Intelligent resilience support tools: modern approaches for critical infrastructures*

Oleksandr Dodonov[1,†], Olena Gorbachyk[1,*,†] and Maryna Kuznietsova[1,†]

[1] *Institute for Information Recording of the National Academy of Sciences of Ukraine, Shpaka str. 2, 03113 Kyiv, Ukraine*

Abstract

The problem of critical infrastructure stabile functioning under modern threats and emergencies is set, and new approaches to resilience providing are discussed. Tasks for ensuring cybersecurity and existing methods and measures for solving them are identified. The current state of modern intelligent tools application in critical infrastructures is analyzed. The effectiveness and problems of Internet of Things, Big Data analytics and Artificial Intelligence models using are assessed. A generalized scheme for critical infrastructures resilience support using intelligent tools and technologies is proposed. The technical, technological, organizational and cost aspects of implementing intelligent tools, their mutual influence and integration within a separate critical infrastructure are discussed.

Keywords

Critical infrastructure, resilience, intelligent tools, Artificial Intelligence, Internet of Things

1. Introduction

One of the key requirements for the critical infrastructure (CI) operation is ensuring its resilience, that is, its ability to maintain functionality, stability and recoverability in the event of emergencies caused by natural disasters, terrorist acts, cyber-attacks or technical failures. The development of effective means of protection and response to emergencies is complicated today by the diversity of threats and their constant evolution, the presence of structural and functional vulnerabilities in CI, and the interdependence of CIs. Under these conditions, there is a need for the methods and tools continuous development and modification to respond adequately to emergencies and their consequences, and for the identification and implementation of innovative management approaches, modern information technologies and intelligent systems, as well as qualitatively new methods, tools and measures to enhance the resilience of critical infrastructure.

The management processes digitalization, widespread information technologies and specialised information and communication systems introduction have helped to improve the speed of threats response, refine methods for the emergence forecasting and development analysis, enhance the means of mitigating the emergencies consequences, and reduce the negative impacts scale. However, the challenge of developing well-founded management decisions in real time under conditions of limited resources remains a pressing issue.

The use of intelligent automated control tools, such as artificial intelligence (AI), and the transition to risk-based management methods will help to improve the accuracy of critical infrastructure analysis, enhance the control systems adaptability for dynamic changes in the operating environment whilst minimising resource expenditure, and ensure the continuity of their

* *ITS-2025: Information Technologies and Security, December 11, 2025, Kyiv, Ukraine*

* Corresponding author.

† These authors contributed equally.

dodonovua@gmail.com (O. Dodonov); bges@ukr.net (O. Gorbachyk); marglekuz@gmail.com (M.Kuznietsova)

0009-0008-8473-6280 (O. Dodonov); 0000-0001-8492-4478 (O. Gorbachyk); 0000-0001-6054-418X (M.Kuznietsova)

© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-11-26

CEUR-WS.org/Vol-4337/paper1.pdf

real-time operation. This can also be viewed as one of the avenues for enhancing the critical infrastructure resilience.

2. Research Objectives

The emergence and proliferation of new high-tech means of remotely attacking critical infrastructure (CI) assets, as well as the constant rise in cyber risks, significantly increase the vulnerability of infrastructure systems, and, given the high interdependence of the physical, informational and organizational components of CI, this complicates the processes of ensuring their resilience and increases the likelihood of cascading failures. Under such conditions, ensuring the CI resilience depends to a large extent on the ability of the CI management system to detect threats in a timely manner, adapt management processes and maintain operational continuity. Therefore, particular attention must be paid to the issue of ensuring the functional stability of automated organisational management systems for CI, which must maintain controllability, information consistency and decision-making efficiency even in the event of an emergency development.

In modern information technology practice, one of the leading trends is the implementation of Artificial Intelligence (AI) methods and tools. Machine learning algorithms, predictive models, and neural network architectures of varying complexity are used to analyse, evaluate and predict the state of complex systems, refine the parameters of the processes under investigation, justify management decisions, and identify hidden information dependencies.

The search for technological solutions and engineering approaches to ensuring the resilience of cyber-physical systems, based on the integrated application of Artificial Intelligence methods, Big Data analysis technologies and the Internet of Things (IoT) concept to address the challenges of enhancing the automated organisational management system functional stability in critical infrastructure, taking into account the potential for emergencies in CI, is the aim of this research. The study is directed towards the development of intelligent monitoring systems, analysis and support of management decisions, capable of ensuring the destructive influences timely detection, forecasting the development of crisis processes and adapting management mechanisms to conditions of heightened uncertainty.

The research is conducted in several stages, ensuring a systematic analysis of existing approaches, a comprehensive review of technological solutions, and the structuring and synthesis of the results obtained.

3. Problem definition

The complexity and interdependence of cyber-physical systems continue to grow, their vulnerability is increasing, and it is precisely the intelligent tools and methods of AI that could enhance the capacity to manage such vast networks effectively.

From the very first studies devoted to the intellectualization of computerized means of data storage, processing, analysis, transmission and management decision support, it became clear that, whilst such technologies held significant potential for improving efficiency, their practical implementation was complex. Papers [1–3] examine the characteristics of AI and its functioning in the context of digital transformation. The development of expert and knowledge-based systems, neural network approaches, statistical methods of data analysis and machine learning algorithms has significantly expanded the possibilities for automating the analysis of complex processes in socio-technical systems. The technological transformation and intellectualization of tools, supporting management processes, have been driven by the widespread adoption of Big Data processing tools, the development of the Internet of Things (IoT), the emergence of Large Language Models (LLM), and, at the present stage, the appearance of Generative Artificial Intelligence

(GenAI) technologies. These technological trends have significantly influenced the functional capabilities, structural characteristics and operational parameters of CI and its control systems, particularly in the fields of energy, transport, communications, security and public administration. Tech giants such as Google, Meta, Alibaba, Baidu, OpenAI, Anthropic and others are actively developing AI technologies. According to Statista [4], the global AI market grew from 93.3 to 184 billion US dollars between 2020 and 2024, an increase of 97.2%, and growth is forecast to continue – reaching US$243.7 billion in 2025, US$415.6 billion in 2027 and US$826.7 billion in 2030.

