

CHAPTER 2. CYBERSECURITY AND INFORMATION PROTECTION UNDER HYBRID THREATS: NATIONAL AND EUROPEAN APPROACHES

2.1. Distributed Cyber Sensors for Monitoring Threats to Ukraine's Critical Information Infrastructure

Yevhen ZHYVYLO

Alina YANKO

Tetiana FESENKO

Yuliia KALASHNIKOVA

National University "Yuri Kondratyuk Poltava Polytechnic"

Yurii KUCHMA

LLC Private Higher Education Institution "University of Modern Technologies"

The transformation of today's security environment, greatly intensified by the full-scale armed aggression of the Russian Federation against Ukraine, has moved the protection of critical information infrastructure (hereinafter, CII) from the sphere of purely local technical tasks into the category of strategic imperatives for national survival. As substantiated in the study (Zhyvylo Ye. O., Dokil V. M., 2025), the essence of cybersecurity in the national segment of cyberspace under crisis management is determined by the need to ensure the resilience of critical infrastructure in the face of hybrid threats. This confirms the strategic nature of this task for the national security of the state (Onyshchenko S. et al., 2023). Modern cyberattacks on energy, transport, water supply and electronic communications facilities have taken on the features of coordinated hybrid operations in which the destruction of physical assets precedes destructive interference with technological and information systems or takes place at the same time (Krasnobayev V., Yanko A., Hlushko A., 2023). Clear examples include the attacks on Ukraine's energy system in 2015–2016 using the BlackEnergy and Industroyer malicious software (hereinafter, malware), incidents involving industrial control systems at chemical industry facilities, and systematic campaigns using wiper malware (WhisperGate, CaddyWiper, HermeticWiper) aimed at fully destabilising the operation of state institutions. Studies of cyberattacks as a new front in warfare and

analysis of Ukraine's experience in countering Russia's cyber aggression show the need for a comprehensive approach to CII protection that combines technological, organisational and legal mechanisms (Kalashnikova Yu. V., 2025).

A separate strategic challenge that must be taken into account when designing long-term CII protection architectures is ensuring that systems can withstand future quantum attacks. In particular, integrating post-quantum cryptographic algorithms into defence communications systems and sensor networks is a relevant direction that shapes the further development of national cybersecurity (Fesenko T. M. et al., 2026). Overall, these incidents and the evolution of threats show the urgent need to use comprehensive cyber-risk management technologies to improve the cyber resilience of strategic sectors of the national economy, as systematically examined in (Onyshchenko S. et al., 2024; Yanko A. et al., 2023).

As European integration processes intensify, Ukraine has faced the need not only to harmonise its legal framework but also to fundamentally restructure its national cyber-defence architecture. This process involves implementing key European directives and regulations (Directive (EU) 2022/2555 of the European Parliament and of the Council, 2014; Directive (EU) 2022/2557 of the European Parliament and of the Council, 2022; Regulation (EU) 2024/2847 of the European Parliament and of the Council, 2024; Regulation (EU) 2025/38 of the European Parliament and of the Council, 2024). These international acts effectively form a new paradigm of cyber resilience, in which the key focus is not so much on static perimeter protection as on continuous visibility, deployment of distributed monitoring, and operation of automated cyber-intelligence exchange systems.

At the same time, an analysis of the current state of domestic research and practical work in CII cybersecurity shows a significant imbalance. Most Ukrainian research publications, dissertations and regulatory and methodological documents focus on risk-management tools (ISO/IEC 27001:2022, The NIST Cybersecurity Framework, 2024), concepts for building centralised security operations centres, and the implementation of security information and event management systems. These elements are certainly basic components of cyber defence, but they describe mainly a reactive or

highly aggregated security model that does not fully account for the specific features of operational technology (hereinafter, OT) and deterministic industrial Internet of Things networks.

As a result of this focus, the architecture of distributed cyber-monitoring sensor networks, the role of telemetry-collection agents, and the operation of cyber-intelligence systems directly at the network “edge” remain relatively understudied in Ukrainian research. At the same time, sensors, local agents and distributed subsystems for collecting primary data form the first layer of visibility for CII facilities. The lack of a thorough theoretical basis and understanding of the specific requirements for deploying them in industrial control system environments (ICS/SCADA), deterministic networks and legacy systems means that even the most modern domestic SIEM systems operate on incomplete or distorted data and may be unable to identify complex targeted attacks at the OT level in time.

The European approach established in the above-mentioned legal acts requires a shift from isolated sectoral monitoring to federated distributed sensor networks (Yanko A. S. et al., 2022) that can generate standardised telemetry in near real time. This direction is particularly relevant in the context of developing the European Cybersecurity Operations Centre and the network of national security centres of EU Member States, with which Ukraine seeks to integrate.

The purpose of this monograph section is to address this scientific and technical gap by systematising European practices in the use of distributed cyber sensors; analysing the specific features of their integration into Ukraine’s heterogeneous IT/OT CII environment; comparing commercial and open-source solutions; substantiating a three-tier architectural model of a sensor network with intelligent data processing at the edge; and developing practical recommendations for implementation in view of European legislative requirements and the challenges of martial law.

To build an integrated monitoring architecture for CII facilities, it is necessary to clearly distinguish traditional information protection tools (hereinafter, IPTs) from distributed cyber sensors. Traditional IPTs, such as firewalls and intrusion prevention systems, actively block or filter data flows based on known signatures and deterministic

rules. Cyber sensors and local agents, in contrast, are intended for the continuous collection of cyber-intelligence, telemetry and metadata. Their main task is to detect anomalies, transient threats and hidden vectors of infrastructure compromise (Yanko A. S., Makarenko O. I., 2022).

The fundamental difference between these classes of systems is that a cyber sensor is primarily a tool for passive observation and analysis, whereas an IPT enforces security policies. This difference is critical in a CII environment because actively blocking suspicious traffic in an OT segment can very likely disrupt the stability of a technological process, cause emergency equipment shutdown, or even lead to catastrophic physical consequences. Therefore, a modern CII monitoring architecture should be based on the fundamental principle “comprehensive visibility first, coordinated response next”. This approach is fully consistent with the CII risk-management methodology based on the “threats–vulnerabilities–consequences” triad, substantiated in (Zhyvylo Ye., Kuz V., 2023), which emphasises the clear priority of preventive monitoring over purely reactive measures.

In view of this principle, distributed sensors should be classified according to the level at which they interact with the infrastructure and the environment in which they operate.

1. Network-based sensors. The first category consists of network sensors that monitor without interfering with the operation of network equipment. These include passive traffic analysers (TAP/SPAN), specialised hardware devices that duplicate network traffic (Yanko A. S., Padusenko Ya. V., 2026). They are critical for OT segments because optical TAP devices provide complete galvanic and logical isolation from the monitored segment, preventing any reverse effect on the network. They are complemented by flow-telemetry sensors (NetFlow, IPFIX, sFlow), which collect aggregated metadata about network sessions. This makes it possible to detect anomalous communication patterns between ICS controllers and remote terminals, as well as promptly record unauthorised connections.

DNS sensors are used to detect the early stages of compromise. These tools analyse DNS requests and are designed to identify algorithmically generated domain

names used by botnets or command-and-control (C2) server addresses. Identifying these attack vectors at an early stage is a key element of the cyber-risk management system for CII facilities, as described in detail in (Zhyvylo Ye., 2024). In addition, because traffic encryption is widespread, TLS/SSL metadata analysis sensors are used. These modules record parameters of secure connections, including JA3/JA3S hashes, SNI fields and certificate characteristics, without decrypting the traffic itself. This makes it possible to identify malicious activity even in an encrypted environment.

2. Host-based agents and endpoints. The next level of the taxonomy consists of host sensors and agents that monitor endpoints directly. Telemetry-collection agents (eBPF, Wazuh, Osquery) are lightweight software that operates at the operating-system kernel level on engineering workstations, HMI panels and data-historian servers. In particular, the use of eBPF technology minimises computational overhead while providing full monitoring of system calls, registry modifications and process creation.

File integrity monitoring (FIM) sensors are used to protect against targeted modifications. These modules monitor critical configuration files and system directories in SCADA environments. They are highly effective in detecting unauthorised changes to the operating logic of programmable logic controllers, a characteristic attack vector in Triton/Trisis attacks. A further development of this direction is the use of application control and integrity verification mechanisms for PLC firmware.

