, and computational capabilities [1]. The interaction paradigm must therefore accommodate heterogeneous communication requirements, varying temporal constraints, and real-time responsiveness.

In practice, the behavior of ISNs is shaped by the underlying interaction models-whether they are event-triggered, schedule-based, or opportunistic. Each model defines the conditions under which nodes exchange information, synchronize states, or delegate computation. Event-triggered interactions are often employed in anomaly detection, where a sensor activates a transmission only when predefined thresholds are breached. Scheduled models rely on predefined communication intervals, useful in energy-sensitive applications with predictable patterns. Opportunistic strategies, on the other hand, enable information exchange based on proximity or channel availability, which is particularly relevant in mobile or dynamically changing industrial layouts [2].

Furthermore, the choice of interaction model has a direct impact on the network's ability to self-organize and adapt. In industrial contexts characterized by noise, interference, and component failures, systems must maintain operational coherence without centralized control. This necessitates peer-to-peer negotiation protocols, dynamic topology discovery, and local rule execution. The balance between global coordination and local autonomy becomes a key factor in designing ISNs that can function reliably under stress, while still supporting complex industrial processes such as condition-based maintenance, decentralized control, and distributed diagnostics.

The structure of communication in ISNs is often layered to separate concerns such as sensing, aggregation, decision-making, and actuation. This layered interaction allows for modular system design, where each node can specialize in one or more functional roles depending on its position in the network [3]. For example, edge-layer nodes may primarily perform data collection and preliminary filtering, while intermediary units focus on local aggregation and consensus building. This architectural modularity supports scalability and fault isolation, which are essential in IIoT scenarios that span multiple physical zones and operational domains.

A critical aspect of interaction design is the selection of communication protocols tailored to the constraints of industrial environments. Factors such as electromagnetic interference, spatial coverage gaps, and real-time delivery requirements necessitate the use of robust, lightweight protocols. Popular choices include time-slotted channel hopping (TSCH), WirelessHART, and deterministic Ethernet variants. These protocols are designed to support synchronized multi-hop communication, minimize packet collisions, and ensure deterministic message delivery-properties that are especially relevant in safety-critical systems such as automated assembly lines or energy grid control units [4].

Moreover, effective interaction relies not only on communication fidelity but also on contextual awareness and task alignment among nodes. Sensors must understand not only when and how to communicate but also what information is relevant to share under specific operational circumstances. This is achieved through embedded rule engines, dynamic priority queues, and semantic data models that allow nodes to make informed decisions about data relevance, urgency, and destination. Such context-driven interaction mechanisms reduce unnecessary traffic, preserve bandwidth, and enhance the overall responsiveness of the IIoT system.

Topological configurations for sensor interaction in industrial environments

The physical and logical topology of sensor networks plays a central role in shaping how interaction unfolds across an IIoT system. Common topological configurations include star, mesh, cluster-tree, and hybrid arrangements, each offering distinct trade-offs in terms of resilience, scalability, and latency [5]. In industrial settings, where equipment layout, electromagnetic interference, and reliability requirements vary significantly, the topology must be chosen or adapted dynamically based on operational constraints.

Star topologies, while easy to manage, suffer from single-point failure vulnerabilities and limited scalability. Mesh configurations, by contrast, support robust multi-path communication and can self-heal by rerouting data around failed nodes, but they impose higher protocol complexity and require careful synchronization. Cluster-tree topologies represent a structured compromise, enabling localized interaction within clusters while maintaining global coordination through a hierarchical backbone [6]. Hybrid models increasingly combine these features to exploit spatial hierarchies and optimize traffic flows in real-time.

Figure 1 illustrates typical topological interaction models employed in ISNs within industrial facilities. The figure highlights the structural roles of nodes, interaction flows, and communication dependencies that define each topology.

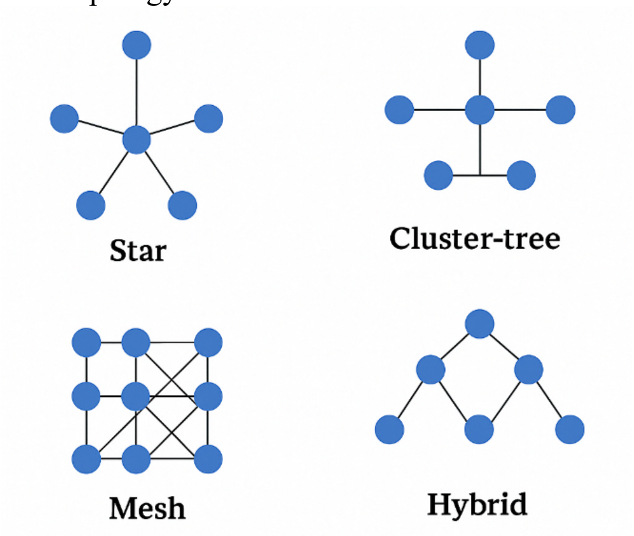

Figure 1. Topological interaction models for intelligent sensor networks in IIoT environments