The current state of critical infrastructures development is characterized by the widespread and integrated use of Internet of Things, Big Data analytics and Artificial Intelligence technologies, underpinned by advanced information and telecommunications technologies and systems. The application of intelligent tools in the field of critical infrastructures covers a wide range of tasks, including maintaining the continuity of management processes in various sectors (finance, transport, healthcare, and the management of water, gas and heating supply), analysis of user behaviour, automation of routine operations, monitoring and analysis of network traffic, development of adaptive models and algorithms for the functioning of CI components, support for decision-making processes management, as well as enhancing the level of cybersecurity and resilience of information and communication infrastructure. The application of GenAI technology is gradually transforming various aspects of the critical systems operation and management. GenAI can be used to model complex systems, simulate alternative scenarios for the events development in the energy sector, and develop new strategies for optimising management processes and risk management. For instance, in energy systems, GenAI models can predict potential power grid failures, design more efficient network topologies and develop improved control algorithms. This technology not only enhances operational efficiency but also expands the ability to respond to new challenges, disruptions and emergency situations. It should be noted that the potential of GenAI extends beyond current applications, opening up opportunities for a significant increase in the resilience, innovation and productivity of AI operations.

On the one hand, the use of AI tools creates new opportunities for more effective management of complex risks and for enhancing cyber security; on the other hand, however, it gives rise to additional threats associated with the use of a fundamentally new class of digital technologies. Thus, with the spread of GenAI technologies, particularly from around 2023 onwards, the number and variety of cyber threats have significantly increased, including phishing, leaks of confidential data, ransomware, ‘data poisoning’ attacks, and so on. AI technologies are used to automate, optimise and scale both physical and cyberattacks. In particular, this refers to the potential use of autonomous systems (such as unmanned aerial vehicles) to attack physical infrastructure, and the use of AI to prepare and carry out cyber compromise of information systems. AI tools are capable of significantly reducing the technical barriers to carrying out various stages of offensive cyber operations, including reconnaissance, vulnerability analysis and the development of malicious software.

AI systems are becoming increasingly integrated into the functioning of critical infrastructures, making them an ever more attractive target for cybercriminals, which leads to an expansion of the attack surface and the emergence of new channels of compromise. Potential threats include ‘data poisoning’ and ‘model poisoning’ attacks, as well as the compromise of the underlying software and hardware platforms and infrastructure on which AI systems are deployed. The compromise of AI systems that perform or support critical control functions can have immediate and significant consequences for the operation of critical infrastructure. An additional risk factor is the relative novelty and complexity of such technologies, as well as the limited practical experience of their operation by network and CI system operators, which increases the likelihood of disruptions to their stable functioning [5].

4. Problems of rapid and reliable assessment of functional stability

Critical infrastructure consists of complex structures characterised by a hierarchical structure, functional and resource distribution, a large number of actively interacting elements, modules and subsystems, as well as a complex management system. Information systems and technologies constitute the primary information asset of CI. The information and communication infrastructure (ICI) of the CI is a key factor influencing the speed of information exchange, information support for solving applied tasks, and managerial responses to unforeseen events within the CI. The CI's ICI operates continuously, constantly recording the states of the internal and external environments. Information exchange is shaped by the functional tasks of users who initiate the execution of applied tasks and require application interaction during their implementation. The components of the ICI implement information processing functions (computing, accumulation, accounting, control, storage, search, display, and transformation of information); information exchange functions; and decision-making functions (transformation of information content to create new information during analysis, forecasting, or operational management).

In the context of military operations in Ukraine, emergencies in critical infrastructure are characterized by the simultaneous destruction of both the physical and digital components of the infrastructure, as well as a significant increase in the risk of cascading failures in critical infrastructure with catastrophic consequences. Moreover, management during emergencies in critical infrastructure most often involves operating under conditions of lost network connectivity and backup control channels, as well as strict time constraints on restoring the critical infrastructure functioning. Calculating the risk from emergencies for critical infrastructure as a whole, taking into account the complexity of the structure of events within critical infrastructure, is possible using the formula [1]:

$$R = P \iint_{S} \int_{J_{min}}^{J_{max}} p(J)\,\varphi(x,y)\,f(x.y.J)\,dJdxdy,$$

where R – the risk to critical infrastructure resulting from the occurrence of adverse events is defined as the loss of functionality of critical infrastructure assets within a given territory;
P – the probability of an event (accident or emergency) resulting in the emergence of a damaging factor characterized by parameter J;
S – the area of the territory where damaging factors are active (integration domain);
$p(J)$– the probability of CI objects being affected depending on J as a parameter;
$\varphi(x,y)$– the density of CI objects within the territory (x,y)under consideration;
J_{min}, J_{max} – the minimum and maximum values of the damaging factor parameter, respectively;
$f(x.y.J)$– the distribution density of the intensity of parameter (x,y).

