Conflict-aware collaborative decision support for critical infrastructure

Oksana Mulesa[1,2,*,†], Larysa Chala[3,†], Olena Melnyk[2,†], Olga Kachmar[2,†], Svitlana Baloha[2,†] and Hanna Tiutiunnykova[2,†]

[1] University of Prešov in Prešov, Námestie legionárov 3 080 01 Prešov, Slovakia
[2] Uzhhorod National University, Narodna Square 3 33100 Uzhhorod, Ukraine
[3] Kharkiv National University of Radio Electronics, Nauky av. 14 61166, Kharkiv, Ukraine

Abstract

Critical infrastructure, including energy, transport, and healthcare systems, is becoming increasingly interdependent and vulnerable to cascading risks. Traditional decision support systems typically operate within a single domain and rarely account for cross-domain conflicts. This paper introduces a conceptual model of a Conflict-Aware Collaborative Intelligent Decision Support System, integrating three key components: a cross-domain influence matrix for identifying conflicts between subsystems of critical infrastructure, multi-criteria decision analysis with an additional conflict impact criterion, and a human-AI collaborative cycle that harmonizes algorithmic recommendations with expert knowledge. The proposed approach is illustrated using examples from energy, transport, and healthcare, where potential conflicts are identified, and alternatives ranked using the TOPSIS method. The results demonstrate that incorporating conflict awareness and human-AI collaboration enhances the transparency, adaptability, and resilience of decision support systems in critical infrastructure management.

Keywords

decision support systems, critical infrastructure, cross-domain conflicts, cross-domain Influence matrix, multi-criteria decision analysis, TOPSIS, human-AI collaboration

1. Introduction

The security of critical infrastructure, including energy, transport, healthcare, and communication systems, is a fundamental element of the effective functioning of modern society [1]. The reliability and stability of these objects are crucial for both national security and the well-being of citizens. Factors directly affecting the stability of critical infrastructure include increasing complexity, interdependence, and digitalization. These factors create an environment in which decisions made in one domain can lead to conflicts or cascading consequences in others [2]. For example, energy-saving strategies in smart grids could reduce electricity availability for hospitals or emergency services, while traffic optimization measures might hinder evacuation efforts during emergencies.

Traditional decision support systems are often focused on analyzing and optimizing processes within a single domain [3]. These systems rarely consider conflicts that may arise between different domains or model the systemic consequences of localized decisions [4]. Such limitations restrict the practical applicability of these systems, especially when there is an urgent need to prevent the spread of risks and enhance the resilience of critical infrastructure during crises.

Rapid advancements in artificial intelligence (AI), multi-criteria decision-making (MCDM), and risk modeling allow for more effective handling of uncertainty, complex system interconnections,

*AISSLE-2025: International Workshop on Applied Intelligent Security Systems in Law Enforcement, October, 30–31, 2025, Vinnytsia, Ukraine

1,* Corresponding author.
† These authors contributed equally.
oksana.mulesa@unipo.sk (O. Mulesa); larysa.chala@nure.ua (L. Chala); olena.melnyk@uzhnu.edu.ua (O. Melnyk); olgakachmar63@gmail.com (O. Kachmar); switlana.baloha@uzhnu.edu.ua (S. Baloha); ganna.tyutynnykova@uzhnu.edu.ua (H. Tiutiunnykova)
0000-0002-6117-5846 (O. Mulesa); 0000-0002-9890-4790 (L. Chala); 0000-0001-7340-8451 (O. Melnyk); 0009-0007-5139-7801 (O. Kachmar); 0000-0002-1221-9072 (S. Baloha); 0000-0003-0859-6382 (H. Tiutiunnykova)

and dynamically changing conditions. Modern tools (models, methods, algorithms) are effective at detecting deviations in large data streams, evaluating trade-offs between alternatives, and automating routine decisions [5, 6]. However, despite these advantages, many of these tools allow for isolated decisions, often within a single sector, and fail to account for cross-domain impacts. As a result, the lack of a unified, conflict-aware approach limits their practical value in critical infrastructure management, where decisions have intersectoral impacts and may result in cascading effects.

