Technological process management for cloud-based critical infrastructure under emerging threats and challenges[*]

Tetiana Smirnova[1,*,†] and Oleksandr Dobrynchuk[2,†]

[1] *Central Ukrainian Technical University, 8 University ave, 25000 Kropyvnytskyi, Ukraine*
[2] *State University "Kyiv Aviation Institute," 1 Liubomyra Huzara ave., 03058 Kyiv, Ukraine*

Abstract

In the context of cyber threats, global digitalization, and the need for rapid response to emergencies, there is a need to use modern methods and support models of TP that provide flexibility, scalability, and a high level of reliability. The article analyses CI in Europe, Asia, the USA, and Ukraine. It has been determined that in the context of cyber threats, global digitalization, and the need for rapid response to emergencies, there is a need to use modern methods and support models of TP that provide flexibility, scalability, and a high level of reliability. It was determined that modern TP support is based on a combination of cloud technologies, IIoT, digital twins, big data analytics and cyber protection, CI enterprise management, integrated into a single ICT infrastructure based on modern network protocols. For CI enterprises, the main criterion for selecting IT solutions is to ensure the continuity and stability of TP while meeting the requirements of reliability, security, scalability, and economic efficiency. An objective contradiction has been identified and the task for further research has been formalized, which consists in developing methods and models for supporting TP in the state's CI based on Cloud Technologies that will ensure: increased efficiency and flexibility of TP management; creation of means for multi-parameter monitoring of key performance indicators; improvement of information and communication systems and networks for the automation of production processes; an adequate level of cyber data protection; the formation of holistic approaches, methodologies and recommendations for the implementation of Cloud Technologies in the state's critical infrastructure.

Keywords

critical infrastructure, cloud technologies, technological process, support, cyber threat, monitoring, security

1. Introduction

Recent decades have been characterized by a rapid increase in the complexity and interdependence of TP in state's CI [1–3], affecting all vital areas. The effectiveness of these systems directly affects national security, the economy and social stability. In the context of cyber threats, global digitalization, and the need for rapid response to emergencies, there is a need to use modern methods and support models of TP that provide flexibility, scalability, and a high level of reliability. Cloud Technologies [4, 5] are gradually becoming a key tool for modernizing of CI due to their ability to provide centralized data storage and processing, integration of distributed systems and increased cybersecurity [6]. They enable the implementation of adaptive TP management mechanisms, the application of AI algorithms for analyzing large data sets [7], and the creation of models for predicting risks and incident development scenarios. This opens up new opportunities for building intelligent DSS in CI. At the same time, the introduction of Cloud Technologies in CI is accompanied by a number of challenges, including ensuring confidentiality, integrity, data availability, compatibility with existing ACSs, and compliance with international standards. Therefore, an important task of modern scientific research is to systematize and analyze existing approaches, models, and methods of supporting TP based on cloud technologies in order to identify their advantages, limitations, and prospects for further development.

[*] *CPITS-II 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2025, Kyiv, Ukraine*
[*] Corresponding author.
[†] These authors contributed equally.

sm.tetyana@gmail.com (T. Smirnova); dobrynchuk85@icloud.com (O. Dobrynchuk)
0000-0001-6896-0612 (T. Smirnova); 0009-0002-2877-844X (O. Dobrynchuk)

2. Critical infrastructure in Europe, Asia, the United States, and Ukraine: concept, structure, threats, and challenges

Critical infrastructure is generally understood to refer to systems, networks and services whose failure would have a significant impact on security, the economy, health or the well-being of the population. Recent approaches have seen a noticeable evolution from purely ‘object-based’ protection to risk management for interconnected cyber-physical systems and their supply chains.

For example, in the *United States*, this approach has been formalized as a partnership model between the state and operators for 16 specific sectors [8]. In April 2024, the United States issued National Security Memorandum-22 (NSM-22) [9] was issued, replacing PPD-21 and confirming 16 CI sectors, assigning a ‘sector risk management agency’ (SRMA) to each, and emphasizing a move towards minimum mandatory security requirements where voluntary approaches do not work. Practical implementation remains a partnership: CISA coordinates risk assessment, information sharing, and industry guidance for infrastructure operators. The current US model is characterized by stricter regulation, a shift from voluntary to mandatory standards, widespread use of innovation, and an emphasis on collective responsibility of business and government in the field of CI protection. A distinctive feature of this approach is the distributed responsibility model: the government sets framework standards and coordinates responses, but a significant portion of CNI is privately owned, and private companies bear primary responsibility for security. To this end, a system of Information Sharing and Analysis Centers (ISACs) and Public-Private Partnerships (PPPs) has been created to facilitate the exchange of information between the government and businesses.