The functional stability of the ICI component of the CI system under cyberattacks can be characterized by the function $\varphi(t,h,\mu,\wp)$, the average value of which over the interval ΔT [1]:

$$\varphi_c = \frac{1}{T}\int_{0}^{T} \varphi(t,h,\mu,\wp)\,dt,$$

where $h=\{F,N,T\}$ – characteristics of a cyberattack.
$F=\{F_i(t)\}$, where $F_i(t)$ – the probability distribution of the random variable η_i representing the time interval until the start of the i-th cyberattack, $i=\overline{1,N}, N$ – the number of cyberattacks, $t\in(0,T], \Delta T$ – the period of time from the start to the end of a negative impact, such as a cyberattack, $\Delta T=(0,T]$, where T – the time at which the cyberattack ended.

$\mu = \{T_{rec}, S\}$ – a measure of the functional resilience of a particular j-th component of the information and communications infrastructure, which characterises the component's ability to restore its functionality following an i-th cyberattack.

$T_{rec} = \{\tau_i^{low}, \tau_i^{up}\}$ – the set of estimates of the lower τ_i^{low} and upper τ_i^{up} values of the recovery time intervals for the j-th component, obtained either through the use of expert methods or by conducting specialised studies.

$S = \{S_i(t)\}, i = \overline{1, N}$ – the set of distribution functions of the random time intervals required for the component to recover its functionality following the i-th cyberattack.

$\wp$ – a set of indicators of the functional resilience of components φ, characterising a component's ability to maintain its functionality after withstanding a cyberattack.

$\wp = \{p_i\}, i = 1, N, N$ – the number of cyberattacks, p_i – the probability of a component being compromised during the i-th cyberattack (obtained either through the use of expert methods or as a result of statistical modelling).

To assess the functional stability of a component of the ICI CI, one may use a metric that characterizes the probability of the component being in a state of full functionality at any given moment $t \in (0, T]$:

$$\kappa_\varphi = \lim_{\substack{t \to T \\ n \to N}} \varphi(t, h, \mu, \wp)$$

T and N – the earliest possible time of occurrence for a set of cyberattacks and the maximum predicted number of cyberattacks within that set are determined, respectively, through the use of expert methods.

The proposed assessments of functional stability [1] involve the use of statistical modelling methods, which generally require a significant time investment. Given the dynamic nature of the security environment, this may result in delayed assessment results and a loss of their practical relevance for management decisions supporting. Furthermore, the reliability of such assessments depends to a large extent on the completeness of statistical data, the validity of the assumptions made, and the adequacy of the constructed models to the actual processes of system operation. In conditions of uncertainty, incomplete information and rapid changes in the states of control systems, this can lead to a significant reduction in the reliability of the results obtained. In this regard, there is a need to apply modern intelligent technologies that will ensure the promptness of results and enhance their reliability in the context of the control systems development.

5. Using intelligent tools to maintain CI resilience

The application of intelligent tools in CI requires addressing several issues, particularly those relating to data, its quality (accuracy, completeness, consistency, and timeliness), quantity (sufficiency and diversity), and security (authenticity, integrity, and confidentiality). With the intelligent tools introduction, data quality becomes even more important. A key challenge for CI is the creation of automated intelligent security tools for data management systems capable of self-analysis and configuration, taking into account existing conditions and events based on defined criteria and knowledge of previous system states [1], as well as the ability to monitor a significant number of different parameters for behavioural anomalies.

The application of IoT architecture in critical infrastructures creates the conditions for the continuous real-time monitoring of a wide range of operational parameters relating to technical and organisational-technological processes. Thanks to an extensive network of sensors, actuators and communication modules, IoT enables the generation of large data streams characterising the state of infrastructure elements, environmental parameters and the operating modes of CI systems. The effective use of this data requires the application of Big Data analytics methods, which ensure its systematization, processing and intelligent analysis. Analytical tools enable the identification of

hidden patterns in the CI operation, the prediction of equipment failures, the assessment of risks of emergencies, and the optimisation of operational modes for infrastructure facilities. However, the large-scale integration of a vast number of connected devices, their limited computational and energy resources, and the use of wireless communication channels result in an increased level of cyber-vulnerability in such systems. Thus, denial-of-service (DoS) attacks, aimed at compromising the confidentiality, integrity and availability of data, may significantly affect the stability of CI operation.

Thanks to the synergistic effect of combining IoT, Big Data and AI technologies, new opportunities are emerging to enhance the efficiency of monitoring, forecasting and adaptive CI management, thereby laying the groundwork for the smart measures development to support management decisions and, consequently, contributing to the CI resilience increasing [3]. For instance, the application of IoT technology enables continuous monitoring of the infrastructure's condition. Big Data tools process monitoring data, whilst AI tools can identify patterns and risks. The intelligent technologies combination provides operators and managers with a clearer understanding of the infrastructure's condition in real time, improving their situational awareness, their ability to anticipate and manage potential threats, and to respond swiftly and appropriately to faults or anomalies.

By utilising AI tools to predict critical events (such as overloads, mechanical failures or cyberattacks), managers at various levels can identify high-risk components within critical infrastructure, optimise maintenance schedules and effectively allocate resources, thus significantly reducing the probability of cascading effects and catastrophic failures. Furthermore, in the event of a failure in the critical infrastructure, AI algorithms can automatically initiate corrective measures, optimize recovery processes and manage resources in emergency situations. For example, in a smart grid, AI can redirect electricity to undamaged sections, isolate damaged sections and prioritize resources for rapid restoration.

