Neutrosophic Systems with Applications, Vol. 3, 2023
https://doi.org/10.61356/j.nswa.2023.18

Neutrosophic MCDM Methodology for Assessment Risks of Cyber Security in Power Management

Ahmed M.AbdelMouty [1,*] and Ahmed Abdel-Monem [2]

[1] Information system department, Faculty of Computers and Informatics, Zagazig University, Alsharkiya, Egypt; a_abdelmouty@zu.edu.eg.

[2] Decision support department, Faculty of Computers and Informatics, Zagazig University, Alsharkiya, Egypt; aabdelmonem@zu.edu.eg.

* Correspondence: a_abdelmouty@zu.edu.eg.

Abstract: Every day, new reports of cyberattacks on interconnected control systems emerge. The vulnerability of their communication mechanism makes similar control systems a target for malicious outsiders. Protecting sensitive data and maintaining network reliability and availability are two of the main reasons why network security is so important. Strong and dependable network security strategies use a number of safeguards to protect users and businesses from malware and cyber assaults like distributed denial of service. A safety analysis is an essential step that must precede the introduction of any security measures. There hasn't been much experience with cyberattacks on power control systems yet, therefore it's important to develop a method for thoroughly assessing the safety of power control technologies used in data transmission systems. A prior study has identified the authority control process evaluation of security and the safety level of each control stage as two of the primary obstacles to effective security assessment. For this reason, this article provides a safety risk evaluation of the communication networks of power management and control technologies (PMCT) using the neutrosophic Evaluation Based on Distance from Average Solution (EDAS) method. A prime instance of a multi-criteria decision-making (MCDM) issue is used to solve the security risk assessment in the power system. In this study, we offer an interval-valued neutrosophic version of the EDAS approach for solving the MCDM issue. The neutrosophic EDAS method is used to rank and assess the security risks in power system.

Keywords: Power Management; Risk Assessment; Cyber Security; Neutrosophic Sets; MCDM.

1. Introduction

The primary uses of information and communication technology (ICT) in today's power systems include tariffing and trading, network scheduling, oversight, and computerization grid linking of green power and electric shipping, managing power, electrical security measures, cyber security, and abundant data-based executions like (predicting) maintenance. Huge R&D efforts are now in progress in each of these fields. Power is seen as crucial to a country's development plan, yet in the present climate, utilization is inadequate and costs are on the rise [1, 2].

Therefore, sustainable power sources should be used for long-term use. And renewable sources of power, such as solar, are only accessible during daylight hours. By employing sources of clean power as part of an integrated power grid, it is crucial to provide a steady supply of electricity throughout the day. Power management and control technologies (PMCT) aim to reduce a building's power and operational costs while maintaining safe and healthy conditions for the building's inhabitants. Due to developments in electronics, computing technology, and state-of-the-art

interactions, PMCTs have been developed to improve indoor quality while conserving more electricity.

Fire alarms, security cameras, badge readers, lighting systems, etc. are just a few of the many outside sensors and solutions that make up the PMCT framework. Heating, ventilation, and air conditioning (HVAC) structures, as well as supporting power systems like microgrids and power restores, are also included. The growing focus on EMCS security has resulted in the inclusion of additional stakeholders, such as the building managers in charge of the at-risk PMCT design.

This article provides essential factors that may greatly improve data safety control rules for those now responsible for guaranteeing that PMCT has the requisite degree of cyber security procedures as part of its essential risk control programs. Protection of PMCT is complicated by the nature of many of the components utilized to deliver a wide variety of support services. Components of the PMCT that are still in use present often have a lengthy history. When element design and distribution initially started, the idea of connected devices did not yet exist [3, 4].

Unfortunately, PMCT still has a long way to go before it can be considered adequately cyber secure. Multiple advanced and intricate control networks have recently been developed using easily accessible networking technology. They still need a concerted effort and engagement from numerous stakeholders to secure them against hostile actors, despite increased understanding from a cybersecurity perspective. Organizations providing support for vital infrastructure must ensure that all operating equipment, regardless of age, is adequately protected against intrusion. Several agencies mandate rigorous cyber security for all power administration and oversight systems. An effective risk management strategy must be put in place for every business [5, 6].