This paper proposes a conceptual model of Conflict-Aware Collaborative Decision Support Systems (CIDSS), which extends the capabilities of traditional decision support systems (DSS). This extension is achieved through the integration of three key components:

- Identifying conflicts between interdependent subsystems using influence matrix models.
- Performing multi-criteria risk analysis using fuzzy logic methods and entropy-based indicators to assess uncertainty.
- Implementing human-AI collaboration (HAIC), enabling more effective real-time decision-making.

Thus, we present a unified model that identifies and quantifies conflicts between subsystems, integrates collaboration mechanisms to enhance resilience, transparency, and continuous functioning of critical infrastructure.

2. Prior Work

Recent research has significantly advanced the development and implementation of DSS and MCDM methods to solve problems in various applied scientific domains. These studies have shown that MCDM is an effective tool for comparing alternatives across multiple criteria, which is especially necessary when analyzing complex systems [7, 8]. For instance, studies [9, 10] have proven that MCDM has become foundational in solving modern engineering and environmental problems. However, these solutions tend to focus on optimization within a single domain and do not account for cross-domain conflicts.

Equally interesting and relevant are studies focused on anomaly detection and cybersecurity threats in critical infrastructure. Recent publications highlight the limitations of traditional defense mechanisms in addressing increasingly complex and rapidly evolving cyber threats [11, 12]. The growing digitalization of critical infrastructure significantly increases the potential for cyberattacks and system failures. As a result, new detection and prevention tools are being developed. For instance, the paper [12] explored unsupervised anomaly detection models integrated into IIoT technologies. This approach proved effective for detecting cyberattacks in near-real time. A systematic review of adaptive anomaly detection methods for cyber-physical systems demonstrated that models combining rapid adaptation and real-time data processing are the most promising for identifying evolving attacks [11]. Additionally, the study [13] stressed the importance of combining supervised and unsupervised methods for improving anomaly detection accuracy in critical infrastructure. Research [14] described a combination of digital sensors and intelligent data analysis for AI-based anomaly detection in smart city IoT networks, offering practical recommendations to enhance the resilience of smart cities against cyber threats. However, these studies primarily focus on anomaly detection without proposing integrated mechanisms for harmonizing decisions across sectors.

Another relevant area of research is the application of fuzzy and entropy methods for handling uncertainty. These methods are especially useful when the parameters of conflicts and risks lack clear, unambiguous interpretations. For instance, [15] applied Enhanced Entropy-Fuzzy DSS in risk management for hydraulic engineering projects, enabling the processing of complex, ambiguous information for more accurate risk assessments. A fuzzy Shannon entropy model was used for ranking water management scenarios under uncertainty [16]. Similarly, [17] combined fuzzy DSS

and unstructured data processing techniques to optimize energy systems, showing how fuzzy models enhance decision-making reliability in uncertain conditions. These and other approaches are well-suited for evaluating uncertainty, but are generally limited to specific tasks.

Furthermore, research on HAIC in decision-making processes has gained traction. Works [18,19] propose methods for integrating human expertise with AI capabilities in decision support systems. These studies suggest multi-channel decision support architectures where decisions are made through interactions among multiple channels. In case of conflicts between these channels, decision-making is entrusted to competent experts. In [20], a decision tree framework for selecting evaluation metrics for HAIC across different modes balances both quantitative and qualitative measures. The study [21] outlines seven interaction patterns between AI and humans, emphasizing the need for well-designed protocols to ensure effective collaboration. These studies demonstrate that AI can serve as an effective partner in decision-making, rather than replacing human expertise. A related direction is represented by the work [22], which developed a neural network system for predicting anomalous data in applied sensor networks. Their results illustrate how AI-based predictive models can support human experts by detecting abnormal patterns and preventing decision conflicts in real-time monitoring systems.