In *Europe*, the framework is set by two complementary directives: NIS2 (cyber resilience of networks and information systems) [10] and CER (physical/operational resilience of critical entities) [11]. Member States had to transpose NIS2 by 17 October 2024, expanding the scope of ‘essential’ and ‘important’ organizations in sectors ranging from energy and transport to healthcare, water supply, ICT and public administration. The CER Directive applies from October 2024 and requires critical entities in 11 sectors to be identified by July 2026 and to be required to carry out risk assessments and resilience measures.

In *United Kingdom*, the Critical National Infrastructure (CNI) protection system is coordinated at the highest government level through the National Cyber Security Centre (NCSC), which is a division of the GCHQ intelligence service and is responsible for policy development, cyber incident response and support for operators in critical sectors. The CNI covers 13 sectors, including energy, transport, finance, healthcare, water, telecommunications, government services, defense and food security. The legislative framework consists of the Investigatory Powers Act (2016) [12], the UK National Cyber Strategy (2022–2030) [13], and regulations under the National Security and Investment Act (2021) [14], which impose strict requirements for cyber protection, audits, and risk management. The British model is distinguished by a combination of centralized coordination and decentralized responsibility: each CNI operator is required to independently ensure cyber protection in accordance with NCSC requirements, but receives support from the state in the form of methodologies, analytics and cyber intelligence services. An important feature is active interaction with the private sector and the creation of Public-Private Partnerships (PPP) for the exchange of information about threats. In addition, the UK invests in AI/ML and big data systems to predict attacks and improve cyber resilience, and has a strong focus on international cooperation within NATO, the EU (despite Brexit, cooperation in the field of cybersecurity continues) and the Five Eyes. A unique feature of the British approach is its focus on trust and transparency, where CNI operators are required to share real data on cyber incidents with the state, allowing for the development of a joint strategy to counter threats.

Approaches in Asia are diverse, but the trend is similar—critical information infrastructures (CII) and regulatory oversight of operators are prioritized:

- In *Singapore*, the Cybersecurity Act (updated in 2024) [15] establishes a regime for CII operators in 11 sectors (energy, water, healthcare, finance, transport, information communications, government services, security, as well as media and space technology) with CSA agency powers for prevention and response. The Singapore model is based on the principles of strict regulation, technological innovation and partnership with the private sector, with a particular emphasis on the development of national SOCs, early warning systems and the exchange of threat data. An important feature is the integration of cyber defense into the overall Smart Nation development strategy, where AI is seen as the foundation of the digital economy and smart services for the population. A unique feature of Singapore's approach is its proactive cyber resilience policy, which includes cyber attack simulation, mandatory training for public and private entities, and large-scale cybersecurity training programs.
- In *India*, the definition of CII [16] is enshrined in the IT Act 2000 (Section 70) [17]; the national center NCIIPC identifies the areas of energy, telecommunications, banking and financial systems, transport, government networks, space and defense technologies, and healthcare. The Indian model is based on the principles of centralized state control and interagency coordination, but actively involves the private sector in partnerships through mandatory system certification, security audits and incident information sharing. Particular emphasis is placed on the development of national monitoring and response centers (CERT-In), which are responsible for handling cyber incidents, as well as on the development of a regulatory framework, including legislation [17]. A unique feature of the Indian approach is the combination of digital transformation policy with large-scale government programs (Digital India, Smart Cities Mission), where CI is seen not only as an object of protection, but also as the basis for the socio-economic development of the state.
- In *Japan*, CI protection is coordinated at the national level through the National Information Security Strategy Centre (NISC) [18], which reports to the Cabinet Office and is responsible for policy formulation, risk assessment and coordination between government agencies and private operators. Fourteen CI sectors have been officially designated, including energy, transport, finance, information communications, medicine, water supply, government systems, etc. The Japanese model is distinguished by a voluntary-mandatory approach, whereby the state sets framework requirements and recommendations, and private operators are required to implement security measures through self-regulation and partnership mechanisms. An important feature is the close link with the BCP concept, which takes into account both cyber threats and natural disasters (earthquakes, tsunamis), with an emphasis on resilience and recovery of systems after incidents. In addition, Japan is actively introducing AI, IoT and Cloud Technologies into infrastructure monitoring and management, developing pilot projects in the field of smart cities, energy networks and transport systems. All this makes the Japanese CIP model a unique combination of state coordination, private responsibility and technological innovation.
- In *the PRC*, the concept of CII is enshrined in the Cybersecurity Law (2017 [19]) and developed in the Regulations on the Security Protection of Critical Information Infrastructure (2021) [20]. According to these documents, CII covers information systems and services in the fields of public communications, energy, transport, finance, public administration, defense, science and technology, healthcare and others that are important for national security and public welfare. The Chinese model differs from the European and American models in its more centralized and directive nature, combined with a policy of 'cyber sovereignty' that gives the state broad powers to regulate and monitor the entire national cyberspace. From a practical standpoint, the PRC emphasizes the combination of traditional physical security with cyber defense and actively implements AI, Big Data and

Cloud Technologies tools in CI monitoring. This creates a powerful but extremely closed system for international cooperation, reflecting the specifics of the Chinese state management model.