For protection against targeted modifications, file integrity monitoring (FIM) sensors are used. These modules monitor critical configuration files and system directories in SCADA environments. They are highly effective in detecting unauthorised changes to the operating logic of programmable logic controllers, which is a characteristic vector in Triton/Trisis attacks. Endpoint Detection and Response (EDR) agents further develop this approach by combining detailed log collection with built-in behavioural analysis and machine-learning algorithms on endpoints.

3. OT/ICS protocol-specific sensors. The specific features of the CII environment require a third category, OT/ICS protocol sensors. Industrial protocol decoders play a key role. They perform deep packet inspection and can parse traffic from specific industrial protocols (Modbus TCP/RTU, DNP3, IEC 60870-5-104, IEC 61850,

PROFINET, OPC UA, EtherNet/IP, BACnet). These sensors analyse not only packet structure but also command semantics, such as attempts to change process setpoints without authorisation or to send critical equipment-control commands.

For comprehensive monitoring, these sensors are supplemented by physical-state and IT/OT-convergence sensors that monitor physical-environment parameters, including server-cabinet temperature, equipment vibration, voltage fluctuations and humidity. This makes it possible to detect complex cyber-physical attacks that leave no obvious digital traces in network traffic. Special attention is also paid to sensors on engineering workstations. They provide specialised monitoring of peripheral-device connections and the launch of engineering development environments (TIA Portal, RSLogix, EcoStruxure), reducing the risk of compromising automation firmware.

This classification shows that the main difference between a modern distributed sensor network and a conventional hierarchical SIEM architecture is the implementation of the “Edge-to-Core Analytics” concept. At Ukrainian CII facilities, communication channels between remote technological sites and the central control centre often have limited bandwidth or are unstable because they use microwave radio links, satellite communications or cellular networks. Continuous transfer of all raw traffic to a single security operations centre is therefore technically and economically impossible. As a result, modern edge cyber sensors must have sufficient computing resources to perform primary aggregation and filtering and to run intelligent models directly at the network edge. This approach sends only verified incidents and compressed threat vectors to the central core, enabling effective monitoring even when communications infrastructure is limited.

The European Union has developed a clear and consistent legal framework that effectively sets new standards for CII monitoring architectures. Successful integration of Ukraine into the European security space requires not only formal harmonisation but also the technical adaptation of these regulatory requirements. Distributed sensors are a basic element of the national cyber-intelligence system. The key legal acts and their effect on sensor-network architecture are considered below.

1. The NIS2 Directive and baseline visibility requirements. EU Directive

2022/2555 (NIS2), which significantly expanded the range of CII entities, requires in Article 21 the implementation of comprehensive cybersecurity risk-management measures, including mandatory threat monitoring and incident handling. The NIS2 requirements for continuous monitoring are implemented through distributed sensor infrastructure that operates throughout the CII cyber-risk assessment cycle, from threat identification to analysis of the consequences of compromise. This is consistent with the methodology described in (Zhyvylo Ye., 2024). To implement these requirements in practice, CII operators must deploy sensor networks that provide visibility not only into internal network traffic but also into potential supply-chain compromise vectors. This requires dynamic integration of sensors with software bill-of-materials registries to automatically identify vulnerabilities in deployed automation-system components.

2. *The CER Directive and the convergence of physical and cyber resilience.* The next step in the development of European regulation was EU Directive 2022/2557 on the resilience of critical entities. It emphasises the need for comprehensive protection against cyber and physical threats at the same time. Architecturally, this requires distributed sensors to support data convergence. Hardware and software monitoring systems must correlate events from physical security systems, including video surveillance, access-control systems and perimeter sensors, with anomalies in network telemetry. In practice, an attempt to gain unauthorised physical access to a control cabinet should automatically initiate enhanced logging and traffic mirroring, including a full PCAP network capture on the relevant switches, for subsequent digital forensic analysis. This convergence of physical and cyber security components reflects current trends in risk assessment and privacy auditing in information systems and is systematically substantiated in (Zhyvylo Ye., Shevchenko D., 2022).

3. *The Cyber Resilience Act and embedded telemetry.* The further development of the regulatory framework is associated with the implementation of EU Regulation 2024/2847 (Cyber Resilience Act), which establishes horizontal requirements for products with digital elements and obliges manufacturers to apply security-by-default principles. A key requirement of the regulation is that industrial devices include built-in mechanisms for the secure generation and transmission of security telemetry. In this

context, the future architecture of Ukraine's CII will partly be formed through the integration of agents embedded in industrial equipment. This can significantly reduce the cost of deploying third-party sensor systems and enable monitoring at the level of individual components.

4. *The Cyber Solidarity Act and standardised data exchange.* The regulatory framework is completed by EU Regulation 2024/1084 (Cyber Solidarity Act), which aims to create a common European data-exchange platform, the European SOCC. To ensure interoperability between Ukrainian systems and European partners, CII distributed sensors must normalise events and indicators of compromise in the standard STIX 2.1/TAXII 2.1 formats and provide native integration with MISP threat-sharing platforms. This provides a technical basis for automated cyber-intelligence exchange in near real time.

5. *A matrix mapping sensors to EU regulatory requirements.* To formalise and systematise these requirements, a compliance matrix has been developed. It links types of distributed cyber sensors to specific articles of European legal acts (Table 2.1).

Table 2.1

Sensor Compliance Matrix with the Requirements of EU Legal Acts

Sensor type	NIS2 Directive	CER Directive	CRA Regulation	Cyber Solidarity Act
Passive network TAP sensors	Art. 21(2)(d) – cyber-threat monitoring requirements	Art. 13(2) – technical resilience measures	Art. 13(1) – mandatory product certification	Automated IoC exchange support; integration with the EU platform Participation in European platforms
OT protocol analysers (Modbus, IEC 61850, DNP3, PROFINET)	Art. 24(2)(d) – supply-chain security	Art. 21(2)(d) – convergence of physical and cybersecurity	Art. 4(1) – security by design	
Host agents	Art. 16(1)(a) – technical security measures	Art. 13(1) – comprehensive risk assessment	Art. 4(1) – security by design	
Edge ML models (anomaly detection)	Art. 21(2)(e) – incident management	Art. 13(2) – technical resilience measures	support	

Sensor type	NIS2 Directive	CER Directive	CRA Regulation	Cyber Solidarity Act
Physical IoT sensors (temperature, pressure, vibration)	Art. 16(1)(a) – technical security measures	Art. 13(1) – comprehensive risk assessment	Art. 13(4) – embedded security telemetry	
PMU sensors (IEEE C37.118 for energy)	Art. 13(1) – Mandatory product certification		Art. 46(1) – software update mechanisms	
DNS/cyber-intelligence sensors	Art. 21(2)(d) – cyber-threat monitoring requirements		Not applicable	
Data diodes (one-way gateways)	Integration requirement	Integration requirement	Not applicable	
STIX/TAXII gateways (standardised exchange)	Integration requirement			Mandatory
MISP integration nodes (threat-sharing platforms)	Art. 21(2)(f) – business continuity			Mandatory

Source: compiled by the authors on the basis of Directive (EU) 2022/2555 (NIS2); Directive (EU) 2022/2557 (CER); Regulation (EU) 2024/2847 (Cyber Resilience Act); Regulation (EU) 2024/1084 (Cyber Solidarity Act).

The compliance matrix systematises the relationship between architectural components of distributed sensor networks and the regulatory provisions of the European legal framework for CII protection. The colour coding of the cells illustrates the degree and nature of the impact of specific types of cyber sensors on the implementation of regulatory requirements. A green indicator identifies direct regulatory compliance of a sensor class with specific articles of the directives; blue indicates an indirect or partial contribution to meeting the requirements; and yellow indicates support for the fundamental principles of cyber resilience and security by default. The absence of a visual marker in a cell means that there are no direct regulatory requirements to use the corresponding type of sensor equipment to verify the specific article.

An analysis of international and national legal acts on critical infrastructure

protection shows that their fundamental purpose is to minimise the risks of cyber threats that could disrupt the continuity of critical services, lead to loss of control over technological processes, compromise information resources or cause technological accidents.

At the same time, regulatory documents define only general risk-management principles and do not provide a unified mathematical framework for quantitatively assessing cyber risk when designing distributed cyber-monitoring sensor networks. Therefore, it is appropriate to represent risk as an integral indicator that accounts for both the probability of a threat occurring and the potential consequences of its impact on a critical infrastructure facility.

Thus, the risk of a specific cyber threat is determined by the following relationship:

$$R_i = P_i \cdot I_i, \quad (2.1)$$

where R_i is the risk of the i -th threat; P_i is the probability that the threat will occur; and I_i is the magnitude of the threat's potential impact on a critical infrastructure facility.

