Tensor Model for Representing Critical Infrastructure

Iaroslav Dorohyi[1,2,3,†], Vladyslav Kravchuk[1,†] and Vasyl Tsurkan[2,4,*,†]

[1] *Donetsk National Technical University, 76, Sambirska Str., Drohobych, Lviv region, 82111, Ukraine*

[2] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37, Prospect Beresteiskyi (former Peremohy), Kyiv, Ukraine, 03056, Ukraine*

[3] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska Street, Kyiv, 01033, Ukraine*

[4] *G. E. Pukhov Institute for Modeling in Energy Engineering of National Academy of Sciences of Ukraine, 15, Oleha Mudraka Str., Kyiv, 03164, Ukraine*

Abstract

Critical infrastructure ensures the stability of society, economic growth, and national security. This paper presents a tensor-based model for assessing infrastructure resilience, considering technical, economic, environmental, social, and managerial aspects.

The proposed model represents infrastructure subsystems – generation, transportation, and resource consumption–across different operational phases: pre-disaster, crisis, and recovery. Tensor analysis enables a comprehensive evaluation of interactions between system components, multiple threat impacts, and resilience criteria such as functionality, recovery time, threat resistance, adaptability, and economic efficiency.

By defining threat vectors for various disruptions, including cyberattacks, natural disasters, and technological failures, the model identifies vulnerabilities and provides insights for strengthening infrastructure resilience. The findings support strategic management, risk mitigation, and policy development in national security and engineering planning.

Keywords

resilience of critical infrastructures, tensor analysis, resilience criteria, threat modeling, risk management, strategic planning, multidimensional analysis, system adaptability, cyberattacks, environmental sustainability.

1. Introduction

Critical infrastructures, including energy, transportation, communications, water supply, and healthcare, are essential for national security and economic stability. However, these systems face increasing threats from natural disasters, cyberattacks, technological failures, and geopolitical conflicts. Their interconnected nature makes resilience a key priority.

Resilience defines a system's ability to maintain functionality, resist external impacts, and recover after crises. It involves technical, organizational, social, and economic factors that ensure adaptability to dynamic threats. A structured approach to assessing resilience requires clear criteria, mathematical modeling, and analytical methods.

This paper explores tensor analysis as a tool for modeling resilient critical infrastructure. Tensor models enable the evaluation of complex interactions between system components, threat scenarios, and adaptive strategies. The proposed approach integrates technical, economic, and managerial aspects to enhance infrastructure security and operational stability.

ITS-2024: Information Technologies and Security, December 19, 2024, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

yaroslav.dorohyi@donntu.edu.ua (I. Dorohyi); vladkrava15@ukr.net (V. Kravchuk); v.v.tsurkan@gmail.com (V. Tsurkan)

0000-0003-3848-9852 (I. Dorohyi); 0009-0000-7929-6796 (V. Kravchuk); 0000-0003-1352-042X (V. Tsurkan)

2. Literature Review

The article [1] presents an innovative approach to assessing the resilience of critical infrastructure under conditions of multi-level threats, particularly for transportation facilities as key components of critical infrastructure. The authors have developed an adaptive methodology that integrates various risk parameters, providing a robust foundation for decision-making during crises. This approach serves as a basis for further research in infrastructure resilience and risk management.

The following study [2] focuses on a novel framework for evaluating the resilience of multi-component critical infrastructure. Specifically, it demonstrates how modern approaches in engineering systems management can enhance resilience to complex threats. To achieve this, the authors pay significant attention to mathematical models for analyzing inter-system dependencies, which are critical for ensuring the uninterrupted functioning of infrastructure during emergencies.

In article [3], a quantitative method for evaluating the resilience of interdependent infrastructures is proposed. The mathematical model developed by the authors enables the assessment of functionality losses and recovery rates after emergency events. This approach is particularly relevant as it considers interconnections between infrastructure components, making it valuable for practical risk management solutions.

The analysis of urban critical infrastructure resilience, exemplified by Ahvaz, Iran, is presented in study [4]. The authors employ an indicative approach to assess vulnerabilities in urban networks such as water supply, electricity, and transportation. This method emphasizes the integration of environmental, social, and technical factors, thereby enhancing the overall resilience of urban systems to crises.

The work [5] proposes metrics and frameworks for analyzing the resilience of engineering and infrastructure systems. The research focuses on methods for evaluating systems' ability to withstand external impacts, quickly adapt, and restore functionality. This study provides a theoretical foundation for further works in resilience and risk management for infrastructure.

Research [6] emphasizes the impact of dynamic cost changes on assessing infrastructure resilience. It highlights the importance of incorporating time factors to improve the accuracy of resilience forecasting, developing methodologies for adaptive risk assessment and infrastructure management.

The development of metrics and methods for quantitative assessment of the resilience of power systems is presented in study [7]. The authors propose an integrative approach to analyzing operational and structural resilience. The suggested metrics allow the formulation of strategies for risk minimization and enhancing the reliability of energy supply systems.

Article [8] presents a comprehensive framework for evaluating the resilience of critical infrastructure components by incorporating technical, organizational, and social dimensions. This multidimensional approach aids in designing measures to enhance resilience across different sectors of critical infrastructure, offering a holistic view of how various factors interact.

Study [9] introduces a methodology for assessing the resilience of networked infrastructures, with a focus on the interdependencies among system elements and the effects of their potential failure. The findings provide a foundation for creating effective risk management strategies to maintain and strengthen critical infrastructure resilience.

In article [10], operational models for analyzing infrastructure resilience are examined. The study focuses on identifying vulnerabilities in networks and finding optimal solutions for ensuring continuous infrastructure operation during crises, making this work a significant step in developing resilience strategies.

Article [11] explores the resilience of power systems, considering approaches to assessing critical infrastructure resilience and criteria established by government policies. The work presents an interdisciplinary approach integrating technical and regulatory aspects to enhance the reliability of energy infrastructure.

Research [12] highlights the use of expert judgment to assess the resilience of critical infrastructures. The authors propose a model that incorporates subjective expert evaluations for quantitatively determining resilience levels. This study is useful for rapid risk analysis in situations with limited data.

