energies

MDPI

Article

Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector

Mohammed Alghassab

Electrical Engineering Department, College of Engineering, Shaqra University, Riyadh 11911, Saudi Arabia; malghassab@su.edu.sa

Abstract: Monitoring and control systems in the energy sector are specialized information structures that are not governed by the same information technology standards as the rest of the world's information systems. Such industrial control systems are also used to handle important infrastructures, including smart grids, oil and gas facilities, nuclear power plants, water management systems, and so on. Industry equipment is handled by systems connected to the internet, either via wireless or cable connectivity, in the present digital age. Further, the system must work without fail, with the system's availability rate being of paramount importance. Furthermore, to certify that the system is not subject to a cyber-attack, the entire system must be safeguarded against cyber security vulnerabilities, threats, and hazards. In addition, the article looks at and evaluates cyber security evaluations for industrial control systems, as well as their possible impact on the accessibility of industrial control system operations in the energy sector. This research work discovers that the hesitant fuzzy-based method of the Analytic Hierarchy Process (AHP) and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) is an operational procedure for estimating industrial control system cyber security assessments by understanding the numerous characteristics and their impacts on cyber security industrial control systems. The author evaluated the outputs of six distinct projects to determine the quality of the outcomes and their sensitivity. According to the results of the robustness analysis, alternative 1 shows the utmost effective cybersecurity project for the industrial control system. This research work will be a conclusive reference for highly secure and managed monitoring and control systems.

Keywords: hesitant fuzzy; AHP; fuzzy TOPSIS; cybersecurity; cyber-attack; industrial control systems; security assessment

Citation: Alghassab, M. Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector. *Energies* **2022**, *15*, 218. https://doi.org/10.3390/en15010218

Academic Editors: Raees Ahmad Khan, Alka Agrawal and Rajeev Kumar

Received: 9 November 2021
Accepted: 22 December 2021
Published: 29 December 2021

1. Introduction

Any energy infrastructure's central nervous system is comprised of control systems. It consists of extensive networks of linked electronic devices that are critical for monitoring and controlling power generation and transmission in the electric grid, as well as in petroleum and gas production. An industrial control system is a broad term that involves a variety of things employed in industries and essential infrastructures, such as multiple configuration control systems, supervisory control, distributed control systems, and data collection [1–3]. In addition, chemicals, water and sewage, power, oil and natural gas, and transportation are just a few of the industries that use industrial control systems. Vulnerabilities in industrial control systems are caused by the operating system, hardware, and industrial control system failures, as well as arrangement challenges and insufficient system maintenance.

A failure in the energy sector's monitoring and control systems may lead to a huge blackout. Many energy firms offer power system stabilizing devices that quickly control the system (for example, shutting off a plant) in the case of a system malfunction, preventing widespread disruptions. The central arithmetic unit (which calculates control information), the central control unit (which performs fault detection, control decision, and control

command output), and the terminal unit make up the power system stabilizing systems [4]. The following Figure 1 shows the general architecture of monitoring and control systems in the energy sector.

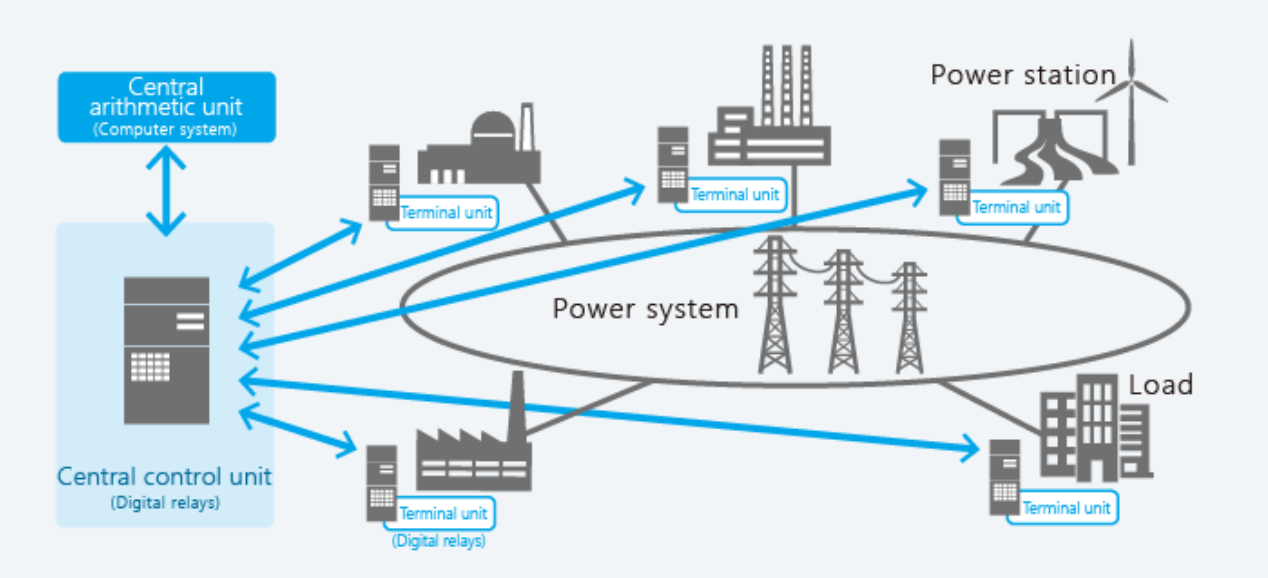

Figure 1. The architecture of monitoring and control systems in the energy sector (Source: Toshiba-Energy).

Vulnerabilities can be mitigated using a range of security measures, including network security, physical security systems, operating systems, and program patching [4,5]. Because most industrial control system advances do not adhere to the security criteria of a given instruction, cyber-attacks on their integrity, availability, and confidentiality can be carried out. A cyber threat to availability, for example, involves removing efficiency tools and making significant control and sophisticated information inaccessible at all times. Manipulation of complicated data on resources constitutes a threat to integrity, whilst listening in on relevant data constitutes a threat to secrecy.

Further, conducting a cyber-security evaluation is essential for minimizing and closing the gap between cyber security issues in industrial control systems [6–8]. Malicious attacks on industrial control systems have increased dramatically in recent years. Any hacker with a tainted USB stick or a single spear-phishing email can access a remote network, as proved by the BlackEnergy and Stuxnet assaults. To protect industrial systems from safety procedures, traditional security, and cyber-attacks are insufficient. Given the surge in threats to critical infrastructure and systems, finding the best technology provider and consultant to protect our infrastructure and systems is critical.

The authors are focusing our efforts on securing fog platforms for industrial control systems so that practitioners can detect any harmful or unusual activity. To put it another way, we are investigating how to build a secure industrial control system with an advanced intrusion detection system to protect it from cyber-attacks. It is vital that we first look at the cloudification of industrial control systems, as well as current work on industrial control system cyber-security vulnerabilities. The authors employed the Multiple Criteria Decision Making (MCDM) technique to analyze the cyber security assessment of the industrial control system and compile it more effectively [9–15].

For solving decision-related problems, there are numerous MCDM techniques [16–18]. This research work employed the hesitant fuzzy-based AHP and TOPSIS procedure for the projected paper [18–25]. Additional, AHP and TOPSIS are two common MCDM techniques for finding precise solutions among a variety of options and characteristics. The nature of the characteristics involved in estimating a cyber security assessment of the industrial

control system necessitates the use of an AHP-based hierarchy-based MCDM technique. TOPSIS technique also appears to be a good MCDM technique for choosing the best option among numerous choices. This hybrid procedure has been employed by a number of academics to solve decision-making difficulties [26–30].