- In *the Republic of Korea*, CI protection is carried out within the framework of a comprehensive national cybersecurity system coordinated by the National Intelligence Service (NIS) and the Ministry of Science and ICT, which are responsible for policies in the areas of cyber defense, cyber incidents and the continuity of strategic facilities. The CI sectors include energy, transport, financial systems, telecommunications, government and defense networks, medicine and manufacturing enterprises, with a strong focus on cyber threats against high-tech and semiconductor industries. The Korean model is characterized by a high level of digital integration: real-time monitoring systems, AI and Big Data are widely used to analyze cyber threats and predict attacks. The legislative framework is provided by the Framework Act on National Informatization [21] and the Act on Promotion of Information and Communications Network Utilization and Information Protection [22], which impose strict requirements on CI operators in terms of cyber protection, auditing and certification. A distinctive feature of the South Korean approach is the combination of strict state regulation with a high level of technological innovation, as well as constant readiness for external cyber threats from North Korea, which shapes a strategy with a strong emphasis on cyber defense, information exchange and resilience to hybrid attacks.
- In *Kazakhstan*, the CI protection system is being developed as part of the state cybersecurity policy 'Cyber Shield of Kazakhstan' [23], which was approved in 2017 and defines strategic directions for countering cyber threats. Coordination is carried out by the Ministry of Digital Development, Innovation and Aerospace Industry together with the National Security Committee, which control the activities of telecommunications operators, state information systems and strategic enterprises. Critical infrastructure includes energy, transport, finance and banking, ICT, DIC and state information resources, for which mandatory cyber protection standards, auditing and licensing of activities in the field of information security are provided. An important feature of the model is the creation of a National Cybersecurity Centre, which is responsible for monitoring and responding to incidents, as well as for the work of the KZ-CERT government response team. Unlike European approaches, Kazakhstan relies on strict regulation and centralized control, including the ability to restrict access to Internet resources in the event of cyber attacks or threats to national security.

In Ukraine, according to [24], 24 sectors of the state's critical infrastructure have been identified (Table 1). The number of subsectors in each sector was indicated, as well as the presence of certain TP.

Table 1
Sectors of critical infrastructure in Ukraine according to current legislation

Sector	Sub-sectors	TP
Fuel and energy sector	7	+
Digital technologies	1	+
Information security	1	+
Food industry and agro-industrial complex	1	+
State material reserves	1	–
Healthcare	5	+

Capital markets and organized commodity markets	1	–
Financial sector	1	–
Transport and postal services	6	+
Life support systems	1	+
Local self-government	1	–
Industry	6	+
Public safety sector	2	+/–
Civil protection of the population and territories	1	+
Environmental protection	3	+/–
Defense sector	1	+
Justice	1	–
Enforcement of criminal penalties, detention and imprisonment of prisoners of war	1	–
State registration	1	–
Scientific research and development	1	+
Financial sector	3	–
Elections and referendums	1	–
Social protection	5	–
Information sector	1	–
State authority	1	–

Given the full-scale aggression of the Russian Federation and its impact on Ukraine's critical infrastructure, the following features of critical infrastructure formation and protection can be identified [25–27]:

Threats:

- A combination of missile and drone strikes, sabotage, cyberattacks, and information operations.
- Main targets: energy (HPP/TPP/WPP/networks), fuel logistics, communications/ICT, transport hubs, water supply, healthcare, state registers, and payments [25].

Resilience:

- Decentralization and dispersion of assets: microgrids/generators, duplicate substations, backup data centers.
- Large-scale backup: diesel/gas and renewable energy sources, autonomous communication nodes (including satellite channels), cross-regional power supply schemes.
- Business continuity planning (BCP) and disaster recovery planning (DRP) as mandatory attributes of CI operators.

Cyber protection:

- OT/ICS segmentation and isolation, 24/7 monitoring (SOC), incident response with purple team practice.

- Zero Trust, multi-factor authentication, vulnerability management, and patch management in shortened cycles.
- Mandatory interaction with national centers (e.g., CERT-like), exchange of indicators of compromise, and rapid incident reporting.
- Supply chain protection: supplier verification, software/PLC update signing, bill of materials (SBOM).

Regulatory framework:

- Transition to risk-based regulation, harmonization with the EU (NIS2/CER, industry standards).
- Identification of "vital" and "important" operators; sectoral supervisory authorities; joint training, audits, stress tests.
- Public-private interaction: data exchange, joint exercises, coordination during crises (energy, cyberattacks, UAV threats).