The purpose of this research was to use the neutrosophic Evaluation Based on Distance from Average Solution (EDAS) method to evaluate the security threat posed by PMCT. Additionally, the neutrosophic EDAS method was applied to problems involving group decision-making in a neutrosophic environment. It is the method of choice when all of the factors being considered are of equal weight yet there is little information available to help narrow the field [7]–[10]. Figure 1 shows the security risk assessment in power system. The criteria and alternatives are collected from the power system and cyber security risk assessment then entered as input to the interval-valued neutrosophic set and EDAS multi-criteria decision making (MCDM) methodology. The assessment of security in power system has many and various criteria, so the concept of MCDM. Then we applied the steps of EDAS method to compute the weights of criteria and rank the high risks in security assessment in power system.

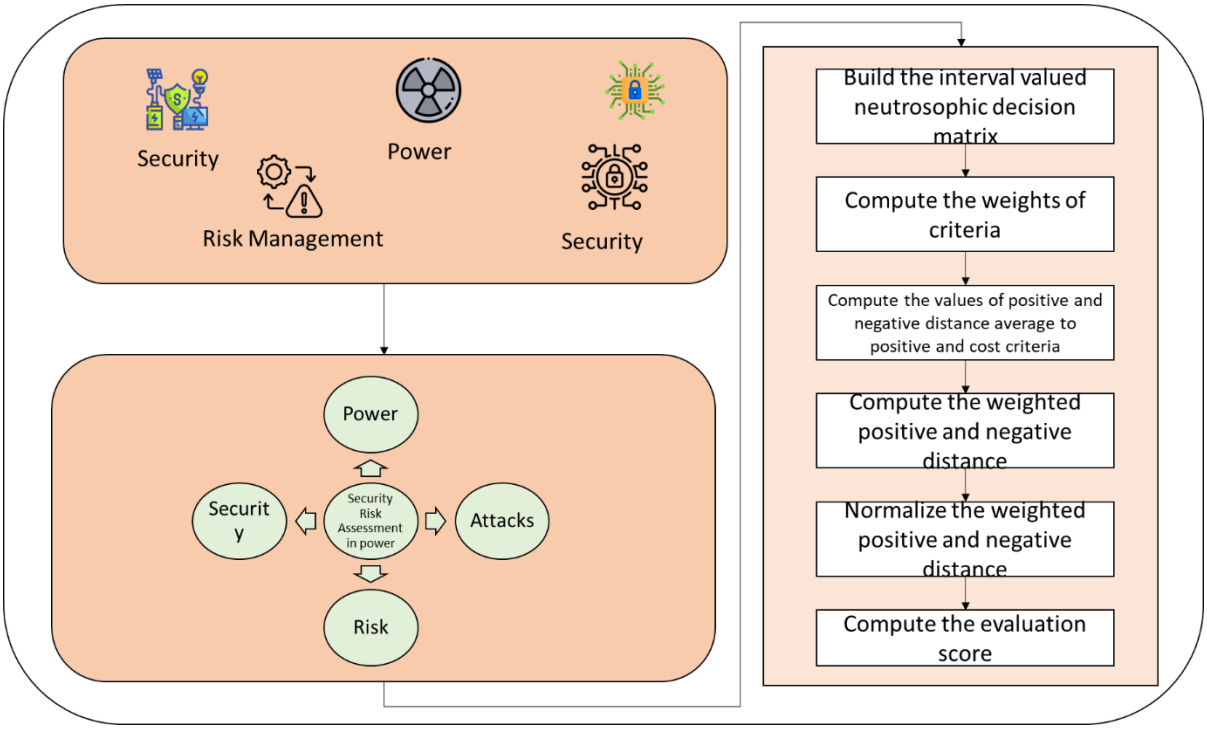

Figure 1. The security risk assessment in power system framework.

