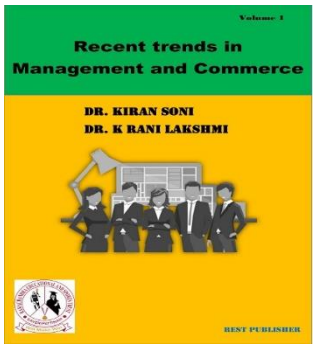
Recent trends in Management and Commerce

Vol: 1(1), 2019

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

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



Examining Ways Cyber Security Affects Energy Industry Monitoring and Control Systems

*** Darekar Harshada Sunil**

SST College of Arts and Commerce, Maharashtra, India

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

Abstract: *Energy industry monitoring and certain information structures, such as control systems, are exempt from the same IT regulations as other information systems worldwide. The administration of critical infrastructure, such as water management systems, nuclear power plants, oil and gas installations, and other things, also uses industrial control systems .System functionality must be consistent since system availability rate is crucial. To certify that a system is not susceptible to a cyberattack, it must be completely protected against cyber security flaws, risks, and dangers. Analyzes and assesses industrial control system cyber security evaluations, as well as any potential effects they may have on how accessible The energy sector may operate industrial control systems. Knowing the Attitude towards behavior method of Analytical Hierarchy Process and the ARAS allows one to assess operational assessments of the cyber security of industrial control systems. Confidentiality, availability, integrity, authentication, reliability, performance, and accessibility are all considered aspects of security. Durability, survivability, availability, maintainability, and accessibility are taken into consideration as evaluation parameters, and A1, A2, A3, A4, and A5 are considered as alternatives. characteristics and how they affect the cyber security of industrial control systems. To assess the calibre of results and their sensitivity, the author examined outputs from six different programmes. The robustness analysis's findings indicate that Alternative 3 is the best option for the industrial control system's cyber security strategy. This study will serve as a reliable resource for more regulated and secure monitoring and control systems.*

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

1. INTRODUCTION

Control systems are the brains and spinal cord of every energy infrastructure. It is made up of vast networks of electronically connected devices that are crucial for controlling and managing the production of electricity, the transport of electricity, and the extraction of oil and gas. A broad phrase known as "industrial control system" refers to a variety of tools and infrastructure components utilised in industries [1-3]. Data gathering, necessary part, programmable logic controllers, and multi-structural control systems are a few examples. In furthermore, the chemical, water and wastewater, energy, natural gas and oil, and transportation sectors also make use of industrial control systems. Failures of the operating system, organisational 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. In the event of a system failure (such as the shutdown of a plant), In order to quickly take control of the system and stop widespread problems, a number of power providers offer power system stabilisation devices. A central maths unit computes control the flow of information, a central control unit makes control decisions and outputs control commands, and a terminal unit performs fault diagnosis for the power system stabilisation systems [4]. Cyberattacks on the integrity, availability, and confidentiality of industrial control system innovations are possible since the majority of The directive's security requirements are not being met by improvements in industrial control systems. For instance, the cyber threat to availability disables performance tools, makes important controls inaccessible at all times, and disables advanced information. Integrity is threatened by handling complex data in resources, and secrecy is threatened by requests for related data. Cybersecurity evaluation is crucial to reducing and bridging the gap between industry control system cybersecurity concerns [6–8]. Cyberattacks and conventional security measures cannot adequately protect industrial systems from security practises. Given the increasing risks to our infrastructure and systems, finding the appropriate technology provider and consultant is crucial for their security. Protecting fog locations for industrial controls systems is the authors' first priority so that professionals can identify any unsafe or unforeseen activity. We are looking into ways to develop an industrial control system that is secure and has

cutting-edge intrusion detection technology to protect against cyberattacks. Prior to moving on, it is important to review recent studies on industrial computer control encryption and cyber-security issues. Authors assessed and more efficiently compiled the industrial control system's cyber security using multiple criteria decision making (MCTM) methodologies [9–15]. There are numerous MCDM strategies available to address decision-related issues [16–18]. The hesitant ARAS approach for scheduled paper [18–25] was applied in this research project. ARAS is a popular MCDM technique for selecting precise solutions from a variety of alternatives and features. The implementation of an AHP-based hierarchical MCDM technique is required due to the nature of the aspects involved in evaluating the cyber security of an industrial control system. The ARAS method looks to be a useful MCDM technique for determining the optimal choice from a list of options. To address issues with decision-making, many scholars have used this hybrid approach [26–30].

