https://doi.org/10.31891/csit-2025-2-3
UDC 004.7

ANDRIEIEV Dmytro, LYHUN Oleksii, DROZD Andriy
Khmelnytskyi National University
PONOCHOVNA Olena
Poltava State Agrarian University

MONITORING SYSTEM FOR CRITICAL INFRASTRUCTURE OBJECTS BASED ON DIGITAL TWINS

Critical infrastructures are fundamental to the seamless operation of modern societies, encompassing sectors such as energy, healthcare, transportation, and communications. Ensuring their reliability, performance, continuous operation, safety, maintenance, and protection is a national priority for countries worldwide.

The digital twins play a crucial role in critical infrastructure, as they enhance security, resilience, reliability, maintenance, continuity, and operational efficiency across all sectors. Among the benefits offered by digital twins are intelligent and autonomous decision-making, process optimization, improved traceability, interactive visualization, and real-time monitoring, analysis, and prediction. Furthermore, the study revealed that digital twins have the capability to bridge the gap between physical and virtual environments, can be used in combination with other technologies, and can be integrated into various contexts and industries.

The use of digital twins was explored as the foundation for developing a modern monitoring system for critical infrastructure facilities enables multi-level assessment of asset conditions in real time, ensuring precise threat detection, anomaly identification, and timely decision-making. Integration with artificial intelligence and big data technologies allows not only the collection and analysis of large volumes of information but also the creation of adaptive behavioral models for systems in emergency situations. Special attention was given to the method of optimizing critical IT infrastructure using digital twins, which combines virtual modeling, predictive algorithms, and automated management. The proposed approach enhances the reliability of digital systems, minimizes downtime, optimizes maintenance costs, and strengthens cybersecurity. This system is especially relevant in the context of growing risks and increasing demands for the stability of strategically important infrastructure assets.

The application of digital twins for monitoring and optimizing critical infrastructure demonstrates considerable potential for improving its resilience, safety, and operational efficiency. The approaches discussed in the study confirm the relevance of implementing digital models as tools for timely risk identification, failure prediction, and informed decision-making. By integrating such technologies, organizations can reduce operational costs, minimize downtime, and improve the overall stability of infrastructure operations. Therefore, digital twins represent a vital step toward the digital transformation and modernization of mission-critical systems across various sectors.

Keywords: digital twins, critical infrastructure, cybersecurity

АНРДЄЄВ Дмитро, ЛИГУН Олексій, ДРОЗД Андрій
Хмельницький національний університет
ПОНОЧОВНА Олена
Полтавський державний аграрний університет

СИСТЕМА МОНІТОРИНГУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ЦИФРОВИХ ДВІЙНИКІВ

Критична інфраструктура є основою безперебійного функціонування сучасного суспільства, охоплюючи такі сектори, як енергетика, охорона здоров'я, транспорт і зв'язок. Забезпечення їхньої надійності, продуктивності, безперервної роботи, безпеки, обслуговування та захисту є національним пріоритетом для країн усього світу.

Цифрові двійники мають вирішальне значення для критичної інфраструктури, адже вони сприяють підвищенню безпеки, стійкості, надійності, обслуговування, безперервності та ефективності роботи інфраструктури в усіх секторах. Серед переваг, які пропонують цифрові двійники, можна виділити інтелектуальне та автономне прийняття рішень, оптимізацію процесів, покращену трасованість, інтерактивну візуалізацію, а також можливості для моніторингу, аналізу та прогнозування в режимі реального часу. Крім того, дослідження показало, що цифрові двійники здатні усувати розрив між фізичним і віртуальним середовищами, можуть використовуватися разом із іншими технологіями та інтегруватися у різноманітні контексти й галузі. Застосування цифрових двійників, як основи для створення сучасної системи моніторингу об'єктів критичної інфраструктури, дозволяє здійснювати багаторівневу оцінку стану об'єктів у реальному часі, забезпечуючи високоточне виявлення загроз, виявлення аномалій та своєчасне прийняття рішень. Інтеграція з технологіями штучного інтелекту та великих даних дозволяє не лише збирати та аналізувати великі обсяги інформації, а й створювати адаптивні моделі поведінки систем у надзвичайних ситуаціях. Особливу увагу приділено методу оптимізації критичної IT-інфраструктури за допомогою цифрових двійників, що поєднує віртуальне моделювання, алгоритми прогнозування та автоматизоване управління. Запропонований підхід забезпечує підвищення надійності цифрових систем, мінімізацію часу простоїв, оптимізацію витрат на обслуговування та підвищення рівня кіберзахисту. Така система є надзвичайно актуальною в умовах підвищених ризиків та вимог до стабільності роботи стратегічно важливих об'єктів інфраструктури.