AHP, on the other hand, is the most extensively employed MCDM procedure, and it is recognized as providing more accurate findings. In AHP, the hierarchy model is employed for an estimate, while in the Analytic Network Process (ANP), the networked model is employed for estimating in decision making. Furthermore, both methods collect pair-wise assessment matrix statistics and prioritize the options for outcome testing. Every property of the mentioned hierarchy is self-determining in itself, and the same is also implemented in alternatives, which is a complementary advantage of AHP. The qualities and options, on the other hand, are mutually dependent on each other, as shown in real-time scenarios [31–34].

Bijoyeta Roy et al. employed the MCDM procedure of hesitant fuzzy AHP-TOPSIS for industrial control systems selection [35]. This tactic assisted in prioritizing the greatest available solutions from a plethora of project decisions, as well as alternative positions. Madjit Tavana et al. employed the hesitant fuzzy AHP-TOPSIS method to estimate a single variable, for example, community, for e-governance willingness [36]. Using the hesitant fuzzy AHP technique, Baozhu Li et al. assessed the security features of computers [37]. As a result, a review of existing research in this area reveals that there are a variety of MCDM tactics for tackling decision-related problems [38]. The authors employed the hesitant fuzzy-based Analytic Hierarchy Process (AHP) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) for the proposed article [39–41]. AHP and TOPSIS are two common MCDM methodologies for locating accurate solutions among a variety of options and features.

The remainder of the article is organized as follows. The authors will address the characteristics and consequences of industrial control system cyber security in Segment 2. We will also discuss the consequences of recent cyber-attacks in Segment 3. We will talk about the security concerns and issues with industrial control systems in Segment 4. In Segment 5, we will go through the approach, and in Segment 6, we will go over data analysis and outcomes, sensitivity analysis, and containment comparisons using various methods. Finally, in Segment 7, we reach the end of the document and also discuss possible future research directions.

2. Industrial Control System

An industrial control system is a collection of control systems and related equipment that includes networks, devices, systems, and controls employed to operate and/or systematize industrial procedures. Each industrial control system is designed to handle work efficiently and electronically, and performs differently depending on the industry. Devices and protocols for industrial control systems may now be found in almost every critical infrastructure and industrial location, including transportation, manufacturing, water, and energy treatment [40–45]. In the perspective of information security, the confidentiality, integrity, and availability triangle is a well-known approach for designing security rules. Each character redirects an initial data security aim in instruction to accomplish success:

- *Integrity*

To protect against unauthorized information tampering or loss, a statement of non-repudiation, correctness, and validity of information is necessary.

- *Confidentiality*

Maintaining allowed access and transparency limits while protecting data privacy and classified information.

- *Availability*

Ensure that information is readily available and is employed in a timely and accurate manner.

In the safety triangle, the availability and integrity of industrial control systems are more important than secrecy. They seek to increase availability so that systems can run and execute without being accidentally disrupted. In control systems, data integrity is critical. It could have a substantial influence on the operation or even security if the operator's screen in the command center does not precisely represent what is going on. Integrity and confidentiality are frequently less of a concern in industrial control systems than availability. Because data in an industrial control systems environment, such as speed, vibration, and temperature is only temporary, this is the case.

Industrial control systems are generally designed to work as reliably as possible for as long as possible. Industrial control systems are often designed to endure 20 years or more [12–15]. Further, it is difficult to upgrade the security patch. Furthermore, conducting various forms of cyber security assessments on industrial control systems is difficult, especially when guaranteeing that the cyber security assessment does not disrupt the system.

2.1. Impact of Industrial Control System: Electric Power Grid Perspective

To integrate generating, transmission and distribution functions, the information technology infrastructure for energy utilities today uses many types of industrial control systems [11–15]. From a cyber-security standpoint, the danger has increased as an outcome of the improved connectivity and network linkages. Consequently, the integration of operating technology systems and information technology is widened, and as a result the occurrence of the power supply area is widened. These two components have been separated in the past, yet they are still linked in many situations. In the operating technology sector, the industrial control systems platform is likewise based on a commercial information technology operating system. This suggests that the operational technology environment has exposed weaknesses in the information technology environment.

Because of software compatibility, which is primarily supported by the unique apparatus industrialist for software updates, a typical way of increasing the system security in an operational technology environment is frequently not to reinforce or preserve the information technology environment [15]. This shows that operational technology systems are falling behind their information technology counterparts defensively. Many industrial control systems networks eventually lack authentication methods and regulated access regulations, and cyber security management is often insufficient or non-existent, leaving them susceptible.

2.2. Impact of Cyber-Attack: Industrial Control System Perspective

Cyber security evaluation in control systems of industry assists the asset owner or organization in determining the cyber security strength of its infrastructure [4,15–17]. It also aids in the detection of any vulnerabilities or flaws that could permit a hacker to interrupt or seize control of the system. Following the discovery of ambiguities and vulnerabilities, the flaws are corrected and mitigated in an attempt to prevent cyber-attacks that could jeopardize industrial control systems. As seen in Table 1, many cyber incidents have happened as an outcome of insufficient cyber security evaluation.

The availability of a security triad has long been a primary priority for industrial control systems. Some systems refuse to apply patches or system updates because they may jeopardize the system's availability. The lack of modernizing or the most recent patch version can result in catastrophic cyber-attacks. As a result, several vulnerabilities and security issues exist in control systems of industry [20–23]. A cyber security assessment is required in instruction to distinguish these security problems and vulnerabilities in industrial control systems. To do so, the information security professional must be familiar with the industrial control systems they are evaluating. A single blunder when conducting a cyber-security assessment in an industrial control systems environment might cause downtime and disrupt routine operations. As a result, this research looks at different methods for conducting cyber security assessments in control systems of industry.

Table 1. Impact of Cyber-Attack.

Cyber Occurrence Name	Place Happened	Year	Impact
BlackEnergy	Ukraine Power Grid	2014/2015	In Ukraine, a 6-h power outage occurs, affecting an estimated 230,000 people.
Industroyer/Crash Override	Ukraine Power Grid (North City of Kiev)	2016	1 h of power outage causes Ukraine to lose 1/5 of its electric capacity, according to estimates.
Triton	Oil and Gas Plant Saudi Arabia	2017	The attackers intended to produce a plant-wide explosion, however, their scheme was foiled due to a vulnerability and defect in their virus.

2.3. Impact of Scanning Tools/Techniques: Industrial Control System Perspective

In the industrial control systems context, a standard system or software application is utilized to undertake cyber security assessment [24–27]. The majority of the tools utilized are comparable to those employed by analysts to examine the IT infrastructure. Due to the assessment itself, several tools employed in the information technology environment can have an influence on the accessibility of control systems of industry, such as causing some systems and disturbing operations to failure. The following (Table 2) are some of the most frequent tools employed by analysts, which may have an influence on accessibility.

Table 2. Scanning tools for industrial control systems.