In practice, multiple interrelated cyber threats may exist at the same time at a CII facility. Therefore, the total risk is defined as:

$$R_{total} = \sum_{i=1}^n R_i, \quad (2.2)$$

where n is the number of current threats to the relevant critical infrastructure facility.

The proposed model makes it possible to quantify the overall level of cyber risk and rank threats by their severity, which is necessary for developing a risk-oriented architecture for a distributed sensor network.

Given the specific features of critical infrastructure facilities, an integral

criticality indicator should be used to set priorities for protecting individual information assets and technological processes:

$$\text{Criticality} = \alpha C + \beta I + \gamma A, \quad (2.3)$$

where C is the level of impact on confidentiality; I is the level of impact on integrity; A is the level of impact on availability; and α, β, γ are weighting coefficients for the significance of the respective components, subject to the condition:

$$\alpha + \beta + \gamma = 1, \quad \alpha, \beta, \gamma \in [0, 1]. \quad (2.4)$$

Unlike the classical CIA model, for most critical infrastructure facilities the most important parameter is continuity of technological processes. This makes it appropriate to assign a higher weighting coefficient to availability:

$$\gamma > \alpha, \quad \gamma > \beta. \quad (2.5)$$

For energy, transport and water-supply enterprises, the following distribution of weighting coefficients may be used:

$$\alpha = 0.2, \quad \beta = 0.3, \quad \gamma = 0.5 \quad (2.6)$$

In this case, the integral criticality indicator takes the following form:

$$\text{Criticality} = 0.2C + 0.3I + 0.5A. \quad (2.7)$$

The proposed indicator serves as an analytical tool for ranking CII facilities by criticality and setting priorities for cyber-sensor deployment. The resulting values make it possible to optimise the distributed-computing architecture by placing edge and fog nodes rationally. In addition, this tool supports the selection of relevant cyber-incident response scenarios, providing a basis for a comprehensive risk-oriented cyber-defence strategy.

Thus, the proposed formal model enables a shift from qualitative analysis of

regulatory requirements to quantitative risk assessment. It provides a methodological basis for designing distributed cyber-monitoring sensor networks for critical infrastructure facilities using the risk-oriented approach required by NIS2, ISO/IEC 27005, IEC 62443 and Ukrainian national cybersecurity legislation.

The main methodological and engineering problem in designing sensor networks for domestic CII facilities is that classical IT solutions cannot be directly extrapolated to OT environments. Industrial automation and control systems of the ICS/SCADA class have specific architectural and functional features that significantly limit the use of standard monitoring tools. Their key characteristics include strict determinism of operating processes, a long service life for legacy equipment (20 to 30 years), a lack of built-in cryptographic protection inherited from earlier designs, limited computing capabilities of industrial controllers, and zero tolerance for network delays. For these reasons, sensor-network architecture must be adapted to the specific features of each critical sector (Yanko A. S., Vyhivskyi R. A., 2022).

We will consider sensor use, starting with the energy sector, which is the most critical and technologically complex. Main and distribution power-grid facilities, including 330/750 kV substations and dispatch centres, use specific protocols such as IEC 61850 (GOOSE, SV, MMS), DNP3 and IEC 60870-5-104. Standard IT sensors cannot correctly parse the structure and semantics of these packets. An effective threat-detection tool is the deployment of specialised OT-IDS sensors connected to the network through hardware optical traffic splitters, which ensures non-invasive monitoring. Particular attention in the energy sector should be paid to monitoring synchrophasor measurements, which transmit data at a high rate of up to 120 frames per second using the IEEE C37.118 protocol. This requires edge sensors to provide microsecond-accurate timestamps and minimal data-processing latency.

While the energy sector is characterised by high data-transmission speeds and complex real-time protocols, water-supply and wastewater systems face a different challenge, the geographical dispersion of facilities. These systems use low-speed communication channels (GPRS/4G/LoRa) to transmit Modbus RTU/TCP traffic, which has no built-in authentication mechanisms. The optimal approach is to deploy

distributed sensor modules directly at remote telemetry terminals, with deep contextual analysis of industrial commands. Since active blocking of suspicious traffic by a sensor may cause an emergency shutdown of pumping equipment, a passive protection model is used. The sensor creates a cryptographically signed event log and transmits it through secure tunnels (IPsec/WireGuard) to a central aggregation node. A key task is to record anomalous changes in process setpoints, such as pressure or reservoir fill level, which may indicate an attempt to cause physical damage to the infrastructure.

Transport infrastructure is another critical sector that requires specific monitoring approaches. Rail transport (JSC Ukrzaliznytsia), aviation dispatch systems and seaports use highly specialised, often proprietary control protocols such as EBICAB 900, ETCS (European Train Control System) and AIS (Automatic Identification System). Cyber sensors for these systems must undergo strict industry certification and provide non-invasive monitoring of specialised engineering data buses. Integrating these sensors into the general security system requires close interaction with existing traffic-dispatch and navigation systems without disrupting their deterministic operating cycles.

Unlike traditional industrial systems, the telecommunications sector and related financial platforms are based on highly dynamic cloud architectures. Electronic communications network operators use virtualised network functions (NFV), software-defined networks (SDN) and cloud orchestration systems (Kubernetes, OpenStack). Sensor infrastructure in this sector must monitor not only network flows but also configuration files in virtualisation and containerisation environments, as these are primary targets of modern APT groups. The cybersecurity features of electronic communications systems examined in (Zhyvylo Ye. O., 2024) highlight the need for specialised sensors to monitor transaction platforms. Integrating such tools into the overall CII distributed-monitoring architecture is especially relevant for the financial sector as a key element of the state's critical infrastructure, where delays in data processing are unacceptable.

Regardless of sector, a common challenge for all CII sectors is the mistaken belief that Ukraine's OT networks are completely isolated from external cyberspace.

In practice, hidden communication channels exist through engineering USB drives, vendor remote-maintenance modems, or connections to IT segments for business reporting. To securely transfer telemetry from cyber sensors in isolated OT zones to a corporate SOC or cloud analytics systems, one-way hardware data gateways, known as data diodes, must be used. At the physical level, for example, through an optical transmitter with no return receiver, these devices make it impossible to penetrate or affect the technological process in the reverse direction through the threat-monitoring channel. They thus ensure fundamental protection of critical production processes.

To substantiate architectural decisions and select an optimal technology stack, it is necessary to review systematically the OT-monitoring platforms currently available on the market. This analysis covers both commercial solutions from leading global vendors and open-source platforms that can be adapted to the specific needs of Ukraine's CII.

1. Commercial OT platforms. Nozomi Networks (the Guardian platform) is one of the leading systems in the OT/ICS security segment. It uses high-performance passive sensors for automatic asset inventory and behavioural anomaly detection based on machine-learning algorithms. The platform supports more than 100 industrial protocols and provides native integration with external SIEM systems through STIX/TAXII standards and the Apache Kafka protocol.

Claroty (the Continuous Threat Detection platform) offers a sensor architecture focused on real-time anomaly detection. Its key feature is a powerful analytical toolkit for identifying vulnerabilities in legacy equipment without active scanning, as well as extensive support for specific protocols such as IEC 61850 and DNP3.

Dragos (the Dragos Worldview platform) is positioned as a specialised system for identifying attackers' industrial tactics, techniques and procedures. The platform is distinguished by unique sector-specific scenarios developed specifically for the energy and oil and gas sectors.

Comprehensive ecosystems are offered by Fortinet (FortiGate-OT and FortiSIEM) and Palo Alto Networks (IoT Security and Cortex XDR). These solutions combine next-generation firewalls, security-event management systems and network-

access control tools. In particular, Palo Alto’s solution focuses on identifying IoT/OT devices and analysing their behaviour, followed by integration with Cortex XDR for extended threat response. Another development direction in commercial solutions is security operations centre automation. Integrated orchestration platforms such as Cisco SecureX can significantly reduce incident-response time and unify distributed sensor operations in complex heterogeneous networks (Fesenko T., Kalashnikova Yu., 2025).

2. *Open-source platforms.* Unlike commercial ecosystems, open-source solutions offer high flexibility and no dependency on a specific vendor.

Zeek (formerly Bro) is a powerful network analyser specialising in metadata collection and the creation of structured event logs. With support for extensions for industrial protocols (Modbus, DNP3), it serves as the technological foundation for many commercial OT solutions.