Despite the significant potential of IoT, Big Data and AI technologies for ensuring the critical infrastructure resilience, their practical integration is accompanied by a number of systemic scientific and technical challenges that need to be addressed:

1) *The challenge of ensuring information security and data confidentiality.* IoT networks, upon which the monitoring of infrastructure assets is based, are characterised by heightened vulnerability to cyber threats. The data generated by such systems may contain confidential technical or operational information. So, comprehensive mechanisms are required for data protection, secure device authentication and cryptographic protection of information transmission channels.
2) *The issue of interoperability and standardization.* The heterogeneity of IoT devices, big data processing platforms and intelligent analytical systems leads to the different protocols, data formats and architectural solutions using. Such fragmentation complicates the integration of components into a single information and analytical environment. Therefore, an important task is the development of unified interaction standards that ensure the compatibility and continuous operation of heterogeneous systems.
3) *The issue of network infrastructure reliability and data processing delays.* The effective decision-support systems operation in the defence sector requires the rapid analysis of large data volumes in real time, which places heightened demands on the communications infrastructure reliability, network bandwidth, and delays minimisation in the information transmission and processing.
4) *The issue of scalability and cost.* The application of comprehensive intelligent monitoring and management platforms based on IoT, Big Data and AI across large-scale infrastructure systems involves significant financial and organisational costs, that is particularly acute in the CI sector. Thus, research aimed at creating modular, scalable, and cost-effective architectures for the intelligent tools implementation has particular relevance.

Currently, in both academic research and practical efforts to ensure the CI resilience, the following priority areas for the application of intelligent tools are identified:

- analysis, assessment and management of risks associated with the CI operation;
- ensuring the physical protection of its individual components and systems as a whole;
- optimisation of the infrastructure components structure and operating modes, primarily its information and communication systems and technologies;
- cybersecurity enhancement;
- critical elements redundancy, duplication and timely replacement organizing to maintain the continuity of infrastructure operations;
- scenarios for emergencies and effective response protocols developing.

Together, these areas define the conceptual framework for smart technologies using to enhance the adaptability, stability and recoverability of CI in the face of growing risks and uncertainty, and consequently, to increase the critical infrastructure resilience.

5. 1. Risk analysis for CI resilience

The CI risk analysis is based on a combination of expert assessment, mathematical modelling and statistical data analysis, which enables the assessment of the probability of hazardous events (*P*) and the magnitude of potential losses or damage (*A*). In general, risk can be represented as a function of the probability of a hazardous event (P), the system's vulnerability (*V*) and the magnitude of possible consequences: *R=f (P,V.A).* Risk has become an integral feature of the CI state and its operating environment. Risk analysis is a continuous, adaptive process involving the constant monitoring of the CI state, its structural elements and the external environment, as well as adaptation to new threats. This becomes particularly important in the modern hybrid challenges context, where natural, man-made, social and cyber threats can arise simultaneously and reinforce one another. The management effectiveness is largely determined by the system's ability to detect potential threats in a timely manner, forecast scenarios for their development, formulate adequate response strategies. For the ensuring the CI resilience, a proactive risk management strategy takes on particular significance. The strategy is focused on the potential destabilising factors early detection and forecasting, and its implementation involves the risk analysis processes intellectualization and the methods for solving a complex set of interrelated tasks development:

- *threat detection* – identifying potential sources of danger based on historical data analysis, system performance parameters and environmental characteristics;
- *vulnerability assessment* – identifying structural, functional and organisational weaknesses in the system that could be exploited by threat sources;
- *risk assessment and optimisation of response strategies* – quantitative or qualitative assessment of overall risk using statistical, simulation and intelligent forecasting models;
- *formulation of risk management strategies* – development of a set of organizational, technical and managerial measures to reduce the likelihood of hazardous events occurring or to minimise their consequences.

5. 2. Physical security

Intelligent technologies are also used *to enhance the physical security* of critical infrastructure facilities, in particular to reinforce protective structures and perimeter security systems, thereby reducing the risk of physical damage to infrastructure facilities, in video surveillance systems, where intelligent image analysis methods enable the automated detection of intruders or suspicious activity, in biometric identification systems, and in access control and management systems. In the context of modern security challenges and ongoing military aggression, there is a growing need for integrated intelligent security platforms capable of consolidating and analysing data from diverse sensor sources (radars, thermal imaging and acoustic systems). Data integration and the application

of intelligent data analysis methods in such platforms enable the formation of more comprehensive *situational awareness*, allowing for the early detection, classification and identification of potential threats, in particular enemy unmanned aerial vehicles, and to deploy countermeasures in a timely manner to neutralize them at a safe distance from critical infrastructure.

5. 3. IT-structure modernization

Intelligent tools can be effectively used to evaluate, plan and *optimise the modernisation of IT infrastructure*, particularly when deploying new information systems on top of existing on-premises environments, migrating services to cloud platforms, implementing new technological solutions or integrating heterogeneous information systems. AI algorithms simplify the analysis of ICI configurations and settings, enhance the efficiency of testing during infrastructure modernization, and enable the automation of compatibility, performance and security checks for software and hardware systems, ensuring the timely detection of configuration conflicts, software errors and potential vulnerabilities that may arise during modernisation or operating environment changes.

5. 4. Cybersecurity enhancement

AI already plays a vital role in *enhancing cyber stability and the operational efficiency* of digital infrastructure. ICI is a fundamental element of CI operation; therefore, the use of AI-based cybersecurity systems capable of detecting, analysing and neutralising threats in real time is one of the key factors in ensuring the reliability and continuity of interconnected CI operation [5]. The functional capabilities of intelligent tools in the field of ICI are as follows:

1) *Ensuring the security of AI-driven cybersecurity systems:*
   - cyber threats real time detection and neutralization based on network traffic analysis;
   - endpoint protection through the detection of anomalous device behaviour;
   - the cloud environments security ensuring, including maintaining data availability, integrity and confidentiality;
   - intelligent analysis of information security events in Security Information and Event Management (SIEM) systems and Security Operations Centres (SOCs).