Застосування цифрових двійників для моніторингу та оптимізації критичної інфраструктури демонструє значний потенціал у підвищенні її стійкості, безпеки та функціональної ефективності. Розглянуті в дослідженні підходи підтверджують актуальність впровадження цифрових моделей як інструменту для своєчасного виявлення ризиків, прогнозування відмов і прийняття обґрунтованих управлінських рішень. Завдяки інтеграції таких технологій можна досягти зниження експлуатаційних витрат, зменшення часу простоїв та підвищення загальної стабільності роботи інфраструктури. Таким чином, цифрові двійники є важливим кроком на шляху до цифровізації та модернізації критично важливих систем у різних секторах.

Ключові слова: цифрові двійники, критична інфраструктура, кібербезпека

Introduction

Critical infrastructure encompasses both virtual and physical assets, systems, and processes, integrating technological advancements to function seamlessly across various domains. As a fundamental component of modern societies, critical infrastructure is vital for ensuring reliable, secure, and efficient operations that underpin economic prosperity and social well-being. Its definition evolves in response to societal changes to maintain community functionality and welfare. Given its essential role in a sustainable future, maintaining the resilience and continuous operation of critical infrastructure, even amid complex challenges and threats, is imperative. Cybersecurity concerns, including risks and vulnerabilities, are significant, as critical infrastructure often becomes a target for cyberattacks. Consequently, enhancing the security, availability, resilience, continuity, and performance of critical infrastructure has become an urgent national priority for many countries.

Related works

Critical infrastructure forms the backbone of contemporary society, encompassing[1, 2] sectors like energy, transportation, water supply, communications, and healthcare. The seamless operation of these sectors is vital for national security, economic stability, and public safety. However, they are susceptible to various threats, including natural disasters, cyberattacks, human errors, and deliberate sabotage. Consequently, effective monitoring[3, 4] is essential for risk mitigation and ensuring resilience.

Significance of Continuous Monitoring. Implementing continuous monitoring for critical infrastructure offers several key benefits:

- ✓ Proactive Threat Detection: Identifies potential issues before they escalate, enabling timely preventive measures.
- ✓ Enhanced Operational Efficiency: Maintains optimal system performance, reducing downtime and maintenance expenses.
- ✓ Regulatory Compliance and Reporting: Facilitates adherence to standards and simplifies accurate documentation.
- ✓ Improved Incident Response: Allows for swift reactions to emergencies, minimizing adverse impacts.
- ✓ Informed Resource Allocation: Supports data-driven decisions regarding resource distribution and investment strategies

Deploying robust monitoring systems is imperative to protect critical infrastructure and uphold societal well-being.

Advancements in technology are revolutionizing the monitoring of critical infrastructure (CI) through several key innovations:

1. Internet of Things (IoT): The integration of IoT devices facilitates the deployment of extensive sensor networks, delivering real-time data on various operational parameters.
2. Artificial Intelligence (AI) and Machine Learning (ML): AI and ML algorithms enable the analysis of large datasets, identification of patterns, and prediction of potential failures, enhancing proactive maintenance strategies.
3. Cloud Computing: Cloud platforms provide scalable and cost-effective solutions for data storage, processing, and analysis, supporting the efficient management of CI monitoring systems.
4. Digital Twins: These virtual representations of physical assets allow for simulation and maintenance forecasting, improving operational efficiency and asset management.
5. 5G and Edge Computing: The implementation of 5G networks and edge computing technologies ensures faster data transmission and processing, facilitating real-time monitoring and control of critical infrastructure.

These emerging technologies collectively enhance the resilience, efficiency, and security of critical infrastructure monitoring systems. A digital twin serves as a virtual counterpart[5, 6] to a physical asset or system, leveraging data to emulate its performance and behavior. In recent years, digital twins have gained prominence, particularly within critical infrastructure sectors. In critical infrastructure contexts, digital twins offer precise representations of current system states and potential future scenarios, enabling operators to enhance operational efficiency and reduce risks. This discussion delves into the applications of digital twins in critical infrastructure[7].

Digital twins offer several advantages[8, 9], including:

1. Intelligent and autonomous decision-making.
2. Process optimization.
3. Enhanced tracking.
4. Interactive visualization and monitoring.
5. Real-time analysis and forecasting.

Digital twins have the capability to bridge the gap between physical and virtual environments, collaborate with other technologies, and integrate into various sectors

Critical infrastructure comprises virtual and physical assets, systems, and processes that leverage technological advancements for seamless integration and operation across different domains. It is an integral part of

modern societies, which are increasingly dependent on it. The definition of critical infrastructure evolves in response to the need for reliable, secure, and efficient functioning of communities, economic development, and social well-being. Given that critical infrastructure is essential for a sustainable future, ensuring its resilience and continuous operation, even under challenging conditions and threats, is crucial. Cybersecurity issues, risks, and vulnerabilities pose serious challenges to critical infrastructure, as it often becomes a target for cyberattacks. Therefore, enhancing the security, availability, resilience, continuity, and efficiency of critical infrastructure is an urgent national priority for many countries.