In article [13], the concept of resilience curves for infrastructure is presented. The study identifies new performance metrics and data aggregation methods to evaluate the effectiveness of infrastructure systems during emergencies. The proposed approach allows for a detailed analysis of recovery dynamics and functionality losses.

Study [14] introduces a framework for evaluating the resilience of both infrastructural and economic systems. It offers an in-depth analysis of methods for modeling interdependencies among system components, facilitating a clearer understanding of their responses to different types of threats.

Work [15] presents a scenario-based methodology for assessing the resilience of critical infrastructures, with a particular focus on the seismic resilience of seaports. The authors develop a multi-level approach that integrates scenario modeling and impact assessment, enabling precise forecasting of potential risks.

Article [16] conducts a systematic review of quantitative resilience indicators for water infrastructure systems. The research focuses on developing metrics that quantify the ability of water systems to recover functionality after adverse impacts. This study serves as a foundation for strategic decision-making in water resource management.

Study [17] analyzes approaches to measuring the resilience of transportation infrastructure. The work focuses on developing indicators and methods for resilience assessment in the context of transport systems, although it provides limited information on the specifics of the infrastructure.

In article [18], the performance of green infrastructure is investigated through the lens of urban resilience. The authors propose an analytical methodology for assessing the impact of green infrastructure on the recoverability of urban systems, considering environmental and socio-economic aspects.

Research [19] focuses on evaluating and enhancing organizational resilience in Slovakia's critical infrastructure. The work presents a multi-level approach to strengthening organizational capacity for adaptation and crisis response.

Article [20] examines principles and criteria for evaluating the resilience of energy systems in urban environments. This review study highlights key factors ensuring the reliability and continuity of energy supply under rapidly changing conditions.

In article [21], time-dependent resilience of urban infrastructural systems is assessed. The authors propose a methodology for resilience evaluation that accounts for dynamic changes in infrastructure functionality over time, enabling more precise planning for resilience improvements.

Study [22] offers a continuous and multidimensional assessment of resilience based on functional analysis for interconnected systems. This work emphasizes the importance of an integrated approach to infrastructure resilience assessment, where each element interacts with others, creating a complex network of interdependencies.

Article [23] explores metrics and methods for measuring resilience in transportation infrastructure. The work discusses the current state of development of criteria and methodologies for resilience assessment in transport systems, particularly in the context of climate change and extreme events.

Research [24] focuses on the assessment of infrastructure resilience, exploring different methods and approaches for measuring how infrastructure systems adapt to changing conditions.

Article [25] examines the integrity of infrastructure systems through a systemic perspective, highlighting the significance of integrating multiple components to ensure they can operate cohesively under unexpected circumstances.

In article [26], the concept of system resilience in the context of infrastructure is analyzed using Latvia as a case study. The research applies theoretical approaches to assessing infrastructure resilience in countries with transitional economies.

Study [27] proposes a unified approach to assessing the resilience and sustainability of urban infrastructure. This approach incorporates various parameters to evaluate infrastructure resilience under climate change and extreme events.

Article [28] proposes a qualitative methodology for evaluating the performance of IT infrastructure elements, considering technical characteristics and operating conditions. The author developed a model to assess the reliability and performance of IT system components, predict potential failures, and optimize operations, emphasizing the approach's versatility for various types of infrastructure.

Article [29] discusses a new approach to measuring the resilience of transportation infrastructure networks. The work focuses on developing methods for resilience assessment that consider various extreme event scenarios.

Research [30] addresses the assessment of resilience in interdependent infrastructure systems, emphasizing the modeling and analysis of joint recovery processes following damage.

Article [31] evaluates the resilience of interdependent infrastructures by examining different response strategies, with a focus on their capacity to recover during major disasters or crises.

3. Results

3.1. Key Criteria for Critical Infrastructure Resilience

Based on the analysis of the literature, the main criteria for the resilience of critical infrastructures have been identified (Table 1):

- *Infrastructure Functionality* – assessment of the ability of infrastructure to perform its core functions during and after stress events (e.g., natural disasters or man-made catastrophes).
- *Recovery Capability* – the ability of infrastructure to quickly recover after damage or functional disruptions. This criterion includes time, resources, and measures needed to return to normal conditions.
- *Resistance to External Threats* – the ability of infrastructure to withstand extreme factors, such as natural disasters, technological accidents, economic and social crises.
- Flexibility and Adaptability – the capacity of infrastructure to adapt to new conditions and changes, such as climate change, technological advancements, or shifts in political and economic contexts.
- *Economic Cost Assessment* – evaluation of recovery costs after a disaster, including direct costs of restoration and indirect losses from service interruptions.
- *Integration with Other Systems* – assessment of how infrastructure systems interact and depend on each other. This criterion is important for identifying how one failure may affect others.
- *Instant Analysis and Forecasting* – utilization of data for real-time evaluation of the current state of infrastructure and prediction of potential issues.
- *Flexibility of Management Structures* – the ability of management bodies and organizations responsible for infrastructure to quickly adapt to new conditions, organize effective responses, and coordinate recovery efforts.
- *Data Security and Protection* – ensuring the security of data and information systems against cyberattacks and other threats that may disrupt infrastructure operations.
- *Environmental Sustainability* – assessment of the extent to which infrastructure complies with environmental standards and can adapt to changes in the surrounding environment.

Table 1
Key Criteria for Critical Infrastructure Resilience

Criterion	Criterion Description	Sources (References)
Infrastructure Functionality	Assessment of the ability of infrastructure to perform its core functions during and after stress events.	[1], [6], [12], [17], [19], [29]
Recovery Capability	The ability of infrastructure to quickly recover after damage or functional disruptions, including time, resources, and measures needed for restoration.	[2], [9], [14], [17], [18], [29]
Resistance to External Threats	The ability of infrastructure to withstand extreme factors, such as natural disasters, technological accidents, economic, and social crises.	[3], [7], [15], [20], [24], [28]
Flexibility and Adaptability	The capacity of infrastructure to adapt to new conditions and changes, such as climate change, technological advancements, or shifts in political and economic contexts.	[4], [12], [14], [17], [26], [30]
Economic Cost Assessment	Evaluation of recovery costs after a disaster, including direct restoration costs and indirect losses from service interruptions.	[8], [11], [18], [23], [28]
Integration with Other Systems	Assessment of how infrastructure systems interact and depend on each other, identifying how one failure may impact others.	[5], [11], [15], [18], [22], [29]
Instant Analysis and Forecasting	Utilization of data for real-time evaluation of the current state of infrastructure and prediction of potential issues.	[6], [9], [19], [21], [30]
Flexibility of Management Structures	The ability of management bodies and organizations responsible for infrastructure to quickly adapt to new conditions, organize effective responses, and coordinate recovery.	[5], [14], [20], [29], [30]
Data Security and Protection	Ensuring the security of data and information systems against cyberattacks and other threats that may disrupt infrastructure operations.	[13], [15], [17], [28]
Environmental Sustainability	Assessment of the extent to which infrastructure complies with environmental standards and can adapt to changes in the surrounding environment.	[4], [7], [10], [15], [27]