The figure highlights how different topological configurations influence the interaction capabilities of intelligent sensor networks in industrial systems. While star structures provide centralized simplicity, they lack robustness under node failure. Mesh and cluster-tree (with lowercase «tree») arrangements offer enhanced resilience and dynamic adaptability, crucial for high-availability scenarios [7]. Hybrid models, integrating multiple topologies, present a balanced approach that supports both localized autonomy and system-wide coordination. These configurations serve as the structural basis for designing interaction models capable of maintaining communication integrity and operational continuity in IIoT environments.

Layered communication frameworks for coordinated sensor behavior

In complex industrial environments, sensor networks must operate across multiple abstraction levels to ensure both local responsiveness and system-wide coherence [8]. Layered communication frameworks are employed to decompose responsibilities into functional strata-typically including physical, data link, network, coordination, and application layers. This stratification facilitates modularity, simplifies integration, and supports heterogeneity in hardware and protocols. Each layer is responsible for a specific aspect of interaction: for example, the coordination layer handles consensus and synchronization, while the application layer interprets semantic content for decision support systems.

Such frameworks are particularly beneficial in large-scale deployments, where diverse sensor types and roles coexist. For instance, condition monitoring sensors may interact within their local layer to detect anomalies, while simultaneously reporting summaries upward to a supervisory control system [9]. Meanwhile, actuators respond to coordinated commands derived from aggregated sensor input. This vertical communication model is complemented by horizontal interactions between peer nodes, enabling fault isolation, redundancy, and local optimization. The overall framework ensures that data flow, control signals, and analytical feedback propagate across the network in a structured, traceable manner.

Figure 2 presents a generalized schematic of a layered communication framework for ISNs in industrial systems, illustrating the flow of messages and interaction logic across hierarchical layers.

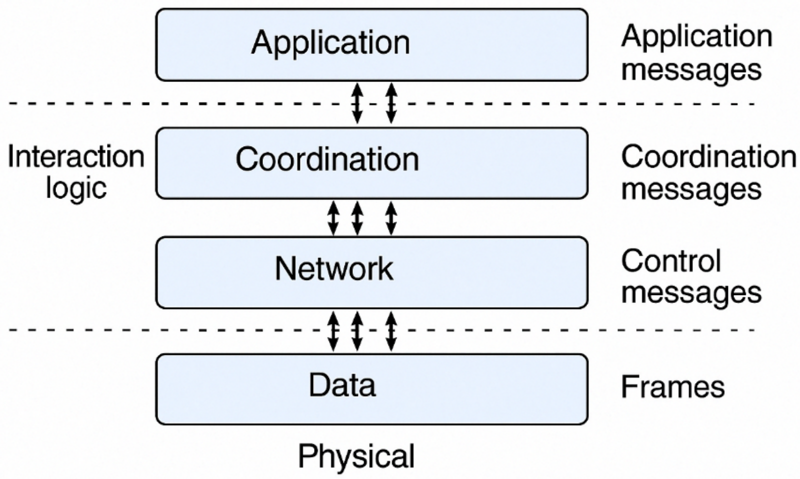

Figure 2. Layered communication framework for intelligent sensor networks in industrial systems

The figure illustrates a modular architecture in which each communication layer manages specific tasks-from raw data handling to semantic interpretation-enabling structured and scalable interaction among intelligent sensors. This layered approach enhances system maintainability, promotes interoperability across platforms, and ensures that data exchange aligns with both operational constraints and application-level objectives.

Behavior coordination strategies for decentralized sensor clusters

In large-scale IIoT deployments, sensor nodes are often grouped into autonomous clusters that must coordinate behavior without central supervision. These decentralized sensor clusters are expected to perform tasks such as fault detection, load balancing, or collaborative event classification in real time. Coordination within such groups relies on local information exchange, probabilistic consensus, and shared behavioral rules. The challenge lies in enabling consistency of group behavior despite variable connectivity, partial observability, and asynchronous communication patterns [10].