Thus, current research demonstrates a wide range of approaches to DSS design. However, most of them have been implemented in isolation: either within one sector or without considering cross-domain consequences. This creates a need for conflict-aware collaborative decision support systems that can integrate various approaches and ensure the harmonization of decisions to improve critical infrastructure resilience.

3. Methodology

In this study, we propose a conceptual model for Conflict-Aware Collaborative Decision Support Systems in critical infrastructure systems. This model integrates conflict identification, multi-criteria risk analysis, and human–AI collaboration. The model emphasizes the need to identify relationships between subsystems to prevent conflicts during decision-making. Both AI tools and expert knowledge will be utilized to harmonize decisions.

3.1. Influence Matrix Modeling

The first important task of the developed model is to identify and describe interdependencies between subsystems of critical infrastructure. The model uses an influence matrix $M = (m_{ij})$, where the elements contain formalized information about the relationships between decisions made in one subsystem and their consequences for other subsystems. This approach is based on the concept of cross-impact analysis, where matrices define pairwise direct impacts between variables representing the complexity of social, economic, and technological systems [22]. The rows of the matrix correspond to the subsystems where decisions are made, and the columns correspond to the parameters that can change as a result of the decisions made. The element m_{ij} indicates the degree of influence of the decision in subsystem i on the parameter in subsystem j, and its interpretation is as follows:

- If $m_{ij} > 0$, the local decision enhances the efficiency of the other subsystem;
- If $m_{ij} < 0$, the decision creates threats or constraints;
- If $m_{ij} <= 0$, there is no significant influence.

The elements of the influence matrix are typically calculated based on statistical data, expert conclusions, and scenario simulation results [23].

The use of the influence matrix in this way helps to form the input information for multi-criteria analysis and fuzzy-entropy methods for evaluation.

3.2. Conflict Detection

After constructing the influence matrix, a procedure for identifying cross-domain conflicts is initiated. A conflict occurs when optimizing or improving a parameter in one subsystem leads to deterioration of a parameter in another subsystem. Clearly, a conflict occurs if $m_{ij} < 0$. To reduce noise, we propose introducing a threshold value α. Thus, the conflict set C in the system can be formed using rule (1):

$$C = \{(i, j) | m_{ij} < 0, |m_{ij}| > \alpha\}. \quad (1)$$

The set described by (1) defines all identified critical conflicts in the system.
Conflicts are classified as follows:

- Direct conflicts, where a decision from one subsystem directly reduces the efficiency of another;
- Indirect conflicts, where the impact is transmitted through a chain of consequences to the subsystem;
- Cascading conflicts, which lead to system failures.

To identify conflicts in the influence matrix, threshold analysis, graph approaches, and clustering are used [24].

According to the proposed concept, the identified conflicts serve as input data for the multi-criteria risk analysis phase, and the conflict detection module acts as an intermediate module between the formal description of dependencies and the multi-criteria risk analysis module.

3.3. Multi-Criteria Risk Analysis

The next step, after identifying the conflict set, is the evaluation of alternatives and the formation of a set of compromise solutions. In this approach, multi-criteria decision analysis is used, which allows for the consideration of various types of criteria, including conflicting ones, as well as cross-domain impacts.

The mathematical formulation of the task is as follows:

- Let $A = \{a_1, a_2, \ldots, a_n\}$ be the set of alternatives representing the decisions within the given subsystem;
- $K = \{k_1, k_2, \ldots, k_m\}$ be the set of criteria by which the influence of alternatives on the given and other subsystems is evaluated;
- $D = (d_{ij})_{n \times m}$ be the evaluation matrix, where d_{ij} represents the evaluation of alternative a_i with respect to criterion k_j;
- $W = (w_1, w_2, \ldots, w_m)$ be the vector of criterion weights, where $\sum_{j=1}^{m} w_j = 1$;
- $M = (m_{il})_{n \times n}$ be the matrix of cross-domain influences;
- C be the set of conflicts, defined as in equation (1).