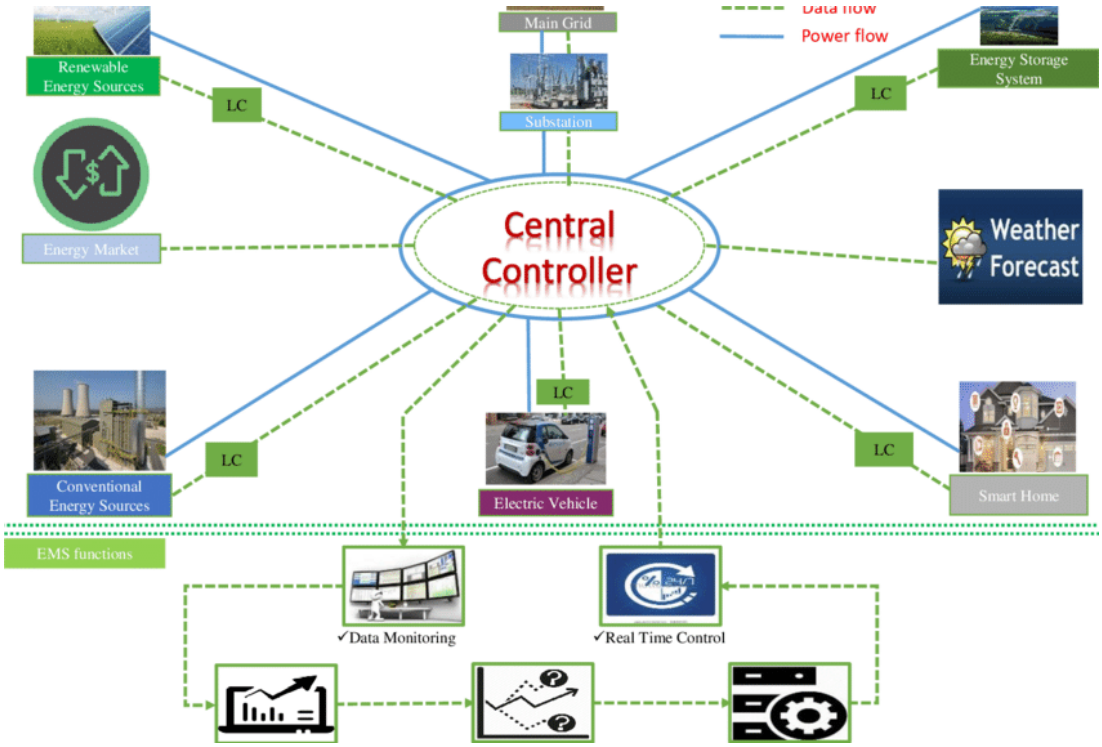


FIGURE 1. Central controller

Industrial computer control cyber security is described in terms of its characteristics and effects. There is discussion of the effects of recent cyber attacks. about issues with industrial control systems and safety worries. Using various techniques, we will walk through the methodology, Examine control comparisons, sensitivity analysis, and data analysis and results. Finally, we draw a conclusion to the paper and identify potential future research areas.

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 prioritise 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 preference

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.

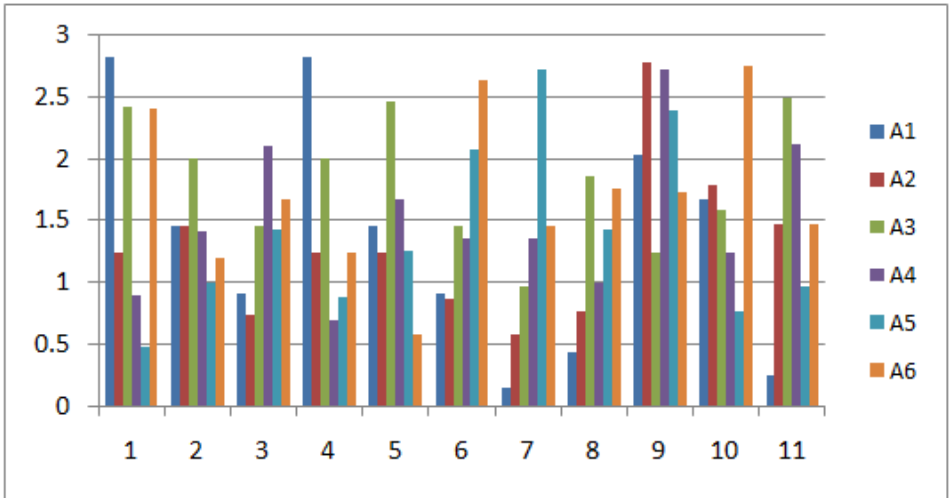


FIGURE 1. For the data set

Figure 1 shows the A6 values are the lowest and A1 values are the highest.