Several strategies have been proposed to support coordination in sensor clusters, including leader election, behavior imitation, and reputation-based mechanisms. In leader-based models, a representative node temporarily orchestrates communication and decision flow, while in imitation-based systems, nodes replicate the behavior of more reliable or better-performing neighbors. Reputation-based strategies add a layer of trust scoring, allowing nodes to weigh received information based on the credibility of the sender. Each method introduces different trade-offs between convergence speed, resilience to adversarial behavior, and energy efficiency.

Figure 3 illustrates typical coordination patterns in decentralized ISN clusters. It shows how local rules and neighborhood awareness lead to emergent system behavior, enabling reliable operation without centralized logic.

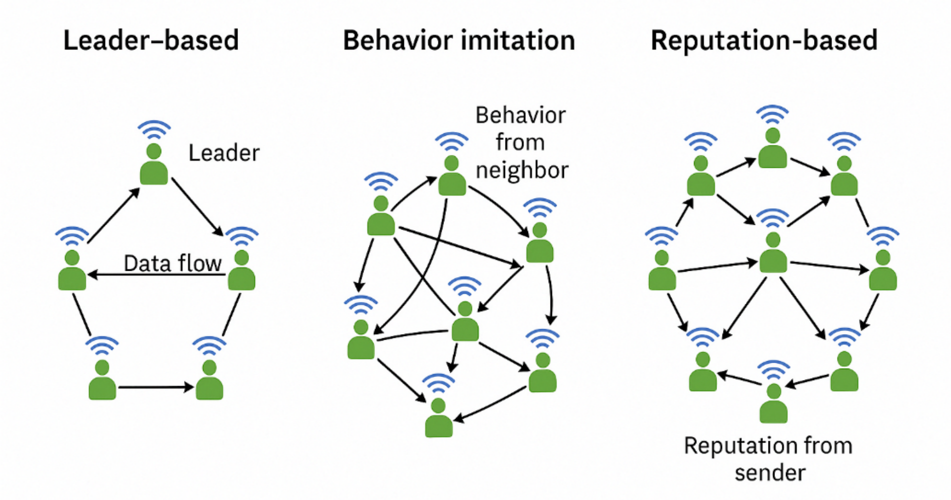

Figure 3. Coordination strategies in decentralized sensor clusters

This figure illustrates three primary coordination approaches in ISNs: leader-based control, behavior imitation among peers, and reputation-weighted consensus. Each method supports decentralized decision-making by leveraging local context and interaction history, enabling autonomous cluster operation without reliance on a central authority. The visual distinctions in structure and data flow demonstrate how different strategies achieve balance between autonomy, trust, and synchronization.

Temporal synchronization and consistency maintenance in dynamic sensor environments

Maintaining temporal coherence across distributed sensor nodes is a fundamental requirement for ensuring accurate and reliable operation in IIoT systems. Time-sensitive applications-such as event detection, process control, or energy optimization-depend heavily on the ability of individual nodes to interpret events within a consistent temporal frame of reference. In decentralized architectures, where sensor nodes operate asynchronously and may experience delays, jitters, or local clock drift, achieving network-wide synchronization poses significant technical challenges.

Synchronization protocols for ISNs are broadly categorized into clock synchronization schemes and event-driven synchronization. Clock synchronization protocols aim to align internal clocks of nodes using message exchanges and statistical correction techniques. Examples include protocols such as precision time protocol (PTP), flooding time synchronization protocol (FTSP), and reference broadcast synchronization (RBS). These schemes use techniques like averaging timestamps, minimizing skew, and recursive adjustments to maintain coherence. However, their efficiency degrades in noisy or mobile environments where packet loss and topology changes are frequent. In such contexts, event-driven synchronization is often favored, where coordination is based on shared sensing events rather than time alignment, reducing overhead but limiting global temporal accuracy.

In dynamic industrial settings, maintaining consistency is further complicated by partial visibility, inconsistent sensing intervals, and transient node failures. To address this, modern ISN architectures implement consistency maintenance layers that include buffer alignment, timestamp reconciliation, and data version control [11]. These mechanisms ensure that even in the presence of network fragmentation or reconfiguration, critical data remains temporally valid and usable for downstream analysis. Additionally, distributed consensus algorithms such as Paxos and Raft have been adapted for use in sensor environments to synchronize state and ensure that updates are propagated reliably, even under failure-prone conditions.