The task of multi-criteria risk analysis is to identify the alternative $a^{¿} \in A$ that minimizes the integral risk and the level of conflict, taking into account the weights of the criteria and any constraints. Thus, the problem can be represented in the form of equation (2):

$$a^{¿} \in \arg\min_{a_i \in A} R(a_i), \quad (2)$$

where the integral risk assessment of an alternative is defined by equation (3):

$$R(a_i)=\sum_{j=1}^{m} w_j \cdot f\left(d_{ij}^{'}\right)+w_c \cdot g\left(k_c(a_i)\right). \tag{3}$$

In equation (3) $d_{ij}^{'}$ is the evaluation of alternative a_i with respect to criterion k_j, adjusted for conflicts; $f\left(d_{ij}^{'}\right)$ is the normalized utility function; $k_c(a_i)$ is the conflict index of alternative; $g(\bullet)$ is the penalty function that converts the conflict value into additional risk; w_c is the weight of the conflict criterion.

Thus, the multi-criteria risk analysis problem is a task of simultaneously minimizing both risk and conflict.

As indicated by the formulated task, conflicts in equation (2) can be integrated by penalizing local evaluations, introducing an additional criterion that describes the conflict, and utilizing a fuzzy representation of conflict.

Local evaluations can be penalized as follows: if alternative ai creates a conflict with another subsystem, i.e., $(i,j)\in C$, its evaluations are modified according to equation (4):

$$R(a_i)=\sum_{j=1}^{m} w_j \cdot f\left(d_{ij}^{'}\right)+w_c \cdot g\left(k_c(a_i)\right). \tag{4}$$

where $\gamma_{ij}=|m_{ij}|$ is the intensity of the conflict, $\beta\in[0,1]$ is the scale coefficient.

An additional criterion describing conflict can be represented as an aggregated conflict index (5):

$$k_c(a_i)=\sum_{j:(i,j)\in C} |m_{ij}|. \tag{5}$$

Furthermore, the application of fuzzy set theory and linguistic variables can be employed to assess the intensity of conflicts linguistically, for instance, categorizing them as “low”, “medium”, or “high”.

The outcomes derived from solving the problem outlined in equation (2) can provide a robust foundation for the ranking of alternatives, incorporating both the conflicts and inter-domain risks.

3.4. Human–AI Collaboration

The final component of the proposed CIDSS is the integration of human expertise in the decision-making process. As shown in Figure 1, the architecture consists of three key elements: the AI Module, the Collaboration Interface, and the Human Expert.

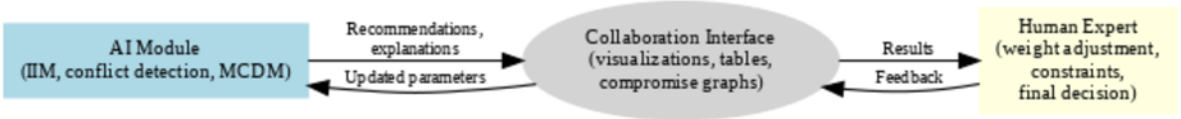

Figure 1: Conceptual model of Human-AI collaboration as the final component of CIDSS.

According to the proposed model, the AI Module performs automated tasks such as the Inter-domain Influence Matrix (IIM), conflict detection, and MCDM. The outcomes of these tasks are recommendations and explanations, which are presented through the Collaboration Interface. The Collaboration Interface, in turn, displays the results in the form of visualizations, tables, and compromise graphs, etc., thus making the process transparent and interpretable. At this stage, an environment is created where the user gains access not only to the final result but also to the explanations upon which it is based.

The Human Expert stage represents the final component of the collaborative model, which provides results in the form of a preliminary ranking or decision, as well as feedback through weight adjustment, additional constraints, and the final decision. All of this data is fed back into the

system as updated parameters, triggering a new iteration of the analytical cycle.