Next, we will examine the tensor model of critical infrastructure resilience based on the identified resilience criteria.

3.2. Tensor Model of Resilient Critical Infrastructure

To construct a tensor model of resilient critical infrastructure based on the defined criteria, each criterion can be considered as a separate component interacting with others through specific parameters. A tensor model is a multidimensional mathematical object that allows for the description of interconnections between various characteristics of infrastructure and its resilience.

Let T represent the tensor describing the resilient critical infrastructure. Each element of the tensor corresponds to a specific resilience characteristic of the infrastructure, grouped according to its various parameters. The model can be represented as a third-order tensor:

$$T_{i,j,k}$$

where:

i – index representing individual resilience criteria,

j – index representing subsystems or components of infrastructure (e.g., energy, transportation, utility systems),

k – index representing the time aspect or stages of recovery (e.g., pre-disaster, during disaster, post-disaster).

Principles of the model operation are as follows:

- the tensor $T_{i,j,k}$ defines all the interrelationships between resilience criteria, subsystems, and stages;
- for each stage k changes in infrastructure resilience can be assessed based on specific criteria, as well as interdependencies between subsystems;
- tensor parameters can be calculated based on expert assessments, mathematical models, or statistical data.

The proposed model can easily be expanded by introducing additional tensors. For example, we can introduce an additional threat tensor Z, which demonstrates the impact of specific threats on the resilience criteria of the system.

Let there be n threats affecting the resilience of the system. Then, for each resilience criterion, we have the following threat vector Z_i, which reflects the impact of each threat on criterion i:

$$Z_i = (Z_{i1} \quad \dots \quad Z_{in}).$$

The result of the impact of threats on the resilience of subsystems can be represented by tensor S, composed of the corresponding matrices S_j^i, which contain the result of multiplying T_i by the corresponding threat element Z_{ij}. Thus, for each criterion i we will obtain a matrix of size $j \times k$, where each element of this matrix is calculated as:

$$S_{i,j,k}^l = T_{i,j,k} \times Z_{il},$$

where:

$S_{i,j,k}^l$ – element of the matrix for criterion i, subsystem j and stage k for threat l.

$T_{i,j,k}$ – element of the matrix for criterion i, subsystem j and stage k.

Z_{il} – element of the threat vector for criterion i and threat l.

The general appearance of the matrix S_j^i for each threat l is as follows:

$$S_i^l = \begin{bmatrix} S_{i,1,1}^l & S_{i,1,2}^l & S_{i,1,3}^l \\ S_{i,2,1}^l & S_{i,2,2}^l & S_{i,2,3}^l \\ S_{i,3,1}^l & S_{i,3,2}^l & S_{i,3,3}^l \end{bmatrix}.$$

Additional tensors can also be introduced into the model, which, for example, describe vulnerabilities and protection mechanisms within the system. Additionally, further interaction and mutual influence rules between tensors can be defined.

3.3. Scenarios for model research

The model, built on multidimensional tensors for assessing system resilience under the influence of threats, allows for a series of experimental studies to analyze systems in different scenarios:

1. Analysis of the impact of different threats on system resilience

- *Objective* – to investigate how different types of threats affect different resilience criteria.
- *Experiment*:
    - change the values of tensor Z to simulate varying threat intensities;
    - analyze the resulting tensor S to identify resilience criteria most affected by the threats.
- *Result* – identification of the most vulnerable criteria or subsystems.

2. Evaluation of the effectiveness of protection measures

- *Objective* – to verify how specific protective measures reduce the impact of threats.
- *Experiment*:
    - add a correction tensor to Z representing the influence of protective measures;
    - recalculate S and compare it to the baseline value.
- *Result* – assessment of the effectiveness of specific measures.

3. Analysis of disaster scenarios

- *Objective* – to model various disaster scenarios and assess system resilience at each stage.
- *Experiment*:
    - for each stage (pre-disaster, during disaster, post-disaster), modify the corresponding values of tensor T and analyze the changes in tensor S;
    - specifically, study how the system recovers after a disaster.
- *Result* – identification of critical stages requiring the most attention.

4. Comparison of systems with different resilience characteristics

- *Objective* – to assess which system has higher resilience under the same threat conditions.
- *Experiment*:
    - use different initial values of tensor T (e.g., for different organizations, regions, or system types);
    - analyze the resulting tensors S and identify the systems with the best performance.
- *Result* – ranking of systems based on resilience level.

5. Determination of system sensitivity to changes in threat intensity

- *Objective* – to investigate how changes in one or more elements of Z affect the resulting S.
- *Experiment*:
    - gradually change the threat values (e.g., increase or decrease the impact of a specific threat on a specific criterion);
    - analyze the dynamic changes in S.

- *Result* – identification of critical threats with the most significant impact on the system.

6. Determination of interrelationships between resilience criteria

- *Objective* – to find out how the impact of one threat on a specific criterion can change other criteria.
- *Experiment*:
    - analyze the matrices in tensor S corresponding to different resilience criteria;
    - build correlations between the results.
- *Result* – identification of interdependencies between criteria.

7. System parameter optimization

- *Objective* – to determine optimal parameter values to reduce the impact of threats.
- *Experiment*:
    - use optimization algorithms to find values of T that maximize resilience S with fixed Z.
- *Result* – recommendations for improving the system.