2. Power Security

Chester called the idea of power security "polysomic" and "slippery," meaning that it might stand for a number of different things at once. various parties have various ideas on what constitutes adequate security and how to get there. The significance that various stakeholders place on various parameters. Additionally, developed and underdeveloped nations might have varying objectives and access to resources. Access to power for the impoverished in rural regions and for the fast-growing manufacturing and service industries in urban areas are two key factors in ensuring power security in the latter situation. The different perspectives may also be attributable to the scientists' educational backgrounds; for instance, scholars of politics, engineers, and complicated system analysts may see power safety from a more sovereign, strong, or resilient perspective [11, 12].

Power security is inherently fluid, since the vantage point may change depending on the time period under consideration. Analysts that focus on longer time horizons, for instance, often prioritize stability above efficiency. As a result of these divergent viewpoints and objectives, academics have been debating the future of power security and the best ways to adapt to it. The goal of any given power security study will dictate both the issues to be considered and their relative importance. As a result, it is unlikely, and probably even undesirable, that academics will settle on a single, universally accepted concept and understanding of power security.

There are several potential dangers or hazards that might cause intentional or unintentional disruptions in the flow of power. However, there are two distinct but interconnected features that customers care about securing: (1) the physical, which includes factors like available, dependable, and/or affordable power supply; and (2) the economic, which includes factors like fluctuating prices and accessibility. Since physically unstable supply or scarce resources may have an effect on market pricing, these factors are related. Supply disruption refers to the impact of low or variable prices on the physical aspect by discouraging investment in network and manufacturing facilities. Therefore, markets should be structured such that prices may serve as a go-between for suppliers and buyers and serve as an early warning system for impending shortages or surpluses [13, 14].

While numerous descriptions of power security place emphasis on the physical and economic aspects of the concept, it is less typical for such definitions to include examples such as when high prices constitute a danger to power security. In other words, many definitions emphasize angles and vantage points but fail to specify cutoffs.

3. Security Assessment

Power system management and monitoring need dynamic security evaluation (DSA). Growing requests, privatization, and innovation in the power industry force modern power systems to keep running under strained circumstances approaching their stability limitations. When things are like that, even a little change might throw the system into chaos. This highlights the critical need of conducting regular internet security audits [15, 16].

Stability difficulties caused by both minor and major disturbances are thoroughly explored during a power system's DSA. The capacity of an integrating power system to maintain synchronization after a significant disruption is known as transient stability. The most difficult of these evaluations is the transient stability assessment (TSA), which requires extensive processing time. Time-constrained online assessment for immediate management and management of operations reveals the limitations of conventional model-based techniques for performing accurate TSA.

The real-time DSA evaluates the reliability of the grid in the face of plausible disruptions. Many nonlinear differential and algebraic equations must be solved numerically in this investigation. The longer the calculation cycle, the more quickly the solutions from traditional methods become obsolete. The standard time for a computing cycle is 15-30 minutes, according to the literature. The accuracy and applicability of DSA findings, however, improve with an increase in the frequency of computing cycles [17, 18].

4. Security Risk Assessment

As data and industry advance at a fast pace, the importance of cyber security grows. As technology has progressed, however, several issues with cyber security have become apparent. About 40% of nations worldwide observe cyberattacks as a possible danger, and as a consequence, cyber security measures are realized at all stages. As the internet and computers have grown more interconnected, several online programs including online banking, online shopping, and m-commerce have been vulnerable to cyber assaults. Despite many benefits, the expanding digital world also poses serious risks to vital governmental sectors like the defense industry [19, 20].

As the number of cybercrimes continues to rise, the notion of cyber security has emerged as one of critical importance in the modern world. Due to damages caused by cyber-attacks, innovators in the information security area have found it imperative to build trustworthy and effective security solutions. Cybersecurity is a broad subject, and several definitions of it may be found in the literature. For example, " assesses adopted to safeguard a system or machine (as on the Internet) against unauthorized access or intrusion" is how Merriam-Webster defines cyber security[21, 22].

In addition, the International Telecommunications Union (ITU) determines this term as an ensemble of resources like regulations, safety ideas, safety measures, instructions, risk management methods, behaviors, learning, best practices, trust, and innovations that can be used to keep a company's or an individual's data and resources safe online. Organizational and individual resources in the cyber sphere include computers and their associated hardware and software, as well as human resources, physical facilities, networks, apps, services, and networks for communication and data. Preventing and mitigating security breaches in the cyber environment is the goal of cyber security measures [23, 24].