Thus, the final component of the model ensures a closed-loop cycle: from automated conflict detection and recommendation generation to human interpretation, parameter adjustment, and the final decision-making process. This allows for the integration of the computational power of AI with human expertise, which is critical for managing complex and interdependent subsystems of critical infrastructure.

4. Case study

To illustrate the application of the developed conceptual model, a numerical example is presented, depicting the interrelationships among multiple subsystems of critical infrastructure. The following sections will outline the procedure for constructing the influence matrix, identifying conflicts, and ranking alternatives for the selected domains.

4.1. Scenario Description and IIM Construction

Consider a scenario involving three interrelated subsystems of critical infrastructure: energy, transportation, and healthcare. These subsystems are crucial due to the fact that energy ensures continuous electricity supply, which is essential for the functioning of most other sectors; transportation encompasses logistics hubs that are critically dependent on the energy sector; healthcare, in turn, relies both on the stability of energy supply and the accessibility of transportation infrastructure.

In accordance with the developed concept, the interrelationships between the subsystems can be represented using the IIM with three rows and three columns. The method for constructing this matrix is presented in Table 1.

Table 1
Example IIM for the Energy, Transport, and Healthcare subsystems

Subsystems	Energy	Transport	Healthcare
Energy	0	-0.7	-0.9
Transport	-0.3	0	-0.5
Healthcare	-0.2	-0.4	0

As seen in Table 1, decisions in the energy sector have a significant impact on transport and healthcare, while decisions in the healthcare sector minimally affect other domains.

4.2. Scenario Description and IIM Construction

Based on the constructed Inter-domain Influence Matrix (Table 1), we perform the identification of potential conflicts and form the conflict set C according to equation (1). In this case, it was observed that $\alpha = 0.4$. As shown in the analysis of Table 1, the conflict set is given by equation (6):

$$C=\{(E,T),(E,H),(T,H),(H,T)\}. \quad (6)$$

The visualization of the conflict set is presented in Figure 2.

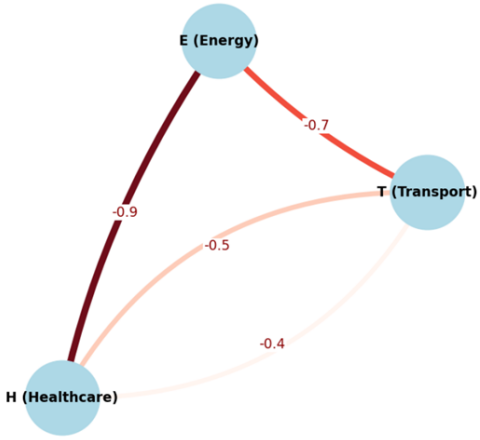

Figure 2: Conceptual model of Human-AI collaboration as the final component of CIDSS.

In Figure 2, the conflict set is represented as a graph, where the edges show significant negative impacts between the subsystems.

4.3. Multi-Criteria Analysis of Alternatives

After forming the conflict set C, we proceed with multi-criteria analysis. According to the developed concept, we construct the evaluation matrix D. In this matrix, the rows correspond to the alternatives, and the columns correspond to the evaluation criteria. In this model, we consider the following alternatives for the energy subsystem:

- A1 – Reducing production to save resources;
- A2 – Maintaining a stable level of production;
- A3 – Increasing production during peak periods.

The evaluation criteria are effectiveness, cost, stability, and conflict impact. The evaluation matrix is presented in Table 2.

Table 2
Evaluation Matrix

Alternative	Effectiveness	Cost	Stability	Conflict impact
A1	0.6	0.8	0.4	0.9
A2	0.7	0.6	0.7	0.4
A3	0.9	0.4	0.8	0.2

As shown in Table 2, alternative A1 is attractive in terms of cost, but it has a very high conflict impact, significantly limiting the transport and healthcare sectors. On the other hand, alternative A3 is more expensive but significantly reduces conflicts and increases system stability.