Operational practices on site:

- Physical perimeter: engineering shelters, modular/mobile solutions, electronic warfare/air defense systems around facilities, video analytics, and thermal imaging surveillance.
- Fail-safe/fail-secure modes for TP.
- Manual procedures in case of SCADA/communication loss.
- Regular TTX and red team exercises, testing of backup routes for power and data lines; staff training [26].

Key challenges:

- Constant depletion of equipment and personnel, shortage of spare parts/transformers, dependence on imports of components for OT/ICT.
- High dynamics of enemy tactics (combining kinetic and cyber), requiring rapid updates of procedures and technologies.

Tasks for CI operators:

- Complete inventory of IT/OT assets and dependency map (including people and suppliers).
- Update threat and impact model, link countermeasures to RTO/RPO.
- Continuous vulnerability assessment/penetration testing, network segmentation, logging, and centralized monitoring.
- Multi-backup: power, communications, computing, data (offline backups + geo-backup).
- Regular training of BCP/DRP, crisis management team communications, interaction with government agencies and related operators.
- Synchronization with the EU, cross-border communication channels, joint CERT/CSIRT mechanisms, CI modernization assistance programs [27].

3. Technological processes at CI of Ukraine

Table 1 identifies the CI sectors (12 out of 24) associated with specific TP. Let us elaborate on the processes themselves:

1. ***Fuel and energy sector:***

- Energy generation: nuclear, thermal, hydro, renewable.

- Transmission and distribution: power grids, substations, dispatch control.
- Extraction and transportation: oil, gas, coal, pipelines.
- Storage and processing: oil depots, refineries, gas storage facilities.
- Monitoring and balancing: SCADA/EMS systems, smart grid.

2. ***Digital technologies:***

- Telecommunications: mobile communications, internet, satellite access.
- Data centers and cloud technologies: processing, storage, and backup.
- National registries and electronic services.
- Critical information systems: e-government, e-services.
- Communication channel protection: encryption, VPN, cyber monitoring.

3. ***Information protection:***

- Information resource management: databases, document flow.
- Protection of state secrets and personal data.
- SOC and CERT operations.
- Response to incidents and cyber threats.
- Implementation of standards.

4. ***Food industry and agro-industrial complex:***

- Agricultural production: crop farming, livestock farming.
- Processing/storage: elevators, cold stores, meat and dairy plants.
- Food logistics: transportation, export, import.
- Food quality and safety control.
- Agrotechnology and smart farm systems (AgroTech, IoT).

5. ***Healthcare:***

- Medical information systems: e-Health, telemedicine.
- Provision of medicines and vaccines: supply chains.
- Sanitary and epidemiological monitoring.
- Emergency response (ambulances, mobile hospitals).

6. ***Transport and postal services:***

- Traffic management: air, rail, metro, maritime transport.
- Safety infrastructure: traffic lights, navigation, signaling.
- Logistics of cargo and postal items.
- Intelligent transport systems.
- Integration with international transport corridors.

7. ***Life support systems:***

- Water supply and sewerage.
- Heat supply and ventilation.
- waste disposal and recycling.
- Monitoring of water, air, and resource quality.

- Backup systems (generators, pumping stations, filtration).

8. ***Industry:***

- Metallurgy, chemistry, mechanical engineering.
- Production lines and automation (MES, SCADA).
- Supply chains and logistics.
- Energy consumption and waste disposal.
- Quality control and ISO/IEC standards.

9. ***Public safety sector:***

- Functioning of the police, State Emergency Service, border guard service.
- 112 and emergency response systems.
- Municipal safety: video surveillance, Safe City.
- Anti-Terrorism and anti-sabotage measures.
- Coordination of actions in crisis situations.

10. ***Environmental protection:***

- Environmental monitoring: water, air, soil, radiation.
- Waste and emissions management.
- Prevention and elimination of natural disasters (floods, fires).
- Eco-energy and carbon footprint reduction.
- Early warning systems (Earth Observation, IoT).

11. ***Defense sector:***

- Troop command and control systems.
- Weapons and military equipment (production, repair, logistics).
- Reconnaissance, cyber and electronic warfare operations.
- Protection of bases, warehouses, facilities.
- Joint training and cooperation with partners (NATO, EU).

12. ***Research and development:***

- State and university research centers.
- Applied R&D in the fields of security, energy, IT, medicine.
- Innovation, science, and industrial parks, startup ecosystem.
- International scientific cooperation (Horizon Europe, NATO SPS, Erasmus).
- Technology transfer and commercialization of innovations.

