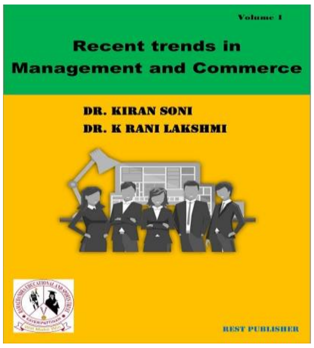
Recent trends in Management and Commerce

Vol: 1(1), 2019

REST Publisher; ISBN No: 978-81-936097-6-7

Website: http://restpublisher.com/book-series/rmc/



Volume 1

Recent trends in Management and Commerce

DR. KIRAN SONI
DR. K RANI LAKSHMI

REST PUBLISHER

Examining How Cyber Security Impacts the Monitoring and Control Systems Used in The Energy Sector

*Agrawal Deepa Manoj

SST College of Arts and Commerce, Maharashtra, India

*Corresponding Author Email: deepaagrawal@sstcollege.edu.in

Abstract: *The same IT regulations that apply to other information systems globally do not apply to the monitoring of the energy sector or to specific information structures, such as control systems. Industrial control systems are also used in the management of essential infrastructure, such as water management systems, nuclear power plants, oil and gas installations, and other things. Since system availability rate is important, system functionality must be consistent. It is necessary for a system to be fully protected against cyber security flaws, risks, and dangers in order to be certified as being impervious to a cyber assault. Methodology: examines and evaluates industrial control system cyber security assessments, along with any possible repercussions they might have on how accessible Industrial control systems may be used in the energy industry. Understanding the Analytical Hierarchy Process' Attitude Toward Behavior Method and the GRA enables one to evaluate operational evaluations of the cyber security of industrial control systems. Aspects of security include things like confidentiality, accessibility, availability, integrity, authentication, dependability, performance, and reliability. A1, A2, A3, A4, and A5 are taken into consideration as alternatives, and durability, survivability, availability, maintainability, and accessibility are taken into consideration as assessment criteria. Results: qualities and how they affect the cyber security of industrial management systems. To assess the accuracy and sensitivity of the findings, the author examined the output from six different programs. The industrial control system's cyber security strategy should use Alternative 1, according to the robustness analysis's findings. This study will be a useful tool for creating monitoring and control systems that are safer and more regulated.*

Keywords: *control systems, Cyber security, cyber attacks, MCDM Method.*

1. INTRODUCTION

Every energy infrastructure's brain and spinal cord are control mechanisms. It is made up of broad networks of electronically linked devices that are crucial for managing and controlling the production and transportation of energy as well as the mining of oil and gas. A broad term used to describe a range of instruments and infrastructure elements used in industries is "industrial control system" [1-3]. Examples include data collection, required components, programmable logic controllers, and multi-structural control systems. The chemical, sewage and wastewater, energy, natural gas, and oil sectors, as well as the transit sector, all use industrial management systems. Operating system defects, organizational problems, and inadequate system maintenance all contribute to industrial control system vulnerabilities. A significant blackout could result from a breakdown in the monitoring and control systems for the electricity industry. A number of power providers offer power system stabilisation devices in the event of a system failure (such as the shutdown of a plant), in order to swiftly take control of the system and halt widespread issues. A terminal unit carries out fault diagnosis for the power system stabilization systems, a central math unit computes control the flow of information, a central control unit makes control choices and outputs control commands [4]. Since most of The Directive's security requirements are not fulfilled by advancements in industrial control systems, cyberattacks on the integrity, availability, and confidentiality of those systems are possible. As an illustration, the cyber threat to availability disables sophisticated information, critical controls, and performance tools. Handling complicated data in resources puts integrity at risk, and requests for related data put confidentiality at risk. The gap between industry control system cybersecurity issues must be closed and bridged with the help of cybersecurity evaluation [6–8]. Industrial systems cannot be sufficiently protected from security practices by cyberattacks or traditional security methods. Finding the right technology supplier and consultant is essential for their security given the growing threats to our infrastructure and systems. Protecting fog locations for industrial controls systems is the authors' top priority so that specialists can quickly identify any potentially dangerous or unforeseen activity. In order to defend against cyberattacks, we are investigating how to create an industrial control system that is secure and equipped with cutting-edge intrusion detection technology. Reviewing current research on industrial computer control encryption and cyber-security issues is crucial before continuing. The cyber security of industrial control systems was evaluated and more effectively compiled by the authors [9–15] using multiple criteria decision making (MCTM) methods. To address decision-related issues, a variety of MCDM strategies are offered [16–18]. In this study, the tentative GRA method for scheduled papers [18–25] was used. GRA is a well-liked MCDM method for picking exact solutions from a wide range of options and features. It is essential to implement an AHP-based hierarchical MCDM method because the variables involved in determining the cyber security of an industrial control system are complex. In order to choose the best option from a list of options, the GRA approach seems to be a useful MCDM technique. Many academics have used this hybrid approach to handle issues with decision-making [26–30]. Using a computer in the workplace Cybersecurity's characteristics and effects are explored. The consequences of recent cyberattacks are discussed. about safety concerns and problems with factory control systems. We will go over the methods, examine control comparisons, conduct sensitivity analysis, and discuss the data analysis and findings using a variety of techniques. In our final section, we reach a conclusion for the paper and suggest areas for possible future research.