Based on the evaluations and the weight coefficients of the criteria, MCDM ranking is performed. To illustrate this process, the TOPSIS method [7,26] was applied. The idea behind this method is that the best alternative should be as close as possible to the ideal solution and as far as possible from the anti-ideal solution. As a result of applying this method, the evaluation of the alternatives is as follows: C_{A1} = 0.32, C_{A2} = 0.55, C_{A3} = 0.78. Thus, the best alternative is A3, which demonstrates the highest performance and resilience with minimal conflict impact.

4.4. Role of Human-AI Collaboration

The final stage of the Conflict-Aware CIDSS involves aligning decisions with the help of competent experts. The results obtained in the previous section allowed us to create an initial ranking of alternatives based on predefined criteria (effectiveness, cost, stability, and conflict impact). However, these results reflect only the algorithmic evaluation, without considering the context, regulatory requirements, or organizational priorities. At this stage, the expert is introduced to the process. According to the schema in Figure 1, the expert receives a visualization of the ranking results (e.g., using the TOPSIS method). The expert can adjust the weight coefficients, apply additional constraints, and submit the updated parameters back to the system. The system then automatically repeats the TOPSIS evaluation with the updated parameters. Thus, the final human-AI collaboration ensures a transparent iterative process: AI generates recommendations through MCDM analysis (specifically, TOPSIS), and the human expert adapts these recommendations to real-world conditions and makes the final decision. This allows for combining computational optimality with expert context and enhancing the resilience of critical infrastructure management.

During each iteration, the expert can modify the weight vector $\mathbf{w}$ based on organizational priorities or contextual constraints (e.g., prioritizing stability over cost during emergencies). These adjustments directly influence the TOPSIS distance measures and may change the ranking order of alternatives, allowing the expert to explore "'what-if' scenarios."

5. Discussion

The proposed concept offers several advantages over traditional DSS by incorporating a conflict-aware approach into decision-making processes for critical infrastructure. Unlike classical DSS, this model accounts for cross-domain impacts and conflicts, making the system more adaptable and effective in responding to the growing interdependence of critical infrastructure systems.

The key contribution of this research is the introduction of the conflict impact criterion into multi-criteria analysis. By including this criterion, we have shown that an alternative with the lowest cost or highest effectiveness may be unacceptable due to its high conflict level with other domains. This is particularly relevant in scenarios where locally optimal decisions can create systemic cross-domain risks.

An essential feature of the proposed concept is the human–AI collaboration component. This module enables the integration of expert knowledge into the decision-making process, which increases trust in automated solutions. This iterative process has been shown to significantly enhance decision-making in human-centered AI environments.

However, the model has limitations. It is sensitive to the availability of reliable data for constructing the Inter-domain Influence Matrix, and its performance depends heavily on the expertise and accuracy of the experts involved. Additionally, as the number of subsystems increases, the computational complexity of the methods will rise significantly. Future research directions include the integration of explainable AI (XAI) methods to further enhance the transparency of the recommendations. Thus, the results confirm the feasibility of integrating conflict-aware approaches into DSS for critical infrastructure and outline directions for future research and improvement of the proposed model.

At this stage, the system remains conceptual. The next step will involve prototyping the CIDSS within an existing resilience DSS environment, using simulated datasets. Potential application domains include energy and smart city management, where conflict-aware decision support can improve coordination between sectors during crisis response.

6. Conclusions

This paper presents a conceptual model of a Conflict-Aware Collaborative Intelligent Decision Support System for managing critical infrastructure. Unlike traditional decision support systems, this model considers cross-domain conflicts within critical infrastructure systems. The main

findings of this research are as follows:

1. The use of the Inter-domain Influence Matrix to formalize relationships between subsystems of critical infrastructure.
2. The identification of a conflict set C which is integrated into MCDM by introducing a *conflict impact* criterion.
3. The application of the TOPSIS method has been demonstrated as an example of an MCDM technique for ranking alternatives in the energy sector, taking into account their impact on transportation and healthcare.
4. The development of the final component of the model – Human-AI Collaboration – which allows experts to interact with the system, adjust weights, impose constraints, and make final decisions.