Software	Objective	Impact on Accessibility
Nmap	To identify and detect hosts on a network, as well as obtain information about them, such as the services they provide and the ports they open.	Yes
Shodan	To execute and conduct searching and scanning for hosts or services that run on internet-connected devices.	No
Nessus	To execute vulnerability analysis and host investigation on an identified host, as well as to provide a summary of the discovered vulnerability and a method to fix it.	Yes

2.3.1. NMAP

Nmap is a network scanning program that is often employed to identify and detect hosts on a network [4–9]. Concurrently, this program collects data about the host, for example, the facilities they provide and the host's primary port. When employed in industrial control systems, Nmap might cause the system to crash, causing havoc in the environment. If the tool scans legacy systems or devices, the device will crash. Rare legacy systems may have difficulty processing the stack of TCP/IP requirements from the scanner, and in some situations, the device may be unable to accept numerous requests from Nmap, leading the device to crash or misbehave.

The effect of this tool is that the scanned devices or systems may crash, thereby disrupting the procedure of industrial control systems. Finally, Nmap should be fine-tuned to work in the context of control systems of industry. Nmap should not run disturbing scans, and the system's threshold and time should be fine-tuned. This reduces the risk of system crashes and misbehavior during scanning and ensures that the network is not overburdened with scanning traffic.

2.3.2. SHODAN

Shodan is a search engine that is employed to find systems that are associated with the internet [6–9]. It differs from other famous search engines, like Yahoo, Bing, and Google, in that it searches for systems that are connected with the internet. Misconfiguration errors are revealed when devices or systems are visible on Shodan. Shodan scans the network for connected devices. It looks for accessible terminals, and a customer can use Shodan to look for specific facilities that run on a certain host. As an outcome, if a single IP address hosts many services, Shodan displays a list of all available services at that address. An illustration of a Shodan search outcome is shown in Figure 2.

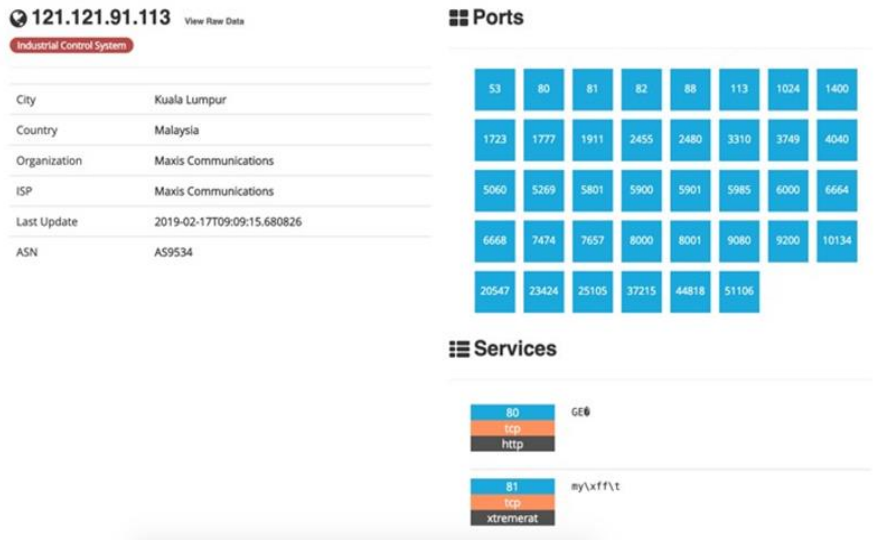

Figure 2. A sample of Shodan search outcome.

Shodan collects data in metadata format, which includes hostnames, operating systems, geographic locations, and features relevant to transport or application layer protocols, such as server message blocks, SSH, SSL, and TLS protocol. The observable system that Shodan has distinguished should be evaluated to see if it is harmless. In instruction to perimeter the approachability the of Shodan search engine scan in obtaining data, the system should be configured.

2.3.3. NESSUS

The Nessus tool is employed to do vulnerability analysis and host discovery on discovered hosts, as well as to provide an outline of the identified vulnerability and the method to fix it [10–16]. Nessus has the capability to continually test each method employed to build internal services in order to uncover potential susceptibilities based on host replies to each probe and request. The vulnerability signature is then compared to the Nessus database to discover probable flaws (Figure 3).

Denial of service testing, dictionary attack plugins, and brute force, for example, should be immobilized first. These two plugins have the potential to cause the system to crash or malfunction. A dynamic investigation on the host might cause a system crash and denial of service, disrupting the availability of industrial control systems. This incident might occur in either information technology or an operational technology setting. Finally, Nessus needs to be fine-tuned to work in the industrial control systems environment. Prior to scanning using Nessus, make sure you have a complete picture of the system.

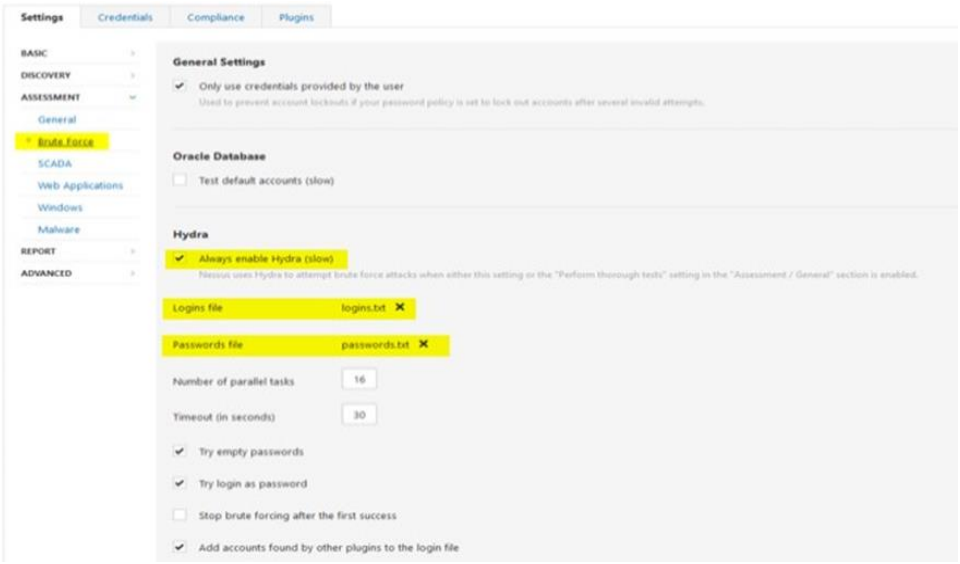

Figure 3. A sample of Nessus feature can cause crash.

To avoid a crash and allow the industrial control systems to work normally, appropriate extenuation planning should be completed to verify if the system misbehaves. Because of software compatibility, which is primarily supported by the unique apparatus industrialist for any modernizes of software, a typical way of increasing the security of a system in an operational technology environment is usually not to patch or preserve the information technology environment. This shows that operational technology systems are falling behind their information technology counterparts defensively. Many industrial control systems networks eventually lack authentication methods and regulated access regulations, and cyber security management is often insufficient or non-existent, leaving them susceptible.

3. Issues and Challenges Related to Industrial Control System

Attacks on industrial control systems have risen year after year. Some have had a significant impact at the national level, while others are tiny occurrences. With the recent cyber incidents that have targeted the industrial control systems industry, there is a compelling need to undertake a cyber-security estimation to determine the robustness of industrial control systems from a cyber-security standpoint. The majority of cyber security evaluations are geared toward information technology systems and do not take into account the limits that industrial control systems face. As a result, this study offers many appropriate ways of conducting assessments of cyber security in control systems of industry.