4. IT solutions to support TP in state information systems

Modern support of TP (including in state critical infrastructure) is based on a combination of cloud technologies (IaaS, PaaS, SaaS, Hybrid Cloud, Edge Cloud, Serverless Computing), IIoT, digital twins, big data analytics (Hadoop, Spark, Power BI, Tableau, Qlik) and cyber security (SIEM, Zero Trust, PQC), CI enterprise management (ERP, MES, APS) integrated into a single ICT infrastructure based on modern network protocols (e.g., 5G/6G technologies) [28].

For CI enterprises, the main criterion for selecting IT solutions is to ensure the continuity and stability of TP while meeting the requirements of reliability, security, scalability, and cost-effectiveness.

5. Methods and support models of TP

Management methods of TP can be represented as an evolutionary scale: from simple controllers (PID) → through optimization models (MPC) → to intelligent ones (AI/ML) → and finally to digital twins and cloud platforms that allow systems to be managed in conditions of uncertainty and cyber risks [29].

Monitoring methods of TP can be represented as a multi-level system:

- Basic level—SCADA/DCS for data collection.
- Analytical level—statistical and ML models for detecting deviations.
- Predictive level—digital twins and AI for predicting the development of situations.
- Infrastructure level—cloud and IoT platforms that provide scalability and integration.

Methods for evaluating TP effectiveness can be divided into three levels:

- Operational level—KPI, OEE, SPC.
- Analytical level—DEA, SFA, multi-criteria models.
- Forecasting and strategic level—digital twins, ML/AI, simulation models that take into account risks and resilience [30].

6. Analysis of problems and unresolved issues

The previous sections of the first chapter of the dissertation analyzed CI in Europe, Asia, the US, and Ukraine (concept, structure, threats, and challenges), modern IT solutions for supporting TP in various sectors of state CI, and methods and models for supporting technological processes in CI. Despite the large number of scientific studies in this area [3–6, 31–34], a number of unresolved issues remain, in particular:

- The lack of effective models for supporting TP using Cloud Technologies.
- The lack of means for multi-parameter monitoring of key indicators of TP efficiency in CI.
- Insufficient number of specialized information and communication systems and networks for the automation of production processes.
- Shortcomings in data security in information and communication systems and networks related to TP in CI.
- Insufficient study of the use of cloud technologies as a basis for supporting TP in CI.
- Lack of comprehensive approaches (standards, recommendations, methodologies) for supporting TP in the state's CI.

7. Formalization of the task for further research

In the field of state critical infrastructure, there is a growing need to ensure the efficiency, stability, and security of critical infrastructure on the one hand [34–37], and a lack of sufficiently developed methods, models, and tools that would integrate the capabilities of cloud technologies to support these processes on the other [38–43]. This contradiction manifests itself between:

- *The practical need* to implement multi-parameter monitoring, automation, and cyber protection of TP in the state's CI.

- and *The scientific and methodological inadequacy* of existing approaches, which do not provide for the comprehensive use of cloud technologies to support such processes.

Thus, the relevance of the topic is determined by the need to overcome this contradiction by developing new methods and models for supporting TP in the state's critical infrastructure based on Cloud Technologies.

In this regard, the task of further research is to develop methods and models for supporting TP in state critical infrastructure based on cloud technologies, which will ensure:

- Increased efficiency and flexibility of TP management.
- Creation of means for multi-parameter monitoring of key performance indicators.
- Improvement of information and communication systems and networks for the automation of production processes.
- An adequate level of cyber data protection.
- The formation of comprehensive approaches, methodologies, and recommendations for the implementation of cloud technologies in the state's critical infrastructure.

The mathematical formalization of the research problem can be expressed as follows:

1. Lack of effective cloud support models: a set of solutions without the use of Cloud Technologies $\Omega_{legacy} \cap R = \varnothing$, i.e., existing models do not meet the requirements of *R*.
2. Lack of effective multi-parameter monitoring: the number of monitored indicators is less than required$q < q_{min}$, and there are no effective models and algorithms.
3. Lack of specialized ICSM for TP automation: characteristics (including those related to security) do not meet the recommended $C \neq C_{req}$ or exceed (are lower than) the limit parameters$l < l_{min} \, V \, l > l_{max.}$
4. Data security shortcomings: probabilities of violation of basic security characteristics $\rho_{conf} > \varepsilon_{conf}$, $\rho_{intgr} > \varepsilon_{intgr,} \, 1 - \alpha > \varepsilon_{avlb}$.
5. Insufficient research on the use of Cloud Technologies for similar tasks: there are no reliable models of dependencies between efficiency $l(r)$, delay $\alpha(r)$, and resource cost$c(r)$.
6. Lack of comprehensive standards and methodologies: the set of rules *S* defining restrictions is incomplete or contradictory:

$$R = s \in S \, R_s ,$$
$$S = \varnothing \, V \, \exists \, s_1 , s_2 : R_{s1} \cap R_{s2} \neq \varnothing .$$