The practical significance of this approach lies in its potential to serve as a foundation for developing decision support systems that enhance the resilience of critical infrastructure under crisis conditions. The model can be applied in the energy, transport, healthcare, and other interdependent domains.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] R. Shawe, "The crucial role of safeguarding critical infrastructure in ensuring the stability and security of the U.S. supply chain," American Journal of Industrial and Business Management, vol. 15, pp. 1055–1071, 2025. https://doi.org/10.4236/ajibm.2025.157051

[2] G. P. Cimellaro, A. Cardoni and A. Reinhorn, "Modelling infrastructure interdependencies and cascading effects using temporal networks," Resilient Cities and Structures, vol. 3, pp. 28–42, 2024. https://doi.org/10.1016/j.rcns.2024.05.002

[3] [3] I. Izonin, T. Hovorushchenko and S. K. Shandilya, "Quality and security of critical infrastructure systems," Big Data and Cognitive Computing, vol. 8, no. 10, 2024. https://doi.org/10.3390/bdcc8010010

[4] M. Benfer and M. Hörger, "Bridging planning silos: A cross-functional decision support system for capacity, order and supplier decisions in global production networks," CIRP Annals, vol. 74, pp. 603–607, 2025. https://doi.org/10.1016/j.cirp.2025.04.029

[5] T. Radivilova, L. Kirichenko, A. S. Alghawli, D. Ageyev, O. Mulesa, O. Baranovskyi, A. Ilkov, V. Kulbachnyi and O. Bondarenko, "Statistical and signature analysis methods for intrusion detection," in: R. Oliynykov, O. Kuznetsov, O. Lemeshko and T. Radivilova (Eds.), Information Security Technologies in the Decentralized Distributed Networks, Lecture Notes on Data Engineering and Communications Technologies, vol. 115, Springer, Cham, 2022, pp. 115–131.

[6] A.-A. Bouramdane, "Cyberattacks in smart grids: Challenges and solving multi-criteria decision-making for cybersecurity options including AI-based ones using AHP," Journal of Cybersecurity and Privacy, vol. 3, pp. 662–705, 2023. https://doi.org/10.3390/jcp3040031

[7] M. Madanchian and H. Taherdoost, "A comprehensive guide to the TOPSIS method for multi-criteria decision making," Sustainable Social Development, vol. 1, 2023. https://doi.org/10.54517/ssd.v1i1.2220

[8] J. Więckowski, W. Sałabun, B. Kizielewicz, A. Bączkiewicz, A. Shekhovtsov, B. Paradowski and J. Wątróbski, "Recent advances in multi-criteria decision analysis: Applications and trends," International Journal of Knowledge-Based and Intelligent Engineering Systems, vol. 27, pp. 367–393, 2023. https://doi.org/10.3233/KES-230487

[9] A. Štilić and A. Puška, “Integrating MCDM methods with sustainable engineering: A comprehensive review,” Engineering, vol. 4, pp. 1536–1549, 2023. https://doi.org/10.3390/eng4020088

[10] P. Digkoglou, A. Tsoukiàs, J. Papathanasiou and K. Gotzamani, “Meta-analysis of review literature on MCDM for environmental issues,” Applied Sciences, vol. 14, p. 10862, 2024. https://doi.org/10.3390/app142310862

[11] P. Moriano, S. C. Hespeler, M. Li and M. Mahbub, “Adaptive anomaly detection for identifying attacks in CPS: A systematic review,” Artificial Intelligence Review, vol. 58, p. 283, 2025. https://doi.org/10.1007/s10462-025-11292-w