As digital twins are data-driven and accurate virtual replicas[10] of real-world objects, they bridge the gap between physical and virtual environments and can be utilized across various contexts and domains. By receiving input from physical objects and leveraging their diverse dimensions and capabilities, digital twins facilitate the optimization of services, products, and devices. They also enhance cybersecurity through continuous real-time monitoring.

Digital twins exhibit essential attributes such as domain specificity, synchronization, autonomy, and self-evolution. They are characterized by communication capabilities[11, 12], unique identifiers, integration of actuators and sensors, artificial intelligence, security and privacy measures, trustworthiness, and virtual representation. These features facilitate their application across various sectors. Technologies enabling digital twins include augmented reality, robotics, haptic devices, data-driven modeling, machine vision, cloud computing[13, 14], tactile internet, 5G networks, artificial intelligence, and the Internet of Things. The implementation of digital twins holds the potential to enhance the safety, resilience, continuity, and functionality of critical infrastructure across all sectors.

Digital twins can be applied across various sectors, enhancing processes and delivering numerous benefits. In the context of built environments, they assist in the planning, construction, operation, and maintenance of assets. However, successful integration[15, 16] necessitates meticulous attention to tasks, security protocols, data preservation, and temporal factors, especially when dealing with critical infrastructure.

The foundation of digital twin technology lies in the integration of three fundamental components:

1. Physical Entity: A real-world infrastructure element, such as a bridge or power plant, equipped with sensors that monitor critical parameters like temperature, strain, vibration, and pressure.
2. Comprehensive Virtual Model: A detailed digital representation created using simulation software and physical modeling techniques, such as finite element analysis.
3. Secure Data Transmission Channels: Reliable pathways that facilitate seamless real-time data flow from the physical sensors to the digital model.

Advanced analytics systems and machine learning algorithms process these data streams to predict future behavior, detect anomalies, and identify potential failures before they occur.

Implementing extensive sensor networks integrated with the Internet of Things (IoT)[17, 18] is a fundamental approach to monitoring critical infrastructure through digital twins. These sensors gather real-time operational data, which is transmitted to the digital model, facilitating continuous monitoring and analysis. For example, in civil engineering, sensors such as accelerometers, strain gauges, and fiber-optic devices can be installed on bridges and buildings to monitor structural health. Similarly, in energy systems, smart meters and SCADA[19, 20] systems collect data to oversee grid performance and anticipate operational failures. This integration enables engineers and decision-makers to swiftly detect and address potential issues, thereby enhancing the safety and resilience of critical infrastructure. Digital twins employ modeling tools that utilize sensor input to create real-time representations of an object's state. Two key methodologies include:

1. Physics-Based Modeling: Utilizing finite element analysis[21, 22] (FEA) or statistical finite element methods to predict stress distribution, fatigue, and potential failure points. These modeling techniques are particularly beneficial in civil engineering applications.
2. Machine Learning and Artificial Intelligence: Advanced algorithms[23, 24, 25] process historical and real-time data to forecast future conditions, schedule maintenance, and optimize operations. Machine learning techniques, particularly anomaly detection methods, can identify subtle patterns in sensor data that may signal early signs of equipment degradation or potential cyberattacks. This proactive approach enables timely interventions, thereby enhancing the safety and reliability of critical infrastructure.

A method for optimizing critical IT infrastructure with digital twins

A digital twin is a virtual model of a physical IT system that accurately reflects its structure, behavior, and dynamics in real time. It functions as an interactive digital replica of servers, networks, storage systems, and other key components, allowing for experimentation, simulation, and optimization without impacting the real environment.

A digital twin is a virtual model of a physical IT system that accurately reflects its structure, behavior, and dynamics in real time. It functions as an interactive digital replica of servers, networks, storage systems, and other key components, allowing for experimentation, simulation, and optimization without impacting the real environment.

The main purpose of using digital twins is optimization.

Stages of the digital twin optimization method in a critical information structure (Fig. 1)

1. Collecting and processing data from the physical infrastructure

The goal is to get a complete, up-to-date and detailed picture of the state of all components of the IT system.

What it includes: Collecting telemetry data from all sources: servers, routers, switches, storage systems (storage), power supplies, cooling systems. Monitoring of key metrics: CPU, RAM, disk I/O, bandwidth utilization, component temperature, power consumption, latency. Detecting load patterns, anomalies, incident rates, seasonal fluctuations.

Tools: Monitoring systems: Zabbix, Prometheus, Grafana. Data collection agents: Telegraf, Collectd. Log processing systems: ELK Stack, Graylog. Data access protocols: SNMP, IPMI, Redfish, REST API.

The result is the formation of a structured data stream for building an accurate digital display.

2. Building and updating the digital model

The goal is to create an up-to-date digital copy (Digital Twin) that reflects the physical infrastructure with maximum accuracy.