8. Modeling long-term consequences

- *Objective* – to assess how the system responds to prolonged periods of threat impact.
- *Experiment*:
    - use a variable tensor Z to model long-term or periodic threats;
    - analyze changes in S over time.
- *Result* – forecasting the long-term resilience of the system.

9. Model validation on real data

- *Objective* – to compare the model's results with real-world data.
- *Experiment*:
    - use empirical data to build T and Z.
    - compare the resulting S with actual performance indicators of systems.
- *Result* – validation of the model and its potential use for real systems.

3.4. Example of using the model for the energy sector

To apply the tensor model of critical infrastructure resilience to the energy sector, it is necessary to define how each of the resilience criteria affects energy systems and determine the values for each criterion and subsystem (e.g., energy networks, generation, and electricity transmission).

We describe the resilience criteria of the model as follows:

- *infrastructure functionality* i_1 – the ability of electrical networks and stations to perform their functions after natural disasters or man-made accidents.
- *recovery capability* i_2 – the time required to restore power supply after an accident or disaster.
- *resilience to external threats* i_3 – the ability of energy systems to withstand natural disasters (floods, snowstorms) or technological accidents.
- *flexibility and adaptability* i_4 – the ability to adapt to changes in electricity demand or new technologies, such as the integration of renewable energy sources.
- *economic cost assessment* i_5 – the cost of restoring energy infrastructure after a disaster.

- *integration with other systems* i_6 – the impact of energy disruptions on other critical infrastructures, such as transportation or utilities.
- *real-time analysis and forecasting* i_7 – the use of data to assess the current state of energy systems.
- *flexibility of management structures* i_8 – the ability of management bodies to respond quickly to energy crises.
- *data security and protection* i_9 – protection of energy systems from cyberattacks.
- *environmental resilience* i_{10} – adaptation of energy systems to environmental requirements, particularly reducing CO_2 emissions.

Let us assume there are three main subsystems of energy infrastructure:

- j_1: energy generation;
- j_2: electricity transmission;
- j_3: electricity consumption (distribution and consumption).

We will evaluate the resilience of the energy system at three stages:

- k_1: before the disaster (normal state);
- k_2: during the disaster (damage);
- k_3: after the disaster (recovery).

For each criterion (10 criteria), we have a 3x3 matrix, where each matrix represents a subsystem at different stages. Therefore, the overall form of the tensor T will be as follows (1):

$$T = \begin{bmatrix} T_1 \\ \dots \\ T_{10} \end{bmatrix}, (1)$$

where each T_i is a matrix that describes the corresponding criterion.

In particular, for each T_i (2):

$$T_i = \begin{bmatrix} T_{i,1,1} & T_{i,1,2} & T_{i,1,3} \\ T_{i,2,1} & T_{i,2,2} & T_{i,2,3} \\ T_{i,3,1} & T_{i,3,2} & T_{i,3,3} \end{bmatrix}. (2)$$

We have a three-dimensional structure where each element T_i is a matrix of size 3×3 and represents a subsystem at different stages for each resilience criterion,

where:

- the first index i represents the resilience criterion (for $i = 1,2,\dots,10$),
- the second index j (1 – generation, 2 – transportation, 3 – consumption),
- the third index k (1 – before the disaster, 2 – during the disaster, 3 – after the disaster).

Let there be 4 threats that affect the system's resilience. Then, for each resilience criterion, we have the following threat vector Z_i, which reflects the impact of each threat on criterion i (3):

$$Z_i = (Z_{i1} \quad \dots \quad Z_{i4}). (3)$$

The result of the impact of threats on subsystem resilience can be represented by a tensor S, consisting of the corresponding matrices S_j^i, which contain the result of multiplying T_i by the corresponding threat element Z_{ij}. Thus, for each criterion i, a matrix of size 3×3 will be obtained, where each element of this matrix is computed as (4):

$$S_{i,j,k}^l = T_{i,j,k} \times Z_{il}, (4)$$

where:

$S_{i,j,k}^l$ is the element of the matrix for the i-th criterion, the j-th subsystem, and the k-th stage for the l-th threat.

$T_{i,j,k}$ is the element of the matrix for the i-th criterion, the j-th subsystem, and the k-th stage.

Z_{il} is the element of the threat vector for the i-th criterion and the l-th threat.

The general form of the matrix S_j^l for each threat l is as follows (5):

$$S_i^l = \begin{bmatrix} S_{i,1,1}^l & S_{i,1,2}^l & S_{i,1,3}^l \\ S_{i,2,1}^l & S_{i,2,2}^l & S_{i,2,3}^l \\ S_{i,3,1}^l & S_{i,3,2}^l & S_{i,3,3}^l \end{bmatrix}. \quad (5)$$

For the considered example, we will model the task of analyzing disaster scenarios. The model allows assessing the resilience of the energy system to disasters by analyzing the impact of threats on key resilience criteria. Let us have the following matrices T_i for three criteria:

- infrastructure functionality (T_1):

$$T_1 = \begin{bmatrix} 0.9 & 0.8 & 0.7 \\ 0.85 & 0.8 & 0.75 \\ 0.7 & 0.6 & 0.5 \end{bmatrix}.$$

- recovery capability (T_2):

$$T_2 = \begin{bmatrix} 0.7 & 0.6 & 0.5 \\ 0.6 & 0.55 & 0.5 \\ 0.4 & 0.3 & 0.2 \end{bmatrix}.$$

- resilience to external threats (T_3):

$$T_3 = \begin{bmatrix} 0.8 & 0.7 & 0.6 \\ 0.75 & 0.65 & 0.55 \\ 0.5 & 0.4 & 0.3 \end{bmatrix}.$$

Four main threats for the three criteria ($Z_i \quad = [Z_{i1}, Z_{i2}, Z_{i3}, Z_{i4}]$):

- for T_1: $Z_1 = [0.9,0.8,0.7,0.6]$,
- for T_2: $Z_2 = [0.85,0.75,0.65,0.55]$,
- for T_3: $Z_3 = [0.8,0.7,0.6,0.5]$.

