

An intelligent Model for Identifying Risks of Power Supply Projects for Critical Infrastructure Facilities in the Conditions of Emergency and Martial Law

Anatoliy Tryhuba^{1,†}, Inna Tryhuba^{1,†}, Roman Oliinyk^{2,†}, Oleh Andrushkiv^{2,†}, Marian Kotsylovskiy^{1,†}

¹ Lviv National Environmental University, 1, V. Velykoho str., Dubliany-Lviv, 80381, Ukraine

² Lviv State University of Life Safety, 35, Kleparivska str., 79007, Lviv, Ukraine

Abstract

A substantiated method is presented for assessing risks associated with energy supply initiatives targeting critical infrastructure. The foundation of the proposed model lies in the integration of spatial data, enabling the quantification of threat influence through numerical values that reflect both their likelihood and intensity. The use of geoinformation sources, in particular OpenStreetMap, combined with the flexibility of the Python toolkit, ensures the efficiency and relevance of the information obtained. Based on the use of the developed model and the created program code, high-risk areas for energy supply projects for critical facilities in the Zaporizhzhia region were identified. It was found that Enerhodar and Zaporizhzhia have the highest risk values ($R_1=11.4$ and $R_2=10.8$, respectively), which corresponds to a high-risk area. These territories contain strategic critical infrastructure facilities (Zaporizhzhia NPP) and have a high density of industrial facilities exposed to military attacks. The results are visualized and classified by risk level. Further research should be conducted in the direction of integrating the proposed model into a management decision support system. This will ensure automated risk identification and visualization of risk zones on maps.

Keywords

Intelligent model, risk identification, energy supply, infrastructure, decision, system, project, management.

1. Introduction


Currently, the stable functioning of critical infrastructure facilities depends on the effectiveness of project management and, in particular, the management of risks associated with their energy supply [1-4]. This issue is especially relevant in the context of a state of emergency and martial law, when traditional sources of power supply are damaged and logistics routes are disrupted. Unlike standard approaches to risk management in energy projects, the risks of power supply to critical infrastructure facilities have a number of specific features. In particular, it is crucial to continuously

ITPM-2025: VI International Workshop "IT Project Management", May 22, 2025, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

✉ trianamik@gmail.com (Anatoliy Tryhuba); trinle@ukr.net (Inna Tryhuba); romanoliynuk1395@gmail.com (Roman Oliinyk); andruskivoleg6@gmail.com (Oleh Andrushkiv); m.kotsylovsky@gmail.com (Marian Kotsylovskiy)

 0000-0001-8014-5661 (Anatoliy Tryhuba); 0000-0002-5239-5951 (Inna Tryhuba); 0009-0009-9846-6303 (Roman Oliinyk); 0009-0007-1672-7633 (Oleh Andrushkiv); 0009-0005-2958-637X (Marian Kotsylovskiy)



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

observe and consider the evolving conditions surrounding the project environment [5-8]. This includes external threats, the state of the transport network, and dynamic changes in a number of factors that determine the effectiveness of critical infrastructure energy supply projects during a state of emergency and martial law.

The proposed risk management model for critical infrastructure energy supply projects is an intelligent type. It involves the integration of modern technologies that ensure the adaptation of risk management processes to dynamic changes in the project environment (network destruction, logistics constraints, security threats) [9-12]. This method rejects traditional static risk assessment practices and instead incorporates real-time data on the operational status of energy infrastructure components.

One of the distinctive aspects of the model is its reliance on geospatial information derived from sources such as OpenStreetMap (OSM) and Google Earth Engine [13-15]. These platforms provide current spatial data, enabling the construction of a comprehensive risk landscape. Through this data, it becomes feasible to pinpoint damaged infrastructure zones, evaluate the accessibility of transport pathways, and highlight regions exposed to elevated risk. Consequently, strategic decisions regarding the development and deployment of energy supply initiatives are made with full awareness of the fluid and unstable conditions within the project environment, including shifts in external threat levels and internal resource limitations.

In addition, the model takes into account the specifics of critical infrastructure power supply projects in emergency and military conditions. This necessitates a flexible response from project managers, prompt adjustment of management decisions on the implementation of backup power sources, re-planning of resource supply, and prioritization of damaged network restoration scenarios.

2. Analysing the State of the Art in the Research Area

Contemporary research on risk management in energy provision for critical infrastructure demonstrates a growing academic focus on enhancing the safety, flexibility, and robustness of such systems under conditions of heightened and dynamic threats. An analysis of the available literature leads to the conclusion that the dominant approaches are those that prioritize the integration of information technology into risk management processes, in particular, through the application of flexible management frameworks that incorporate real-time variations in environmental conditions [16-20].

The ISO 31000 standard outlines the fundamental principles of risk management and serves as a foundational guideline for the development of risk management frameworks across numerous nations [21]. The main provisions of ISO 31000:2018 define the principles, framework, and processes of risk management that can be adapted to the specifics of energy projects. The standard emphasizes the need for a systematic approach to risk assessment, which includes the identification, analysis, evaluation, and monitoring of risks at all stages of the project life cycle. At the same time, the application of the provisions of ISO 31000 in a state of emergency or martial law requires modification, as the standard is focused on stable project conditions and does not take into account the specifics of a changing project environment and critical threats. That is why several authors propose to adapt the provisions of the standard to the conditions of a changing project environment. This may be achieved by embedding advanced information technologies for spatial data forecasting

and analysis into innovative risk management frameworks, which remain a focal point of ongoing scholarly discourse in the domain of project management [22-26].