This includes: Virtualization of all physical and logical components: servers, VMs, storage, network topology, management systems. Taking into account the specifications of each element: failure rate, temperature limits, delay lines, dependencies between modules. Continuous synchronization of the digital model with the physical network: via APIs, agents, or direct connections to control systems.

Tools: Digital twin platforms: Siemens NX, AnyLogic, Azure Digital Twins, IBM Maximo. CAD/CAE models, emulators and emulation environments (GNS3, EVE-NG - for the network part). Integration tools: OPC UA, MQTT, REST.

3. Analysis of the current state of the system

The goal is to identify problem areas and assess the effectiveness of the current operation.

What it includes: Building key metrics: average load, peak activity, availability, average response time, latency, resource utilization. Identification of bottlenecks - system segments that limit overall performance. Visualization of the risk zone, excessive redundancy, or vice versa - critical underload.

The result is the creation of an informed basis for modeling scenarios and selecting optimization areas.

4. Scenario modeling

The goal is to predict how the infrastructure will behave under different conditions.

This includes: Running What-if scenarios: switch failure, traffic spike, cyber incident, server hardware upgrade. Stress load simulation: DDoS simulation, 500% increase in requests in a short period of time, disconnection of selected clusters. Testing the impact of changes: for example, how moving virtual machines between data centers will affect latency.

The result is tested hypotheses about the system's behavior in critical situations without harming the real environment.

5. Application of optimization algorithms

The goal is to find the best architecture and system parameters according to the selected performance criteria.

This includes: Defining the objective function. For example: $Z = \alpha * Response\_time + \beta * Resource\_consumption + \gamma * Failure\_probability$. Application of modern optimization algorithms: Genetic - evolutionary search for the best combinations; Gradient methods - local optimization of parameters; Heuristics/metaheuristics - fast search in the face of incomplete information; Machine learning methods (Supervised, Reinforcement Learning).

Tools: SciPy, TensorFlow, PyTorch, DEAP (genetic algorithms), Optuna, RayTune.

6. Validate the results on a digital model

The goal is to check on the model whether the proposed changes really improve the situation.

What it involves: Running a simulation in an optimized configuration. Comparison of KPIs before and after: response time, utilization, power consumption, availability. Assessment of new risks: creation of new conflicts, increased load on neighboring components.

The result is confirmation that the chosen solution is stable and effective.

7. Implementation of changes in the real environment

The goal is to integrate the optimized model into the real infrastructure.

This includes: Implementation of changes through automation systems: Ansible, Puppet, Chef, Terraform. Performing migration, load balancing, changing service priorities. Monitoring how changes affect the live environment in real time.

Security: changes can be initially implemented in a test or staging environment, and then deployed gradually (canary deployment).

8. Self-learning and adaptation

The goal is to transform the digital twin into a system that adapts to environmental changes on its own.

This includes: Accumulation of historical data for trend analysis. Training of forecasting models: prediction of loads, probability of failure, optimal time for maintenance. Using Reinforcement Learning to automatically make

decisions based on previous experience. Constant updating of the digital model depending on external and internal changes.

As a result, the system becomes adaptive and capable of autonomous self-improvement.

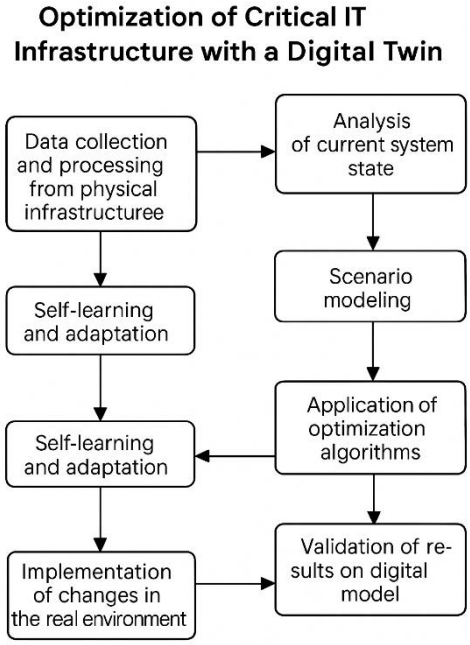

Fig. 1. Optimization of critical IT infrastructure using a digital twin

The method of optimizing critical IT infrastructure using digital twins is a modern approach that combines virtual modeling, real-time analytics, and artificial intelligence algorithms to maximize system efficiency, reliability, and adaptability.

Practical application of the method of optimization of the critical IT infrastructure of NPC "Ukrenergo" using digital twins

Digital twins are playing an increasingly important role in the modernization of critical systems due to their ability to integrate virtual simulations with real-time data from physical objects. Such technologies have great potential for improving resilience to external threats, ensuring cybersecurity, efficient maintenance management, and optimizing overall system performance.

In particular, considerable attention has been paid to the use of digital twins in such industries as

- energy networks, where they help to balance the load, forecast consumption and detect failures;
- transportation infrastructure, for monitoring the condition of roads, bridges, rail systems and predicting their wear and tear;
- water supply and wastewater treatment plants, where digital models can detect leaks, improve service quality, and reduce water losses.