For each resilience criterion T_i we calculate the matrices S_i^l for all threats l using formula (4). Below are a few examples:

- threat 1, criterion 1 ($Z_{11} = 0.9$):

$$S_1^1 = \begin{bmatrix} 0.9 \cdot 0.9 & 0.8 \cdot 0.9 & 0.7 \cdot 0.9 \\ 0.85 \cdot 0.9 & 0.8 \cdot 0.9 & 0.75 \cdot 0.9 \\ 0.7 \cdot 0.9 & 0.6 \cdot 0.9 & 0.5 \cdot 0.9 \end{bmatrix} = \begin{bmatrix} 0.81 & 0.72 & 0.63 \\ 0.765 & 0.72 & 0.675 \\ 0.63 & 0.54 & 0.45 \end{bmatrix}.$$

- threat 2, criterion 1 ($Z_{12} = 0.8$):

$$S_1^2 = \begin{bmatrix} 0.9 \cdot 0.8 & 0.8 \cdot 0.8 & 0.7 \cdot 0.8 \\ 0.85 \cdot 0.8 & 0.8 \cdot 0.8 & 0.75 \cdot 0.8 \\ 0.7 \cdot 0.8 & 0.6 \cdot 0.8 & 0.5 \cdot 0.8 \end{bmatrix} = \begin{bmatrix} 0.72 & 0.64 & 0.56 \\ 0.68 & 0.64 & 0.6 \\ 0.56 & 0.48 & 0.4 \end{bmatrix}.$$

- threat 1, criterion 2 ($Z_{21} = 0.85$):

$$S_2^1 = \begin{bmatrix} 0.7 \cdot 0.85 & 0.6 \cdot 0.85 & 0.5 \cdot 0.85 \\ 0.6 \cdot 0.85 & 0.55 \cdot 0.85 & 0.5 \cdot 0.85 \\ 0.4 \cdot 0.85 & 0.3 \cdot 0.85 & 0.2 \cdot 0.85 \end{bmatrix} = \begin{bmatrix} 0.595 & 0.51 & 0.425 \\ 0.51 & 0.4675 & 0.425 \\ 0.34 & 0.255 & 0.17 \end{bmatrix}.$$

The results presented indicate the following:

- resilience reduction during a disaster (k_2):
    - for criterion T_1, the most vulnerable stages are in the transportation subsystem (j_2) and consumption subsystem (j_3).
    - for criterion T_2, the impact of the disaster reduces the ability for quick recovery, particularly in the generation subsystem.

4. Discussions

The results displayed on the heatmaps (Figures 1-9) provide crucial information about changes in systems and threat levels at different stages of a disaster. Each heatmap shows the values of the tensor SS for a specific stage of the disaster (before, during, after) for each criterion, such as "Infrastructure Functionality," "Restoration Capability," and "Resilience to Threats." The color scale, such as "seismic," allows for visualization of contrasts between high and low values. Warm colors like red and orange may indicate high values or critical threat levels, while cool colors like blue and purple represent low values or the absence of threats.

The threat levels can have varying impacts on different subsystems, which is reflected in the heatmap. Generally, higher threat levels lead to significant changes in the values of tensor SS, indicating vulnerabilities in infrastructure or restoration capability. Different stages of the disaster also have varying impacts on these indicators. In the pre-disaster stage, values may be relatively stable, but weak points may already be identified that require attention. During the disaster stage, tensor values can change dramatically, indicating a high level of threats and potential degradation of system efficiency. After the disaster, the recovery or stabilization process may be visible, although tensor values may remain high due to the long-term effects of the disaster (Figures 3, 6, 9).

The heatmap also shows how each subsystem, such as generation, transportation, and consumption, responds to different threat levels at various stages. For example, the "Transportation" subsystem may be more vulnerable during the disaster, while "Generation" might show more stable results before the disaster. It is important to compare the heatmaps for different disaster stages to understand how system behavior changes over time. This helps identify trends, such as an increase in system vulnerability at certain times, depending on the type of disaster and threat level.

Overall, the heatmaps help visualize how various threat levels and disaster stages impact the functionality of systems and subsystems, as well as indicate areas where improvements are necessary to enhance resilience and infrastructure recovery.

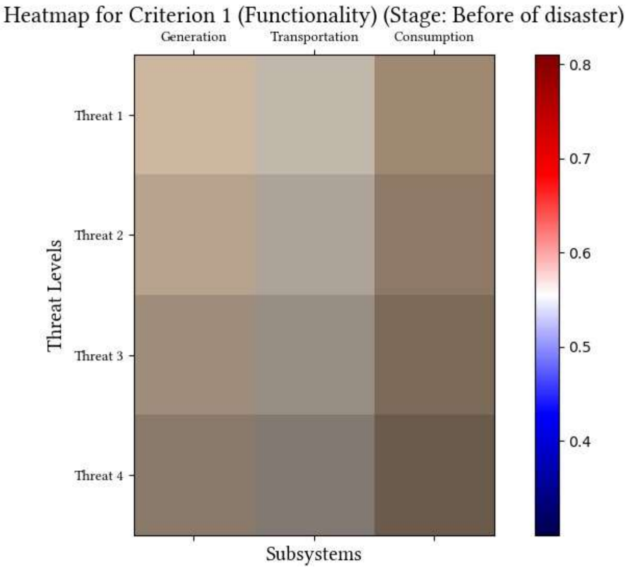

Figure 1: Heatmaps for Criterion 1 at stage “Before of disaster” of disaster analysis

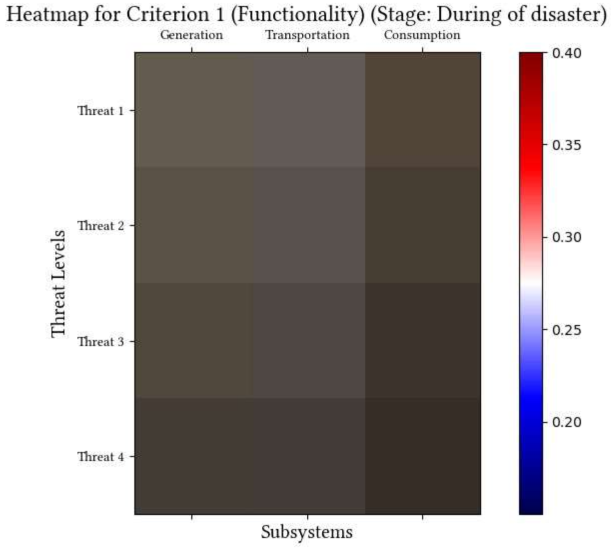

Figure 2: Heatmaps for Criterion 1 at stage "During of disaster" of disaster analysis