Obtaining real-time and unbiased datasets is a major difficulty when using machine learning methods. Numerous datasets are inner and cannot be united due to confidentiality and consumer privacy concerns, or they may be missing key statistical properties. Because of these difficulties, most industry settings avoid exchanging their protected network data. As a result, researchers choose to create datasets for testing and training in confined or simulated experimental contexts, which may be limited in scope. When machine learning frameworks are educated on a single dataset, the semantic gap between the outcomes and their application is common. The supervised machine learning frameworks that perform well with one dataset may or may not perform well with totally various datasets generated under various simulation or experimental circumstances, according to Bhamare et al. [5]. To demonstrate this, Bhamare et al. employed a separate dataset to test the aforementioned frameworks and found that they performed significantly worse, as presented in Figures 4 and 5.

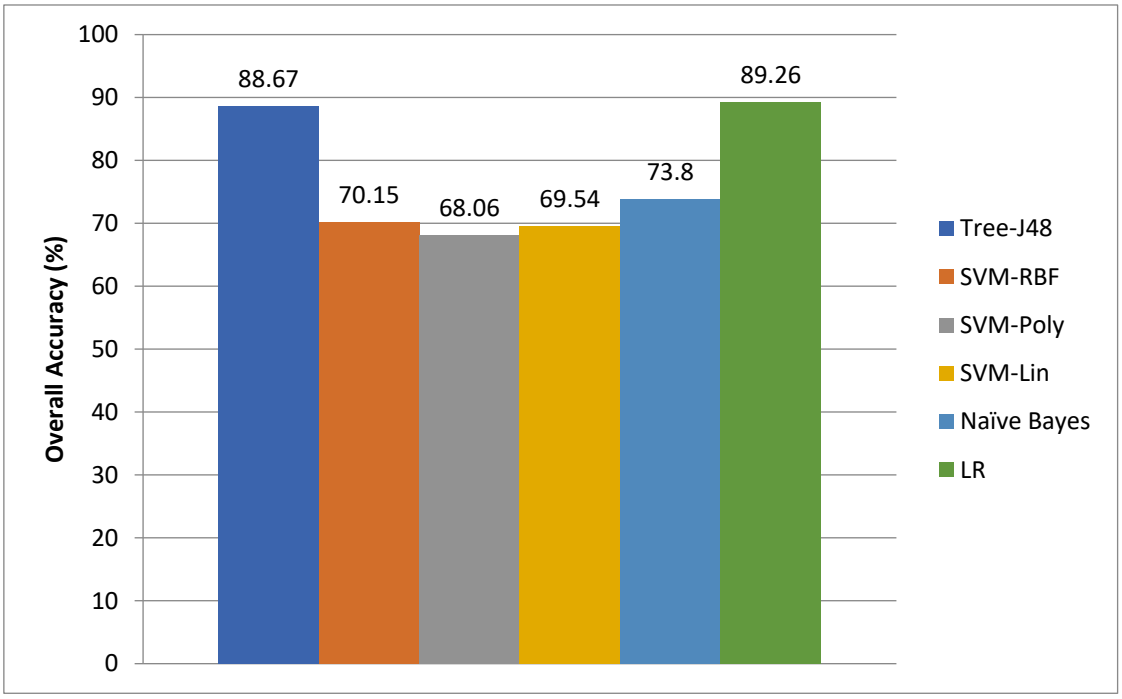

Figure 4. Overall Accurateness.

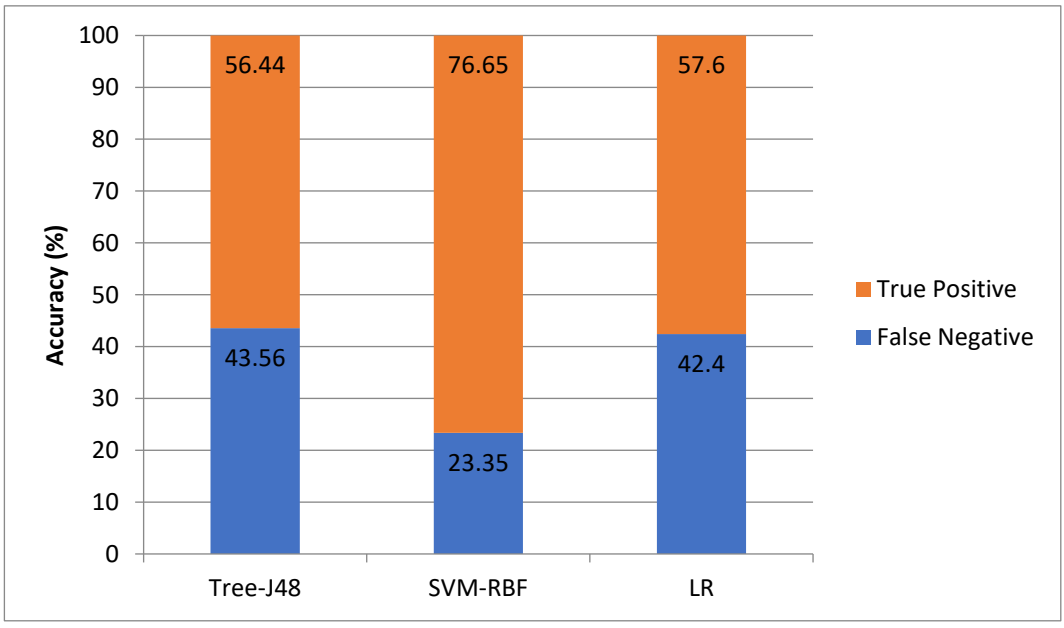

Figure 5. Rates of true negative and true positive.

A similar difficulty arises when machine learning approaches are applied to the cybersecurity of industrial control systems. There is a scarcity of research that shows the efficacy of machine learning frameworks across diverse datasets collected in various situations. There is a scarcity of research that shows the efficacy of these frameworks across many datasets collected in various situations. It is stated that machine learning frameworks must be tested for resilience, especially under a variety of operating situations, which are common in control system scenarios. The findings highlight the necessity for a security testbed for industrial control systems, which can be employed to mimic genuine industrial control systems and investigate the consequences of assaults on them. Researchers would

be able to investigate cyber-attacks and defense measures while assessing their influence on control systems in an innovative setting.

4. Security Attributes in Perspective of Industrial Control System

Security is one of the primary characteristics of an industrial control system that has an indirect impact. Figure 6 shows how using the security factor in the secure phase can improve the quality of the industrial control system. In Figure 6, six options for selecting the best option between two industrial control systems have been shown.

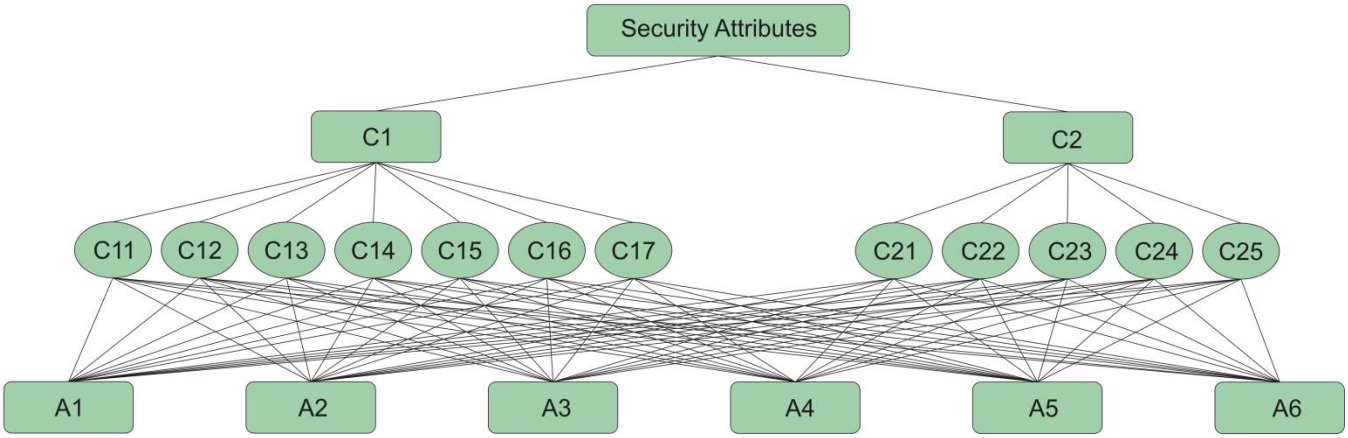

Figure 6. A tree structure of security parameters.