The PMBOK Guide, developed by the Project Management Institute (PMI), is a well-established standard in the project management discipline [27]. Its most recent versions, particularly the sixth and seventh editions, highlight the importance of risk-related practices as a core knowledge area. These practices encompass the planning of risk strategies, identification of potential threats, both qualitative and quantitative assessments, development of mitigation plans, and continuous oversight of risk factors. Nevertheless, experts note that the conventional framework presented in the PMBOK does not fully address the complexities inherent in managing projects under crisis conditions, where the scope and nature of risks are subject to rapid and unpredictable changes. As such, there is a pressing need to modify the PMBOK's process model by incorporating real-time data processing techniques, including the application of satellite-based imagery, geographic information systems (GIS), and advanced predictive algorithms.

In addition, in the context of risk management, it is advisable to take into account the provisions of ISO 22301 on business continuity management [28]. However, similar to ISO 31000 and PMBOK, this standard needs to be adapted to the emergency conditions of martial law, which necessitates further research in the direction of integrating these approaches with modern IT risk management tools.

Papers [29-33] propose a conceptual framework for risk management in the energy sector based on a systematic approach and providing for the formalization of the processes of collecting and processing information about the project environment. Paper [34] substantiates the feasibility of using a multi-level risk management system that allows for both strategic and operational control over the state of critical infrastructure.

Particular emphasis should be placed on the legislative basis governing the protection of critical infrastructure. In Ukraine, the Law "On Critical Infrastructure" [35] establishes the principal legal provisions for ensuring the security and functioning of key infrastructure assets. However, the current legislation does not yet contain specific mechanisms for integrating modern IT solutions for automated risk identification and management, which creates a certain gap between theoretical developments and practical implementation [36-38].

In summary, the review of recent research indicates a clear shift away from static approaches to project risk management toward more adaptive systems that leverage information technologies for continuous monitoring and real-time analysis of critical infrastructure conditions. Simultaneously, there remains a significant demand for the advancement of tools that can consolidate data from diverse sources to enable timely risk evaluation and forecasting, thereby underscoring the importance of continued investigation in this domain.

3. Objectives of the Study

The purpose of the article is to substantiate an approach and a model for identifying risks of energy supply projects for critical infrastructure facilities in the context of emergency and martial law based on the use of geospatial data processing tools and modern information technologies. The proposed model involves the integration of data from open sources, in particular OpenStreetMap (OSM), to assess the condition of energy infrastructure facilities, as well as the use of machine learning algorithms for real-time risk analysis. To achieve this goal, the study used Google Earth Engine software and the Overpass API using the Overpass QL

query language, as well as Python tools for data processing and model building in the Jupyter Notebook environment.

In order to realize the research aim, the study addressed several key tasks:

- to substantiate the approach and model for identifying risks of critical infrastructure energy supply projects based on the analysis of geospatial data in the conditions of emergency and martial law;
- based on the developed model, to identify high-risk areas for critical infrastructure energy supply projects in the conditions of emergency and martial law.

4. Substantiation of an Approach and Model for Identifying Risks of Critical Infrastructure Energy Supply Projects Based on Geospatial Data Analysis in the Context of Emergency and Martial Law

In the current conditions of Ukraine's development, where there are emergencies and martial law in some areas, there is a problem of reliable energy supply to critical infrastructure facilities [39-40]. Addressing this issue requires the initiation of energy supply projects aimed at supporting critical infrastructure. During their execution, a key scientific and practical challenge emerges – the need for robust risk management strategies. Given the dynamic nature of the project environment, it is essential to apply a risk identification approach that reflects the unique characteristics of geospatial information and the presence of military threats.

The methodology outlined in this study relies on evaluating the condition of the project environment for energy supply initiatives involving critical infrastructure by combining geospatial datasets with insights into potential hazards and system vulnerabilities. Figure 1 presents the core elements of the proposed model for identifying risks in such projects.

The first phase involves gathering and preprocessing geospatial information, which serves as the foundation for constructing a risk identification model related to energy provision for critical infrastructure. Relevant data for the target area are obtained from sources such as: 1) geographic information systems (GIS); 2) open-access platforms like OpenStreetMap and Google Earth Engine. This stage starts with compiling spatial datasets, which may be formally represented as a set of:

$$D = \{d_1, d_2, \dots, d_n\}, \quad (1)$$

where D – a set of geodata on infrastructure objects, d_i – a single critical infrastructure object (coordinates, condition, type of object).

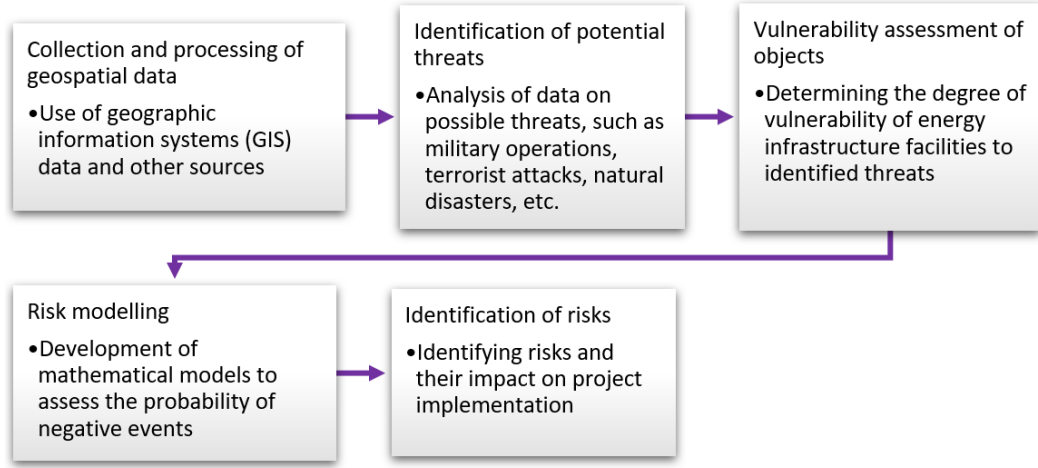


Figure 1: Structural scheme of the model for identifying risks in power supply systems of critical infrastructure