2) *AI-based infrastructure management:*
   - data centre operation optimization, including load balancing and efficient resource allocation;
   - the infrastructure energy efficiency improving;
   - hardware and software components automated inventory and configuration management;
   - information systems modernization and integration support.

3) *Intelligent automation and operational support:*
   - automated IT support based on virtual assistants and chat-bots;
   - intelligent methods using during the software development, testing, verification and validation;
   - the predictive maintenance mechanisms for ICI implementation, enabling the anticipation of potential equipment or software component failures and minimising system downtime.

Intelligent cyber defence systems are already being implemented; these ensure more effective monitoring of network activity, speed up responses to information security incidents and contribute to an overall increase in ICI resilience. In particular, machine learning algorithms are used to monitor suspicious activity, conduct automated vulnerability scans, assess cyber risk levels,

and identify content generated by AI for the purpose of carrying out disinformation or fraudulent attacks.

Intelligent technologies enable the automated processing and analytical review of information security reports, the detection of unauthorised intrusions, and the monitoring and analysis of network traffic to identify anomalies, as well as reducing the number of false positives ('false alarms'), using behavioural models and adaptive learning algorithms. Furthermore, using of AI methods facilitates the development of predictive cyber defence mechanisms, which enable the early identification of potential threats and the formulation of proactive response strategies. Such capabilities are implemented in multi-layered cybersecurity systems, which combine network protection tools, data protection systems, access control mechanisms, and intrusion detection and prevention systems (IDS/IPS).

Using smart tools will significantly reduce the impact of cyber threats and ensure the continuous CI operation. Attack and intrusion detection systems are typically implemented as software or hardware-software solutions. They provide automated monitoring of events in information systems and networks with the aim of promptly detecting signs of potential threats or unauthorised access, and are an integral component of modern cybersecurity architecture. One promising area is the automation of penetration testing using machine learning methods and intelligent algorithms such as support vector machines (SVM), random forests (RM), naive Bayes classifiers, decision trees, and reinforcement learning methods. Large Language Models can be used in the process of automating cyber defence to analyse logs, classify cyber threats, generate reports, and provide recommendations for addressing identified vulnerabilities. Thanks to their ability to process large volumes of data, such models enhance the efficiency and quality of analytical support for cybersecurity management.

5. 5. Resources organization

The task of maintaining the CI functionality, stability and recoverability under an emergency requires the *availability of appropriate resources*, as well as the technological and organizational mechanisms for their use. Current practice in CI resilience ensuring is based on the concept of resilience engineering, which involves following basic principles: redundancy, diversity, distribution and adaptability. *Redundancy* involves the creation of duplicate system elements capable of performing the functions of primary components in the event of their failure or damage (creating backups of critical data and software systems, using redundant hardware components, and implementing fault-tolerant data storage technologies, in particular Redundant Array of Independent Disks (RAID) arrays). *Diversity* involves the use of alternative technical solutions and diverse hardware and software resources to perform the functions of the system's core components, thereby reducing the likelihood of simultaneous failures caused by a single type of threat or vulnerability. *Distributed architecture* is achieved by creating spatially distributed elements of the ICI, in particular geographically remote data centres or backup network nodes, thereby reducing the risk of a complete loss of system functionality in the event of local damage, man-made accidents or natural disasters. *Adaptability* is the system's ability to change its structure, configuration or operating modes in response to changes in external conditions or the emergence of new threats. Adaptability is largely linked to the use of intelligent methods of data analysis, forecasting and decision support. It ensures the CI dynamic adaptation to new risks and emergency scenarios.

Undoubtedly, the continuity of the CI operation is also ensured by the availability of backup power supplies, disaster recovery systems, and the establishment of alternative communication channels.

5. 6. Emergencies modelling and response generation

Intelligent tools are used to *model the occurrence of emergencies*, examine various scenarios of their development, assess potential environmental impacts, and *determine optimal response strategies* and methods for restoring the functioning of infrastructure systems within the framework of the modern approach known as scenario-based resilience analysis. An important tool for implementing this approach is the 'Digital Twins' technology, which represents a dynamic virtual model of an infrastructure system capable of reproducing its behaviour in real time. The digital twins application allows the infrastructure systems behaviour under emergency conditions to investigate, potential cascading failures to analyse, and well-founded insights into possible emergency scenarios to form for the effective response measures selection. GenAI models are often used to simulate the consequences of rare or hypothetical events, including multi-factor failures and complex emergency scenarios. Such models allow the potential risks investigation, that are difficult or impossible to replicate in real-world conditions, and enable the development of effective response strategies for non-standard and low-probability events.

Intelligent technologies provide the foundation for the development of decision-support systems for emergency management, which enable the formulation of informed management decisions regarding the containment, resolution and mitigation of the consequences of emergencies. Furthermore, opportunities have arisen for the emergency response plans development and regular updating, and for training personnel to act in emergency situations. In this context, training technologies such as virtual reality (VR) and augmented reality (AR) play an important role. Simulating emergencies in a safe training environment helps to develop practical response skills, enhances the level of personnel professional training and ensures readiness for operational action in real-life emergencies.