There are two tiers to the security attributes: C1 and C2 in level-1 signify security and trust. C11, C12, C13, C14, C15, C16, and C17 in security signify confidentiality, availability, integrity, authentication, reliability, efficiency, and accessibility (level-2). Durability, survivability, availability, maintainability, and accessibility are categorized as C21, C22, C23, C24, and C25 in terms of trustworthiness at level-2. The following is the definition of the qualities of industrial control systems:

Emotional stability is a key feature of pre-adolescents. When acquiring a pre-owned automobile, security is an important factor to consider. Security is a vital component for preserving and protecting industrial control systems from damaging attacks and other threats presented by malicious data and hackers. Confidentiality in the perspective of security denotes permitting approved access to secure and sensitive data [24]. We must protect data from leakage since confidentiality is the foundation of cybersecurity and privacy. The value of the data will be lost if it is leaked. If hackers attack the data and change it or locate hidden information, the benefit of cyber security may be lost. Integrity is a demand characteristic that ethical assurance and resolution recognize. Integrity is also necessary for obtaining useful and reliable data. We cannot analyze the proper conclusion if the data is wrong or partial, especially if the missing data is the most sensitive and useful. From a computer system perspective, availability refers to a customer's ability to access data or assets for a specific amount of time [27].

This work contributes to a fuzzy AHP assessment of cyber security. Because cyber security and privacy necessitate a large amount of network bandwidth, efficiency is especially important. Authenticity is required to ensure that data sources, processors, and authorized data requesters are trustworthy. The identification of a user profile is determined by the authentication of industrial control systems. It is the procedure of defining whether or not a customer is who they claim to be [5]. It might help you to avoid erroneous analysis results and get the most out of your cyber security. Reliability is a capability that demonstrates an application's performance consistency in a controlled environment over a period of time. Cyber security's capacity to restrict user information rights within a secure environment is known as accessibility. Figure 6 depicts a tree structure of cyber security features.

The capacity to manage and provide data solely to authorized users is referred to as confidentiality. Level-2 is depicted in Figure 6. According to the definitions of trustworthiness, cyber security industrial control systems are trustworthy if they can prevent, respond to, and survive assaults, malfunctions, and other potentially detrimental scenarios. The control system's trustworthiness ensures that it will function as planned. The need for safety is paramount. The term "durability" refers to a cyber-security system's ability to last for an extended length of time [21]. Security durability has a big impact on cyber security because the time limit of security has a substantial impact on total cyber security. The capacity to define patching and rearrangements in industrial control systems for a certain course of work is known as maintainability. Survivability refers to a cyber-security system's ability to achieve its goal, whether it is in the face of an assault or a failure. Only authorized users have access to the information, which is referred to as availability. In the perspective of cyber-security, availability states to a user's ability to access data or resources for a set period of time. Cyber security's capacity to restrict user information rights within a secure environment is known as accessibility.

5. Methodology

Some real-world problems necessitate one-of-a-kind or multi-choice-based solutions that allow users to pick the best option from a variety of possibilities without relying on a solid foundation. Various scholars [12–14] have employed MCDM methodologies to address this circumstance and provide an optimal quantitative solution to these issues. In comparison to other approaches, the particularly approved AHP tactic joined with a fuzzy set theory is easy and extra effective. Several earlier research projects [15–17] have demonstrated this. If there is more than one selection for assessment in the approach during the computing process, this situation has a stronger impact on the computed outcomes. The authors use a hesitant fuzzy set-based MCDM approach in the suggested study, which delivers added efficiency in outcomes from the perspective of assessment. In addition, the TOPSIS technique was utilized to examine the impact of cyber security on industrial control systems. Furthermore, this work employs the hesitant fuzzy-based TOPSIS approach to obtain more productive and correct findings. The TOPSIS methodology is the most suited strategy accessible among the MCDM methodologies for testing the evaluated findings. The most significant benefit of this system is that it considers both positive and negative impacts in the computation.

In our study, we employed HF-AHP procedures to determine the important characteristics of security risk, and then we employed their HF-TOPSIS approach to examine alternatives for similar criteria [45]. In brief, the following is the sequential procedure:

Step 1: The establishment of a factor hierarchy is the first stage in the adopted approach.

Step 2: Investigators employ linguistic terms in Table 3 to develop precise and useful estimation criteria for experts.

Table 3. Scale for HF-AHP technique.

Rank	Linguistic Term	Abbreviation	Triangular Fuzzy Numbers
10	Absolutely High Importance	AHI	(7.00, 9.00, 9.00)
9	Very High Importance	VHI	(5.00, 7.00, 9.00)
8	Essentially High Importance	ESHI	(3.00, 5.00, 7.00)
7	Weakly High Importance	WHI	(1.00, 3.00, 5.00)
6	Equally High Importance	EHI	(1.00, 1.00, 3.00)
5	Exactly Equal	EE	(1.00, 1.00, 1.00)
4	Equally Low Importance	ELI	(0.33, 1.00, 1.00)
3	Weakly Low Important	WLI	(0.20, 0.33, 1.00)
2	Essentially Low Importance	ESLI	(0.14, 0.20, 0.33)
1	Very Low Importance	VLI	(0.11, 0.14, 0.20)
0	Absolutely Low Importance	ALI	(0.11, 0.11, 0.14)

Step 3: The incorporation of fuzzy wrappers [46–48] from Equation (1) is the next stage in approach evaluation.

$$OWA(a_1, a_2, \ldots a_n) = \sum_{j=1}^{n} W_j b_j \tag{1}$$

In the same way that professionals estimate the trapezoidal numbers, $\widetilde{C} = (a, b, c, d)$ by the Equations (2)–(5) after Equation (1).

$$a = min\left\{a_L^i,\ a_M^i, a_M^{i+1},\ \ldots\ldots a_M^j, a_R^j\right\} = a_L^i \tag{2}$$

$$d = max\left\{a_L^i,\ a_M^i, a_M^{i+1},\ \ldots\ldots a_M^j, a_R^j\right\} = a_R^j \tag{3}$$

$$b = \left\{ \begin{array}{c} a_M^i, if\ i+1 = j \\ OWA \\ w^{2(a_m^j,\ \ldots\ldots a_m^{\frac{i+j}{2}})},\ if\ i+j\ is\ even \\ OWA \\ w^{2(a_m^j,\ \ldots\ldots a_m^{\frac{i+j+1}{2}})},\ if\ i+j\ is\ odd \end{array} \right\} \tag{4}$$

$$c = \left\{ \begin{array}{c} a_M^{i+1}, if i+1 = j \\ OWA \\ w^{2(a_m^j a_m^{j-1},\ \ldots\ldots a_m^{\frac{(i+j)}{2}})},\ if\ i+j\ is\ even \\ OWA \\ w^{2(a_m^j, a_m^{j-1}\ \ldots\ldots a_m^{\frac{(i+j+1)}{2}})},\ if\ i+j\ is\ odd \end{array} \right\} \tag{5}$$

Following the application of Equations (3)–(5), the practitioners choose the first and second form of weights, i.e., the number between [0, 1] and Equations (6) and (7) to acquire these values.