Subsequently, the collected data undergo a preprocessing phase that encompasses noise elimination, image adjustment, and transformation into a unified coordinate reference system. This stage can be mathematically described by the following preprocessing function:

$$D' = F_{\text{prep}}(D), \quad (2)$$

where D' – processed data set; F_{prep} – preprocessing operator (geometric and radiometric correction).

To identify energy infrastructure objects, a classification based on spectral features is used. The classification task is formalized as a function:

$$C = f(D'), \quad (3)$$

where $C = \{c_1, c_2, \dots, c_m\}$ – is a set of classified critical infrastructure objects; f – is a classification algorithm (e.g., maximum likelihood or neural network).

After identifying the relevant objects, they are incorporated into a geographic information system (GIS) to enable subsequent analytical procedures. Comparison between these objects is carried out through a spatial matching (joining) operation:

$$S = G(C, L), \quad (4)$$

where S – integrated map; L – layers of additional data (population, hazardous objects, damage), G – spatial joining operator.

Thus, the formalisation of the data collection and processing process allows for the integration of various data sources that form a database for further risk assessment in critical infrastructure energy supply projects.

The next stage involves the identification of potential threats, which is an important process in the risk analysis of critical infrastructure power supply projects. This stage involves the systematization and processing of information on all possible factors of the project environment that affect the stability of the power grids and the creation of threats during their operation in a state of emergency or martial law. For this purpose, the spatial and temporal characteristics of threats are formalized. All identified potential threats are collectively represented as the following set:

$$T = \{t_1, t_2, \dots, t_m\}, \quad (5)$$

where T – is a set of types of threats (military operations, terrorist attacks, natural disasters, etc.); t_i – is a refers to an individual threat element defined by attributes such as spatial position (x_i, y_i) , threat intensity (I_i) , probability of occurrence (P_i) , and time parameter (t_i^{time}) .

The magnitude of a current threat is expressed mathematically as a function dependent on:

$$I_i = f(A_i, D_i), \quad (6)$$

where A_i – represents the geographical region impacted by the threat; D_i – denotes the spatial density of critical infrastructure elements within the affected zone.

A spatio-temporal matrix M is computed for each threat category, capturing its distribution across space and time, and is structured as follows:

$$M = \begin{bmatrix} P_1 & I_1 & (x_1, y_1) & t_1^{time} \\ P_2 & I_2 & (x_2, y_2) & t_2^{time} \\ \vdots & \vdots & \vdots & \vdots \\ P_m & I_m & (x_m, y_m) & t_m^{time} \end{bmatrix}, \quad (7)$$

The collected data are incorporated into a geographic information system (GIS) to enable spatial representation. Incorporating temporal attributes facilitates the prediction of fluctuations in threat intensity and their geographic spread over time. Thus, this stage provides a comprehensive understanding of risk zones and creates a basis for further vulnerability assessment of energy facilities.

The subsequent phase involves assessing the vulnerability level of each critical infrastructure object, as previously identified, in relation to possible threats. This takes into account the set of technical characteristics of the facilities, their physical condition and spatial location relative to high-risk areas. The level of vulnerability associated with a critical infrastructure facility can be expressed through the function:

$$V_i = f(C_i, S_i, L_i), \quad (8)$$

where V_i – is the vulnerability index of the i -th critical infrastructure facility; C_i – the technical attributes of the critical infrastructure object, such as its capacity, substation classification, and presence of auxiliary power sources; S_i – the present condition of the critical infrastructure unit, characterized by factors such as the degree of physical wear and extent of structural damage; L_i – the spatial positioning of the critical infrastructure facility, taking into account its proximity to hazard zones and ease of logistical access.

For each critical infrastructure facility, a vector of its main characteristics is formed:

$$X_i = [C_i, S_i, L_i]. \quad (9)$$

Vulnerability is normalised according to a scale from 0 to 1, where 1 means maximum vulnerability and 0 means no vulnerability. A weighted evaluation approach is applied and can be mathematically expressed in the following form:

$$V_i = w_c \cdot \frac{C_i}{C_{\max}} + w_s \cdot \frac{S_i}{S_{\max}} + w_l \cdot \frac{L_i}{L_{\max}}. \quad (10)$$

where w_c, w_s, w_l – corresponding weighting factors that represent the influence of individual elements within the project environment.

Numerical evaluation of critical infrastructure vulnerability makes it possible to determine which facilities demand urgent protective measures or upgrades. This is the basis for making management decisions to reduce risks in critical infrastructure energy supply projects [41-43].

The following phase focuses on modeling risks associated with the execution of power supply projects for critical infrastructure. This stage is the basis for making informed management decisions to reduce risks. At this stage, we quantify the probability of negative events and determine their consequences for energy infrastructure facilities based on previously collected data on threats and vulnerabilities.