TABLE 3 maximum value

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
Max	**2.82**	**2.01**	**2.1**	**2.82**	**2.47**	**2.64**	**2.73**	**1.86**	**2.79**	**2.76**	**2.49**
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 shows the Wireless Network Max or Min value C1=2.82, C2=2.01, C3=2.1, C4=2.82, C5=2.47, C6=2.64, C7=2.73, C8=1.86, C9=2.79, C10=2.76 and C11=2.49

TABLE 4 normalized for data set

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
Max	0.215596	0.190702	0.202117	0.241026	0.221923	0.237197	0.245283	0.167116	0.250674	0.247978	0.22372
A1	0.215596	0.137571	0.087584	0.241026	0.130279	0.081761	0.012579	0.038634	0.183288	0.150045	0.021563
A2	0.094801	0.13852	0.07026	0.105983	0.111411	0.078167	0.052111	0.068284	0.250674	0.160827	0.132075
A3	0.18578	0.190702	0.139557	0.171795	0.221923	0.130279	0.087152	0.167116	0.111411	0.141959	0.22372
A4	0.068043	0.134725	0.202117	0.058974	0.150045	0.122192	0.122192	0.088949	0.245283	0.111411	0.190476
A5	0.035933	0.093928	0.137632	0.075214	0.112309	0.185984	0.245283	0.128482	0.214735	0.068284	0.087152
A6	0.184251	0.113852	0.160731	0.105983	0.052111	0.237197	0.130279	0.158131	0.155436	0.247978	0.132075

Table 5 Data for analysis are transformed into normalized data. In which all values are less than 1. This makes the analysis easier. A weight age value of 0.09 is taken same value for all the data to get the normalised weighted matrix.

TABLE 5 Weighted Normalized Matrix

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
Max	0.019404	0.017163	0.018191	0.021692	0.019973	0.021348	0.022075	0.01504	0.022561	0.022318	0.020135
A1	0.019404	0.012381	0.007883	0.021692	0.011725	0.007358	0.001132	0.003477	0.016496	0.013504	0.001941
A2	0.008532	0.012467	0.006323	0.009538	0.010027	0.007035	0.00469	0.006146	0.022561	0.014474	0.011887
A3	0.01672	0.017163	0.01256	0.015462	0.019973	0.011725	0.007844	0.01504	0.010027	0.012776	0.020135
A4	0.006124	0.012125	0.018191	0.005308	0.013504	0.010997	0.010997	0.008005	0.022075	0.010027	0.017143
A5	0.003234	0.008454	0.012387	0.006769	0.010108	0.016739	0.022075	0.011563	0.019326	0.006146	0.007844
A6	0.016583	0.010247	0.014466	0.009538	0.00469	0.021348	0.011725	0.014232	0.013989	0.022318	0.011887

Weighted Normalized Matrix is obtained in Table 5. With this we can get sum of value.