We have developed a study of the practical application of the method of optimizing the critical IT infrastructure of NPC "Ukrenergo" using digital twins, because it is a crucial component of the uninterrupted functioning of the power system, and its reliability directly affects energy security, resilience to cyber threats, and the efficiency of resource management.

1. Building a digital twin of the IT infrastructure of NPC "Ukrenergo"

Objective: to create a virtual model of the company's critical IT infrastructure, which includes network equipment, servers, network management systems, SCADA systems and information gateways.

Tools: the use of digital twin platforms (e.g., Siemens Digital Twin, Ansys Twin Builder, or specialized SCADA-integrated solutions), combined with proprietary monitoring and telemetry collection modules.

Architecture: a combination of a virtual environment with data from physical sensors and real-time event logs.

2. Integration with monitoring and telemetry systems

Data sources: log files, telemetry from network equipment, traffic between servers, access logs.

Purpose: to provide a constant flow of data for validating the digital twin and training optimization and forecasting algorithms.

Data collection tools: Prometheus, Grafana, Zabbix, ELK Stack, or individual agency solutions.

3. Optimization of load distribution

Objective: load balancing between servers and nodes, taking into account current and forecasted loads.

Algorithm: use of gradient methods or genetic algorithms to select the best configuration of virtual machines, distribute requests, and reserve channels.

Result: reduction of overloads, acceleration of request processing, reduction of peak loads on key nodes.

4. Predicting incidents and technical failures

Method: applying machine learning algorithms (e.g., LSTM or Random Forest) to detect anomalies based on historical data.

Role of the digital twin: testing hypothetical failure scenarios without risking the real system.

Practical benefit: timely warning of possible incidents, which allows for planning preventive actions.

5. Testing new solutions and changes in an isolated environment

Example: before implementing new cybersecurity policies, software updates, or architecture changes, all changes are tested on a digital twin.

Benefits: minimizing the risk of downtime and conflicts, ensuring the safety of changes without interfering with the operation of the productive system.

6. Energy efficiency and resource consumption management

Model: a digital twin records the energy consumption of each node of the IT infrastructure.

Optimization: Implementation of adaptive energy management, such as shutting down backup servers during off-peak hours or transferring tasks to less busy data centers.

Result: reduction of energy consumption by up to 15-25% in certain segments.

7. Improving cybersecurity

Role of a digital twin: used as a testing ground for cyberattack scenarios and to evaluate the effectiveness of countermeasures (e.g., DDoS, intrusions, data substitution attempts).

Tools: simulating attacks, collecting statistics, training detection algorithms.

Practical effect: improved incident preparedness, development of response plans, reduction of the risk of compromising critical nodes.

8. Intelligent control of the entire system

Concept: automated decision-making based on data from a digital twin.

Example: the system decides independently which processes should be moved, which servers should be restarted or which policies should be tightened.

Platforms: AIOps (Artificial Intelligence for IT Operations) combined with a digital twin.

To study the application of digital twins of critical infrastructure in practice in more depth, we developed a pilot project: Digital twin of the IT infrastructure of NPC “Ukrenergo”.

The goal is to create a digital copy of NPC “Ukrenergo's” IT infrastructure that

- integrates real data from SCADA, network devices and servers;
- ensures continuous monitoring, simulation of incident scenarios and optimization of work;
- supports detection of failures and cyber threats;
- allows you to experiment with updates and changes without harming the live infrastructure.

Components of a digital twin

The central core of the digital twin: Object-oriented representation of IT assets (servers, networks, gateways, SCADA). Simulation core (based on physical and information models). Event and trigger handler (anomalies, overloads, intrusions).

Integration with physical sources: SNMP, NetFlow for network devices (switches, routers). SCADA protocols: Modbus, DNP3, IEC 61850. Server-based monitoring agents: Zabbix, Prometheus, psutil.

Information gateways (DMZ / API): Proxies for collecting data from external systems. Secure MQTT/REST APIs for integration with the digital core.

Analytical and forecasting modules: Anomaly detection algorithms (ML/AI).

Load and service forecasting. Cyber threat simulators.

Visualization and Dashboard: Grafana, Siemens Twin Viewer, or your own UI. 3D/2D object models, heat maps, network topology.

Digital twin architecture (Fig. 2)

Tools and platforms:

- Siemens NX & Mindsphere, Ansys Twin Builder, Altair SmartWorks - for complex digital modeling.
- Zabbix / Prometheus / Grafana - for collecting metrics, logs, and monitoring.
- Python + FastAPI + Pandas + scikit-learn - for analytics, event processing, and API development.
- Node-RED / MQTT / OPC-UA - for data flows between SCADA and digital twin.
- Docker / Kubernetes - for virtualization and flexible deployment.