2. MATERIAL AND METHODS

An industrial automation system is a collection of related hardware, software, networks, and controllers used to manage and/or direct industrial operations. Each process control system runs differently and is designed to handle work efficiently and technologically depending on the industry. Each letter explains how to accomplish the main goal of data security: • Integrity, which guards against unintentional information loss or damage and ensures the accuracy and authenticity of information. • maintaining allowed access and transparency limits while remaining discreet to protect data privacy and classified information. Accessibility Make sure information is easily accessible and utilised in a timely and accurate manner. Industrial control system availability and integrity are more crucial than secrecy in the security triangle. In order to prevent unintentional disturbances to computers, they aim to boost availability. Data integrity is vital in control systems. Operations or even safety may be significantly impacted if the operator's screen in the command centre does not adequately depict what is happening. Compared to industrial control systems, integrity and confidentiality are less of an issue. This is valid given that data is ephemeral in the context of industrial control systems like speed, vibration, and temperature. Industrial control systems are generally designed to operate as dependably as possible. Industrial control systems often have a lifespan of 20 years or more [12–15]. It is difficult to update the security patch as well. Regularly assessing the cyber security of an industrial control system may be difficult, especially if the study concludes that the system won't be infiltrated. Each year, there are more and more assaults on industrial control systems. While some had a large national impact, others were less noteworthy. A significant challenge when employing machine learning techniques is acquiring real-time and impartial datasets. Due to internal secrecy and consumer privacy issues, many datasets cannot be combined, or they may be missing crucial statistical properties. Most sector companies steer clear of exchanging their secured network data due to these challenges. Palmer et al. claim that supervised machine learning frameworks may or may not succeed with a variety of datasets created under various simulations or testing situations [5]. One of the key elements of an industrial control system that has an indirect effect is security. There are two levels of security attributes: Level-1 represents security and trust with C1 and C2 respectively. Confidentiality, availability, integrity, authentication, reliability, performance, and accessibility are all terms used to describe security (level-2). Durability, survivability, availability, maintainability, and accessibility are the categories for reliability at level 2. The following is a description of the characteristics of industrial control systems: A crucial aspect of preadolescence is emotional stability. Safety is a crucial element to take into account when purchasing a used car. In order to safeguard industrial control systems from malicious assaults, harmful data, and other dangers posed by hackers, security is a crucial component. Allowing authorised access to safe and sensitive data is referred to as confidentiality from the standpoint of security [24]. Data must be safeguarded against leakage because confidentiality is the cornerstone of both cyber security and privacy. Data loses value if it is compromised. In the event that hackers alter data or discover secret information, the value of cyber security can be lost. Ethical assurance and tenacity see integrity as a challenging quality. Integrity is crucial for collecting accurate and relevant data. Confidentiality is the capacity to control and make data available to only authorised people. If cyber security industrial control systems can thwart assaults, manage outages, and handle other potentially dangerous situations, they are regarded as reliable. It describes a user's capacity to access data or resources over time from the perspective of cyber security. Accessibility is the capacity of cyber security to regulate user information rights in a safe setting. Some real-world issues call for unique or multiple-choice solutions that let consumers select the best decision without relying on a strong foundation from a range of choices. Several researchers [12–14] have addressed this issue and offered an ideal quantitative answer to these challenges using MCDM techniques. Particularly the well-known AHP methodology coupled with a fuzzy set theory is easier and more efficient than other methods. This has been proven in a number of earlier studies [15–17]. The scenario has a significant impact on the calculated outcomes if the strategy offers more than one option for review during the computational process. In the suggested study, the authors employ a reluctant fuzzy set-based MCDM methodology, which adds additional efficiency to the results from the standpoint of evaluation. Additionally, the effect of cyber security on industrial control systems was investigated using the ARAS method. Additionally, the ARAS methodology is used in this study to produce more useful and precise results. The ARAS method is the MCDM method that is most suited for testing estimated results. This method's key benefit is that it computes the outcome while taking both positive and negative aspects into account. In the first few paragraphs, the authors mention a number of safety features for industrial control systems. To determine how secure industrial control systems are, availability and integrity are two level-1 criteria that are labelled as C1 to C11. The characteristics of reliability are confidentiality, availability, integrity, and accessibility when evaluating the security of industrial controlling systems at level 2. Maintainability, accountability, survivability, availability, and accessibility are reliability attributes. Both strategies also priorities the options for outcome testing and gather information for the pair-wise assessment matrix. On the other hand, the attributes and options are interdependent, as demonstrated by real-world scenarios [31–34]