The generalized scientific contradiction can be represented in a formalized mathematical form as follows: the support system of TP in the state's CI must operate efficiently, safely, and continuously $(r_1 , r_2 , \ldots , r_n) \in R$, but in practice (in real conditions) no solutions satisfy the requirements $\Omega_{legacy} \cap R = \varnothing$. Therefore, it is necessary to develop (improve) methods, models, and tools that will allow finding at least one solution$\exists \left(r_1^* , r_2^* , \ldots , r_n^* \right) : \left(r_1^* , r_2^* , \ldots , r_n^* \right) \in R$ (Figure 1).

8. Conclusions

CI in Europe, Asia, the US, and Ukraine was analyzed (concept, structure, threats, and challenges). It was determined that in the context of cyber threats, global digitalization, and the need for rapid response to emergencies, there is a need to use modern methods and models of TP support that provide flexibility, scalability, and a high level of reliability.

It is determined that modern IT support is based on a combination of cloud technologies, IIoT, digital twins, big data analytics and cyber protection,

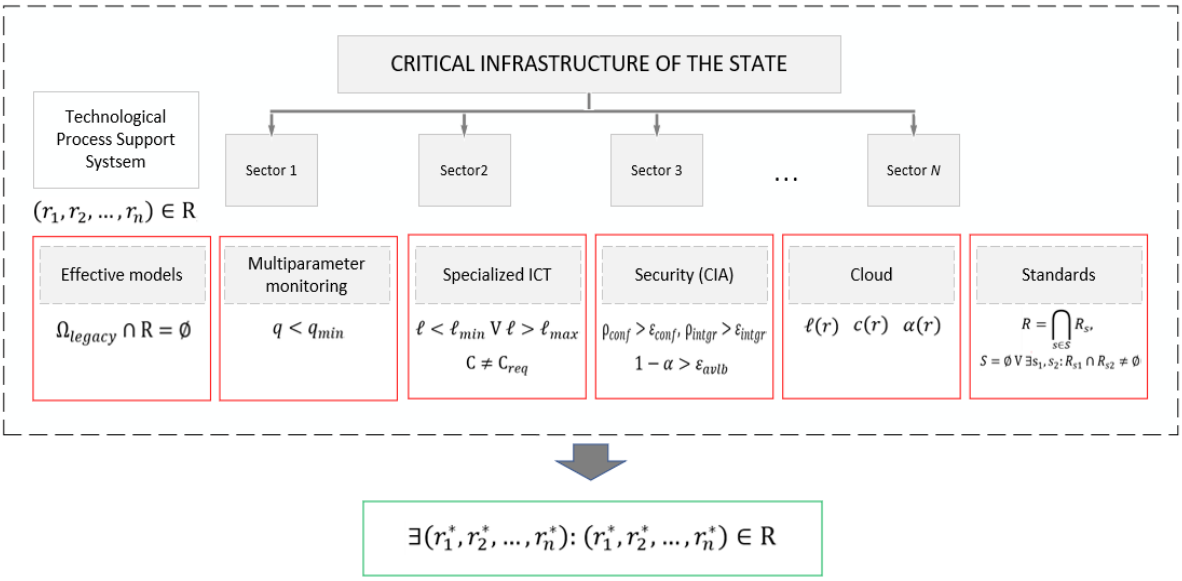
CRITICAL INFRASTRUCTURE OF THE STATE
Technological Process Support Systsem
$(r_1, r_2, \dots, r_n) \in \mathrm{R}$
Sector 1
Sector2
Sector 3
…
Sector N
Effective models
$\Omega_{legacy} \cap \mathrm{R} = \emptyset$
Multiparameter monitoring
$q < q_{min}$
Specialized ICT
$\ell < \ell_{min} \vee \ell > \ell_{max}$
$\mathrm{C} \neq \mathrm{C}_{req}$
Security (CIA)
$\rho_{conf} > \varepsilon_{conf}, \rho_{intgr} > \varepsilon_{intgr}$
$1 - \alpha > \varepsilon_{avlb}$
Cloud
$\ell(r)$ $c(r)$ $\alpha(r)$
Standards
$R = \bigcap_{s \in S} R_s,$
$S = \emptyset \vee \exists s_1, s_2: R_{s1} \cap R_{s2} \neq \emptyset$
$\exists (r_1^*, r_2^*, \dots, r_n^*): (r_1^*, r_2^*, \dots, r_n^*) \in \mathrm{R}$

Figure 1: Schematic representation of contradictions and setting of tasks

CI enterprise management, integrated into a single ICT infrastructure based on modern network protocols. For CI enterprises, the main criterion for selecting IT solutions is to ensure the continuity and stability of TP while meeting the requirements of reliability, security, scalability, and economic efficiency. The main methods and models for supporting (managing, monitoring, evaluating the effectiveness of) technological processes, identified as a result of analyzing modern scientific publications and research projects in the field of TP support in CI, are presented. It has been established that despite the large number of scientific studies in this area, a number of unsolved problems remain.