First type weights $(W1 = (w_1^1, w_2^1, \ldots\ldots\ldots w_n^1))$:

$$w_1^1 = \eta_2,\ w_2^1 = \eta_2(1-\eta_2), \ldots\ldots\ldots w_n^1 \eta_2 (1-\eta_2)^{n-2} \tag{6}$$

Second type weights $\left(W2 = \left(w_1^2, w_2^2, \ldots\ldots\ldots w_n^2\right)\right)$:

$$w_1^2 = \eta_1^{n-1},\ w_2^2 = (1-\eta_1)\eta_1^{n-1} \tag{7}$$

The mathematical system for the highest rank in the formula $\eta_1 = \frac{g-(j-1)}{g-1}$s, and $\eta_2 = \frac{g-(j-1)}{g-1}$ is g and lowest, highest rank factors are displayed by i and j, respectively.

Step 4: Experts employ Equations (8) and (9) to meet the remaining comparison matrix qualities after analyzing the full prior approach. The experts then defuzzify the matrix using Equation (10) to determine the comparison matrix.

$$\widetilde{A} = \begin{bmatrix} 1 & \cdots & \widetilde{c}_{1n} \\ \vdots & \ddots & \vdots \\ \widetilde{c}_{n1} & \ldots & 1 \end{bmatrix} \tag{8}$$

$$\widetilde{c}_{ji} = \left(\frac{1}{cij_u}, \frac{1}{cij_{m2}}, \frac{1}{cij_{m1}}, \frac{1}{cij_1}\right) \tag{9}$$

$$\mu_x = \frac{l + 2m_1 + 2m_2 + h}{6} \tag{10}$$

Step 5: Correct values are obtained during the defuzzification phase. The experts assess the consistency ratio (CR) of these data by using Equations (11) and (12) to analyze the CR.

$$CI = \frac{\gamma_{max} - n}{n-1} \tag{11}$$

$$CR = \frac{CI}{RI} \tag{12}$$

Step 6: The experts evaluate the geometrical mean of the variables in this step using Equation (13).

$$\widetilde{r}_i = \left(\widetilde{c}_{i1} \bigotimes \widetilde{c}_{i2} \ldots\ldots \bigotimes \widetilde{c}_{in}\right)^{\frac{1}{n}} \tag{13}$$

Step 7: Experts estimate the most important criterion in the full collection by using the Equation (14).

$$\widetilde{w}_i = \widetilde{r}_1 \bigotimes \left(\widetilde{r}_1 \bigotimes \widetilde{r}_2 \ldots\ldots .\widetilde{r}_n\right)^{-1} \tag{14}$$

.

Step 8: Examiners use Equation (15) to examine the defuzzified values.

$$\mu_x = \frac{l + 2m_1 + 2m_2 + h}{6} \tag{15}$$

Step 9: Experts convert defuzzified values into normalized values or weights by using Equation (16).

$$\frac{\widetilde{w}_i}{\sum_i \sum_j \widetilde{w}_j} \tag{16}$$

The second TOPSIS procedure is now employed to examine the usefulness of the produced findings after determining the priority list for specified criteria. As a MADM technique, TOPSIS is effective at recommending the most favored alternative for use. Torra and Narukawa [49] provided a definition of the TOPSIS technique. TOPSIS technique is the synthesis of positive and negative thoughts; the most exact and trustworthy factor is the most accurate and effective solution. An unimportant factor, on the other hand, is the worst option. To evaluate and measure the security risk of industrial control systems, the authors employed the hesitant fuzzy AHP TOPSIS technique [45–50]. The TOPSIS approach computes and associates the distance between two linguistic values, such as $H1s$ and $H2s$. The procedure (Equation (17)) has been clarified below:

$$d(H1s, H2s) = |q^* - q| + |p^* - p| \tag{17}$$

Step 10: The following terms are described as the starting process:

- The following written formulas are applied as $(C = \{C_1,\ C_2, \ldots\ldots C_E\})$ and n criteria $(C = \{C_1,\ C_2, \ldots\ldots C_n\})$ to define alternatives and criteria in TOPSIS.
- Similarly, k is employed to show the numeric count of experts in TOPSIS; e_x denotes the experts.
- The equation $\widetilde{X}^l = \left[H^l_{S_{ij}}\right]_{E \times n}$ is employed in the TOPSIS procedure to signify the HF matrix.
- The standards are written for TOPSIS to determine the criteria and effect of outcomes:

  The standard for TOPSIS evaluation lies in between *very poor and very good scale,*
  r^1_1 = *between medium and good* (bt M&G)
  r^1_2 = *at most medium* (am M)
  r^2_1 = *at least good* (al G)
  r^2_2 = *between very bad and medium* (bt VB&M)
  For HF matrix, the following formulas are employed [45–49]:
  $env_F(EGH\ (btM\&G)) = T$ (0.3300, 0.5000, 0.6700, 0.8300)
  $env_F(EGH\ (amM)) = T$ (0.0000, 0.0000, 0.3500, 0.6700)
  $env_F(EGH\ (alG)) = T$ (0.5000, 0.8500, 1.0000, 1.0000)
  $env_F(EGH\ (btVB\&M)) = T$ (0.0000, 0.3000, 0.3700, 0.6700)

Step 11: By applying the Equation (18) formula, the associated combined matrix is created:

$$T_{pij} = min\left\{min^K_{i=1}\left(maxH^x_{t_{ij}}\right), max^K_{i=1}\left(minH^x_{t_{ij}}\right)\right\}$$

$$T_{qij} = max\left\{min_{i=1}^{K}\left(maxH_{t_{ij}}^{x}\right), max_{i=1}^{K}\left(minH_{t_{ij}}^{x}\right)\right\} \quad (18)$$

Step 12: In the TOPSIS assessment, the effective characteristics, where the utmost effective characteristic is specified by Aj, is presented by alpha, and alpha indicates the cost-related preferences. Furthermore, the most recent efficient alternatives necessitate a high level of precision for cost-related choices. To describe and link the cost and effective characteristics, use the following Equations (19)–(22):

$$\widetilde{V}_{pj}^{+} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b \text{ and } min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c\right) \quad (19)$$

$$\widetilde{V}_{qj}^{+} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b \text{ and } min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c\right) \quad (20)$$

$$\widetilde{V}_{pj}^{-} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c \text{ and } min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b) \quad (21)$$

$$\widetilde{V}_{qj}^{-} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c \text{ and } min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b) \quad (22)$$

Step 13: Professionals assess TOPISIS positive and negative ideas components by relating following Equations (23) and (24).