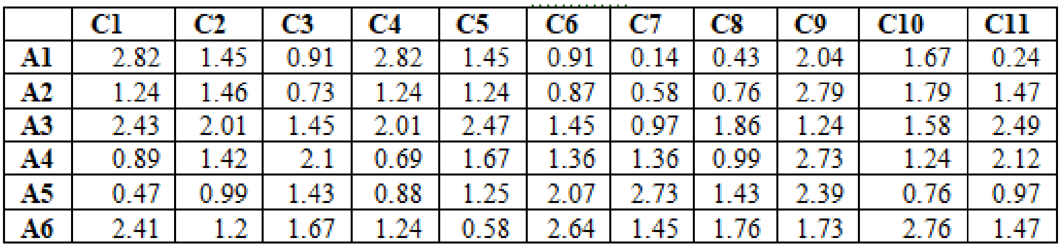
3. RESULTS AND DISCUSSIONS

TABLE 1. evaluation parameter

C1	confidentiality
C2	availability
C3	integrity
C4	authentication
C5	reliability
C6	performance and accessibility
C7	durability
C8	survivability
C9	availability
C10	maintainability
C11	accessibility

Table 1 demonstrates that the evaluation preference is a value table with the values of secrecy, availability, integrity, authentication, dependability, performance, and accessibility.

TABLE 2. data set



	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
A1	2.82	1.45	0.91	2.82	1.45	0.91	0.14	0.43	2.04	1.67	0.24
A2	1.24	1.46	0.73	1.24	1.24	0.87	0.58	0.76	2.79	1.79	1.47
A3	2.43	2.01	1.45	2.01	2.47	1.45	0.97	1.86	1.24	1.58	2.49
A4	0.89	1.42	2.1	0.69	1.67	1.36	1.36	0.99	2.73	1.24	2.12
A5	0.47	0.99	1.43	0.88	1.25	2.07	2.73	1.43	2.39	0.76	0.97
A6	2.41	1.2	1.67	1.24	0.58	2.64	1.45	1.76	1.73	2.76	1.47

Table 2 is given for the data set. A6 values are the lowest and A1 values are the highest.