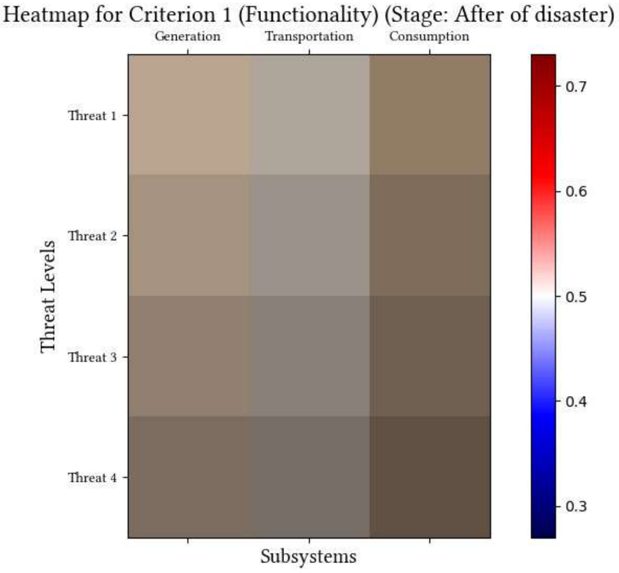

Figure 3: Heatmaps for Criterion 1 at stage "After of disaster" of disaster analysis

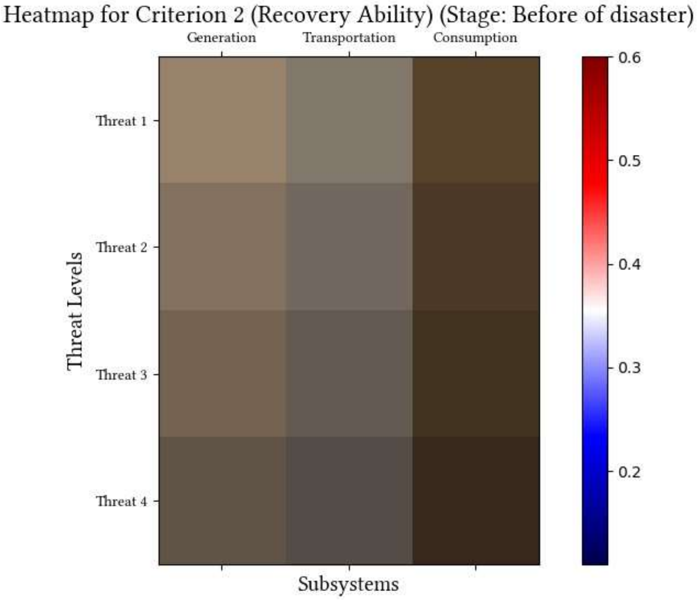

Figure 4: Heatmaps for Criterion 2 at stage "Before of disaster" of disaster analysis

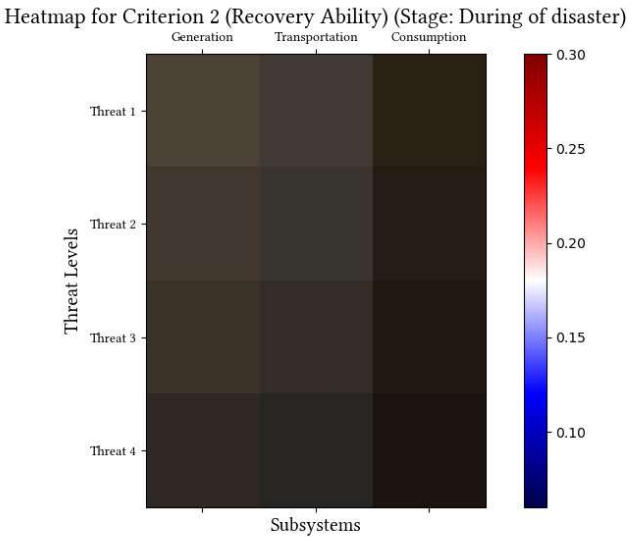

Figure 5: Heatmaps for Criterion 2 at stage "During of disaster" of disaster analysis

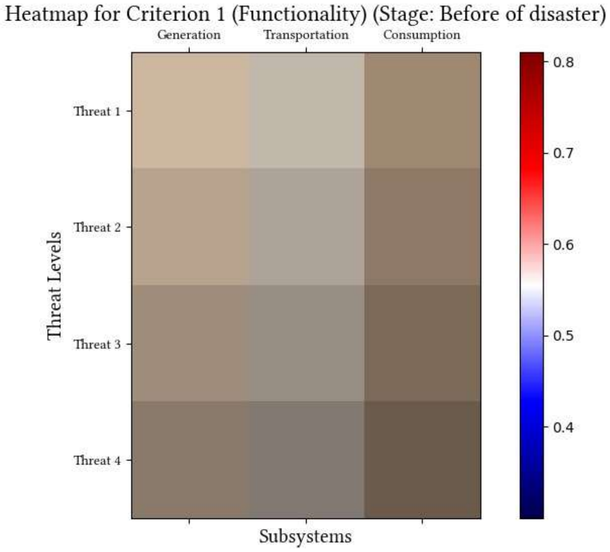

Figure 6: Heatmaps for Criterion 2 at stage "After of disaster" of disaster analysis