Suricata is a high-performance network analyser that supports IDS/IPS/NSM functions (Yanko A. S., Makarenko O. I., 2022). Its flexible rule system makes it highly effective in detecting attacks on OT protocols, and it can be used for both network and host monitoring.

Wazuh is an open-source XDR/SIEM platform that supports both host agents and network sensors. It has specialised OT-security modules and integrates with OpenSearch for scalable data storage and analysis.

OpenDNP3 should also be noted. It is an open-source implementation of the DNP3 protocol and can serve as a basis for building custom OT sensors. Snort is a classic network IPS/IDS that, although less performant than Suricata, remains in demand because of its large community support base. Security Onion completes this list. It is a comprehensive Linux distribution that combines Zeek, Suricata, Wazuh and Elastic Stack in a single integrated security-monitoring platform (Yanko A. et al., 2024).

3. *Comparative analysis of technology solutions.* To formalise the results of the review, the key characteristics of the platforms considered are summarised in a comparative table (Table 2.2).

Table 2.2.

Comparative Analysis of Commercial and Open-Source Solutions for OT Monitoring

Platform	OT protocols	Edge	SIEM/MISP	STIX/TAXII	IEC 62443	Cost	Adaptation
Nozomi	Full support	Full support	Full support	Full support	Full support	USD 500,000–1 million	Partial support
Claroty	Full support	Full support		Full support	Full support		Partial support
Dragos	Full support	Full support		Full support	Full support		Partial support
Zeek	Partial support	Partial support		Partial support	Absent	Free	Full support
Suricata	Partial support						Full support
Wazuh	Partial support	Full support		Partial support			Full support
Sec. Onion	Full support	Partial support		Full support		USD 50,000–100,000	Full support

Source: compiled by the authors on the basis of official documentation from Nozomi Networks; Claroty; Dragos; Zeek Project; Open Information Security Foundation (Suricata); Wazuh Inc.; Security Onion Solutions.

The comparative analysis shows that commercial platforms (Nozomi Networks, Claroty, Dragos) provide comprehensive support for OT protocols, have IEC 62443 certification and extensive edge-analytics capabilities, but are characterised by high licensing costs and dependence on foreign suppliers. Open-source solutions (Zeek, Suricata, Wazuh, Security Onion), in contrast, offer high flexibility for adaptation, no vendor lock-in and minimal software costs, but require significant investment in integration and configuration and qualified engineering staff.

In view of this, a hybrid approach is the optimal strategy for Ukraine's CII. It involves deploying commercial solutions at facilities of national importance, including nuclear and hydroelectric power plants and main power grids, and implementing adapted open-source platforms at municipally and locally owned facilities. A mandatory condition for this strategy is the unification of data-exchange formats at higher aggregation levels, which leads directly to the need to design a unified architectural model.

Summarising the analysis of European practices, the specific features of Ukraine's CII and the review of available technology solutions, this section proposes

a three-tier architecture for a distributed sensor network. The proposed model provides an optimal balance between monitoring depth, computing performance and cyber-resilience requirements.

The current challenges of ensuring the cyber resilience of Ukraine's CII facilities require a shift from centralised monitoring models to distributed architectures with intelligent data processing at the network edge. Traditional approaches based exclusively on centralised SIEM systems and SOC centres are not effective enough when communication bandwidth is limited at remote energy, water-supply and transport facilities, and when OT must be physically isolated from corporate IT networks.

The Edge-Fog-Core architectural paradigm offers a hierarchical model for distributed processing of cyber-monitoring data. It provides an optimal balance between local autonomy at CII facilities and centralised security management at the national level.

To enable quantitative assessment of the proposed architecture's effectiveness, the critical-infrastructure distributed sensor network can be formalised as a directed graph:

$$G = (V, E) , \quad (2.8)$$

where $V = \{v_1, v_2, \dots, v_n\}$ is the set of network nodes and $E = \{e_1, e_2, \dots, e_m\}$ is the set of information links between nodes.

Given the hierarchical structure of the proposed architecture, the set of nodes is defined as:

$$V = V_{Edge} \cup V_{Fog} \cup V_{Core} , \quad (2.9)$$

where V_{Edge} is the set of edge sensor nodes; V_{Fog} is the set of aggregation and local-analysis nodes; and V_{Core} is the set of central nodes at the national and international levels.

The following condition is satisfied:

$$V_{Edge} \cap V_{Fog} \cap V_{Core} = \emptyset, \quad (2.10)$$

which ensures the logical and functional separation of the architectural tiers.

The telemetry-transfer process is described by the routing function:

$$f(v_i) = \begin{cases} Fog_j, & v_i \in V_{Edge} , \\ Core_k, & v_i \in V_{Fog} . \end{cases} \quad (2.11)$$

Thus, each node at a lower tier has a uniquely defined aggregation node at the next higher tier.

The data-flow intensity for an individual node is defined as:

$$L_i = \sum_{k=1}^N \lambda_k, \quad (2.12)$$

where L_i is the total node load and λ_k is the flow intensity from an individual sensor.

The total delay in information transmission and processing in the system is defined by the expression:

$$D_{total} = D_{Edge} + D_{Fog} + D_{Core} , \quad (2.13)$$

where D_{Edge} is the local-processing delay; D_{Fog} is the aggregation delay; and D_{Core} is the central-analysis delay.

The proposed formalisation makes it possible to model the scalability, fault tolerance and performance of the architecture for different numbers of critical infrastructure facilities.

A fundamental basis of this architecture is local intelligent processing, which involves applying machine-learning algorithms directly on edge-level devices. This

makes it possible to detect anomalies in real time without transferring large volumes of raw data, which is critical for deterministic industrial networks with limited latency.

Another key principle is the physical isolation of operational-technology and information-technology environments, achieved through hardware one-way gateways. This approach ensures that technological processes cannot be compromised through monitoring channels while providing the necessary visibility into the state of OT systems. Cyber-physical data convergence also plays an important role. It is implemented by integrating readings from physical sensors with network telemetry and makes it possible to detect complex cyber-physical attacks that cannot be identified by analysing digital artefacts alone.

In addition, standardised European integration is based on STIX/TAXII 2.1 formats and integration with MISP platforms. This provides semantic interoperability with European cybersecurity infrastructure in line with NIS2, CER and the Cyber Solidarity Act. Federated model training completes this set of principles. It is a decentralised approach to improving machine-learning algorithms. It enables threat-detection quality to be improved collectively without transferring confidential data between critical infrastructure facilities, thereby preserving operators' privacy and trade secrets. Particular attention should be paid to federated GNN-XAI models for predicting account compromise in a Zero Trust environment. These models can detect threats at an early stage without centralising sensitive data, as substantiated in (Fesenko T. M., Kalashnikova Yu. V., 2025).

The proposed architecture accounts for the specific features of Ukraine's critical infrastructure, including the large share of legacy equipment with a service life of 20–30 years, limited resources for upgrading municipal CII facilities, and the need to operate under martial law and hybrid cyberattacks.

Figure 2.1 presents a three-tier architecture of a distributed sensor network for comprehensive cyber-threat monitoring at Ukraine's CII facilities.