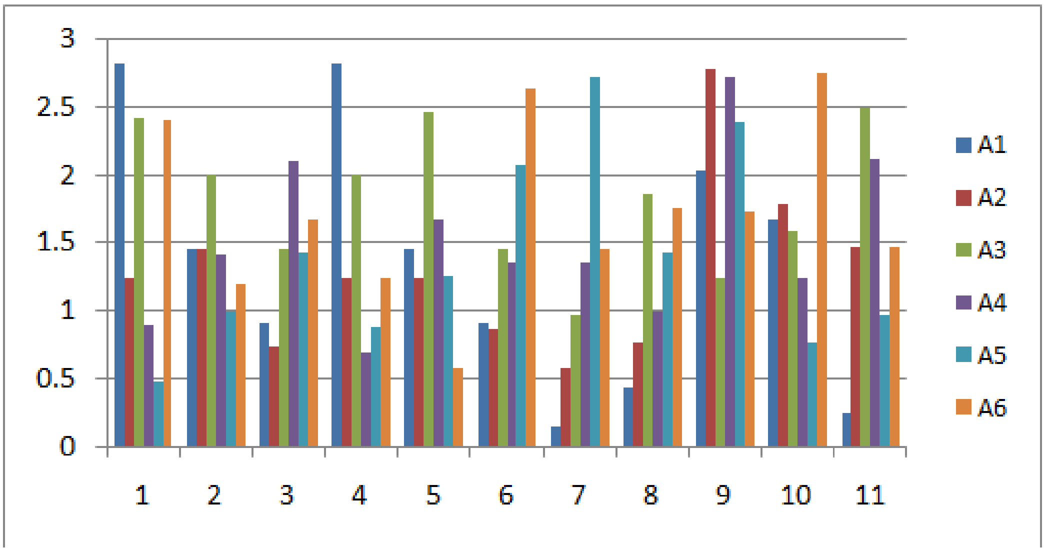


FIGURE 1. For the data set

TABLE 3. Normalized Data

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
A1	0.0000	0.5490	0.8686	0.0000	0.5397	0.9774	1.0000	1.0000	0.4839	0.5450	1.0000
A2	0.6723	0.5392	1.0000	0.7418	0.6508	1.0000	0.8301	0.7692	0.0000	0.4850	0.4533
A3	0.1660	0.0000	0.4745	0.3803	0.0000	0.6723	0.6795	0.0000	1.0000	0.5900	0.0000
A4	0.8213	0.5784	0.0000	1.0000	0.4233	0.7232	0.5290	0.6084	0.0387	0.7600	0.1644
A5	1.0000	1.0000	0.4891	0.9108	0.6455	0.3220	0.0000	0.3007	0.2581	1.0000	0.6756
A6	0.1745	0.7941	0.3139	0.7418	1.0000	0.0000	0.4942	0.0699	0.6839	0.0000	0.4533

Table 3 shown that the normalized data for A1, A2, A3, A4, A5 and A6. These values are calculated using by formulas.

TABLE 4. Deviation sequence

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
A1	1.0000	0.4510	0.1314	1.0000	0.4603	0.0226	0.0000	0.0000	0.5161	0.4550	0.0000
A2	0.3277	0.4608	0.0000	0.2582	0.3492	0.0000	0.1699	0.2308	1.0000	0.5150	0.5467
A3	0.8340	1.0000	0.5255	0.6197	1.0000	0.3277	0.3205	1.0000	0.0000	0.4100	1.0000
A4	0.1787	0.4216	1.0000	0.0000	0.5767	0.2768	0.4710	0.3916	0.9613	0.2400	0.8356
A5	0.0000	0.0000	0.5109	0.0892	0.3545	0.6780	1.0000	0.6993	0.7419	0.0000	0.3244
A6	0.8255	0.2059	0.6861	0.2582	0.0000	1.0000	0.5058	0.9301	0.3161	1.0000	0.5467

Table 4 shown that the deviation sequence values and is calculated that the formulas.