Ultimately, the design of synchronization mechanisms must strike a careful balance between precision, communication overhead, and fault tolerance. For low-power devices, the need to minimize energy consumption may preclude frequent synchronization messages, leading to the adoption of hybrid models that combine loose synchronization with local event correction. Meanwhile, latency-sensitive applications demand strict guarantees, pushing for high-frequency synchronization at the cost of increased resource usage. As IIoT systems continue to evolve, adaptive synchronization strategies that dynamically adjust behavior based on system load, node density, and operational criticality will become increasingly important for sustaining reliable sensor interaction across temporal and spatial scales.

Interoperability and standardization in heterogeneous sensor ecosystems

One of the defining characteristics of industrial IIoT environments is the coexistence of heterogeneous devices originating from multiple vendors, generations, and technological paradigms. Intelligent sensor networks deployed in such settings must therefore support interoperability not only at the hardware and protocol level, but also across data semantics, control logic, and system objectives [12]. Achieving reliable interaction among diverse nodes requires adherence to common standards, modular integration architectures, and adaptive abstraction mechanisms that can bridge technological gaps without sacrificing performance or security.

Interoperability challenges arise in several layers of the interaction stack. At the communication level, differences in wireless technologies (e.g., Zigbee, LoRa, Wi-Fi, 6LoWPAN) and transport protocols (e.g., MQTT, CoAP, OPC UA) can hinder seamless integration, especially when low-power devices operate alongside high-bandwidth systems. Middleware solutions and protocol translation gateways are often introduced to mediate between incompatible stacks, but they introduce latency and additional points of failure [13]. As a response, standardization bodies have promoted cross-compatible specifications, including IEEE 1451 for smart transducer interfaces and ISO/IEC 30141 for IoT reference architectures, aiming to reduce fragmentation and promote plug-and-play functionality across industrial platforms.

At the data level, semantic interoperability becomes a major concern. Sensor outputs must not only conform to shared formats but also carry consistent meaning across applications and analytic modules. Ontology-driven frameworks and semantic annotation techniques are increasingly applied to enrich sensor data streams with machine-readable metadata, facilitating automated processing, integration, and reasoning. These methods enhance the discoverability and composability of sensor services while supporting advanced use cases such as federated learning, decentralized control, and adaptive system configuration.

On the application side, interaction logic must remain robust under variation in node behavior, functional roles, and domain-specific constraints. This requires flexible software architectures built on modular microservices, service-oriented messaging, and event-driven orchestration. Standard APIs and interface contracts enable the replacement or upgrading of individual components without compromising overall system integrity. Furthermore, conformance testing, certification programs, and simulation environments help validate interaction compatibility before deployment, reducing integration risk and ensuring smooth operation across the entire IIoT landscape.

Practical deployment considerations and field-level constraints

Despite significant progress in the theoretical modeling of intelligent sensor interaction, the deployment of such systems in operational industrial environments presents a range of practical challenges. Field-level conditions-such as harsh physical environments, electromagnetic interference, limited accessibility, and safety-critical constraints-impose additional demands on the robustness and adaptability of sensor network interaction models [14]. In such settings, even minor inconsistencies in communication or coordination can have outsized consequences, including system shutdowns, product defects, or compromised worker safety.

Hardware-level reliability is a fundamental concern. Sensor nodes must endure mechanical vibrations, temperature fluctuations, dust, humidity, and other stressors that can degrade performance over time. Redundancy mechanisms, including node duplication and failover routing, are often implemented to mitigate single-point vulnerabilities. However, these add complexity to the interaction model, particularly when synchronizing redundant streams or merging conflicting observations. Energy harvesting methods and ultra-low-power design patterns are also integrated into interaction logic to extend operational life without compromising functionality.

Another critical factor is deployment topology. In dense industrial spaces, signal interference and multipath propagation affect wireless communication quality, necessitating adaptive power control and dynamic channel management. Sensor placement strategies must account not only for coverage and accessibility, but also for maintainability and compliance with regulatory zoning requirements. Interaction models are thus informed by physical layout constraints, necessitating localization awareness, signal quality estimation, and fallback mechanisms in the case of signal degradation [15].

Finally, integration with legacy infrastructure remains a common barrier. Many industrial systems were not designed with IIoT in mind, relying on proprietary protocols or closed-loop control schemes. Bridging these systems with modern ISNs requires careful consideration of timing compatibility, protocol adaptation, and security hardening. Gateways and protocol bridges are often introduced to mediate between legacy systems and modern sensor clusters, but these components themselves must conform to the overall interaction logic to prevent bottlenecks or inconsistencies. Successful deployment therefore depends not only on the strength of the models but also on their ability to adapt to heterogeneous and constrained operational environments.