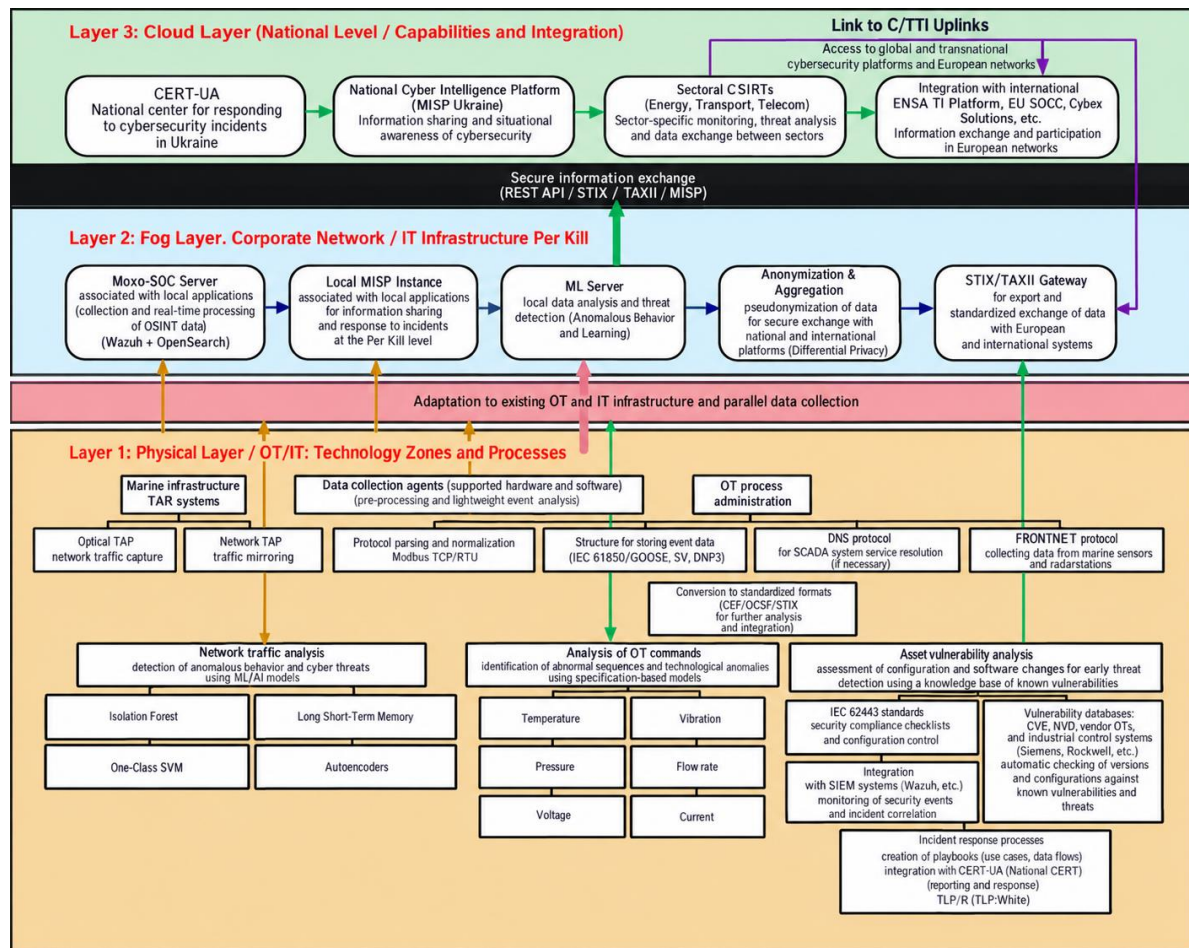


Figure 2.1. General Edge-Fog-Core architecture of a distributed sensor network for Ukraine's CII.

Source: authors' design based on ETSI Multi-access Edge Computing (MEC), OpenFog Reference Architecture (2017), Directive (EU) 2022/2555 (NIS2), and ENISA recommendations on NIS2 implementation.

The Edge tier (Tier 1 zone) is located directly in the operational environment of technological processes. It includes passive optical TAP sensors for duplicating network traffic; industrial protocol analysers (Modbus, IEC 61850, DNP3, PROFINET); eBPF-based host agents that collect telemetry at the operating-system kernel level on HMI stations and engineering workstations; lightweight machine-learning models (Isolation Forest, LSTM) for local anomaly detection; physical IoT sensors that monitor technological-environment parameters (temperature, pressure, vibration); and PMU sensors (IEEE C37.118) for high-precision synchrophasor measurements in power systems.

A Data Diode (the red-strip zone) provides physical one-way isolation between the OT and IT zones. It makes reverse data transmission impossible and protects

technological processes from compromise through monitoring channels. The Fog tier (Tier 2 zone) aggregates and preprocesses data at the level of an individual CII facility. A Micro-SOC server based on Wazuh and OpenSearch provides centralised collection of security events; a local MISP instance correlates them with global threats; an ML server with autoencoders and federated-learning mechanisms performs in-depth analysis to detect complex multi-stage attacks; an anonymisation and aggregation module based on differential privacy prepares data for secure transmission; and a STIX/TAXII gateway transforms information into standard formats for exchange with national and European systems.

The Core tier (Tier 3 zone) represents national and European cybersecurity infrastructure. CERT-UA coordinates responses to cyber incidents at the national scale; the national cyber-intelligence platform (MISP Ukraine) aggregates and correlates threats from different CII sectors; sectoral CSIRTs (energy, transport, telecommunications) provide specialised monitoring of sectoral facilities; and integration with European infrastructure (ENISA TI Platform, EU SOCC, Cyber Solidarity Act) provides access to current cyber intelligence and international mutual-assistance mechanisms.

The data flows are shown by coloured arrows. Orange arrows show the upward telemetry flow from Edge sensors through the Data Diode to the Fog tier. The green arrow marks the secure channel (TLS 1.3/mTLS/IPsec/WireGuard) for transferring aggregated data to the national tier. The purple arrow shows the reverse flow of updates to indicators of compromise and tactics, techniques and procedures from European partners, used to improve local threat-detection systems. Overall, the proposed architecture provides multilayer protection and local autonomy for CII facilities while preserving centralised visibility of threats at the national level. It also fully complies with European cybersecurity legislation for critical infrastructure.

Applying machine-learning algorithms directly at the Edge sensor level addresses the detection of zero-day attacks and anomalous states without placing a significant load on the network. The following mathematical models are substantiated for deployment on CII edge nodes:

Isolation Forest is an asymmetric clustering algorithm characterised by low computational complexity. It is suitable for Edge devices with limited CPU resources because it effectively detects anomalies in multidimensional network-traffic metadata vectors, such as packets per second and packet-length distribution.

Autoencoders are deep-learning models trained only on data from stable technological processes. During operation, anomalous traffic or destructive commands cause a sharp increase in reconstruction error, which serves as an incident trigger.

One-Class Support Vector Machine is a classical method for constructing an optimal separating hyperplane for deterministic data samples. It is suitable for use on local engineering workstations to monitor the stability of command sequences.

Long Short-Term Memory (LSTM) networks are recurrent neural networks designed to analyse time series. They achieve high accuracy in detecting deviations in cyclic industrial processes, for example, by assessing the regularity of GOOSE message transmission in IEC 61850 networks.

Specialised, lightweight and optimised frameworks, including TensorFlow Lite, ONNX Runtime and scikit-learn libraries adapted for POSIX-compatible industrial real-time operating systems, are used to implement these models on Edge sensors. Detecting hidden threats is an important aspect of securing the ML models themselves on edge devices. Stochastic-spectral methods for detecting such threats in neural networks, developed in (Zhyvylo Ye. et al., 2026), can be adapted to ensure the integrity of Edge models that process signals and telemetry.

Ukraine's implementation of European cybersecurity directives (NIS2, CER, Cyber Solidarity Act) requires a reliable architecture for integrating the national cyber-threat monitoring system with European cybersecurity infrastructure. This task is critical because threat information must be exchanged promptly, responses to cross-border cyber incidents must be coordinated, and Ukraine must participate in European mutual-assistance mechanisms.

Figure 2.2 presents the organisational and technical interaction between the national and European segments, implemented through a specialised integration gateway.

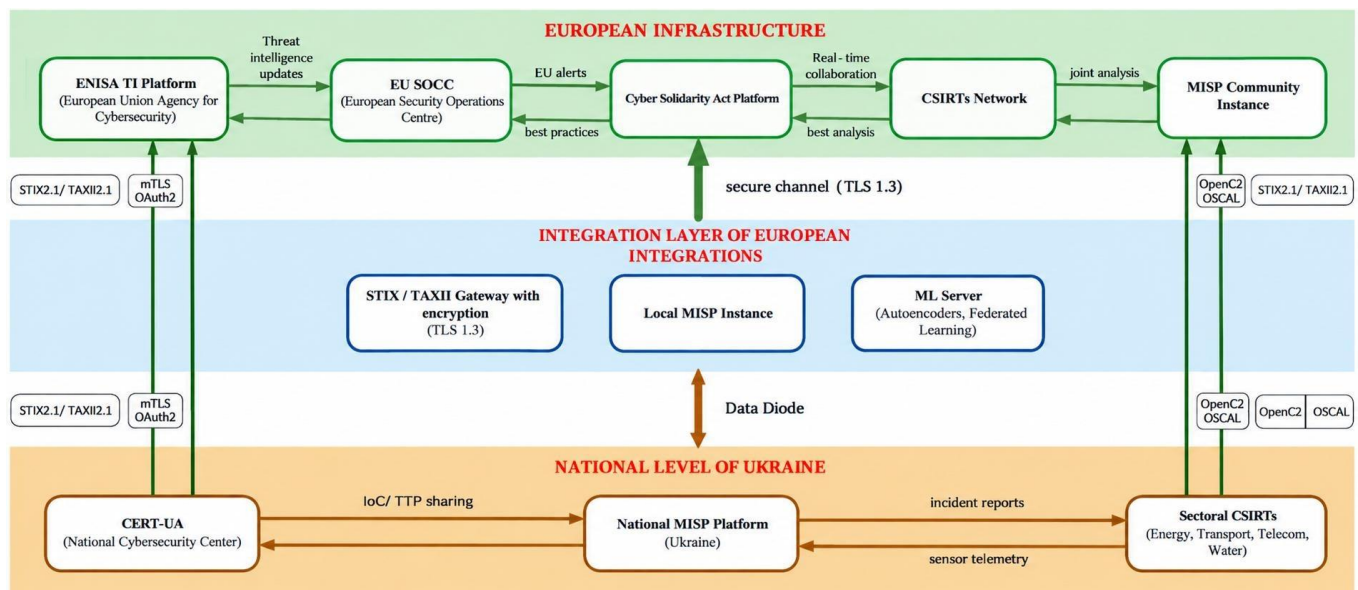


Figure 2.2. Architecture for integrating Ukraine's national sensor network with European cybersecurity infrastructure.