6. Generalized architecture of a critical infrastructure resilience support system using intelligent tools

The implementation of intelligent IoT, Big Data and AI tools to support the CI resilience requires the refinement of its architecture, in particular its technical, technological and organizational components, the framework development for their coordination and integration, and the definition of interrelationships, sequences and technologies for the relevant intelligent solutions application. The architecture of the CI resilience support system must be based on the principles of distribution, autonomy and hierarchical interaction between components, and must ensure the ability to utilise intelligent tools and AI technologies at all levels of the system's operation. We present the architecture of the CI resilience support system as a six-layer structure, with the following structural and functional layers identified, for the sake of clarity:

- Edge Layer
- Communication & Integration Layer;
- Intelligent Core Layer;
- Decision Making & Response Layer;
- Recovery Layer;
- Interface & Management Layer.

Let's take a closer look at the composition of the functional modules of each layer.

Layer 1: Periphery and Data Collection (Edge Layer).

In Module 1.1 we combine intelligent tools of Sensors & IoT, which make continuous collection of "raw" data about the state of physical and cyber infrastructure components (temperature, pressure, voltage, network traffic, access logs, etc.). Usually industrial sensors, smart meters, video surveillance cameras, IoT gateways and others are used.

Module 1.2: Edge Computing Nodes. The primary processing and filtering of data in place is made here. Lightweight AI models are being implemented to quickly detect anomalies that require

immediate response (e.g. blocking a port during a DDoS attack), thus reduces the load on the central system. Often Microcontrollers with AI accelerators, Edge AI platforms are used.

Layer 2: Communication & Integration Layer

The main Module 2.1 is a Secure Communication Bus, that ensures reliable and encrypted data exchange between all layers of the system. Uses protocols that are resilient to communication interruptions. Main technologies that used here for secure and scalable data transmission are: MQTT, AMQP, VPN, SD-WAN, Data Diodes (for one-way transmission of critical data).Layer 3: Intelligent Core Layer

This is the "brain" of the system, consisting of several interconnected modules:

Module 3.1 is for data fusion and analytics. Aggregates data from all sources (Edge, IT/OT systems, external Threat Intelligence sources). Module creates a single picture of the system state in real time with events correlation to detect complex, multi-vector attacks. Usually such smart tools as Big Data platforms (Hadoop, Spark), new generation Security Information and Event Management (SIEM) systems are used here.

Module 3.2: AI Threat Detection & Anomaly Detection Module uses deep learning and behavioural analysis to identify known and unknown threats (Zero-day attacks), as well as deviations from normal equipment operation. Such smart tools as Neural networks (CNN, RNN), machine learning algorithms (RF, SVM) are often used.

Module 3.3: Predictive & Modelling Module - predicts potential failures and attacks based on historical data. Uses Digital Twins to simulate "what-if" scenarios and assess the impact of decisions on system resilience. There are more than 30 Digital Twin Platforms for different critical infrastructures, among which Microsoft Azure Digital Twins for IoT and smart environments, facilitating comprehensive security monitoring and IoT threat detection; Siemens Xcelerator for industrial manufacturing, strong for industrial security, allowing for deep engineering-to-operation simulation to identify vulnerabilities; *AWS IoT TwinMaker* for creating operational twins across multiple data sources, strengthening security with composable views. Digital Twins can simulate cyberattacks or breaches to test system defences, improving security incident response. They provide intellectual Security Operations Centres (iSOC) with live data, enabling better visualization and response to physical intrusions or alarms. Performing predictive maintenance and vulnerability testing, they identify weaknesses in both software and physical systems (e.g., IoT sensors) before they can be exploited.

Layer 4: Decision Making & Response Layer

Module 4.1: Decision Support Module - provides operators with recommendations on optimal actions in crisis situations, fulfils risk assessment and incident prioritization. Expert systems, rule-based systems, data visualization are often used here.

Module 4.2: Autonomous Response & Adaptation Module – its main task is to automatically execute actions to localize the threat, minimize damage, and adapt the system (e.g., isolate a network segment, switch to backup channels, change firewall configuration). Mainly it uses SOAR (Security Orchestration, Automation and Response), and SDN (Software-Defined Networking) controllers. SOAR helps security teams to manage and respond to threats by integrating security tools, automating repetitive tasks, and streamlining workflows. *Orchestration* connects disparate security tools and technologies from different vendors into a single, cohesive system, *Automation* helps to automate repetitive, manual tasks to speed up response time, and *Response* provides tools for managing, investigating, and analysing incidents. SDN controllers fulfil centralized management of software defined network, provide a global view of the network topology and manage traffic across all devices from a single point, accelerate network deployment, configuration changes, and troubleshooting.

Layer 5: Recovery Layer

Module 5.1: Recovery Management Module: coordination of the system recovery process after an incident. Automated deployment of backups, verification of system integrity before returning them to operation. Backup and disaster recovery systems (DRaaS), infrastructure automation tools (Ansible, Terraform - open-source *Infrastructure as Code* (IaC) tools that automate IT environments) can be used for recovery management. DRaaS is a cloud-based managed service that replicates and hosts physical or virtual servers to provide rapid failover and recovery of IT systems during outages, by automating the recovery process.

Layer 6: Interface & Management Layer

Module 6.1: Unified Management Console: main functions of the level are centralized system-wide status monitoring, threat visualization, security policy management, reporting for operators and management. Intelligent smart tools, such as decision support systems, expert systems, visualization systems are combined here.