Conclusion

The interaction between intelligent sensor nodes in industrial Internet of things environments is shaped by a complex interplay of communication protocols, coordination strategies, and system-level constraints. As IIoT systems evolve toward greater autonomy and scalability, the underlying models of interaction must support decentralized decision-making, dynamic topology management, and consistent temporal behavior. These requirements necessitate robust, adaptive, and resource-aware designs capable of maintaining performance across diverse operational contexts.

This study has provided a comprehensive examination of structural and functional principles that guide the behavior of intelligent sensor networks in industrial settings. Through analysis of topological configurations, layered communication frameworks, synchronization mechanisms, and coordination strategies, the paper highlights key factors influencing the reliability and efficiency of distributed sensing infrastructures. Emphasis was also placed on practical considerations such as interoperability, standardization, and field deployment challenges, all of which play a critical role in the transition from prototype systems to production-grade deployments.

In light of emerging industrial demands, future research should focus on the integration of learning-based interaction policies, self-healing coordination mechanisms, and secure interoperability protocols. These developments will be essential in building intelligent sensor networks that are not only functionally effective but also resilient, context-aware, and aligned with the operational realities of next-generation industrial systems.

References

1. Gupta D., de Albuquerque V.H.C., Khanna A., Mehta P.L. Smart Sensors for Industrial Internet of Things // Springer International Publishing. 2021. Vol. 10. P. 978-3.
2. Djenouri Y., Belhadi A., Srivastava G., Houssein E.H., Lin J.C.W. Sensor data fusion for the industrial artificial intelligence of things // Expert Systems. 2022. Vol. 39. No. 5. P. e12875.
3. Smoliarchuk V. Methods and techniques for improving the efficiency of business processes in manufacturing companies // Cold Science. 2025. No. 13. P. 53-60.
4. Majid M., Habib S., Javed A.R., Rizwan M., Srivastava G., Gadekallu T.R., Lin J.C.W. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review // Sensors. 2022. Vol. 22. No. 6. P. 2087.
5. Li J., Dai J., Issakhov A., Almojil S.F., Souri A. Towards decision support systems for energy management in the smart industry and Internet of Things // Computers & Industrial Engineering. 2021. Vol. 161. P. 107671.
6. Sharma S., Verma V.K. An integrated exploration on internet of things and wireless sensor networks // Wireless Personal Communications. 2022. Vol. 124. No. 3. P. 2735-2770.
7. Jiang B., Li J., Yue G., Song H. Differential privacy for industrial internet of things: Opportunities, applications, and challenges // IEEE Internet of Things Journal. 2021. Vol. 8. No. 13. P. 10430-10451.
8. Seng K.P., Ang L.M., Ngharamike E. Artificial intelligence Internet of Things: A new paradigm of distributed sensor networks // International Journal of Distributed Sensor Networks. 2022. Vol. 18. No. 3. P. 15501477211062835.

9. Garifullin R. Application of RxJS and NgRx for reactive programming in industrial web development: methods for managing asynchronous data streams and application state // International Journal of Professional Science. 2024. No. 12-2. P. 42-47.
10. Xu H., Wu J., Pan Q., Guan X., Guizani M. A survey on digital twin for industrial internet of things: Applications, technologies and tools // IEEE Communications Surveys & Tutorials. 2023. Vol. 25. No. 4. P. 2569-2598.
11. Tharewal S., Ashfaque M.W., Banu S.S., Uma P., Hassen S.M., Shabaz M. Intrusion detection system for industrial Internet of Things based on deep reinforcement learning // Wireless Communications and Mobile Computing. 2022. Vol. 2022. No. 1. P. 9023719.
12. Ahmed S.F., Alam M.S.B., Hoque M., Lameesa A., Afrin S., Farah T., Muyeen S.M. Industrial Internet of Things enabled technologies, challenges, and future directions // Computers and Electrical Engineering. 2023. Vol. 110. P. 108847.
13. Nourildean S.W., Hassib M.D., Mohammed Y.A. Internet of things based wireless sensor network: a review // Indones. J. Electr. Eng. Comput. Sci. 2022. Vol. 27. No. 1. P. 246-261.
14. Peter O., Pradhan A., Mbohwa C. Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies // Procedia Computer Science. 2023. Vol. 217. P. 856-865.
15. Lăzăroiu G., Kliestik T., Novak A. Internet of things smart devices, industrial artificial intelligence, and real-time sensor networks in sustainable cyber-physical production systems // Journal of Self-Governance and Management Economics. 2021. Vol. 9. No. 1. P. 20-30.