Risks are structured using a conventional framework that incorporates three core elements: the likelihood of a threat occurring, the vulnerability of the critical infrastructure asset, and the magnitude of possible consequences. The overall risk level for the i -th facility is calculated as follows:

$$R_i = P_i \cdot V_i \cdot C_i. \quad (11)$$

where P_i – denotes the likelihood of a threat impacting the i -th critical infrastructure site; V_i – represents the vulnerability score assigned to that specific facility; C_i – is the scope of possible consequences (economic losses, loss of critical resources, impact on the population, etc.)

The likelihood of a threat materializing is estimated using historical records, expert assessments, or machine learning techniques, with consideration given to both spatial and temporal aspects of the project context. For instance, in the case of facilities situated within zones of ongoing military conflict, the probability approaches a value of 1.

The evaluation of consequences C_i is determined by factors such as the operational performance of the critical infrastructure facility, its significance within the energy network, and the costs associated with its restoration. The value C_i is normalised for ease of comparison:

$$C_i = \frac{E_i}{E_{\max}}. \quad (12)$$

where E_i – is the economic assessment of losses from damage to the i -th facility; E_{\max} – is the maximum possible losses in the power system.

The final phase of the risk identification procedure entails a structured analysis of risks influencing the execution of energy supply projects for critical infrastructure. This includes evaluating their impact on key project parameters such as timeline, financial resources, service quality, and operational safety. The identification process is grounded in the outcomes of prior modeling efforts. For each specific infrastructure facility, risk determination is conducted according to the following conditions:

$$\text{Risk}_i = \begin{cases} 1, & \text{якщо } R_i \geq T_{\text{crit}} \\ 0, & \text{якщо } R_i < T_{\text{crit}} \end{cases}. \quad (13)$$

where R_i – is the risk level of the i -th critical infrastructure facility determined at the previous stage; T_{crit} – is the critical risk threshold, exceeding which requires management interventions in project implementation.

Once risks have been identified, a dedicated risk matrix is created for each facility, outlining the nature of the risk, its origin, severity level, and a concise summary of its potential influence on project execution. This matrix serves as a foundation for constructing an appropriate risk mitigation strategy. Therefore, the concluding phase of the risk identification model delivers

organized input essential for formulating comprehensive risk management plans in the context of critical infrastructure energy supply projects.

5. Outcomes of Detecting High-Risk Zones for Energy Supply Projects Aimed at Critical Infrastructure Under Emergency and Wartime Conditions

By applying the developed model, it was possible to determine areas with elevated risk levels for energy supply projects supporting critical infrastructure during conditions of emergency and martial law. To identify high-risk areas, we collected and processed geospatial data using OpenStreetMap, which contains information on the location of energy infrastructure facilities, transport networks, and other important elements. In addition, high-resolution satellite imagery was obtained using Google Earth Engine, which made it possible to assess the current state of the territories and identify potential threats, such as war zones, damaged facilities, and other risk factors for critical infrastructure power supply projects.

The developed code serves as the informational foundation for generating an interactive map of risk areas, facilitating the detection of potential threats to power supply projects targeting critical infrastructure during emergency and wartime scenarios. This solution was implemented using Python within the Jupyter Notebook environment—one of the most widely adopted platforms for spatial data processing, analytical computations, and data visualization (Fig. 2). The core library employed in the implementation is Folium. It allows for the integration of geospatial data from open mapping sources, including OpenStreetMap, and provides ample opportunities for creating interactive maps with various graphic elements.

The information component of this solution is a structured presentation of risk zones by level (high, medium, low) with a clear geographical location of each event. This allows you to visualize not only the location of threats but also their level of danger to critical infrastructure.

Functionally, the Folium library allows integration with other Python libraries, such as Pandas for tabular data processing, NumPy for mathematical calculations, and GeoPandas for advanced work with geospatial data. This lays the groundwork for advancing the model further, such as incorporating big data analytics, applying machine learning techniques for forecasting risks, and building a system capable of automatically refreshing threat-related information [44-45].


```
[2]: import folium

# Введіть центр досліджуваної області
region_center = [LATITUDE, LONGITUDE] # наприклад: [47.8388, 35.1396]
map_zoom = 8

# Створення базової карти
m = folium.Map(location=region_center, zoom_start=map_zoom, tiles='OpenStreetMap')

for coord in high_risk_coords:
    folium.Circle(
        location=coord,
        radius=20000,
        color='red',
        fill=True,
        fill_color='red',
        fill_opacity=0.35,
        popup='High Risk Area'
    ).add_to(m)

for coord in medium_risk_coords:
    folium.Circle(
        location=coord,
        radius=18000,
        color='orange',
        fill=True,
        fill_color='orange',
        fill_opacity=0.35,
        popup='Medium Risk Area'
    ).add_to(m)

for coord in low_risk_coords:
    folium.Circle(
        location=coord,
        radius=15000,
        color='green',
        fill=True,
        fill_color='green',
        fill_opacity=0.35,
        popup='Low Risk Area'
    ).add_to(m)
```

Figure 2: Code snippet of the risk identification model for critical infrastructure power supply projects

Using the developed model adapted to the context of the Zaporizhzhia region, a spatio-temporal matrix of threats affecting energy supply projects for critical infrastructure was constructed (see Table 1).

The analysis of the spatio-temporal threat matrix for critical infrastructure energy supply projects in Zaporizhzhia region shows the presence of both man-made and natural threats with different levels of intensity, spatial coverage, and density of impact. The most critical man-made threat is the potential hazard associated with the location of Zaporizhzhia NPP in the city of Enerhodar (coordinates 47.5083, 34.5844). The area of influence of this threat is 15 km², with a density of 0.8 units per square kilometer, which in total forms 12 conditional threat units. The impact factor is 0.95, which indicates an extremely high risk to infrastructure facilities in the event of an accident or attack on the plant. This threat is relevant as of May 1, 2024.