$$D^{+} = \begin{bmatrix} d\left(x_{11}, \widetilde{V}_1^{+}\right) + & d\left(x_{12}, \widetilde{V}_2^{+}\right) + & \ldots & +d\left(x_{1n}, \widetilde{V}_n^{+}\right) \\ d\left(x_{21}, \widetilde{V}_1^{+}\right) + & d\left(x_{22}, \widetilde{V}_2^{+}\right) + & \ldots & +d\left(x_{21}, \widetilde{V}_n^{+}\right) \\ d\left(x_{m1}, \widetilde{V}_1^{+}\right) + & d\left(x_{m2}, \widetilde{V}_1^{+}\right) + & \ldots & +d\left(x_{mn}, \widetilde{V}_n^{+}\right) \end{bmatrix} \quad (23)$$

$$D^{-} = \begin{bmatrix} d\left(x_{11}, \widetilde{V}_1^{-}\right) + & d\left(x_{12}, \widetilde{V}_2^{-}\right) + & \ldots & +d\left(x_{1n}, \widetilde{V}_n^{-}\right) \\ d\left(x_{21}, \widetilde{V}_1^{-}\right) + & d\left(x_{22}, \widetilde{V}_2^{-}\right) + & \ldots & +d\left(x_{21}, \widetilde{V}_n^{-}\right) \\ d\left(x_{m1}, \widetilde{V}_1^{-}\right) + & d\left(x_{m2}, \widetilde{V}_1^{-}\right) + & \ldots & +d\left(x_{mn}, \widetilde{V}_n^{-}\right) \end{bmatrix} \quad (24)$$

Step 14: Professionals construct and evaluate the closeness of positive and negative factors assessed by Equations (25) and (26).

$$CS(A_i) = \frac{D_i^{+}}{D_i^{+} + D_i^{-}}, \; i = 1, 2, \ldots . m \quad (25)$$

where

$$D_i^{+} = \sum_{j=1}^{n} d\left(x_{ij}, V_j^{+}\right) \text{ and } D_i^{-} = \sum_{j=1}^{n} d\left(x_{ij}, V_j^{-}\right) \quad (26)$$

Step 15: To bring the procedure to a close, the ranks are assigned, and the tabular form of the options is employed to assess their effectiveness.

A highly detailed and analyzed mathematical calculation of security risk has been undertaken in later stages of this study to improve the life duration of industrial control system cyber security

6. Data Analysis and Results

The authors started by identifying several security features for industrial control systems. Several qualities at level-1, namely availability and integrity, are specified as C1 and C2 for evaluating the security evaluation of industrial control systems. In terms of estimating the security of industrial control systems at level-2, confidentiality, availability, integrity, and accessibility are the properties of dependability, and they are denoted by the letters C11, C12, C13, C14, C15, C16, and C17, accordingly. Maintainability, accountability, survivability, availability, and accessibility are the properties of trustworthiness, and they are denoted by the letters C21, C22, C23, C24, and C25, respectively. The study then gathered the opinions of 110 experts from academia and industry (using a virtual environment) to determine the numerical assessment of these features.

These specialists had between two and ten years of experience in the subject of industrial control system security. The authors then calculated the security of the industrial control system using Equations (1)–(26) and Table 3, in which the authors converted language values into numeric values, then hesitant fuzzy-based crisp numerical values, and produced pair-wise comparison matrixes. The authors employed Equations (10)–(16) to defuzzify the pair-wise comparison matrixes into collective values, as well as determine the consistency ratio. Tables 4 and 5 show the calculated values of the trapezoidal fuzzy number, defuzzification values, and finalized values of the weights at level 1 and level 2.

Table 4. HF Pairwise Comparison Matrix at level 1.

	C1	**C2**
C1	1.00000, 1.00000, 1.00000, 1.00000	1.00000, 1.00000, 3.00000, 5.00000
C2	0.20000, 0.30030, 1.00000, 1.00000	1.00000, 1.00000, 1.00000, 1.00000

Table 5. Final Weights through the Hierarchy.

Criteria of Level 1	**Local Weights of Level 1**	**Criteria of Level 2**	**Local Weights of Level 2**	**Global Weights of Level 2**	**Defuzzified Weights**	**Normalized Weights**	**Ranks**
C1	0.050080, 0.130010, 0.240000, 0.450010	C11	0.140010, 0.290010, 0.370010, 0.680070	0.005114, 0.006131, 0.019171, 0.125300	0.1921120	0.079191	8
		C12	0.050080, 0.130010, 0.240000, 0.450010	0.001150, 0.021119, 0.122264, 0.880081	0.1654270	0.068191	9
		C13	0.090020, 0.180000, 0.330040, 0.690090	0.000211, 0.001560, 0.022595, 0.235612	0.2157120	0.088919	3
		C14	0.040070, 0.130070, 0.250040, 0.350050	0.001412, 0.007788, 0.045673, 0.225336	0.1397560	0.057609	12
		C15	0.030010, 0.060040, 0.120090, 0.270000	0.005950, 0.025419, 0.125864, 0.887381	0.1956340	0.080643	6
		C16	0.030050, 0.080080, 0.180030, 0.340020	0.005212, 0.002688, 0.042773, 0.222336	0.2924730	0.120561	2
		C17	0.300100, 0.400100, 0.902000, 1.612000	0.004720, 0.014628, 0.044873, 0.322227	0.1624520	0.066965	10
C2	0.141200, 0.245000, 0.640000, 0.693000	C21	0.200040, 0.290010, 0.530050, 1.123000	0.002650, 0.024719, 0.124364, 0.885581	0.1994790	0.082228	5
		C22	0.120010, 0.230070, 0.500000, 1.120000	0.005604, 0.007531, 0.013581, 0.118973	0.1934550	0.079745	7
		C23	0.070090, 0.190080, 0.240050, 0.740040	0.015409, 0.048871, 0.157456, 0.165693	0.2955260	0.121820	1
		C24	0.030090, 0.090090, 0.180300, 0.450010	0.005920, 0.015228, 0.045373, 0.325727	0.1622270	0.066872	11
		C25	0.040090, 0.140050, 0.190040, 0.480010	0.005568, 0.035645, 0.125432, 0.335524	0.2116750	0.087255	4

Level 2 of the hierarchy displays a variety of qualities that influence its higher-level features, but their impacts on each aspect are distinct. The authors categorized the characteristics for effective results in this type of situation. The results are shown in Table 6 in a combinative way. With the use of Equations (18) and (19), Tables 7 and 8 depict the normalized and weighted normalized values of alternatives in terms of durability characteristics (24). Finally, as shown in Table 9, satisfaction levels of various choices are evaluated using Equations (25) and (26).

Table 6. Subjective Cognition Outcomes.