An objective contradiction has been identified (manifested between the practical need for multi-parameter monitoring, automation, and cyber protection of TP in the state's critical infrastructure and the scientific and methodological inadequacy of existing approaches, which do not ensure the comprehensive use of Cloud Technologies to support such processes) and formalized the task for further research, which consists in developing methods and models for supporting TP in the state's critical infrastructure based on Cloud Technologies, which will ensure: increased efficiency and flexibility of TP management; creation of means for multi-parameter monitoring of key performance indicators; improvement of information and communication systems and networks for the automation of production processes; an adequate level of cyber protection of data; the formation of integrated approaches, methodologies, and recommendations for the implementation of cloud technologies in the state's critical infrastructure.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] O. Potii, Y. Tsyplinsky, Methods of Classification and Assessment of Critical Information Infrastructure Objects, in: 2020 IEEE 11th Int. Conf. Dependable Syst., Serv. Technol. (DESSERT), 2020, 389–393. doi:10.1109/DESSERT50317.2020.9125028

[2] S. Gnatyuk, et al., The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems, in: 2nd Int. Workshop on Intelligent Information Technologies and Systems of Inf. Security, vol. 3156, 2022, 390–399.

[3] S. Toliupa, I. Parkhomenko, H. Shvedova, Security and Regulatory Aspects of the Critical Infrastructure Objects Functioning and Cyberpower Level Assessment, in: 3rd Int. Conf. Adv. Inf. Commun. Technol. (AICT), 2019, 463–468. doi:10.1109/AIACT.2019.8847746

[4] M. Habiba, M. Criveti, Hybrid Cloud Infrastructure and Operations Explained: Accelerate Your Application Migration and Modernization Journey on the Cloud with IBM and Red Hat, Packt Publ., 2022.

[5] S. Gnatyuk, et al., Cloud-based Cyber Incidents Response System and Software Tools, Commun. Comput. Inf. Sci., 1486 (2021) 169–184.

[6] V. Svanadze, M. Iavich, S. Gnatyuk, Challenges and Solutions for Cybersecurity and Information Security Management in Organizations, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 497–504.

[7] Z. Dong, Research of Big Data Information Mining and Analysis: Technology based on Hadoop Technology, in: 2022 Int. Conf. Big Data, Inf. Comput. Netw. (BDICN), Sanya, China, 2022, 173–176. doi:10.1109/BDICN55575.2022.00041

[8] Critical Infrastructure Sectors. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[9] National Security Memorandum on Critical Infrastructure Security and Resilience. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience

[10] NIS2 Directive: Securing Network and Information Systems. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[11] Critical Entities Resilience Directive. https://www.critical-entities-resilience-directive.com

[12] Cybersecurity Act: Information on the Cybersecurity Act. https://www.csa.gov.sg/legislation/cybersecurity-act

[13] Critical Information Infrastructure. https://financialservices.gov.in/beta/en/page/cii

[14] Section 70 of IT Act. https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=91

[15] Overview of Cybersecurity Policy for CIP. https://www.nisc.go.jp/eng/pdf/cip_policy_abst_2024_eng.pdf

[16] Cybersecurity Law of the People's Republic of China. https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3

[17] Translation: Critical Information Infrastructure Security Protection Regulations, 2021. https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021

[18] Framework Act on National Informatization. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=42620&lang=ENG

[19] Act on Promotion of Information and Communications Network Utilization and Information Protection. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG

[20] National Security Committee of the Republic of Kazakhstan, Cyber Shield. https://www.gov.kz/memleket/entities/knb/activities/250

[21] Investigatory Powers Act 2016. https://www.legislation.gov.uk/ukpga/2016/25/contents

[22] Government Cyber Security Strategy: 2022–2030. https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

[23] National Security and Investment Act 2021. https://www.legislation.gov.uk/ukpga/2021/25/contents

[24] The Procedure for Classifying Objects as Critical Infrastructure, Approved by Resolution of the Cabinet of Ministers of Ukraine No. 1109 of October 9, 2020 (as amended by Resolution No. 1384 of December 16, 2022). https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n42

[25] I. Patias, Cost Distribution in ICT Infrastructure during the AI Era: a Model for Data Centers, Power Grids, and Telecommunications, in: 7th Int. Congr. Human-Computer Interact., Optim. Robot. Appl. (ICHORA), Ankara, Türkiye, 2025, 1–8. doi:10.1109/ICHORA65333.2025.11017137