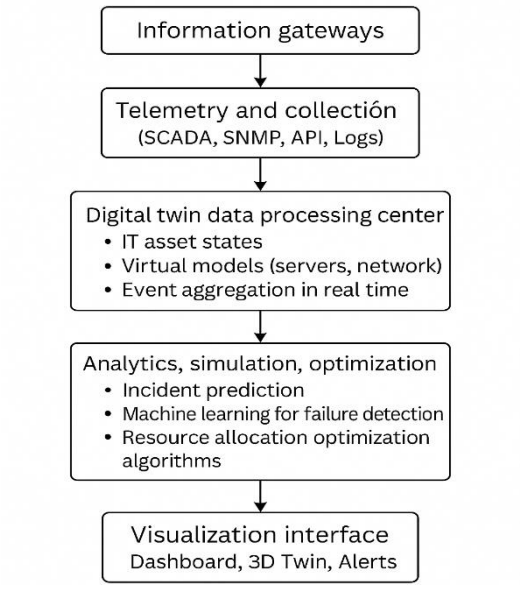

Fig. 2. Digital twin architecture

Example of application scenarios:

- Predicting SCADA server overload based on historical CPU/IO trends.
- Simulation of an attack on an IEC 104 gateway - checking the actions of a digital twin, recovery plan.
- Automatic optimization of traffic routing between regional data centers in real time.
- Simulation of planned software updates - assessing the impact without affecting the main network.
- Early detection of cyber threats through a digital agent that analyzes network behavior.

Let us consider an example that demonstrates the level of overload of the IT infrastructure network of NPC "Ukrenergo" for 8 weeks:

Without digital twins - overload accumulates, problems are detected late.
With digital twins - problems are identified early, the level stabilizes.

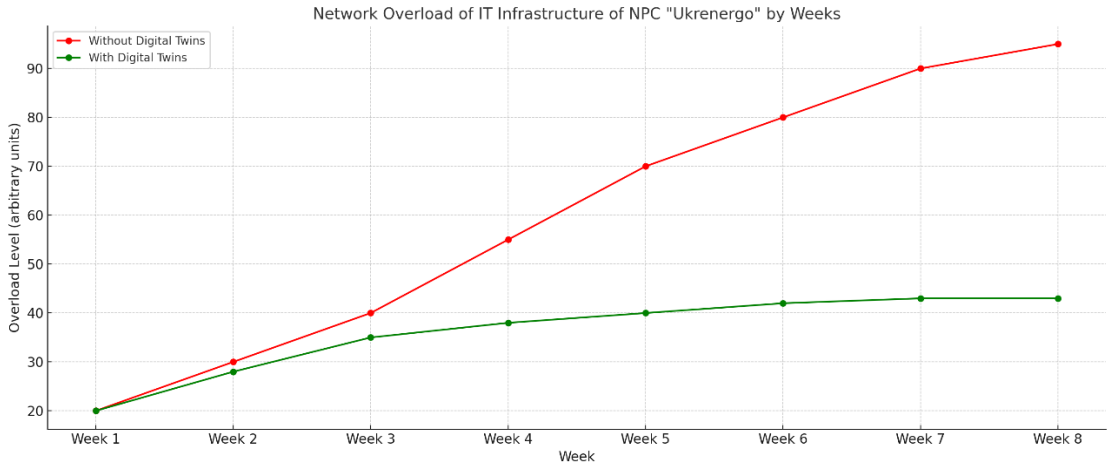

Fig. 3. Network overload of IT infrastructure of NPC "Ukrenergo" by weeks

The graph below clearly demonstrates the comparative dynamics of detecting overload problems in the IT infrastructure of NPC "Ukrenergo" using two approaches: traditional - without the use of digital twins, and innovative - with their use. During the first weeks, the level of overload in the systems without digital twins gradually increases, while the detection of deviations is delayed, which leads to the accumulation of critical problems, reduced stability and increased risk of failures. During peak periods, the system cannot cope with the load, which can lead to disruption of service continuity and cybersecurity threats.

In contrast, when digital twins are used, a proactive response is observed: at the initial stages of problem development, the digital model identifies signs of overload, analyzes the causes, and allows you to make decisions to eliminate them before they become critical. As a result, the load level stabilizes, avoiding peak values ensures business continuity, and the reliability and resilience of critical IT infrastructure is significantly increased.

Digital twins are not only a monitoring tool, but also a forecasting and optimization tool that allows you to move from reactive to preventive management of critical facilities. This significantly reduces risks, saves resources, and ensures the safe operation of IT infrastructure in the face of today's challenges.

Thus, the development of a digital twin of NPC "Ukrenergo's" IT infrastructure demonstrates the powerful potential of modern digital technologies to improve the efficiency, reliability and cyber resilience of critical energy systems. Integration of real-time data with the virtual environment allows for continuous monitoring of equipment status, timely detection of anomalies, forecasting failures, optimization of resource allocation, and testing scenarios in a secure digital environment.