TABLE 5. Grey relation coefficient

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
A1	0.3333	0.5258	0.7919	0.3333	0.5207	0.9568	1.0000	1.0000	0.4921	0.5236	1.0000
A2	0.6041	0.5204	1.0000	0.6594	0.5888	1.0000	0.7464	0.6842	0.3333	0.4926	0.4777
A3	0.3748	0.3333	0.4875	0.4465	0.3333	0.6041	0.6094	0.3333	1.0000	0.5495	0.3333
A4	0.7367	0.5426	0.3333	1.0000	0.4644	0.6436	0.5149	0.5608	0.3422	0.6757	0.3744
A5	1.0000	1.0000	0.4946	0.8486	0.5851	0.4245	0.3333	0.4169	0.4026	1.0000	0.6065
A6	0.3772	0.7083	0.4215	0.6594	1.0000	0.3333	0.4971	0.3496	0.6126	0.3333	0.4777

Table 5 A zeta value is constant and a value of 0.5. Table 6 is given for a grey relation coefficient shown in figure 3.

Copyright@ REST Publisher

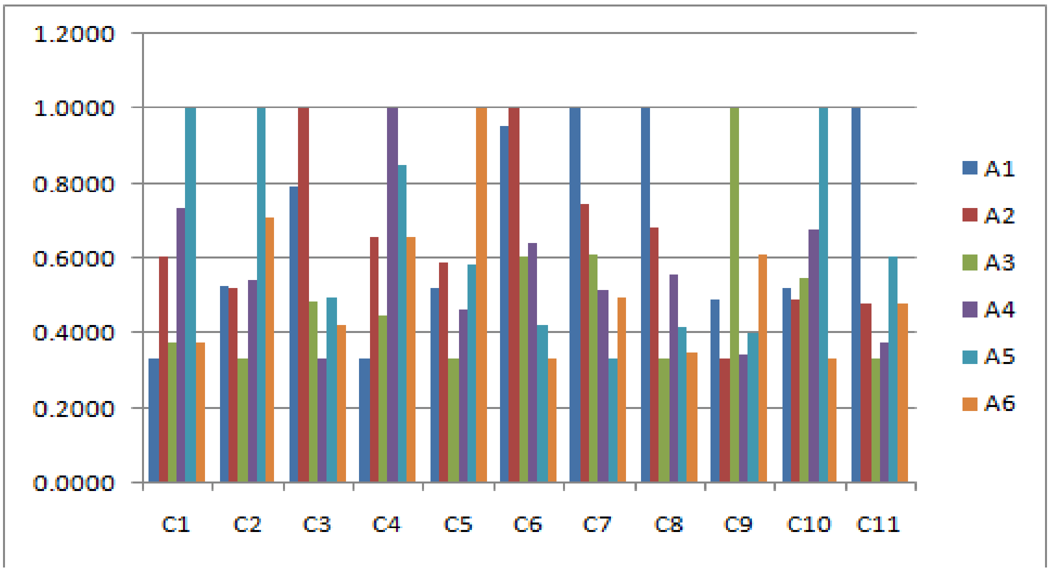


FIGURE 2 Grey relation coefficients

TABLE 6. GRA values

A1	0.6798
A2	0.6461
A3	0.4914
A4	0.5626
A5	0.6466
A6	0.5246

Table 6 shows the Obtained by using formulas to calculate the GRA values, the result of the method was shown above. A1 is highest values for GRA result and A3 lowest values for GRA result showing in figure 4.