Computer, network, program, and data security are all part of what's known as "cyber security," a collection of practices and procedures designed to keep these things safe from harm. A firewall,

anti-virus programs, and an intrusion detection system (IDS) are required components of both securities for computers and network solutions. Information security monitoring systems allow for the detection and analysis of data breaches caused by unauthorized access, replication, modification, or destruction. Both inside and outside assaults on an organization count as security breaches.

When it comes to protecting sensitive data, implementing cyber security measures is crucial. The scholarship presents an extensive number of cybersecurity strategies. Organizations may profit greatly from a ranking of the significance of these innovations and an analysis of the requirement of having these innovations in the first place. However, the dangers posed by such innovations must also be taken into account [25, 26].

5. Interval Valued Neutrosophic EDAS MCDM Methodology

This section provides the steps of the EDAS method under the interval valued neutrosophic set to evaluate the cyber security risks in power systems [27]–[30]. This method constructs the calculations between the criteria of risks assessment and cyber-attacks network.

1) Build the interval valued neutrosophic decision matrix.

   This step builds the decision matrix by using interval valued neutrosophic numbers between criteria and alternatives.

2) Average the interval valued neutrosophic decision matrix

   There are more than one expert to evaluate the criteria and alternatives, so these values are combined into one matrix.

3) Compute the weights of criteria.

4) Compute the values of positive and negative distance average to positive and cost criteria.

   These step specify the positive and negative criteria to compute the PD and ND values

$$PD = [pd]_{m\times n} \quad (1)$$

$$ND = [nd]_{m\times n} \quad (2)$$

$$PD_{mn} = \begin{cases} \frac{z(a_{mn}\ominus w_n)}{S(w_n)} & positive\ criteria \\ \frac{z(w_n\ominus a_{mn})}{S(w_n)} & cost\ criteria \end{cases} \quad (3)$$

$$ND_{mn} = \begin{cases} \frac{z(w_n\ominus a_{mn})}{S(w_n)} & positive\ criteria \\ \frac{z(a_{mn}\ominus w_n)}{S(w_n)} & cost\ criteria \end{cases} \quad (4)$$

Where a_{mn} is a value of decision matrix, w_n refers to the average weight, and $S(w_n)$ refers to the crisp value of average weight.

5) Compute the weighted positive and negative distance

$$EPD_n = \sum_{i=1}^{n}\left(e_j \otimes PD_{mn}\right) \quad (5)$$

$$END_n = \sum_{i=1}^{n}\left(e_j \otimes ND_{mn}\right) \quad (6)$$

6) Normalize the weighted positive and negative distance

$$NEPD_n = \frac{EPD_n}{\max(EPD_n)} \quad (7)$$

$$NEND_n = 1 - \frac{END_n}{\max(EPD_n)} \quad (8)$$

7) Compute the evaluation score

$$AS = 0.5\ (NEPD_n \oplus NEND_n) \quad (9)$$

6. Application

In the past few years, cyber security concerns have become a major issue for online infrastructures. New technology techniques are the primary focus of most initiatives to strengthen cyber security. However, such safety measures capture a lot of data, which presents a significant privacy risk to the people they are meant to safeguard. Therefore, it is crucial to conduct risk assessments for cyber security tools. The aim of this section provides the assessment risks of cyber security in power management. This study used nine criteria and ten alternatives like {NCA1, NCA2, NCA3, NCA4, NCA5, NCA6, NCA7, NCA8, NCA9, NCA10}to rank the network communication in power management. The nine criteria are proposed in Figure 2. The criteria are collected from the literature with the risk assessment security and cyber security assessment.

Figure 2. The cyber security risks criteria.