This approach reduces operating costs, minimizes the risk of failure, and improves operational management of the infrastructure, which is extremely important for the stable operation of the national energy system in the face of modern cyber threats and increased reliability requirements. Digital twins open up new horizons for the transformation of the energy sector and the digitalization of Ukraine's strategic enterprises.

Conclusions

Digital twins are a key technology for improving the efficiency and security of critical infrastructure. They provide an accurate real-time representation of the state of objects, enabling analysis, forecasting, and process optimization without the need for physical system intervention. Through integration with the Internet of Things (IoT), artificial intelligence (AI), cloud computing, and edge computing, digital twins contribute to advanced monitoring and infrastructure management in real time.

One of the main advantages of digital twins is their ability to autonomously make decisions, minimizing human error and enhancing rapid response to potential threats. Implementing this technology allows for failure prediction, maintenance optimization, and risk reduction of cyberattacks. Additionally, digital twins play a significant role in improving infrastructure security and resilience, ensuring quick responses to potential disruptions and maintaining the continuous operation of critical facilities.

The application of digital twins in infrastructure sectors such as transportation systems, energy complexes, water supply, and healthcare enhances their efficiency and longevity. The use of machine learning methods and big data analysis enables the identification of hidden patterns, allowing for the prediction of potential failures and the prevention of emergency situations. Furthermore, virtual models provide a safe environment for testing new development scenarios without risks to real infrastructure.

However, for the full integration of digital twins, it is necessary to address cybersecurity, data protection, and technology standardization issues. Reliable encryption mechanisms, access control, and compliance with international standards play a critical role in the secure deployment of this technology.

The method of optimizing critical IT infrastructure using digital twins is an innovative approach that combines the capabilities of virtual modeling, real-time analytics, and artificial intelligence to enhance system efficiency, reliability, and adaptability. This method enables organizations to reduce the likelihood of downtime, utilize resources more effectively, strengthen fault tolerance, and improve the overall performance of critical IT systems.

The development of a digital twin of the IT infrastructure of NPC "Ukrenergo" demonstrates the significant potential of modern digital technologies in enhancing the efficiency, reliability, and cyber resilience of critical energy systems. The integration of real-time data with virtual modeling enables continuous equipment monitoring, timely anomaly detection, failure prediction, and resource optimization in a secure digital environment.

This innovative approach helps reduce operational costs, minimize failure risks, and improve infrastructure management—factors that are crucial for the stable operation of the national energy system amid growing cyber threats. Digital twins are becoming a key tool in the digital transformation of strategic enterprises in Ukraine's energy sector.

Overall, digital twins are a powerful tool for developing critical infrastructure, enhancing its reliability, security, and efficiency. Further research and implementation of this technology will improve infrastructure management mechanisms and ensure its seamless operation in the face of constant threats and changing environmental conditions.

References

1. Gao, J., & Wu, J. (2022). Digital Twins in Critical Infrastructure. Information, 15(8), 454. https://doi.org/10.3390/info15080454
2. Esnoul, C.; Colomo-Palacios, R.; Jee, E.; Chockalingam, S.; Eidar Simensen, J.; Bae, D.-H. Report on the 3rd international workshop on engineering and cybersecurity of critical systems (EnCyCriS-2022). ACM SIGSOFT Softw. Eng. Notes 2023, 48, 81–84. https://doi.org/10.1145/3573074.3573095
3. Ouyang, M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliab. Eng. Syst. Saf. 2014, 121, 43–60. https://doi.org/10.1016/j.ress.2013.06.040
4. Alcaraz, C.; Zeadally, S. Critical infrastructure protection: Requirements and challenges for the 21st century. Int. J. Crit. Infrastruct. Prot. 2015, 8, 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002
5. Rathnayaka, B.; Siriwardana, C.; Robert, D.; Amaratunga, D.; Setunge, S. Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. Int. J. Disaster Risk Reduct. 2022, 78, 103123. https://doi.org/10.1016/j.ijdrr.2022.103123
6. Khan Babar, A.H.; Ali, Y. Framework construction for augmentation of resilience in critical infrastructure: Developing