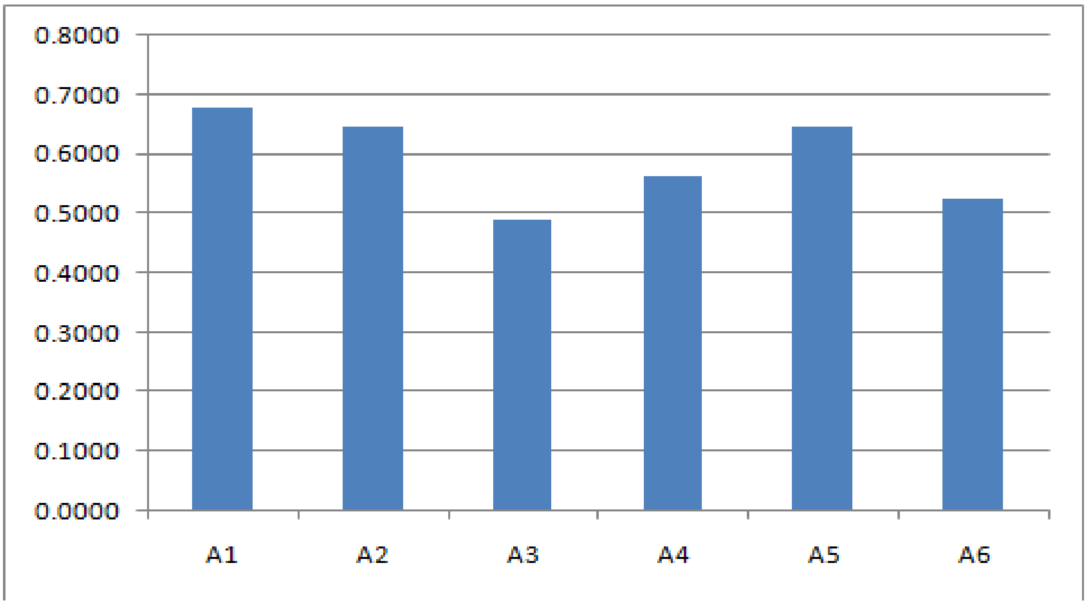
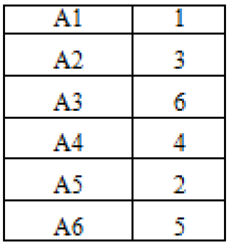


FIGURE 3. Shown that the graph about GRA values

TABLE 7. Rank



A1	1
A2	3
A3	6
A4	4
A5	2
A6	5

Table 7 shows the values concerning the rank are displayed in Table 5. A 1 are ranked first, A 2 are ranked third, A 3 are ranked last, A 4 are ranked fourth, A 5 are ranked second, and A 6 are ranked fifth, as shown in Figure 3's ranking.