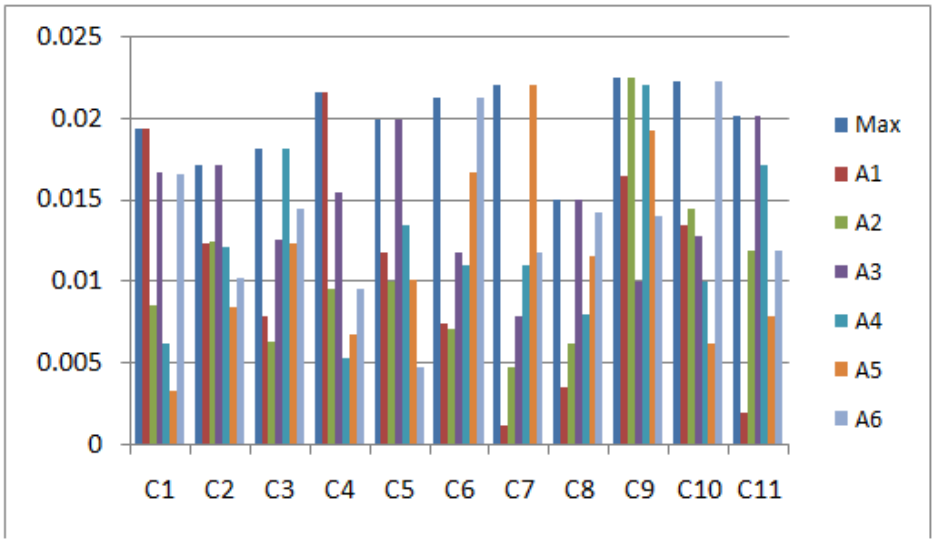


FIGURE 2. weighted normalized matrix

Figure 2 is shown In Table 5, the weighted normalised matrix is obtained. With this we can get sum of value.

TABLE 6. Si and Ki value

	Si	Ki
Max	0.096423	1
A1	0.073085	0.757964
A2	0.046888	0.486272
A3	0.081878	0.849157
A4	0.055251	0.573012
A5	0.040951	0.424707
A6	0.055524	0.575835

From table 6 sum of value is obtained Si and Ki value is obtained. Ki value is obtained by dividing Si Max value. This can be seen in Figure 2.

TABLE 7. Rank

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

The ranking is obtained from Table 7. It is not multiplied by Table 6. In this, A3 is the first and A5 is the last as seen in figure 3.