In general, man-made hazards have higher impact factors (0.90-0.95) and concentrated hazards with a smaller area, while natural hazards, despite covering a larger area, demonstrate lower intensity and impact factors (0.60-0.80). This indicates the need to prioritize the protection of facilities located near critical man-made centers, as well as to develop preventive environmental measures to reduce long-term risks from natural hazards.

Table 1
Spatio-Temporal Threat Matrix for Critical Infrastructure Power Supply Projects

№	Threat type	Description	Coordinates, (x_i, y_i)	A_i , km ²	C_i , units/km ²	I_i	P_i	t_i
---	-------------	-------------	--------------------------------	----------------------------	----------------------------------	-------	-------	-------

1	Technogenic	Zaporizhzhia NPP (Enerhodar)	(47.5083, 34.5844)	15	0.8	12	0.95	2024- 05-01
2	Technogenic	Industrial plant attack (Zaporizhzhia)	(47.8388, 35.1396)	12	1.0	12	0.90	2025- 01-08
3	Natural	Wildfires in Pology district	(47.4833, 36.2833)	18	0.5	9	0.80	2022- 07-10
4	Natural	Wildfires in Vasylivka district	(47.4388, 35.2396)	18	0.6	10.8	0.75	2022- 08-15
5	Natural	Wildfires in Kamianka- Dniprovska forest zone	(47.5, 34.4)	20	0.4	8	0.70	2022- 06-20
6	Natural	Drying of Velyki Kuchuhury wetlands	(47.2744, 34.1222)	15	0.3	4.5	0.60	2023- 06-10

The dataset presented in Table 1 is incorporated into the risk identification model's code to enable subsequent spatial visualization of threats associated with critical infrastructure energy supply projects. Using the results derived from formulas (10–12), the key attributes of high-risk zones within the Zaporizhzhia region have been identified, and these findings are summarized in Table 2.

The risk level was computed as the product of threat intensity and its associated probability P_i , previously established within the spatio-temporal matrix. Threshold values were defined as follows high risk is – $R_i \geq 10$, medium risk is – $6 \leq R_i < 10$, and low risk is – $R_i < 6$.

Based on the data obtained and calculations made, a map was created that shows high-risk areas for critical infrastructure energy supply projects (Fig. 3).

The findings indicate that Enerhodar and Zaporizhzhia exhibit the highest calculated risk levels ($R_i = 11.4$ and $R_i = 10.8$), placing them within the category of high-risk zones (Fig. 3). These territories contain strategic critical infrastructure facilities (Zaporizhzhia NPP) and have a high density of industrial facilities exposed to military attacks. Medium risk is observed in the Vasyliv and Pologiv districts of the Zaporizhzhia region.

Table 2

Results of Determining the Characteristics of Risk Zones for Energy Supply Projects in Zaporizhzhia Oblast

№	Region	Coordinates (latitude, longitude)	Risk level	Main threats
1	Enerhodar (Zaporizhzhya NPP)	47.5083, 34.5844	High	Proximity to a nuclear power plant, military operations, and possible man-made accidents

2	Kamianka-Dniprovska forest zone	47.5, 34.4	High	Fires in forests, damage to infrastructure
3	m. Zaporizhzhia	47.8388, 35.1396	Medium	Attack on industrial enterprises, high density of critical facilities
4	Vasylivskiy district	47.4388, 35.2396	Medium	Fires, shelling, risk of damage to power lines
5	Polohiv district	47.4833, 36.2833	Low	Fires in the steppe zone, logistical vulnerability
6	Velyki Kuchuhury (after the explosion of the Kakhovka HPP)	47.2744, 34.1222	Low	Drying up of water resources, environmental consequences

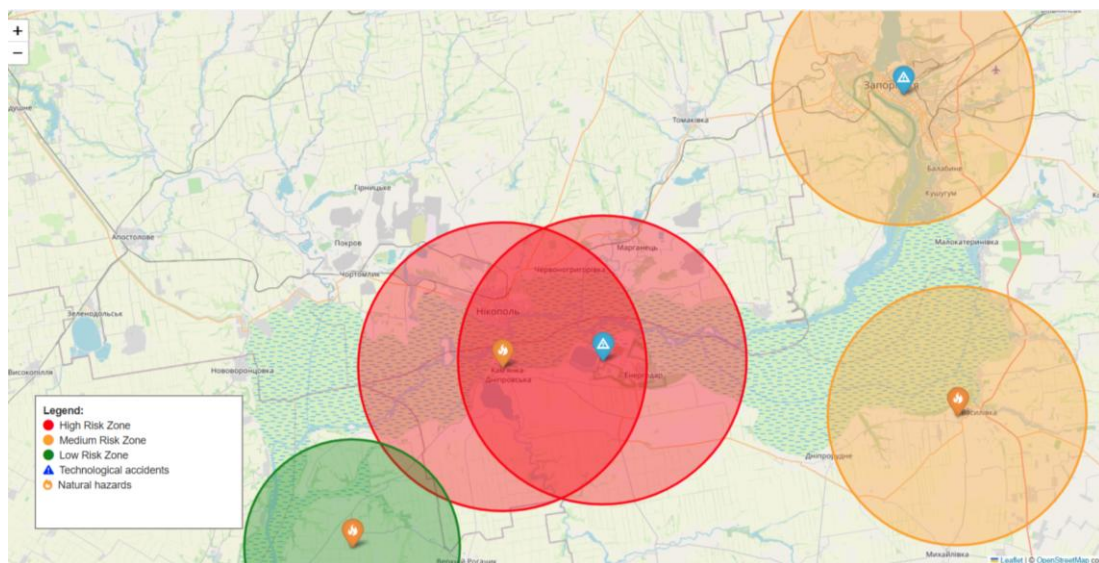


Figure 3: Geospatial map highlighting zones of elevated risk in critical infrastructure energy supply projects