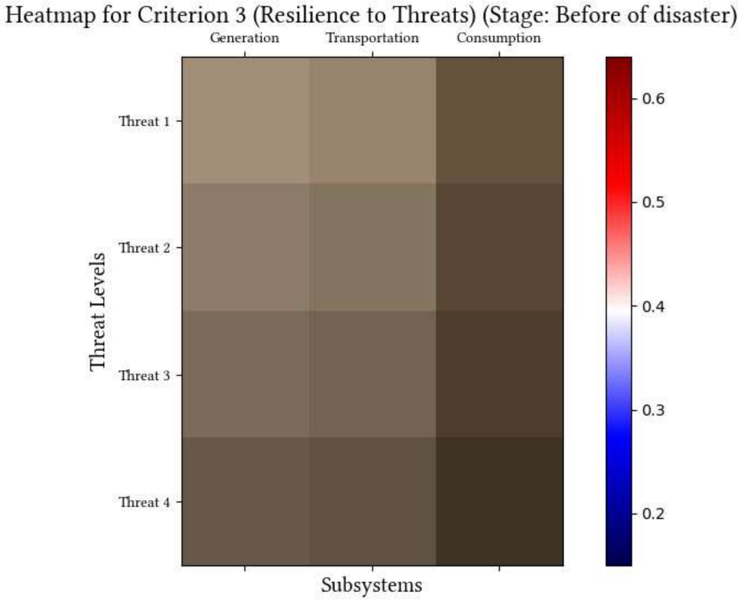

Figure 7: Heatmaps for Criterion 3 at stage "Before of disaster" of disaster analysis

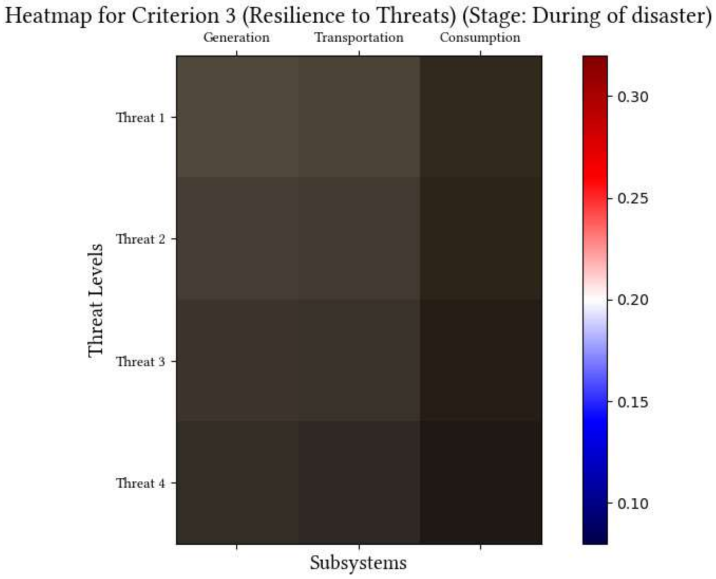

Figure 8: Heatmaps for Criterion 3 at stage "During of disaster" of disaster analysis

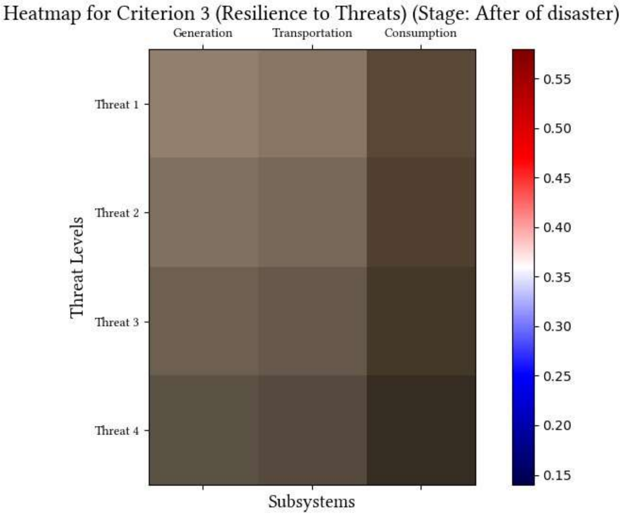

Figure 9: Heatmaps for Criterion 3 at stage "After of disaster" of disaster analysis

5. Conclusions

This paper examines the conceptual and practical aspects of ensuring critical infrastructure resilience in an era of growing complexity and system interdependence. The proposed resilient critical infrastructure model, based on tensor analysis, captures the multidimensional nature of infrastructure, threat impacts, and subsystem dynamics across different operational stages.

The model formalizes key resilience criteria, including functionality, recovery speed, adaptability, economic efficiency, data security, and environmental sustainability. Tensor-based assessments enable precise identification of vulnerabilities and the evaluation of threat impacts, particularly in energy infrastructure.

The findings highlight the model's potential for risk monitoring, forecasting, and strategy development to enhance infrastructure resilience. The approach is valuable for national security agencies, engineers, and researchers in risk management. Future work will expand the model to address intersectoral dependencies and assess the role of digitalization, AI, and blockchain in strengthening adaptive capabilities.

Declaration on Generative AI

During the preparation of this work, the authors used X-GPT-4 in order to: Grammar and spelling check. After using these tools/services, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] S. Argyroudis, S. Mitoulis, L. Hofer, M. Zanini, E. Tubaldi, and D. Frangopol, "Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets.," The Science of the total environment, vol. 714, p. 136854, Jan. 2020, doi: 10.1016/j.scitotenv.2020.136854.

[2] B. Wu, Z. Tan, A. Che, and L. Cui, "A Novel Resilience Assessment Framework for Multi-component Critical Infrastructure," IEEE Transactions on Engineering Management, vol. 71, pp. 14011–14031, 2024, doi: 10.1109/TEM.2024.3438157.

[3] C. Nan and G. Sansavini, "A quantitative method for assessing resilience of interdependent infrastructures," Reliab. Eng. Syst. Saf., vol. 157, pp. 35–53, 2017, doi: 10.1016/j.ress.2016.08.013.

[4] H. Alizadeh and A. Sharifi, "Assessing Resilience of Urban Critical Infrastructure Networks: A Case Study of Ahvaz, Iran," Sustainability, vol. 12, p. 3691, May 2020, doi: 10.3390/su12093691.

[5] R. Francis and B. Bekera, "A metric and frameworks for resilience analysis of engineered and infrastructure systems," Reliab. Eng. Syst. Saf., vol. 121, pp. 90–103, 2014, doi: 10.1016/j.ress.2013.07.004.

[6] C. Poulin and M. Kane, "The Effect of Time-Varying Value on Infrastructure Resilience Assessments," IEEE Access, vol. 9, pp. 134556–134575, 2021, doi: 10.1109/ACCESS.2021.3112944.