countries a case in point. Technol. Soc. 2022, 68, 101809. https://doi.org/10.1016/j.techsoc.2021.101809
7. Wells, E.M.; Boden, M.; Tseytlin, I.; Linkov, I. Modeling critical infrastructure resilience under compounding threats: A systematic literature review. Prog. Disaster Sci. 2022, 15, 100244. https://doi.org/10.1016/j.pdisas.2022.100244
8. Chowdhury, N.; Gkioulos, V. Cyber security training for critical infrastructure protection: A literature review. Comput. Sci. Rev. 2021, 40, 100361. https://doi.org/10.1016/j.cosrev.2021.100361
9. Ani, U.P.D.; He, H.; Tiwari, A. Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. J. Cyber Secur. Technol. 2017, 1, 32–74. https://doi.org/10.1080/23742917.2016.1252211
10. Ghorbani, A.A.; Bagheri, E. The state of the art in critical infrastructure protection: A framework for convergence. Int. J. Crit. Infrastruct. 2008, 4, 215–244. https://doi.org/10.1504/IJCIS.2008.017438
11. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. 2001, 21, 11–25. https://doi.org/10.1109/37.969131
12. Brown, G.; Carlyle, M.; Salmerón, J.; Wood, K. Defending critical infrastructure. Interfaces 2006, 36, 530–544. https://doi.org/10.1287/inte.1060.0252
13. Aradau, C. Security that matters: Critical infrastructure and objects of protection. Secur. Dialogue 2010, 41, 491–514. https://doi.org/10.1177/0967010610382687
14. Rehak, D.; Senovsky, P.; Hromada, M.; Lovecek, T. Complex approach to assessing resilience of critical infrastructure elements. Int. J. Crit. Infrastruct. Prot. 2019, 25, 125–138. https://doi.org/10.1016/j.ijcip.2019.03.003
15. Lee II, E.E.; Mitchell, J.E.; Wallace, W.A. Restoration of services in interdependent infrastructure systems: A network flows approach. IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.) 2007, 37, 1303–1317. https://doi.org/10.1109/TSMCC.2007.905859
16. Laplante, P.; Amaba, B. Artificial intelligence in critical infrastructure systems. Computer 2021, 54, 14–24. https://doi.org/10.1109/MC.2021.3055892
17. Groenewold, M.R.; Burrer, S.L.; Ahmed, F.; Uzicanin, A.; Free, H.; Luckhaupt, S.E. Increases in Health-Related Workplace Absenteeism Among Workers in Essential Critical Infrastructure Occupations During the COVID-19 Pandemic-United States, March-April 2020. MMWR Morb. Mortal. Wkly. Rep. 2020, 69, 853–858. https://doi.org/10.15585/mmwr.mm6927a1
18. Jiang, Y.; Yin, S.; Li, K.; Luo, H.; Kaynak, O. Industrial applications of digital twins. Philos. Trans. R. Soc. A Math. Phys. Eng. Sci. 2021, 379, 20200360. https://doi.org/10.1098/rsta.2020.0360
19. Tao, F.; Qi, Q. Make more digital twins. Nature 2019, 573, 490–491. https://doi.org/10.1038/d41586-019-02849-1
20. Batty, M. Digital twins. Environ. Plan. B Urban Anal. City Sci. 2018, 45, 817–820. https://doi.org/10.1177/2399808318796416
21. Stark, R.; Fresemann, C.; Lindow, K. Development and operation of digital twins for technical systems and services. CIRP Ann. 2019, 68, 129–132. https://doi.org/10.1016/j.cirp.2019.04.024
22. Sharma, A.; Kosasih, E.; Zhang, J.; Brintrup, A.; Calinescu, A. Digital twins: State of the art theory and practice, challenges, and open research questions. J. Ind. Inf. Integr. 2022, 30, 100383. https://doi.org/10.1016/j.jii.2022.100383
23. El Saddik, A. Digital twins: The convergence of multimedia technologies. IEEE MultiMedia 2018, 25, 87–92. https://doi.org/10.1109/MMUL.2018.023121167
24. Lampropoulos, G. Artificial intelligence, big data, and machine learning in industry 4.0. In Encyclopedia of Data Science and Machine Learning; IGI Global: Hershey, PA, USA, 2023; pp. 2101–2109. https://doi.org/10.4018/978-1-7998-9220-5.ch125
25. Piras, G.; Agostinelli, S.; Muzi, F. Digital Twin Framework for Built Environment: A Review of Key Enablers. Energies 2024, 17, 436. https://doi.org/10.3390/en17020436

Dmytro Andrieiev **Дмитро Андрєєв**	master's degree student, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: zonex1995@gmail.com https://orcid.org/0009-0002-3524-872X	Магістрант, Хмельницький національний університет, м. Хмельницький, Україна
Oleksii Lyhun **Олексій Лигун**	PhD student, Khmelnytskyi National University, Khmelnytskyi, Ukraine e-mail: oleksii.lyhun@gmail.com https://orcid.org/0009-0004-5727-5096	Аспірант, Хмельницький національний університет, м. Хмельницький, Україна
Andriy Drozd **Андрій Дрозд**	PhD student, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: andriydrozdit@gmail.com https://orcid.org/0009-0008-1049-1911	Аспірант, Хмельницький національний університет, м. Хмельницький, Україна
Olena Ponochovna **Олена Поночовна**	Assistant at the Department of Economics and International Economic Relations, Poltava State Agrarian University, Poltava, Ukraine, e-mail: olena.ponochovna@pdau.edu.ua https://orcid.org/0000-0002-4377-0633	Асистент кафедри економіки та міжнародних економічних відносин, Полтавський державний аграрний університет, м. Полтава, Україна,