We applied the interval valued neutrosophic EDAS method to obtain the rank of risks in cyber security risks assessment. The decision makers and experts built the decision matrix by the terms in interval valued neutrosophic set. Then these terms are replaced by the interval valued neutrosophic numbers. Then compute weights of criteria as: $\mathrm{SRA}_1 = 0.10412, \mathrm{SRA}_2 = 0.126683, \mathrm{SRA}_3 = 0.013866, \mathrm{SRA}_4 = 0.145245, \mathrm{SRA}_5 = 0.056585, \mathrm{SRA}_6 = 0.142162, \mathrm{SRA}_7 = 0.079966, \mathrm{SRA}_8 = 0.131478, \mathrm{SRA}_9 = 0.199892$. From the weights of criteria, the criterion 9 is the highest and the criterion 3 is the worst.

Then compute the positive and negative criteria by using Eqs. (1-4). Then compute the weighted positive and negative distance average by using Eqs. (5-6) as shown in Table 1-2. Then compute the normalized weighted positive and negative distance average by using Eqs. (7-8). Then compute the evaluation score by using Eq. (9) as shown in Figure 3. From Figure 3, the risk number eight is the highest and risk number 4 is the least.

Table 1. The weighted positive distance.

	SRA1	SRA2	SRA3	SRA4	SRA5	SRA6	SRA7	SRA8	SRA10
NCA1	0.020225	0	0	0	0	0	0	0.013111	0
NCA2	0.020225	0.041728	0	0.054132	0.039544	0.047083	0.014833	0.016247	0.010789
NCA3	0	0	0.000655	0	0.004337	0	0	0.013111	0
NCA4	0.020225	0	0.002782	0	0	0	0.014833	0.002244	0.010789
NCA5	0	0	0	0	0	0	0	0.013111	0.036533
NCA6	0	0	0.002782	0	0	0	0.002717	0	0
NCA7	0.020225	0.041728	0	0	0	0	0	0.013111	0.010789
NCA8	0	0	0.000655	0	0.006643	0.047083	0.014833	0	0.04166
NCA9	0	0	0.002782	0	0.011781	0	0.01282	0.016247	0.036533
NCA10	0.020225	0	0	0	0	0	0	0.013111	0

Table 2. The weighted negative distance.

	SRA_1	SRA_2	SRA_3	SRA_4	SRA_5	SRA_6	SRA_7	SRA_8	SRA_{10}
NCA_1	0	0.019952	0.001931	0.000374	0.006512	0.007572	0.012007	0	0.02673
NCA_2	0	0	0.001931	0	0	0	0	0	0
NCA_3	0.010425	0.126683	0	0.000374	0	0.007572	0.012007	0	0.02673
NCA_4	0	0.00691	0	0.000374	0.018129	0.017687	0	0	0
NCA_5	0.012909	0.019952	0.001931	0.018889	0.006512	0.022227	0.012007	0	0
NCA_6	0.010425	0.00691	0	0.000374	0.018129	0.022227	0	0.050147	0.066903
NCA_7	0	0	0.001931	0.000374	0.006512	0.004653	0.012007	0	0
NCA_8	0.056942	0.015912	0	0.014106	0	0	0	0.050147	0
NCA_9	0.010425	0.00691	0	0.000374	0	0.004653	0	0	0
NCA_{10}	0	0.00691	0.001931	0.018889	0.006512	0.007572	0.012007	0	0.02673