[7] M. Panteli, P. Mancarella, D. Trakas, E. Kyriakides, and N. Hatziargyriou, "Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems," IEEE Transactions on Power Systems, vol. 32, pp. 4732–4742, Feb. 2017, doi: 10.1109/TPWRS.2017.2664141.

[8] D. Rehak, P. Senovsky, M. Hromada, and T. Loveček, "Complex approach to assessing resilience of critical infrastructure elements," Int. J. Crit. Infrastructure Prot., vol. 25, pp. 125–138, Jun. 2019, doi: 10.1016/J.IJCIP.2019.03.003.

[9] D. Reed, K. Kapur, and R. Christie, "Methodology for Assessing the Resilience of Networked Infrastructure," IEEE Systems Journal, vol. 3, pp. 174–180, May 2009, doi: 10.1109/JSYST.2009.2017396.

[10] D. Alderson, G. Brown, and W. Carlyle, "Operational Models of Infrastructure Resilience," Risk Analysis, vol. 35, Apr. 2015, doi: 10.1111/risa.12333.

[11] H. Raoufi and V. Vahidinasab, "Power system resilience assessment considering critical infrastructure resilience approaches and government policymaker criteria," IET Generation, Transmission & Distribution, Jun. 2021, doi: 10.1049/GTD2.12218.

[12] A. Mottahedi, F. Sereshki, M. Ataei, A. Qarahasanlou, and A. Barabadi, "Resilience estimation of critical infrastructure systems: Application of expert judgment," Reliab. Eng. Syst. Saf., vol. 215, p. 107849, Jun. 2021, doi: 10.1016/J.RESS.2021.107849.

[13] C. Poulin and M. Kane, "Infrastructure Resilience Curves: Performance Measures and Summary Metrics," Reliab. Eng. Syst. Saf., vol. 216, p. 107926, Jan. 2021, doi: 10.1016/j.ress.2021.107926.

[14] E. Vugrin, D. Warren, M. Ehlen, and R. Camphouse, "A Framework for Assessing the Resilience of Infrastructure and Economic Systems," pp. 77–116, 2010, doi: 10.1007/978-3-642-11405-2_3.

[15] A. Shafieezadeh and L. I. Burden, "Scenario-based resilience assessment framework for critical infrastructure systems: Case study for seismic resilience of seaports," Reliab. Eng. Syst. Saf., vol. 132, pp. 207–219, Dec. 2014, doi: 10.1016/j.ress.2014.07.021.

[16] S. Shin et al., "A Systematic Review of Quantitative Resilience Measures for Water Infrastructure Systems," Water, vol. 10, p. 164, Feb. 2018, doi: 10.3390/W10020164.

[17] J. F. Hughes and K. Healy, “Measuring the resilience of transport infrastructure,” in Proc., 2014. [Online]. Available: https://api.semanticscholar.org/CorpusID:106702067.

[18] X.-S. Fu, M. Hopton, and X. Wang, “Assessment of green infrastructure performance through an urban resilience lens.,” Journal of cleaner production, vol. 289, Nov. 2020, doi: 10.1016/j.jclepro.2020.125146.

[19] D. Rehak, “Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak Republic,” Safety Science, vol. 123, p. 104573, Mar. 2020, doi: 10.1016/j.ssci.2019.104573.

[20] A. Sharifi and Y. Yamagata, “Principles and criteria for assessing urban energy resilience: A literature review,” Renewable & Sustainable Energy Reviews, vol. 60, pp. 1654–1677, Jul. 2016, doi: 10.1016/J.RSER.2016.03.028.

[21] O. Min and L. Dueñas-Osorio, “Time-dependent resilience assessment and improvement of urban infrastructure systems.,” Chaos, vol. 22 3, p. 33122, Aug. 2012, doi: 10.1063/1.4737204.

[22] D. Kamissoko et al., “Continuous and multidimensional assessment of resilience based on functionality analysis for interconnected systems,” Structure and Infrastructure Engineering, vol. 15, pp. 427–442, Dec. 2018, doi: 10.1080/15732479.2018.1546327.

[23] W. Sun, P. Bocchini, and B. Davison, “Resilience metrics and measurement methods for transportation infrastructure: the state of the art,” Sustainable and Resilient Infrastructure, vol. 5, pp. 168–199, May 2020, doi: 10.1080/23789689.2018.1448663.

[24] W. Xu, J. Cong, and D. Proverbs, “Evaluation of infrastructure resilience,” International Journal of Building Pathology and Adaptation, Jul. 2021, doi: 10.1108/ijbpa-09-2020-0075.

[25] R. Peculis, F. Shirvani, and P. Perez, “Assessing Infrastructure System of Systems Integrity,” 2017, doi: 10.36334/modsim.2017.f1.peculis.

[26] C. Rochas, T. Kuzņecova, and F. Romagnoli, “The concept of the system resilience within the infrastructure dimension: application to a Latvian case,” Journal of Cleaner Production, vol. 88, pp. 358–368, Feb. 2015, doi: 10.1016/J.JCLEPRO.2014.04.081.

[27] L. Wang, X. Xue, Z. Wang, and L. Zhang, “A Unified Assessment Approach for Urban Infrastructure Sustainability and Resilience,” Advances in Civil Engineering, Jul. 2018, doi: 10.1155/2018/2073968.

[28] S. Telenyk, O. Rolick, M. Bukasov, Y. Dorogiy, D. Halushko and A. Pysarenko, "Qualitative evaluation method of IT-infrastructure elements functioning," 2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Odessa, Ukraine, 2014, pp. 165-169, doi: 10.1109/BlackSeaCom.2014.6849031.

[29] L. Wang, X. Xue, and X. Zhou, “A New Approach for Measuring the Resilience of Transport Infrastructure Networks,” Complex., vol. 2020, pp. 7952309–7952309, Aug. 2020, doi: 10.1155/2020/7952309.

[30] O. Min and Z. Wang, “Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis,” Reliab. Eng. Syst. Saf., vol. 141, pp. 74–82, Sep. 2015, doi: 10.1016/J.RESS.2015.03.011.

[31] J. Kong, S. Simonovic, and C. Zhang, “Resilience Assessment of Interdependent Infrastructure Systems: A Case Study Based on Different Response Strategies,” Sustainability, vol. 11, p. 6552, Nov. 2019, doi: 10.3390/su11236552.