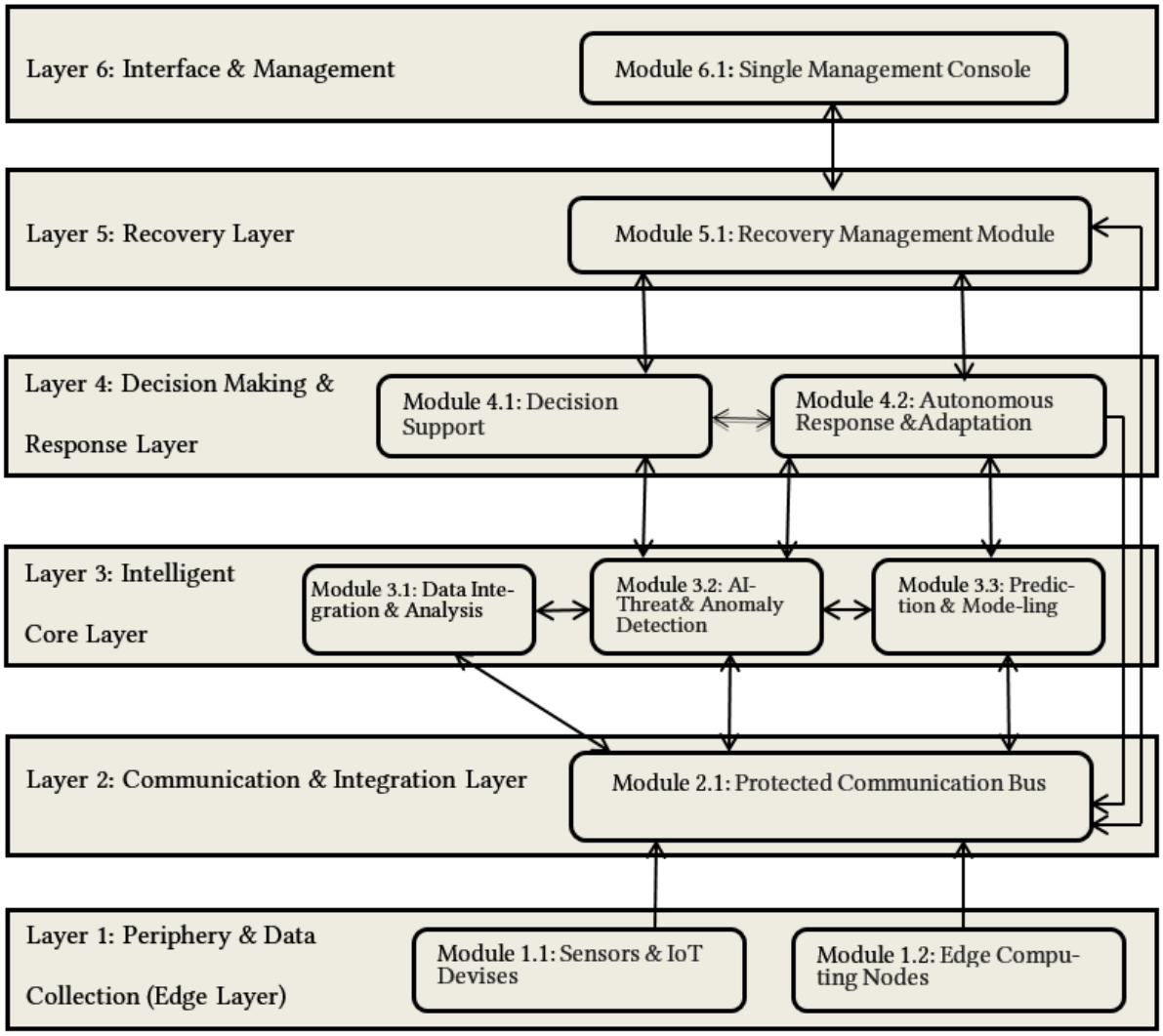


Figure 1: Generalized scheme of CI resilience support system with intelligent tools.

The diagram shown in Figure 1 illustrates the closed-loop cycle of CI resilience support – from continuous monitoring and threat detection to intelligent data analysis, automated response and rapid restoration of CI operations. Various means of automation, intelligent decision support, and mechanisms for automatic and automated incident response may be employed in the relevant modules. At every stage of implementing such an architecture, issues related to ensuring

cybersecurity may arise, necessitating the application of comprehensive, advanced measures for information protection and countering cyber threats.

7. Organizational and regulatory aspects of smart technologies applying in critical infrastructure

The implementation of IoT, Big Data and AI technologies in CI requires an organisational management paradigm transformation. This involves introducing preventive mechanisms to ensure secure and sustainable infrastructure operation, developing cross-functional collaboration between departments, and defining strategic priorities for digital transformation. Usually transformation is accompanied by an operational processes review, organisational roles and responsibilities clarification, new requirements for staff professional competencies establishment, and the risk management practices, compliance systems and control procedures modernisation. Consequently, smart technologies implementation involves the integration of relevant technical solutions and the human capital development for ensuring effective management of the smart systems impact on service delivery and the CI functioning.

The main challenges associated with the smart systems implementation include:

- the high cost of implementing and operating intelligent technologies;
- significant energy consumption;
- issues regarding compatibility and integration with existing information systems;
- insufficient human resources and a shortage of suitably qualified specialists;
- the existence of ethical and regulatory restrictions on the use of smart systems.

The smart systems integration into the public sector involves significant initial costs for the development, testing, implementation and technical support of the relevant solutions. An additional limiting factor is the shortage of highly qualified specialists in the fields of data analysis, AI and cybersecurity. Organisational and psychological factors also act as barriers – staff mistrust of automated systems, fears of changes to the organisation staffing structure, and a reluctance to adapt to new technological approaches. Despite this, the human factor remains a key element, although its role is gradually transforming. Human functions are shifting from operational management and routine information processing to strategic control, data interpretation and managerial decision-making. Intelligent technologies should be viewed not as a replacement for humans, but as a tool to enhance their analytical and managerial capabilities, allowing them to focus on strategic thinking, the moral and ethical assessment of decisions, and responsibility for their consequences. So, the strategy for the CI intellectualization must provide for the existing management systems phased transformation, human resources development, and the mechanisms for continuous personnel training and adaptation to new technological operating conditions establishment.