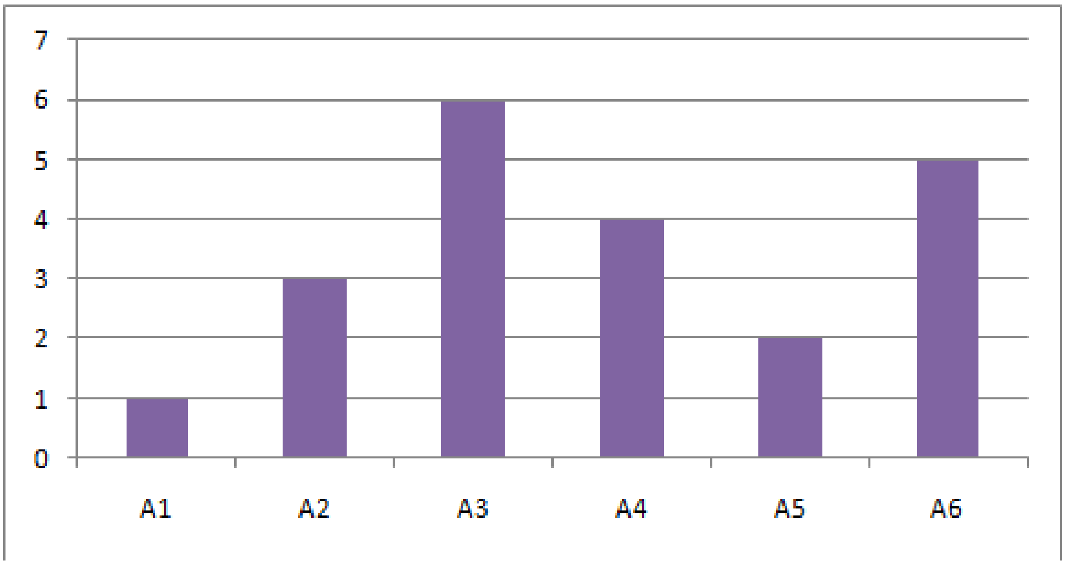


FIGURE 4. shown that the graph about rank

4. CONCLUSION

Creating a hybrid dataset that incorporates information from testbed simulation environments or campuses of the power sector with a number of important online-accessible datasets is required, in our opinion, for future work. In order to evaluate the accuracy of machine learning techniques, we want to expand on our prior work from the perspective of industrial control systems with hybrid datasets, such as the one described in [28-35]. On the other hand, few studies on intrusion detection were found in the papers we collected. serve as a prototype for a standard technical platform that will be used in the future to build testing centers for industrial controlling systems. Why provide businesses with a testing environment that is more efficient than a traditional testbed, yields result that are more remarkable, and lowers simulation and testing costs. to launch cyberattacks against the hybrid surveillance and control system architecture of the energy sector. It is extremely challenging to identify and thwart attacks on control systems at the component level due to the intricacy of malware designed to target controllers, such as nil rootkits and attacks. New intrusion detection methods are thus required for industrial control systems at the process control level. Machine learning methods have shown to be very beneficial in this situation. The major conclusions of the suggested study are listed below. Improvements, study, identification, and prioritization of security techniques will result from the focus on industrial control system cyber security components. MCDM methodologies are used in studies on the safety evaluation of industrial control systems, such as the based GRA strategy.

REFERENCES

[1]. Wei, Gui-Wu. "GRA method for multiple attribute decision making with incomplete weight information in intuitionistic fuzzy setting." *Knowledge-Based Systems* 23, no. 3 (2010): 243-247.

[2]. Zhang, Shi-fang, San-yang Liu, and Ren-he Zhai. "An extended GRA method for MCDM with interval-valued triangular fuzzy assessments and unknown weights." *Computers & Industrial*

Engineering 61, no. 4 (2011): 1336-1341.

[3]. Biswas, Pranab, Surapati Pramanik, and Bibhas C. Giri. "GRA method of multiple attribute decision making with single valued neutrosophic hesitant fuzzy set information." *New trends in neutrosophic theory and applications* (2016): 55-63.

[4]. Lenzen, Manfred, Richard Wood, and Blanca Gallego. "Some comments on the GRAS method." *Economic systems research* 19, no. 4 (2007): 461-465.

[5]. Liu, Sifeng, Yingjie Yang, Ying Cao, and Naiming Xie. "A summary on the research of GRA models." *Grey Systems: Theory and Application* (2013).

[6]. Tonge, Atul M., Suraj S. Kasture, and Surbhi R. Chaudhari. "Cyber security: challenges for society-literature review." *IOSR Journal of computer Engineering* 2, no. 12 (2013): 67-75.

[7]. Ayofe, Azeez Nureni, and Barry Irwin. "Cyber security: Challenges and the way forward." *Computer Science & Telecommunications* 29, no. 6 (2010).

[8]. Kimani, Kenneth, Vitalice Oduol, and Kibet Langat. "Cyber security challenges for IoT-based smart grid networks." *International journal of critical infrastructure protection* 25 (2019): 36-49.

[9]. Rajasekharaiah, K. M., Chhaya S. Dule, and E. Sudarshan. "Cyber security challenges and its emerging trends on latest technologies." In *IOP Conference Series: Materials Science and Engineering*, vol. 981, no. 2, p. 022062. IOP Publishing, 2020.

[10]. Line, Maria B., Inger Anne Tøndel, and Martin G. Jaatun. "Cyber security challenges in Smart Grids." In *2011 2nd IEEE PES international conference and exhibition on innovative smart grid technologies*, pp. 1-8. IEEE, 2011.

[11]. Shapsough, Salsabeel, Fatma Qatan, Raafat Aburukba, Fadi Aloul, and A. R. Al Ali. "Smart grid cyber security: Challenges and solutions." In *2015 international conference on smart grid and clean energy technologies (ICSGCE)*, pp. 170-175. IEEE, 2015.