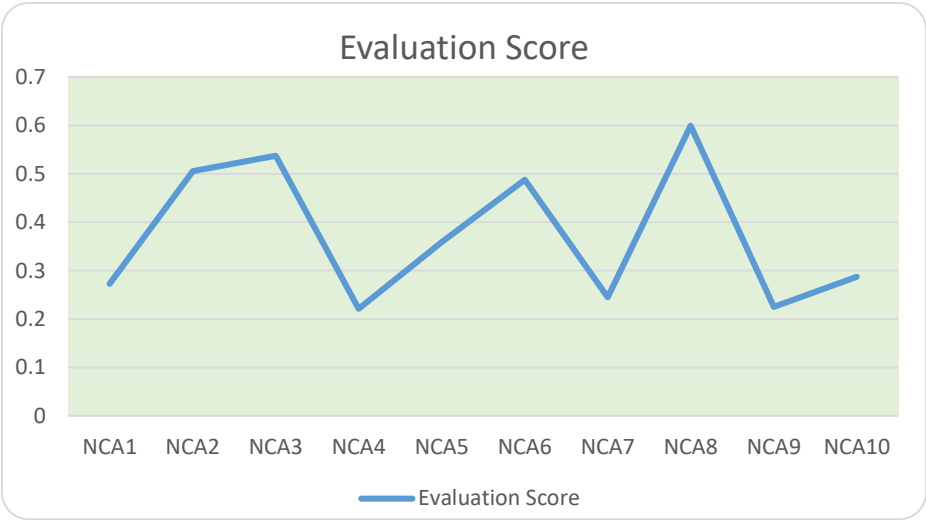

Figure 3. The evaluation scores.

7. Conclusion

Hybrid structures that are interdependent on data and communication are the future of renewable power. While the use of information technology improves the administration and operation of power systems, it also increases the likelihood of cybersecurity problems. As a consequence, safeguarding our information and communication infrastructures has become more important to ensuring the reliability of our power grid. The proposed model uses the neutrosophic EDAS-based MCDM approach to address the challenge of identifying threats inside the interconnected wireless networks of energy administration and control network backbones. This paper used the interval-valued neutrosophic set to overcome the uncertain information. The experts used interval-valued neutrosophic terms to evaluate the criteria and alternatives. Then we replaced these terms with interval-valued neutrosophic numbers. Then we applied the EDAS method to nine criteria and ten alternatives. Risk number eight is the highest and risk number 4 is the least.

Data availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

Conflict of interest

The authors declare that there is no conflict of interest in the research.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. C.-C. Lee, Z. Yuan, and Q. Wang, "How does information and communication technology affect energy security? International evidence," Energy Econ., vol. 109, p. 105969, 2022.
2. S.-W. Huang, Y.-F. Chung, and T.-H. Wu, "Analyzing the relationship between energy security performance and decoupling of economic growth from CO2 emissions for OECD countries," Renew. Sustain. Energy Rev., vol. 152, p. 111633, 2021.
3. C.-C. Lee, W. Xing, and C.-C. Lee, "The impact of energy security on income inequality: The key role of economic development," Energy, vol. 248, p. 123564, 2022.
4. R. Cergibozan, "Renewable energy sources as a solution for energy security risk: Empirical evidence from OECD countries," Renew. Energy, vol. 183, pp. 617–626, 2022.
5. F. Z. Ainou, M. Ali, and M. Sadiq, "Green energy security assessment in Morocco: green finance as a step toward sustainable energy transition," Environ. Sci. Pollut. Res., vol. 30, no. 22, pp. 61411–61429, 2023.
6. D. A. Alemzero, H. Sun, M. Mohsin, N. Iqbal, M. Nadeem, and X. V. Vo, "Assessing energy security in Africa based on multi-dimensional approach of principal composite analysis," Environ. Sci. Pollut. Res., vol. 28, pp. 2158–2171, 2021.
7. Shereen Zaki,Mahmoud M. Ibrahim,Mahmoud M. Ismail, Interval Valued Neutrosophic VIKOR Method for Assessment Green Suppliers in Supply Chain, International Journal of Advances in Applied Computational Intelligence, Vol. 2 , No. 1 , (2022) : 15-22 (Doi : https://doi.org/10.54216/IJAACI.020102)
8. Mahmoud Ismail,Shereen Zaki, Neutrosophic MCDM Methodology to Select Best Industrial Arc Welding Robot, Neutrosophic and Information Fusion, Vol. 1 , No. 1 , (2023) : 08-16 (Doi : https://doi.org/10.54216/NIF.010101)
9. X. Peng and J. Dai, "Algorithms for interval neutrosophic multiple attribute decision-making based on MABAC, similarity measure, and EDAS," Int. J. Uncertain. Quantif., vol. 7, no. 5, 2017.
10. B. W. Ang, W. L. Choong, and T. S. Ng, "Energy security: Definitions, dimensions and indexes," Renew. Sustain. energy Rev., vol. 42, pp. 1077–1093, 2015.
11. B. Kruyt, D. P. Van Vuuren, H. J. M. de Vries, and H. Groenenberg, "Indicators for energy security," Energy Policy, vol. 37, no. 6, pp. 2166–2181, 2009.
12. M. Radovanović, S. Filipović, and D. Pavlović, "Energy security measurement–A sustainable approach," Renew. Sustain. Energy Rev., vol. 68, pp. 1020–1032, 2017.
13. A. Månsson, B. Johansson, and L. J. Nilsson, "Assessing energy security: An overview of commonly used methodologies," Energy, vol. 73, pp. 1–14, 2014.
14. M. Ni, J. D. McCalley, V. Vittal, and T. Tayyib, "Online risk-based security assessment," IEEE Trans. Power Syst., vol. 18, no. 1, pp. 258–265, 2003.
15. A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer, "Google android: A comprehensive security assessment," IEEE Secur. Priv., vol. 8, no. 2, pp. 35–44, 2010.
16. K. Morison, L. Wang, and P. Kundur, "Power system security assessment," IEEE power energy Mag., vol. 2, no. 5, pp. 30–39, 2004.