The region faces both environmental risks (e.g., forest fires) and a heightened probability of infrastructure damage caused by shelling amid ongoing military aggression by Russia. Kamianka-Dniprovska forest area and Velyki Kuchuhury have a relatively low combined risk score, mainly due to the lower density of critical facilities and remoteness from major infrastructure hubs.

The research has confirmed that the developed model is of practical value for risk management in critical facilities energy supply projects. The identified risk zones, among which special attention should be paid to the areas around Zaporizhzhia NPP and industrial districts of Zaporizhzhia, allow for a more accurate prioritization of critical facilities energy supply scenarios. By analyzing the indicators of threat intensity alongside the assessed vulnerability of infrastructure sites, regions in urgent need of enhanced protective measures were identified. This approach contributes to more efficient allocation of limited resources, which is particularly critical under conditions of emergency or martial law. Importantly, the model not only captures

the current state of affairs, but also updates the data over time, which helps to make more informed decisions about further actions. The integration of the model into a management decision support system significantly expedites the justification and planning of energy supply configurations for strategically important facilities in uncertain and rapidly changing conditions.

Future studies should focus on embedding the proposed model into a management decision support system capable of automatically gathering data from open platforms such as OSM, integrating APIs for real-time updates on emergency events (e.g., attacks, incidents, natural disasters), conducting risk prioritization, and generating automated maps. This would enable the development of not just a static visualization instrument, but a dynamic, interactive platform to support real-time decision-making for the deployment of energy supply projects targeting critical infrastructure.

Such a system would provide operational institutions and local authorities with timely insights into the evolving risk landscape. For instance, if part of the power infrastructure is damaged due to shelling or severe weather, the system could immediately highlight affected zones and suggest prioritization strategies for restoration or temporary redistribution of loads across adjacent substations. This flexibility is especially vital in emergency or wartime settings, where delays in response may threaten the functioning of hospitals, water supply systems, or communication lines.

Additionally, the integration of machine learning algorithms could enhance the model's ability to recognize early signs of infrastructure degradation or rising threat levels. By analyzing historical data and correlating it with current geospatial patterns, the system may anticipate zones of elevated vulnerability. This foresight would support preventive planning and allow resource-constrained regions to allocate funding and technical efforts more efficiently, strengthening resilience without the need for reactive crisis management.

6. Conclusions

1. The conducted research resulted in the justification of a methodological approach and the creation of an intelligent model designed to detect risks associated with energy supply projects for critical infrastructure. This model is grounded in the integration of geospatial information, enabling the transformation of potential threats into quantifiable metrics namely, intensity and likelihood of occurrence. The main advantage of this model is the possibility of its further integration into management decision support systems to justify the configurations of energy supply projects under conditions of uncertainty. Leveraging geospatial data sources, particularly OpenStreetMap, together with the versatility of Python-based tools, enables the acquisition of timely and reliable information. This, in turn, substantially enhances the effectiveness of management activities during the planning phase of energy supply projects for critical infrastructure, especially in the context of a dynamically evolving project environment and associated risks.

2. Based on the use of the developed model and the created software code, high-risk areas for critical facilities energy supply projects in the Zaporizhzhia region were identified. Enerhodar and Zaporizhzhia city have the highest risk values (respectively $R_1 = 11.4$ and $R_1 = 10.8$), which corresponds to the high-risk zone. These territories contain strategic critical infrastructure facilities (Zaporizhzhia NPP) and have a high density of industrial facilities exposed to military attacks. The findings are mapped and grouped based on their corresponding risk levels.

3. Future investigations should focus on embedding the developed model into a decision support system for management purposes, enabling automated detection of risks and real-time visualization of risk areas on geospatial maps. This will create not only a static visualization tool, but also a dynamic platform for making management decisions on the implementation of energy supply projects for critical infrastructure facilities in real-time.

Declaration on Generative AI

During the preparation of this work Chat-GPT-4o and Grammarly were used to check grammar and spelling. After using these tool(s)/service(s), the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