[12]. Wells, Lee J., Jaime A. Camelio, Christopher B. Williams, and Jules White. "Cyber-physical security challenges in manufacturing systems." *Manufacturing Letters* 2, no. 2 (2014): 74-77.

[13]. Thuraisingham, Bhavani, Murat Kantarcioglu, Kevin Hamlen, Latifur Khan, Tim Finin, Anupam Joshi, Tim Oates, and Elisa Bertino. "A data driven approach for the science of cyber security: Challenges and directions." In *2016 IEEE 17th International Conference on Information Reuse and Integration (IRI)*, pp. 1-10. IEEE, 2016.

[14]. Duić, Igor, Vlatko Cvrtila, and Tomislav Ivanjko. "International cyber security challenges." In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1309-1313. IEEE, 2017.

[15]. Kotut, Lindah, and Luay A. Wahsheh. "Survey of cyber security challenges and solutions in smart grids." In *2016 cybersecurity symposium (CYBERSEC)*, pp. 32-37. IEEE, 2016.

[16]. Barreto, Luís, and António Amaral. "Smart farming: Cyber security challenges." In *2018 International Conference on Intelligent Systems (IS)*, pp. 870-876. IEEE, 2018.

[17]. Dave, Gaurav, Gaurav Choudhary, Vikas Sihag, Ilsun You, and Kim-Kwang Raymond Choo. "Cyber security challenges in aviation communication, navigation, and surveillance." *Computers & Security* 112 (2022): 102516.

[18]. El-Rewini, Zeinab, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan. "Cybersecurity challenges in vehicular communications." *Vehicular Communications* 23 (2020): 100214.

[19]. Chaturvedi, M. M., M. P. Gupta, and Jaijit Bhattacharya. "Cyber security infrastructure in India: a study." *Emerging Technologies in E-Government ', CSI Publication* (2008).

[20]. Singh, Nimisha, and Abha Rishi. "Pyramid: A case study of cyber security in India." *South Asian Journal of Business and Management Cases* 4, no. 1 (2015): 135-142.

[21]. Al Nafea, Roaa, and Mohammed Amin Almaiah. "Cyber security threats in cloud: Literature review." In *2021 International Conference on Information Technology (ICIT)*, pp. 779-786. IEEE, 2021.

[22]. Dixit, Priyanka, and Sanjay Silakari. "Deep learning algorithms for cybersecurity applications: A technological and status review." *Computer Science Review* 39 (2021): 100317.

[23]. Salloum, Said A., Muhammad Alshurideh, Ashraf Elnagar, and Khaled Shaalan. "Machine learning and deep learning techniques for cybersecurity: a review." In *Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2020)*, pp. 50-57. Springer International Publishing, 2020.

[24]. Abdullah, Aishah, Reem Hamad, Mada Abdulrahman, Hanan Moala, and Salim Elkhediri. "CyberSecurity: a review of internet of things (IoT) security issues, challenges and techniques." In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1-6. IEEE, 2019.

[25]. Leszczyna, Rafał. "Review of cybersecurity assessment methods: Applicability

perspective." *Computers & Security* 108 (2021): 102376.

[26]. Alghassab, Mohammed. "Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector." *Energies* 15, no. 1 (2022): 218.

[27]. Liu, Nian, Jianhua Zhang, Hao Zhang, and Wenxia Liu. "Security assessment for communication networks of power control systems using attack graph and MCDM." *IEEE Transactions on Power Delivery* 25, no. 3 (2010): 1492-1500.

[28]. Syamsuddin, Irfan, and Junseok Hwang. "A new fuzzy MCDM framework to evaluate e-government security strategy." In *2010 4th International Conference on Application of Information and Communication Technologies*, pp. 1-5. IEEE, 2010.

[29]. Torbacki, Witold. "A hybrid MCDM model combining DANP and PROMETHEE II methods for the assessment of cybersecurity in industry 4.0." *Sustainability* 13, no. 16 (2021): 8833.

[30]. Andraško, Jozef, Matúš Mesarčík, and Ondrej Hamuľák. "The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework." *AI & SOCIETY* (2021): 1-14.