Using smart tools for resilience support requires consideration their benefits and the associated risks. Over-reliance on AI systems, which may malfunction or fail to perform their intended functions, can lead to serious disruptions in the CI operation, particularly where they are deeply integrated with sensitive infrastructure components. Additional risks are associated with shortcomings in the deployment, operation and maintenance of AI systems, as well as with an insufficient understanding of their capabilities and limitations.

Recognising both the potential and the risks associated with AI, international organisations and governments are actively developing regulatory and methodological measures. The European Union Agency for Cybersecurity (ENISA) has developed recommendations for the safe integration of AI, emphasising the need to prevent manipulation, cyberattacks and other threats. The European AI Act introduces a risk-based approach to the AI using, providing for the classification of systems by risk level and establishing requirements for algorithm transparency, personal data protection and the principles of ‘trustworthy AI’. The US National Institute of Standards and Technology

(NIST) has proposed a framework for AI risk management, whilst the ISO/IEC 42001 standard sets out requirements for AI management systems, including aspects of cybersecurity, regulatory compliance, ethical risks and algorithmic bias. International standardisation initiatives such as "The technical standardisation of AI" is carried out at international level in ISO/IEC JTC 1 SC 42 (ISO/IEC JTC 1/SC 42 - Artificial intelligence) and at European level in CEN/CENELEC JTC 21 (https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/). They serve as a solid foundation for harmonising global practices, although the main challenge remains ensuring their adoption and compliance by all countries.

Some countries are supplementing their own regulatory mechanisms. Australia's Department of Industry, Science and Resources has published a Voluntary AI Safety Standard, which sets out principles for safe and reliable interaction with AI systems. South Korea has officially adopted the world's first comprehensive AI law – the 'Framework Act on Artificial Intelligence' [7] – which mandates human oversight in high-risk sectors such as healthcare, energy, nuclear safety, water supply, transport and financial services.

A framework for the AI implementation in CI has been developed in the US, which sets out principles of 'security by design', model risk assessment and ensuring transparency in their application [1,6]. Cloud and computing infrastructure providers are encouraged to implement robust access management and physical security for data centres powering AI systems, to support customers and processes beyond the development of AI, by monitoring for anomalous activity and establishing clear channels for reporting suspicious and malicious activity. AI developers must assess the harmful potential of AI models and ensure that the models align with human-centred values, and implement robust privacy practices; conduct assessments to identify potential biases, failure modes and vulnerabilities; and support independent evaluations of models that pose an elevated risk to CI. CI owners and operators are recommended to adopt a range of practices focused on the deployment of AI systems, including supporting cybersecurity, taking into account AI-related risks, protecting customer data, and ensuring significant transparency regarding the AI use.

Consequently, the smart tools application requires the integration of AI-specific risk management mechanisms into security systems of CI facilities, in particular, to ensure human oversight of the AI systems operation, maintain a high level of cybersecurity and data protection, and conduct continuous monitoring and assessment of the smart systems impact on the CI functioning.

8. Conclusions

An analysis of current trends in the CI design and development showed the active integration of intelligent tools, which significantly expands the capabilities for supporting CI resilience through the use of predictive, preventive and partially autonomous control mechanisms.

The generalized scheme for supporting CI resilience proposed in this work provides the structuring and ranking of intelligent tools, AI methods and corresponding software and hardware implementations in accordance with the structural and functional levels of CI operation. This approach allows us to clearly present integration and interaction of intelligent technologies within an infrastructure system, ensures their more informed application, and reduces the risks of failures, compromise or unauthorised interference.

Declaration on Generative AI

During the preparation of this work, the authors used GPT-5.3 in order to Grammar and spelling check. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

1. O. Dodonov, O. Gorbachyk, M. Kuznietsova Methods and Means of Ensuring the Functional Stability of Information Systems of Critical Infrastructures// Selected Papers of the XXIУ International Scientific and Practical Conference "Information Technologies and Security" (ITS 2024), Kyiv, Ukraine, December 19, 2024, pp.1-13; URL: http://ceur-ws.org/Vol-4068/
2. I. Dorohyi, V. Kravchuk, V. Tsurkan Generative AI for critical information infrastructure protection URL:https://ipme.kiev.ua/wp-content/uploads/2025/12/91-2025.pdf
3. Critical infrastructure resilience and artificial intelligence. URL: https://ec.europa.eu/newsroom/cipr/items/884567/en
4. Artificial intelligence (AI) market size worldwide from 2020 to 2030 (in billion U.S. dollars), Statista, Nov. 28, 2024. URL: https://www.statista.com/forecasts/1474143/globalai-market-size
5. Factsheet for Critical Infrastructure, Artificial Intelligence in Critical Infrastructure, June 2025, URL: https://www.cisc.gov.au/
6. USA Framework for AI deployment in Critical Infrastructure URL: https://ec.europa.eu/newsroom/cipr/items/859767/en
7. South Korea launches landmark laws regulate AI. URL: https://www.reuters.com/world/asia-pacific/south-korea-launches-landmark-laws-regulate-ai-startups-warn-compliance-burdens-2026-01-22/
8. L. Floridi The Ethics of Artificial Intelligence. Oxford University Press, 2023.
9. Artificial Intelligence: Achievements, Challenges and Risks. International Scientific Conference, URL: https://www.ipai.net.ua/docs/ai_conf_15.03.2024.pdf