[12] A. Pinto, L.-C. Herrera, Y. Donoso and J. A. Gutierrez, “Enhancing critical infrastructure security using unsupervised learning for anomaly detection,” International Journal of Computational Intelligence Systems, vol. 17, p. 236, 2024. https://doi.org/10.1007/s44196-024-00644-z

[13] A. Kumar and J. A. Gutierrez, “Impact of machine learning on IDS protection for critical infrastructure,” Information, vol. 16, p. 515, 2025. https://doi.org/10.3390/info16070515

[14] H. Zeng, M. Yunis, A. Khalil and N. Mirza, “AI-driven anomaly detection in smart city IoT for enhanced cybersecurity,” Journal of Innovation & Knowledge, vol. 9, p. 100601, 2024. https://doi.org/10.1016/j.jik.2024.100601

[15] Y. Li and Y. Wang, “Enhanced entropy-fuzzy DSS for risk assessment in hydraulic engineering,” Information, vol. 49, 2025. https://doi.org/10.31449/inf.v49i20.7461

[16] M. F. Dehkordi, S. M. Hatefi and J. Tamošaitienė, “Fuzzy Shannon entropy and fuzzy ARAS for water resources risk management,” Sustainability, vol. 17, p. 5108, 2025. https://doi.org/10.3390/su17115108

[17] Z. Zhang, “Energy system optimization using fuzzy DSS and unstructured data,” Energy Informatics, vol. 7, p. 82, 2024. https://doi.org/10.1186/s42162-024-00396-2

[18] S. Dolgikh and O. Mulesa, “Collaborative human-AI decision-making systems,” in: IntSol Workshops, 2021, pp. 96–105. https://ceur-ws.org/Vol-3106/Paper_9.pdf

[19] O. Mulesa, M. Kotsipak, S. Dolgikh, Y. Bilak, T. Radivilova and O. Baranovskyi, “Human-AI collaborative decision systems with numerical channels,” in: Proc. 12th Int. Conf. Advanced Computer Information Technologies (ACIT), IEEE, Ruzomberok, Slovakia, 2022, pp. 5–8.

[20] G. Fragiadakis, C. Diou, G. Kousiouris and M. Nikolaidou, “Evaluating human-AI collaboration: Review and methodological framework,” 2024.

[21] C. Gomez, S. M. Cho, S. Ke, C.-M. Huang and M. Unberath, “Human-AI collaboration is not very collaborative: A taxonomy from systematic review,” Frontiers in Computer Science, vol. 6, p. 1521066, 2025. https://doi.org/10.3389/fcomp.2024.1521066

[22] S. Vladov, V. Vysotska, V. Sokurenko, O. Muzychuk, M. Nazarkevych and V. Lytvyn, “Neural network system for predicting anomalous data in applied sensor systems,” Applied System Innovation, vol. 7, p. 88, 2024. https://doi.org/10.3390/asi7050088

[23] S. Tripathi, N. Bachmann, M. Brunner and H. Jodlbauer, “Analyzing cross-impact matrices for managerial decision-making using DEMATEL,” in: Proc. 11th Int. Conf. Data Science, Technology and Applications, SCITEPRESS, Lisbon, 2022, pp. 370–382.

[24] A. Larsson and C. Große, “Data use and data needs in critical infrastructure risk analysis,” Journal of Risk Research, vol. 26, pp. 524–546, 2023. https://doi.org/10.1080/13669877.2023.2181858

[25] E. K. Elsayed, A. S. E. Ahmed and H. R. Younes, “Enhancing semantic belief function for decision conflict handling in SoS,” PeerJ Computer Science, vol. 7, e468, 2021. https://doi.org/10.7717/peerj-cs.468

[26] M. Behzadian, S. Khanmohammadi Otaghsara, M. Yazdani and J. Ignatius, “A state-of-the-art survey of TOPSIS applications,” Expert Systems with Applications, vol. 39, pp. 13051–13069, 2012. https://doi.org/10.1016/j.eswa.2012.05.056