Source: authors' design based on Directive (EU) 2022/2555 (NIS2), Regulation (EU) 2024/1084 (Cyber Solidarity Act), ENISA recommendations on NIS2 implementation, MISP Project Documentation and OASIS STIX™ 2.1/TAXII™ 2.1 specifications.

The national tier of Ukraine (orange zone) includes CERT-UA (the National Cybersecurity Centre), which coordinates responses to cyber incidents and exchanges indicators of compromise (IoC/TTP sharing); the national MISP platform, which aggregates and correlates cyber-intelligence data; and sectoral incident-response centres (Sectoral CSIRTs) in the energy, transport, telecommunications and water-supply sectors, which transmit sensor telemetry and incident reports.

The European integration gateway (blue zone) provides technical integration with European infrastructure through three main components: an encrypted STIX/TAXII gateway (TLS 1.3) that converts data into standard exchange formats; an API integration layer that provides a unified programming interface for system interaction; and a threat-intelligence correlation engine that performs intelligent analysis and detects complex threats. The European infrastructure (green zone) includes the ENISA cyber-intelligence platform (ENISA TI Platform), which

aggregates threats from all Member States; the European Cybersecurity Operations Centre (EU SOCC), which coordinates responses to cross-border incidents; the Cyber Solidarity Act platform, which provides mutual-assistance mechanisms; the network of national CSIRTs of the Member States, for cooperation and exchange of experience; and the community of MISP instances, for decentralised threat sharing.

Data flows between the tiers include threat-intelligence updates from European infrastructure to the national tier; EU alerts about large-scale threats; shared practices and analysis; real-time collaboration; incident reports and sensor telemetry from the national tier to European infrastructure; and IoC/TTP sharing. The security protocols shown in the diagram include STIX 2.1/TAXII 2.1 for standardised cyber-intelligence exchange; mTLS and OAuth2 for authentication and authorisation; OpenC2 for command and control; OSCAL for assessing security controls; TLS 1.3 secure channels for data transmission; and hardware one-way gateways (Data Diodes) for physical isolation of critical segments. The proposed architecture complies with European cybersecurity legislation, ensures prompt exchange of threat information and enables Ukraine to integrate effectively into the European cybersecurity space.

The practical value of the proposed architecture can be demonstrated through a sensor-network deployment at a water-supply critical infrastructure facility in a medium-sized Ukrainian city with a population of 100,000-200,000. This sector was selected because it is critical to the population's daily life, its infrastructure is widely distributed, and it has specific cyber-physical risks associated with possible impacts on the physical parameters of water quality and the integrity of water-supply systems.

The typical structure of a water-supply and wastewater utility in a medium-sized Ukrainian city (Figure 2.3) includes a central dispatch service equipped with SCADA servers, HMI stations and engineering workstations for controlling technological processes. The water-intake infrastructure includes two or three first-lift pumping stations located 10–30 kilometres from the city centre, which supply water from underground or surface sources. The water-treatment system includes filtration stations and chlorination facilities, where water is prepared to drinking-water standards. The distribution network consists of ten to fifteen second-lift pumping stations in different

city districts and five to ten clean-water reservoirs equipped with level and pressure sensors. The wastewater system includes fifteen to twenty sewage pumping stations and a centralised treatment plant.

The total number of programmable logic controllers and remote terminal units is 50-80; there are 20-30 network switches and 5-10 servers. The hybrid communications-network architecture combines dedicated fibre-optic lines for reliable data transmission at some facilities with 4G/LTE cellular modems at others, where laying cable is economically impractical or difficult. This diversity of communication channels and their differing levels of security create additional cybersecurity challenges.

The sensor network is designed in accordance with the three-tier Edge-Fog-Core architecture, adapted to the specific features of a distributed water-supply infrastructure. At the Edge tier, each remote facility is equipped with a passive TAP sensor installed on an OT-zone switch to collect and analyse Modbus TCP traffic, the main communication protocol between RTU controllers and the central control system.

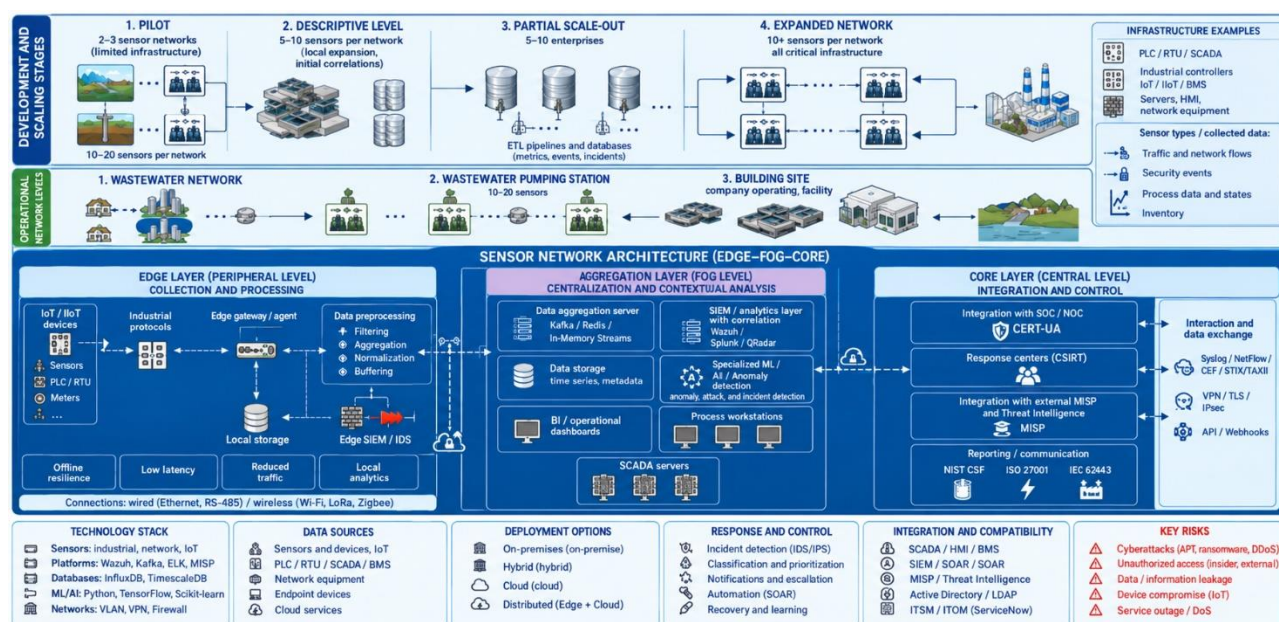


Figure 2.3. Deployment architecture of a distributed sensor network at a water-supply facility in a medium-sized city, with critical monitoring points marked.

Source: authors' design based on IEC 62443, NIST SP 800-82 Rev. 3, ENISA (2024) and CISA recommendations on cybersecurity for water-supply systems.

For local data processing, lightweight Edge analysers are deployed on Raspberry

Pi 4 single-board computers or industrial PCs (IPCs).

They run Zeek software for deep inspection of network traffic, Suricata for signature-based anomaly detection, and an Isolation Forest ML model for real-time anomaly detection without transferring large volumes of raw data to the central system. A critically important component is the installation of hardware one-way gateways (Data Diodes) to physically isolate the OT environment from IT networks while still allowing telemetry to be exported for monitoring.