[26] R. Zeng, et al., A General Real-Time Cyberattack Risk Assessment Method for Distribution Network Involving the Influence of Feeder Automation System, IEEE Trans. Smart Grid, 15(2) (2024) 2102–2115. doi:10.1109/TSG.2023.3302287

[27] D. Penedo, Technical Infrastructure of a CSIRT, in: Int. Conf. Internet Surveill. Protect. (ICISP'06), Côte d'Azur, France, 2006, 27–27. doi:10.1109/ICISP.2006.32

[28] J. Otero-Mosquera, et al., Reproducible Key Performance Indicator (KPI) Measurement Experiments in 6G Networks under Mobility Conditions, in: Joint Eur. Conf. Netw. Commun. & 6G Summit, 2025, 446–451. doi:10.1109/EuCNC/6GSummit63408.2025.11036984

[29] I. Semertzis, et al., Quantitative Risk Assessment of Cyber Attacks on Cyber-Physical Systems using Attack Graphs, in: 10th Workshop Model. Simul. Cyber-Phys. Energy Syst. (MSCPES), Milan, Italy, 2022, 1–6. doi:10.1109/MSCPES55116.2022.9770140

[30] G. Deffenbaugh, S. Kameneni, Cyber Resilience Strategies Throughout the System Development Lifecycle, in: IEEE Int. Conf. Cyber Secur. Resil. (CSR), 2025, 504–509. doi:10.1109/CSR64739.2025.11129978

[31] I. Ostroumov, et al., Relative Navigation for Vehicle Formation Movement, in: 3rd IEEE KhPI Week Adv. Technol., 2022, 1–4. doi:10.1109/KhPIWeek57572.2022.9916414

[32] I. Ostroumov, et al., A Probability Estimation of Aircraft Departures and Arrivals Delays, in: O. Gervasi, et al. (Eds.), Comput. Sci. Its Appl. – ICCSA 2021, Lect. Notes Comput. Sci., vol. 12950, 2021, 363–377. doi:10.1007/978-3-030-86960-1_26

[33] M. Zaliskyi, et al., Heteroskedasticity Analysis during Operational Data Processing of Radio Electronic Systems, in: S. Shukla, et al. (Eds.), Data Sci. Secur., Lect. Notes Netw. Syst., vol. 290, 2021, 168–175. doi:10.1007/978-981-16-4486-3_18

[34] Y. Averyanova, et al., Turbulence Detection and Classification Algorithm using Data from AWR, in: 2nd IEEE Ukr. Microwave Week, 2022, 518–522. doi:10.1109/UkrMW58013.2022.10037172

[35] M. Zaliskyi, Y. Petrova, M. Asanov, E. Bekirov, Statistical Data Processing during Wind Generators Operation, Int. J. Electr. Electron. Eng. Telecommun., 8(1) (2019) 33–38. doi:10.18178/ijeetc.8.1.33-38

[36] N. Kuzmenko, I. Ostroumov, K. Marais, An Accuracy and Availability Estimation of Aircraft Positioning by Navigational Aids, in: 5th IEEE Int. Conf. Methods Syst. Navig. Motion Control (MSNMC), 2018, 36–40. doi:10.1109/MSNMC.2018.8576276

[37] A. Bieliatynskyi, et al., The Use of Fiber Made from Fly Ash from Power Plants in China in Road and Airfield Construction, Constr. Build. Mater., 323 (2022) 126537. doi:10.1016/j.conbuildmat.2022.126537

[38] P. Skladannyi, et al., Model and Methodology for the Formation of Adaptive Security Profiles for the Protection of Wireless Networks in the Face of Dynamic Cyber Threats, in: Cyber Security and Data Protection, vol. 4042, 2025, 17–36.

[39] I. Hanhalo, et al., Adaptive Approach to Ensuring the Functional Stability of Corporate Educational Platforms under Dynamic Cyber Threats, in; Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3991, 2025, 481–491.

[40] O. Mykhaylova, M. Korol, R. Kyrychok, Research and Analysis of Issues and Challenges in Ensuring Cyber Security in Cloud Computing, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3826, 2024, 30–39.

[41] A. Ilyenko, et al., Practical Aspects of Using Fully Homomorphic Encryption Systems to Protect Cloud Computing, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 226–233.

[42] V. Shapoval, et al., Automation of Data Management Processes in Cloud Storage, in: Cybersecurity Providing in Information and Telecomm. Systems, vol. 3654, 2024, 410–418.

[43] Y. Martseniuk, et al, Research of the Centralized Configuration Repository Efficiency for Secure Cloud Service Infrastructure Management, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3991, 2025, 260–274.