17. E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, "Information security assessment in public administration," Comput. Secur., vol. 90, p. 101709, 2020.
18. P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," ISA Trans., vol. 46, no. 4, pp. 583–594, 2007.
19. Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," Comput. Secur., vol. 56, pp. 1–27, 2016.
20. M. Sajko, K. Rabuzin, and M. Bača, "How to calculate information value for effective security risk assessment," J. Inf. Organ. Sci., vol. 30, no. 2, pp. 263–278, 2006.
21. T. R. Peltier, Information security risk analysis. CRC press, 2005.
22. X. Lyu, Y. Ding, and S. Yang, "Safety and security risk assessment in cyber-physical systems," IET Cyber-Physical Syst. Theory Appl., vol. 4, no. 3, pp. 221–232, 2019.
23. G. Wangen, "Information security risk assessment: a method comparison," Computer (Long. Beach. Calif)., vol. 50, no. 4, pp. 52–61, 2017.
24. A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," Comput. Secur., vol. 57, pp. 14–30, 2016.
25. J. R. C. Nurse, S. Creese, and D. De Roure, "Security risk assessment in Internet of Things systems," IT Prof., vol. 19, no. 5, pp. 20–26, 2017.
26. Abedallah Z. Abualkishik,Rasha Almajed, Triangular Neutrosophic Multi-Criteria Decision Making AHP Method for Solar Power Site Selection, International Journal of Advances in Applied Computational Intelligence, Vol. 2 , No. 2 , (2022) : 08-15 (Doi : https://doi.org/10.54216/IJAACI.020201)
27. Ahmed M. Ali, A Multi-Criteria Decision-Making Approach for Piston Material Selection under Single-Valued Trapezoidal Neutrosophic Sets, Neutrosophic and Information Fusion, Vol. 2 , No. 1 , (2023) : 23-43 (Doi : https://doi.org/10.54216/NIF.020102)
28. Ahmed Abdelmonem,Shimaa S. Mohamed, Deep Learning Defenders: Harnessing Convolutional Networks for Malware Detection,International Journal of Advances in Applied Computational Intelligence, Vol. 1 , No. 2 , (2022) : 46-55 (Doi : https://doi.org/10.54216/IJAACI.010203)
29. Shimaa Said,Mahmoud M. Ibrahim,Mahmoud M. Ismail, An Integrated Multi-Criteria Decision-Making Approach for Identification and Ranking Solar Drying Barriers under Single-Valued Triangular Neutrosophic Sets (SVTNSs), Neutrosophic and Information Fusion, Vol. 2 , No. 1 , (2023) : 35-49 (Doi : https://doi.org/10.54216/NIF.020103)
30. A. Karaşan and C. Kahraman, "Interval-valued neutrosophic extension of EDAS method," in Advances in Fuzzy Logic and Technology 2017: Proceedings of: EUSFLAT-2017–The 10th Conference of the European Society for Fuzzy Logic and Technology, September 11-15, 2017, Warsaw, Poland IWIFSGN'2017–The Sixteenth International Workshop on Intuitionistic, Springer, 2018, pp. 343–357.

Received: Aug 23, 2022. Accepted: Mar 27, 2023