At the aggregation tier (Fog), deployed in the central dispatch centre, a data-aggregation server (Micro-SOC) runs Wazuh Manager for centralised collection and correlation of security events and OpenSearch for log storage and indexing. A local MISP instance correlates local events with the global cyber-threat database, enriches data with context and generates structured indicators of compromise. A separate machine-learning server implements Long Short-Term Memory (LSTM) models to analyse time series of physical parameters (pressure, water level and flow rate). This makes it possible to detect complex cyber-physical attacks that appear as deviations of physical parameters from normal values. At the national tier (Core), integration with CERT-UA is provided through standard STIX/TAXII interfaces for automated threat-information exchange. Indicators of compromise are also published on the national MISP platform to warn other critical infrastructure operators about detected threats.

Critical monitoring points are identified by analysing the network architecture, identifying critical assets and assessing potential attack vectors. The first monitoring point is the boundary between OT and IT environments (DMZ), where a TAP sensor is installed together with a hardware Data Diode to monitor all traffic crossing this critical boundary. This placement makes it possible to detect attempts at unauthorised access from the corporate network to the technological network and to monitor legitimate data-transfer channels.

Engineering workstations running controller development and configuration environments (TIA Portal, RSLogix, EcoStruxure) are equipped with Wazuh Agent host agents to monitor the launch of engineering software, record connections to PLCs and monitor changes to control programs. This makes it possible to detect unauthorised

modifications to controller logic that could destabilise a technological process. For an additional layer of protection for privileged access to control systems, it is appropriate to use architectural and cryptographic models with intelligent access adaptation (Yanko A. S., Hlushko A. D., 2026). These combine AES symmetric encryption with machine-learning methods to build behavioural profiles of operators. This approach can reduce the probability of unauthorised use of privileges and adapt access levels in real time (Fesenko T. M. et al., 2026).

Each remote RTU controller is equipped with a passive TAP sensor and an Edge analyser for local monitoring of Modbus TCP and DNP3 traffic, detection of anomalous control commands and deviations in communication-session frequency. Particular attention is paid to chlorination stations, which are additionally equipped with physical-parameter sensors for chlorine concentration, pH and oxidation-reduction potential to detect cyber-physical attacks aimed at changing the chemical composition of water. Correlating cyber events, such as a change in dosing setpoints, with physical parameters makes it possible to detect and localise incidents promptly when they could threaten the life and health of the population.

The estimated cost of deploying a sensor network based on a hybrid approach (open-source software combined with industrial equipment) is approximately USD 180,000. Capital costs include the purchase and installation of Edge sensors (50 units $\times$ USD 1,500), totalling USD 75,000, including hardware components (Raspberry Pi 4 or industrial IPCs), network TAP adapters and peripheral equipment. Hardware one-way Data Diode gateways (10 units $\times$ USD 5,000) cost USD 50,000. This is a critical investment in the physical isolation of the OT environment. Deploying a Fog server with Wazuh and OpenSearch is estimated at USD 30,000, including server hardware, data-storage systems and backup. Commissioning, ML-model configuration, integration with existing systems and staff training cost USD 25,000.

The total project implementation period is estimated at 4-6 months. It includes a preliminary infrastructure audit and detailed project design (1 month); equipment and software procurement (1-2 months); physical installation of sensors and communications infrastructure (1-2 months); configuration of software components

and ML models (1 month); and testing and commissioning (1 month). This period is due to the need to obtain regulatory approvals, the difficulty of integrating with existing technological systems without stopping the process, and the need to train personnel to use the new monitoring systems.

Deploying a distributed sensor network significantly improves the cybersecurity of a critical infrastructure facility across several key indicators. In terms of visibility, it achieves 100% coverage of OT traffic and enables detection of all connections between RTU controllers and the SCADA system, including semantic analysis of industrial protocols at the application level. This removes the blind spots found in traditional monitoring approaches and enables a complete, real-time inventory of OT-environment assets.

Threat-detection time is reduced from hours or days, as is typical for manual log analysis or periodic audits, to seconds or minutes for critical anomalies. This is achieved by applying ML models at the Edge tier and automated event correlation at the Fog tier. It makes it possible to respond to incidents promptly before they cause significant disruption to the technological process or physical damage to equipment.

In terms of integration, automated exchange of indicators of compromise with CERT-UA and European partners is provided through standard STIX/TAXII interfaces. This improves overall situational awareness of threats and enables current cyber intelligence to be received from national and international partners. It meets the requirements of Article 21 of the NIS2 Directive on risk-management measures and Article 23 on incident reporting, thereby ensuring compliance with European legal requirements for cybersecurity of critical infrastructure. It should be emphasised that the results of integrating a distributed sensor network are consistent with cyber-risk management approaches aimed at ensuring the security of the national economic system. This relationship is substantiated in (Onyshchenko S. V. et al., 2024), particularly with regard to minimising operational risks and improving critical-infrastructure resilience.

In Ukraine, the transition from centralised SIEM systems to distributed sensor networks faces a number of specific technical, organisational, regulatory and economic

challenges that require comprehensive solutions at the state and departmental levels.

Technical challenges and dependence on foreign equipment. Most industrial sensors and hardware data diodes are manufactured in EU and US countries. Under martial law, this creates a risk of logistics delays and significant financial dependence. One way to address this challenge is to encourage the development of domestic hardware and software systems based on open-source software (Zeek, Suricata, Wazuh), develop domestic printed circuit boards and involve national laboratories in device certification under IEC 62443.

Regulatory barriers and data protection. Deep packet analysis at CII facilities may conflict with current legislation on the protection of trade secrets and restricted-access information. To address this issue, the State Service of Special Communications and Information Protection of Ukraine should develop new regulations and security profiles that would permit the use of differential privacy and homomorphic encryption when aggregating telemetry in Fog zones.

Staff shortages and operational resilience. Deploying thousands of distributed sensors requires highly qualified staff both at individual CII facilities and at sectoral CSIRTs. Addressing this shortage requires the integration of relevant specialised modules into the curricula of specialised higher education institutions, as well as the creation, under CERT-UA, of a national repository of industrial-threat signatures to provide prompt support to local engineers. These measures are consistent with current research and methodological recommendations on developing professional cybersecurity competencies during the digital transformation of the state (Zhyvylo Ye., 2023). They also take into account the need for joint training of defence forces personnel to perform cyber-defence tasks as part of total defence (Zhyvylo Ye., Zhyvylo I., 2021), which involves directly integrating higher-education programmes with the practical needs of CII operators.

Project funding. Most municipal enterprises cannot finance such systems on their own. This part can be addressed by actively attracting international technical assistance and CII-recovery grants from the World Bank and European funds, making the deployment of cybersecurity sensor systems a mandatory condition for allocating

funds to modernise facilities.

The paradigm for protecting Ukraine's CII is undergoing a fundamental transformation. Moving away from the outdated static model based exclusively on perimeter protection and centralised analysis (SIEM/SOC) in favour of a distributed cyber-sensor architecture is not merely a technical improvement but a strategic condition for ensuring national security and the state's cyber resilience.

The study confirms that distributed cyber sensors and edge-level agents form the initial visibility layer for heterogeneous infrastructure environments. Without this foundation operating properly, higher-level analytical systems (SIEM, SOC) lose effectiveness because their input data are incomplete and fragmented. European legal acts (NIS2, CER, CRA, Cyber Solidarity Act) clearly define the development directions. Sensor systems must be intelligent, native to OT environments and fully interoperable internationally through STIX/TAXII and MISP standards.

The proposed three-tier Edge–Fog–Core architecture, confirmed by a practical case study of a municipal water utility, demonstrates that a highly reliable cyber-monitoring system can be built even when legacy equipment and limited financial resources are used. Further research and practical development in this area should focus on creating domestic hardware and software tools for passive analysis of industrial networks, developing national profiles for cyber-intelligence data exchange, modernising specialised higher education, and fully integrating Ukraine's cybersecurity environment into a unified system of European security operations centres.

REFERENCES FOR SUBSECTION 2.1

1. Zhyvylo Ye. O., Dokil V. M. The Experience of Israel and the Republic of Korea in State Support Mechanisms and Cybersecurity System Organization. *National Interests of Ukraine*. 2025. No. 5 (10). P. 120–139. DOI: [https://doi.org/10.52058/3041-1793-2025-5\(10\)-120-139](https://doi.org/10.52058/3041-1793-2025-5(10)-120-139).
2. The Mechanism of Information Security of the National Economy in

Cyberspace / S. Onyshchenko, A. Yanko, A. Hlushko, O. Maslii, V. Skryl. Proceedings of the 4th International Conference on Building Innovations. ICBI 2022 / ed. by V. Onyshchenko, G. Mammadova, S. Sivitska, A. Gasimov. Cham : Springer, 2023. Vol. 299. P. 791–803. DOI: https://doi.org/10.1007/978-3-031-17385-1_67.