- [1] K. Piliuhina, S. Bushuyev, R. Cirillo, M. Ricotti, W. Janssens, Development of the nuclear competencies based on global trends in the nuclear industry. *Nuclear Engineering and Design*, 2024, 421, 113046.
- [2] A. Tryhuba, V. Boyarchuk, N. Koval, O. Boiarchuk, N. Pavlikha, Risk-Adapted model of the lifecycle of the technologically integrated programs of dairy cattle breeding. *International Scientific and Technical Conference on Computer Sciences and Information Technologies*, 2021, 2, pp. 307–310.
- [3] A. Tryhuba, T. Hutsol, M. Kuboń, T. Hohol, W. Tomaszewska-Górecka, Taxonomy and Stakeholder Risk Management in Integrated Projects of the European Green Deal. *Energies*, 2022, 15(6), 2015.
- [4] O. Bashynsky, I. Garasymchuk, D. Vilchinska, V. Dubik, Research of the variable natural potential of the wind and energy in the northern strip of the Ukrainian Carpathians. *E3S Web of Conferences*, 2020, 154, 06002.
- [5] S. Bushuyev, N. Bushuyeva, V. Bushuieva, D. Bushuiev, L. Tereikovska, Dynamic principles of integrated intelligence model for managing innovation projects. *CEUR Workshop Proceedings*, 2023, 3453, pp. 13–23.
- [6] R. Ahmed, I.Q. Khan, S.P. Philbin, Mediating Role of Switch Leadership between Dynamic Work Environment and Project Success. *International Journal of Information Technology Project Management*, 2022, 13(1).
- [7] N. Koval, I. Kondysiuk, I. Tryhuba, O. Boiarchuk, M. Rudynets, V. Grabovets, V. Onyshchuk, Forecasting the Fund of Time for Performance of Works in Hybrid Projects Using Machine Training Technologies. *Proceedings of the 3rd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS 2021)*, Volume I: Main Conference, Lviv–Shatsk, Ukraine, June 5–6, 2021, pp. 196–206.
- [8] A. Tryhuba, O. Bashynsky, T. Hutsol, A. Rozkosz, O. Prokopova, Justification of Parameters of the Energy Supply System of Agricultural Enterprises with Using Wind Power Installations. *E3S Web of Conferences*, 2020, 154, 06001.
- [9] R. Ratushnyi, O. Bashynsky, V. Ptashnyk, Planning of Territorial Location of Fire-Rescue Formations in Administrative Territory Development Projects, in: *CEUR Workshop Proceedings*. 2020, 2565, pp. 93-105.
- [10] R. Ratushnyi, P. Khmel, E. Martyn, O. Prydatko, Substantiating the effectiveness of projects for the construction of dual systems of fire suppression. *Eastern-European Journal of*

Enterprise Technologies, 4(3-100) (2019) 46–53. URL: <https://doi.org/10.15587/1729-4061.2019.175275>

- [11] O. Kovalchuk, O. Zachko and D. Kobylkin, Criteria for intellectual forming a project teams in safety oriented system, in: 17th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), 2, 2022, pp. 430-433.
- [12] O. Zachko, V. Grabovets, I. Pavlova, M. Rudynet, Examining the effect of production conditions at territorial logistic systems of milk harvesting on the parameters of a fleet of specialized road tanks, in: Eastern-European Journal of Enterprise Technologies, 2018, 5(3-95), pp. 59–69.
- [13] OpenStreetMap. URL: <https://www.openstreetmap.org/>
- [14] Google Earth Engine. URL: <https://earthengine.google.com/>
- [15] I. Kondysiuk, P. Lub. Approach and Software for Risk Assessment of Stakeholders of Hybrid Projects of Transport Enterprise. CEUR Workshop Proceedings, 2022, 3295, pp. 86–96.
- [16] S. Chernov, L. Chernova, L. Chernova, N. Kunanets, V. Pitera, The Synergetic Effect in the Management of Active System with Distributed Control. IEEE 18-th International Conference on Computer Science and Information Technologies (CSIT), 2023, pp. 1–6. DOI: 10.1109/CSIT61576.2023.10324123.
- [17] V. Boyarchuk, O. Ftoma, R. Padyuka, M. Rudynets, Forecasting the risk of the resource demand for dairy farms basing on machine learning (MoML&T&DS-2020). In: CEUR Workshop Proceedings, 2020, vol. 2631.
- [18] I. Kondysiuk, O. Bashynsky, V. Dembitsky, Formation and risk assessment of stakeholders value of motor transport enterprises development projects. International Scientific and Technical Conference on Computer Sciences and Information Technologies, 2021, 2, pp. 303–306.
- [19] S.D. Bushuyev, A.V. Ivko, H. Lyakhovych, Method of Maximizing F-Synergistic Value in IT Development Projects for Self-Managed Organizations. International Journal of Computing, 2024, 23(3), pp. 371–379.
- [20] O. Zachko, V. Demchyna, I. Zachko, Intellectual Models of Projects for the Development of Transport Infrastructure of Urban Territorial Systems. CEUR Workshop Proceedings, 2022, 3295, pp. 159–169.
- [21] ISO 31000:2018, Risk Management – Guidelines. International Organization for Standardization, Geneva, Switzerland, 2018, 16 p.
- [22] L. Chernova, A. Zhuravel, L. Chernova, N. Kunanets, O. Artemenko, Application of the Cognitive Approach for IT Project Management and Implementation. International Scientific and Technical Conference on Computer Sciences and Information Technologies, 2022, pp. 426-429.
- [23] A. Tryhuba, R. Ratushny, I. Tryhuba, N. Koval, I. Androshchuk, The Model of Projects Creation of the Fire Extinguishing Systems in Community Territories, in: Acta universitatis agriculturae et silviculturae mendelianae brunensis. 68(2) (2020). 419-431. doi:10.11118/actaun202068020419
- [24] A. Tryhuba, V. Boyarchuk, I. Tryhuba, V. Tymochko, S. Bondarchuk, Model of Assessment of the Risk of Investing in the Projects of Production of Biofuel Raw Materials. International Scientific and Technical Conference on Computer Sciences and Information Technologies, 2020, 2, pp. 151–154, 9322024.