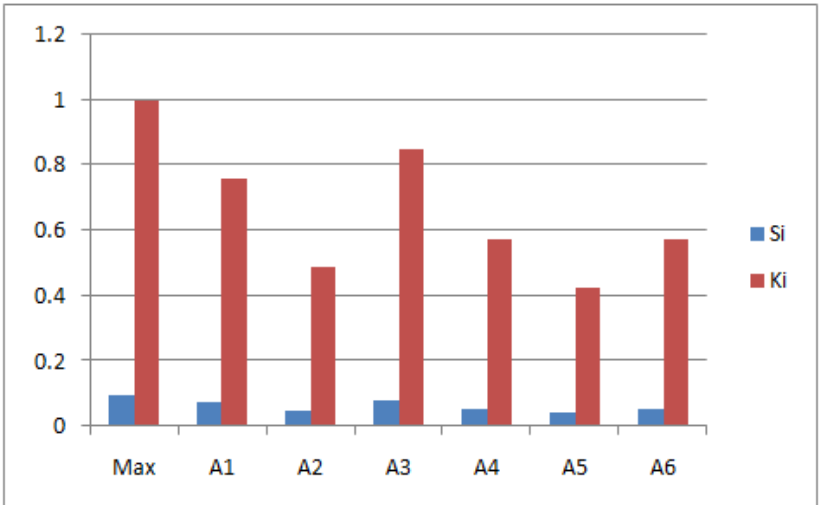


FIGURE 2. graph for Si and Ki value

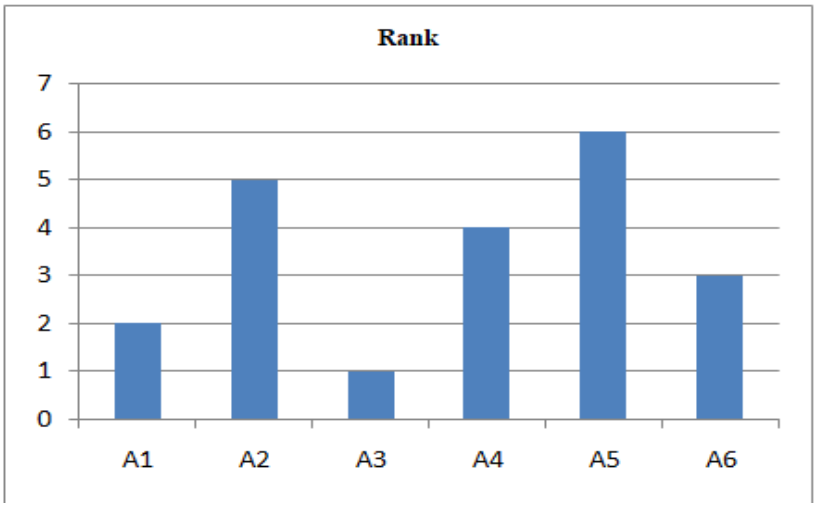


FIGURE 3. Ranking

4. CONCLUSION

According to us, future work must involve the creation of a hybrid dataset that combines data acquired from testbed simulation environments or power industry campuses with a number of key online-accessible datasets. We wish to build on our earlier work from the standpoint of industrial control systems with hybrid datasets, like the one described in [28-35], to assess the precision of machine learning methods. Contrarily, little study has been done on intrusion detection among the papers we gathered. To act as a model for a common technical platform for the construction of upcoming testing facilities for industrial controlling systems. Why to give organisations a test platform that is more effective than a standard testbed, produces findings that are more impressive, and decreases simulation and testing costs. To undertake cyberattacks against an energy industry hybrid monitoring and control system framework. Attacks on control systems at the component level are extremely challenging to identify and prevent due to the complexity of developing malware directed at controllers, such as nil rootkits and attacks. New intrusion detection methods are thus required for industrial control systems at the procedure control level. Machine learning methods have shown to be highly useful in this situation. The key conclusions of the suggested work are listed below. Improvements, study, identification, and prioritisation of security techniques will result from the focus on industrial control system cyber security components. MCDM techniques are used to research the safety evaluation of industrial control systems, such as the based ARAS approach.

REFERENCES

[1]. 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.

[2]. Ayofe, Azeez Nureni, and Barry Irwin. "Cyber security: Challenges and the way forward." *Computer Science*

& Telecommunications 29, no. 6 (2010).
[3]. 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.
[4]. 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.
[5]. 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.
[6]. 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.
[7]. Alghassab, Mohammed. "Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector." *Energies* 15, no. 1 (2022): 218.
[8]. 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.
[9]. 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.
[10]. 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.
[11]. 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.
[12]. Zavadskas, Edmundas Kazimieras, and Zenonas Turskis. "A new additive ratio assessment (ARAS) method in multicriteria decision-making." *Technological and economic development of economy* 16, no. 2 (2010): 159-172.
[13]. Zavadskas, Edmundas Kazimieras, Zenonas Turskis, and Tatjana Vilutiene. "Multiple criteria analysis of foundation instalment alternatives by applying Additive Ratio Assessment (ARAS) method." *Archives of civil and mechanical engineering* 10, no. 3 (2010): 123-141.
[14]. Ghenai, Chaouki, Mona Albawab, and Maamar Bettayeb. "Sustainability indicators for renewable energy systems using multi-criteria decision-making model and extended SWARA/ARAS hybrid method." *Renewable Energy* 146 (2020): 580-597.
[15]. Stanujkic, Dragisa, and Rodoljub Jovanovic. "Measuring a quality of faculty website using ARAS method." In *Proceeding of the International Scientific Conference Contemporary Issues in Business, Management and Education*, vol. 545, p. 554. 2012.
[16]. Kutut, Vladislavas, E. K. Zavadskas, and M. Lazauskas. "Assessment of priority alternatives for preservation of historic buildings using model based on ARAS and AHP methods." *Archives of civil and mechanical engineering* 14, no. 2 (2014): 287-294.
[17]. Liu, Nana, and Zeshui Xu. "An overview of ARAS method: Theory development, application extension, and future challenge." *International Journal of Intelligent Systems* 36, no. 7 (2021): 3524-3565.
[18]. Shaukat, Kamran, Suhuai Luo, Vijay Varadharajan, Ibrahim A. Hameed, Shan Chen, Dongxi Liu, and Jiaming Li. "Performance comparison and current challenges of using machine learning techniques in cybersecurity." *Energies* 13, no. 10 (2020): 2509.
[19]. Macher, Georg, Harald Sporer, Eugen Brenner, and Christian Kreiner. "Supporting cyber-security based on hardware-software interface definition." In *Systems, Software and Services Process Improvement: 23rd European Conference, EuroSPI 2016, Graz, Austria, September 14-16, 2016, Proceedings 23*, pp. 148-159. Springer International Publishing, 2016.
[20]. Alahmari, Abdulmajeed, and Bob Duncan. "Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence." In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, pp. 1-5. IEEE, 2020.
[21]. Buczak, Anna L., and Erhan Guven. "A survey of data mining and machine learning methods for cyber security intrusion detection." *IEEE Communications surveys & tutorials* 18, no. 2 (2015): 1153-1176.
[22]. Leszczyna, Rafał. "Review of cybersecurity assessment methods: Applicability perspective." *Computers & Security* 108 (2021): 102376.
[23]. 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.
[24]. 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.

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

[26]. 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.

[27]. 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.

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

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

[30]. 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.