3. Krasnobayev V., Yanko A., Hlushko A. Information Security of the National Economy Based on an Effective Data Control Method. *Journal of International Commerce, Economics and Policy*. 2023. Vol. 14, No. 3. Article 2350021. DOI: <https://doi.org/10.1142/S1793993323500217>.

4. Kalashnikova Yu. V. Cyberattacks as a New Front of War: Ukraine's Experience in Countering Russian Cyber Aggression. Abstracts of the 77th Scientific Conference of Professors, Lecturers, Researchers, Postgraduate Students, and Students of the University, Poltava, May 16–22, 2025. Poltava : National University “Yuri Kondratyuk Poltava Polytechnic”, 2025. P. 524–526. URL: <https://reposit.nupp.edu.ua/handle/PolNTU/19282> (accessed: July 2, 2026).

5. Architectural and Cryptographic Model for Managing Special-User Systems with Intelligent Access Adaptation / T. M. Fesenko, M. O. Plakhtii, E. Yu. Rubin, Yu. V. Kalashnikova. *Modern Information Technologies in the Sphere of Security and Defence*. 2026. Vol. 55, No. 1. P. 84–99. DOI: <https://doi.org/10.33099/2311-7249/2026-55-1-84-99>.

6. Cyber Risk Management Technology to Strengthen the Information Security of the National Economy / S. Onyshchenko, Ye. Zhyvylo, A. Hlushko, S. Bilko. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2024. No. 5. P. 136–142. DOI: <https://doi.org/10.33271/nvngu/2024-5/136>.

7. Economic Cybersecurity of Business in Ukraine: Strategic Directions and Implementation Mechanism / A. Yanko, A. Hlushko, S. Onyshchenko, O. Maslii. *Economic and Cyber Security*. Kharkiv : PC TECHNOLOGY CENTER, 2023. P. 30–58. DOI: <https://doi.org/10.15587/978-617-7319-98-5.CH2>.

8. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union, Amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972,

and Repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union*. 2022. L 333. P. 80–152. URL: <http://data.europa.eu/eli/dir/2022/2555/oj> (accessed: July 19, 2026).

9. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC (CER Directive). *Official Journal of the European Union*. 2022. L 333. P. 164–198. URL: <http://data.europa.eu/eli/dir/2022/2557/oj> (accessed: July 19, 2026).

10. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No. 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). *Official Journal of the European Union*. 2024. L 2024/2847. 20 November 2024. URL: <http://data.europa.eu/eli/reg/2024/2847/oj> (accessed: July 19, 2026).

11. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 Laying Down Measures to Strengthen Solidarity and Capacities in the Union to Detect, Prepare for and Respond to Cyber Threats and Incidents and Amending Regulation (EU) 2021/694 (Cyber Solidarity Act). *Official Journal of the European Union*. 2025. L 2025/38. 15 January 2025. URL: <http://data.europa.eu/eli/reg/2025/38/oj> (accessed: July 19, 2026).

12. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. 3rd ed. Geneva : International Organization for Standardization, 2022. URL: <https://www.iso.org/standard/27001> (accessed: July 2, 2026).

13. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD : National Institute of Standards and Technology, 2024. 32 p. DOI: <https://doi.org/10.6028/NIST.CSWP.29>. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> (accessed: July 2, 2026).

14. Yanko A. S., Martynenko A. M., Trykoz V. V. Network Sensors and

Detectors as an Effective Tool for Data Monitoring. *Control, Navigation and Communication Systems*. 2022. No. 1 (67). P. 98–101. DOI: <https://doi.org/10.26906/SUNZ.2022.1.098>.

15. Yanko A. S., Makarenko O. I. The Concept of a Network Intrusion Detection and Prevention System. *Control, Navigation and Communication Systems*. 2022. No. 2 (68). P. 59–67. DOI: <https://doi.org/10.26906/SUNZ.2022.2.059>.

16. Zhyvylo Ye., Kuz V. Risk Management of Critical Information Infrastructure: Threats-Vulnerabilities-Consequences. *Theoretical and Applied Cybersecurity*. 2023. Vol. 5, No. 2. P. 68–80. DOI: <https://doi.org/10.20535/tacs.2664-29132023.2.280377>.

17. Yanko A. S., Padusenko Ya. V. A Distributed Intelligent System for Semantic Monitoring of Heterogeneous Data in the Telegram Messenger Based on Vector Representations. *Taurida Scientific Herald. Series: Technical Sciences*. 2026. No. 3. P. 221–229. DOI: <https://doi.org/10.32782/tnv-tech.2026.3.23>.

18. Zhyvylo Ye. Stage of Risk Assessment of Critical Infrastructure Cyber Security Breach. Information Control Systems and Technologies (ICST–ODESA–2024) : materials of the XII International Scientific and Practical Conference, Odesa, 23–25 September 2024. Odesa : Helvetica Publishing House, 2024. P. 52–55. URL: <https://icst-conf.com/2024.pdf> (accessed: July 19, 2026).

19. Zhyvylo Ye. O., Shevchenko D. G. Risk Assessment of Cyber Security and Control of Privacy in Public Administration Information Systems. *Collection of Scientific Works of the Military Institute of Taras Shevchenko National University of Kyiv*. 2022. No. 75. P. 66–77. DOI: <https://doi.org/10.17721/2519-481X/2022/75-07>.

20. Yanko A. S., Vyhivskyi R. A. Computer Network Protection System. *Control, Navigation and Communication Systems*. 2022. No. 2 (68). P. 91–94. DOI: <https://doi.org/10.26906/SUNZ.2022.2.091>.

21. Zhyvylo Ye. O. Macroeconomic Stability of the State under Cyber Threats. *Current Issues in Public Administration*. 2024. No. 2 (65). P. 347–369. DOI: <https://doi.org/10.26565/1684-8489-2024-2-18>.

22. Fesenko T., Kalashnikova Yu. Use of Cisco SecureX for SOC

Automation. *Control, Navigation and Communication Systems*. 2025. No. 4 (82). P. 138–143. DOI: <https://doi.org/10.26906/SUNZ.2025.4.138>.

23. Detection of LDDoS Attacks Using SDN Networks with Machine Learning Elements / A. Yanko, A. Prokudin, I. Fil, O. Kruk. *Measuring and Computing Devices in Technological Processes*. 2024. No. 4. P. 287–296. DOI: <https://doi.org/10.31891/2219-9365-2024-80-36>.

24. Fesenko T. M., Kalashnikova Yu. V. Federated GNN-XAI Model for Predicting Account Compromise in a Zero Trust Environment. *Cybersecurity: Education, Science, Technology*. 2025. Vol. 3, No. 31. P. 602–619. DOI: <https://doi.org/10.28925/2663-4023.2025.31.1049>.

25. Stochastic-Spectral Methods for Detecting Hidden Triggers in Neural Networks for 6G Signal Processing / Ye. Zhyvylo, A. Chorny, I. Romashko, Yu. Kalashnikova. *Measuring and Computing Devices in Technological Processes*. 2026. No. 2. P. 110–119. DOI: <https://doi.org/10.31891/2219-9365-2026-86-14>.

26. Yanko A., Hlushko A. A Method for Binary Representation of Residues Based on the Ring Shift Principle to Enhance the Digital Resilience of Cryptographic Systems. *Transactions of Kremenchuk Mykhailo Ostrohradskyi National University*. 2026. No. 2 (157). P. 187–194. DOI: <https://doi.org/10.32782/1995-0519.2026.2.19>.

27. Zhyvylo Ye. O. Identifying and Acquiring Modern Cybersecurity Workforce Competencies amid the State's Digital Transformation. *Current Issues in Public Administration*. 2023. No. 2 (63). P. 111–127. DOI: <https://doi.org/10.26565/1684-8489-2023-2-08>.

28. Zhyvylo Ye. O., Zhyvylo I. O. Joint Training of the Cyber Security Defense Forces Personnel in the Conditions of Total State Defense. *Theory and Practice of Public Administration*. 2021. No. 2 (73). P. 144–153. DOI: <https://doi.org/10.34213/tp.21.02.16>.