- [25] S. Bushuyev, I. Chumachenko, A. Galkin, D. Bushuiev, N. Dotsenko, Sustainable Development Projects Implementing in BANI Environment Based on AI Tools. Sustainability (Switzerland), 2025, 17(6), 2607.
- [26] V. Piterska, V. Samoilovska, V. Adakhovskiy, Assessment of port concession projects quality based on the information and analytical risk management system. CEUR Workshop Proceedings, 2023, 3453, pp. 71–81.
- [27] Project Management Institute (PMI), A Guide to the Project Management Body of Knowledge (PMBOK® Guide), 7th Edition. Newtown Square, PA, USA: Project Management Institute, 2021, 370 p.
- [28] ISO 22301:2019, Security and Resilience – Business Continuity Management Systems – Requirements. International Organization for Standardization, Geneva, Switzerland, 2019, 18p.
- [29] A. Tryhuba, I. Tryhuba, O. Ftoma, O. Boyarchuk, Method of quantitative evaluation of the risk of benefits for investors of fodder-producing cooperatives, in: 14th International Scientific and Technical Conference on Computer Sciences and Information Technologies, 3, pp. 55– 58, September 2019.
- [30] A. Tryhuba, V. Boyarchuk, I. Tryhuba, O. Boiarchuk, N. Pavlikha, N. Kovalchuk, Study of the impact of the volume of investments in agrarian projects on the risk of their value (ITPM-2021) In: CEUR Workshop Proceedings, 2021, 2851, pp. 303-313.
- [31] A. Tryhuba, S. Komarnitskyi, I. Tryhuba, T. Muzychenko, I. Horetska, Planning and Risk Analysis in Projects of Procurement of Agricultural Raw Materials for the Production of Environmentally Friendly Fuel. International Journal of Renewable Energy Development, 2022, 11(2), pp. 569–580.
- [32] Y. Chernenko, O. Danchenko, B. Mysnyk, O. Bielova, O. Adamov, Optimizing Housing and Communal Services Management Through Digital Transformation and Integrated Information Systems. Lecture Notes on Data Engineering and Communications Technologies, 2024, 222, pp. 33–49.
- [33] N. Kunanets, Y. Zhovnir, Y. Burov, O. Duda, V. Pasichnyk, Designing the Structure and Architecture of Situation-Aware Security Information Systems for Residential Complexes. Eastern-European Journal of Enterprise Technologies, 2025, 1(9(133)), pp. 6–23.
- [34] I. Bondareva, A.A. Khanova, Multi-level Management of Organizational Systems on the Basis of Risk Cascading, Logical-Probabilistic Modeling and Simulation. Studies in Systems, Decision and Control, 2022, 416, pp. 157–166.
- [35] Law of Ukraine “On Critical Infrastructure”. Verkhovna Rada of Ukraine, No. 1882-IX, adopted on November 16, 2021. Official Bulletin of the Verkhovna Rada of Ukraine, 2022, No. 3, Art. 21. [Online]. Available: <https://zakon.rada.gov.ua/laws/show/1882-20>
- [36] O. Verenych, O. Sharovara, M. Dorosh, N. Yehorchenkova, I. Golyash. Awareness management of stakeholders during project implementation on the base of the markov chain. Proceedings of the 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019, 2019, 1, pp. 259–262, 8924375.
- [37] S. Bushuyev, D. Bushuiev, V. Bushuieva, Interaction Multilayer model of Emotional Infection with the Earn Value Method in the Project Management Process, in: 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies, CSIT 2020 Proceedings, 2020, 2, pp. 146-150.

- [38] R. Ratushny, I. Horodetsky, Y. Molchak, V. Grabovets, The configurations coordination of the projects products of development of the community fire extinguishing systems with the project environment. ITPM-2021. In: CEUR Workshop Proceedings, 2021, 2851
- [39] R. Ratushny, O. Bashynsky, V. Ptashnyk, Development and Usage of a Computer Model of Evaluating the Scenarios of Projects for the Creation of Fire Fighting Systems of Rural Communities, in: 2019 11th International Scientific and Practical Conference on Electronics and Information Technologies, ELIT 2019 - Proceedings, 2019, pp. 34–39, 8892320.
- [40] M. Rudynets, N. Pavlikha, I. Skorokhod, D. Seleznev, Establishing patterns of change in the indicators of using milk processing shops at a community territory, in: Eastern-European Journal of Enterprise Technologies, 2019, 6(3-102), pp. 57–65.
- [41] K. Kolesnikova, N. Alpysbay, T. Olekh, T. Chinibayeva, Proceedings of the IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS, 2023, pp. 741–746.
- [42] L. Chernova, I. Zhuravel, S. Chernov, L. Chernova, N. Kunanets, Management of the IT project as a complex system. CEUR Workshop Proceedings, 2024, 3709, pp. 114–125.
- [43] N. Blackwell, A. Evans, P. Lee, B. McCoy, F.T. Davidson, A Methodology for Risk Assessment to Improve the Resilience and Sustainability of Critical Infrastructure with Case Studies from the United States Army. ASME International Mechanical Engineering Congress and Exposition, Proceedings (IMECE), 2021, 8A, V08AT08A056.
- [44] N. Pavlikha, M. Rudynets, N. Khomiuk, V. Fedorchuk-Moroz, Studying the influence of production conditions on the content of operations in logistic systems of milk collection, in: Eastern-European Journal of Enterprise Technologies, 2019, 3(3-99), pp. 50–63.
- [45] I. Kondysiuk, O. Boiarchuk, A. Tatomyr. Intellectual information system for formation of portfolio projects of motor transport enterprises. CEUR Workshop Proceedings, 2022, 3109, pp 44–52.