Criteria/ Alternatives	A1	A2	A3	A4	A5	A6
C11	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	1.4500, 3.0700, 4.9100, 5.6500	0.9100, 2.4500, 4.4500, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	1.9100, 3.7300, 5.7300, 7.5100
C12	1.4500, 3.0700, 4.9100, 5.6500	0.9100, 2.4500, 4.4500, 5.6500	0.9100, 2.4500, 4.4500, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	0.8200, 2.2700, 4.2700, 6.6500
C13	0.9100, 2.4500, 4.4500, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	1.4500, 3.0700, 4.9100, 5.6500
C14	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	0.9100, 2.4500, 4.4500, 5.6500	1.4500, 3.0700, 4.9100, 5.6500	0.9100, 2.4500, 4.4500, 5.6500	0.9100, 2.4500, 4.4500, 5.6500
C15	1.4500, 3.0700, 4.9100, 5.6500	0.9100, 2.4500, 4.4500, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	0.9100, 2.4500, 4.4500, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	1.9100, 3.7300, 5.7300, 7.5100
C16	0.9100, 2.4500, 4.4500, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	0.8200, 2.2700, 4.2700, 6.6500
C17	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	1.4500, 3.0700, 4.9100, 5.6500	0.9100, 2.4500, 4.4500, 5.6500
C21	1.4500, 3.0700, 4.9100, 5.6500	0.9100, 2.4500, 4.4500, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	1.4500, 3.0700, 4.9100, 5.6500	0.9100, 2.4500, 4.4500, 5.6500
C22	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	1.4500, 3.0700, 4.9100, 5.6500	0.9100, 2.4500, 4.4500, 5.6500
C23	1.4500, 3.0700, 4.9100, 5.6500	0.9100, 2.4500, 4.4500, 5.6500	1.4500, 3.0700, 4.9100, 5.6500	0.9100, 2.4500, 4.4500, 5.6500	0.9100, 2.4500, 4.4500, 5.6500	2.8200, 4.6400, 6.6400, 8.5100
C24	0.9100, 2.4500, 4.4500, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	0.9100, 2.4500, 4.4500, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	1.9100, 3.7300, 5.7300, 7.5100	2.8200, 4.6400, 6.6400, 8.5100
C25	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	2.8200, 4.6400, 6.6400, 8.5100	1.4500, 3.0700, 4.9100, 5.6500	0.8200, 2.2700, 4.2700, 6.6500	2.8200, 4.6400, 6.6400, 8.5100

Table 7. The Normalized Fuzzy-Decision Matrix.

Criteria/Alternatives	A1	A2	A3	A4	A5	A6
C11	0.3340, 0.5240, 0.6180, 0.7800	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800
C12	0.4520, 0.6680, 0.7610, 0.8980	0.5740, 0.7250, 0.7920, 0.8960	0.2750, 0.4560, 0.5330, 0.7330	0.2750, 0.4560, 0.5330, 0.7330	0.6110, 0.7720, 0.8560, 0.9450	0.4520, 0.6680, 0.7610, 0.8980
C13	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.2750, 0.4560, 0.5330, 0.7330
C14	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.4520, 0.6680, 0.7610, 0.8980
C15	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.2750, 0.4560, 0.5330, 0.7330	0.3340, 0.5240, 0.6180, 0.7800	0.2750, 0.4560, 0.5330, 0.7330	0.4520, 0.6680, 0.7610, 0.8980
C16	0.03980, 0.10000, 0.19200, 0.3840	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840
C17	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.03980, 0.10000, 0.19200, 0.3840
C21	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800
C22	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.2750, 0.4560, 0.5330, 0.7330	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840
C23	0.03980, 0.10000, 0.19200, 0.3840	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.2750, 0.4560, 0.5330, 0.7330	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840
C24	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800
C25	0.03980, 0.10000, 0.19200, 0.3840	0.3340, 0.5240, 0.6180, 0.7800	0.03980, 0.10000, 0.19200, 0.3840	0.5740, 0.7250, 0.7920, 0.8960	0.2750, 0.4560, 0.5330, 0.7330	0.2750, 0.4560, 0.5330, 0.7330

Table 8. The Weighted Normalized Fuzzy-Decision Matrix.

Criteria/ Alternatives	A1	A2	A3	A4	A5	A6
C11	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0190, 0.0325, 0.0380, 0.0510	0.0555, 0.0870, 0.1040, 0.1220	0.0320, 0.0470, 0.0530, 0.0630	0.1420, 0.1790, 0.1980, 0.2190
C12	0.0555, 0.0870, 0.1040, 0.1220	0.0555, 0.0870, 0.1040, 0.1220	0.0320, 0.0470, 0.0530, 0.0630	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0190, 0.0325, 0.0380, 0.0510
C13	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0555, 0.0870, 0.1040, 0.1220	0.0555, 0.0870, 0.1040, 0.1220	0.0320, 0.0470, 0.0530, 0.0630
C14	0.0555, 0.0870, 0.1040, 0.1220	0.0555, 0.0870, 0.1040, 0.1220	0.0320, 0.0530, 0.0720, 0.0980	0.1420, 0.1790, 0.1980, 0.2190	0.1420, 0.1790, 0.1980, 0.2190	0.0190, 0.0325, 0.0380, 0.0510
C15	0.1420, 0.1790, 0.1980, 0.2190	0.1420, 0.1790, 0.1980, 0.2190	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0470, 0.0530, 0.0630
C16	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0555, 0.0870, 0.1040, 0.1220	0.0555, 0.0870, 0.1040, 0.1220	0.0320, 0.0530, 0.0720, 0.0980	0.0190, 0.0325, 0.0380, 0.0510
C17	0.0555, 0.0870, 0.1040, 0.1220	0.0555, 0.0870, 0.1040, 0.1220	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0470, 0.0530, 0.0630
C21	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0555, 0.0870, 0.1040, 0.1220	0.0555, 0.0870, 0.1040, 0.1220	0.0320, 0.0530, 0.0720, 0.0980	0.0190, 0.0325, 0.0380, 0.0510
C22	0.0555, 0.0870, 0.1040, 0.1220	0.0555, 0.0870, 0.1040, 0.1220	0.1420, 0.1790, 0.1980, 0.2190	0.1420, 0.1790, 0.1980, 0.2190	0.0555, 0.0870, 0.1040, 0.1220	0.0320, 0.0470, 0.0530, 0.0630
C23	0.1420, 0.1790, 0.1980, 0.2190	0.1420, 0.1790, 0.1980, 0.2190	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0190, 0.0325, 0.0380, 0.0510
C24	0.0555, 0.0870, 0.1040, 0.1220	0.0320, 0.0530, 0.0720, 0.0980	0.0555, 0.0870, 0.1040, 0.1220	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0530, 0.0720, 0.0980
C25	0.0320, 0.0530, 0.0720, 0.0980	0.0555, 0.0870, 0.1040, 0.1220	0.0320, 0.0530, 0.0720, 0.0980	0.0555, 0.0870, 0.1040, 0.1220	0.0555, 0.0870, 0.1040, 0.1220	0.0320, 0.0530, 0.0720, 0.0980

Table 9. Closeness Coefficients of Various Alternatives.

Alternatives	d+i	d-i	Gap Degree of CC+i	Satisfaction Degree of CC-i
A1	0.043125254	0.025569685	0.378856965	0.644585699
A2	0.034566598	0.049656387	0.644856974	0.336636544
A3	0.044555269	0.036552654	0.387785859	0.635659756
A4	0.033363657	0.040225254	0.563635544	0.466967721
A5	0.040152547	0.045666398	0.533636598	0.446325454
A6	0.039665874	0.024555696	0.388854745	0.623655987

In the table above, (CC-i) is evaluated. The effectiveness of alternatives is represented in the table above by quantitative values. As can be seen from the alternative assessment outcomes, the influence of security attributes prioritization is a respectable standard. The authors firmly feel and advise that the numeric calculation and result are acceptable and are in good working order. Furthermore, the prioritized table and ranking for industrial control system longevity are also helpful. The data in the table demonstrate that the second option has the greatest impact of all the other options.

The authors of the proposed study identified six options for estimating the security of industrial control systems. As a result, the authors employed the same six options for the sensitivity analysis as well. Table 10 depicts a well-established robustness assessment. Alternative 1 is the utmost active element for industrial control system security, according to the results of the robustness analysis. The principal row of the table signifies real-world computed findings in the context of robustness evaluation. By using robustness analysis criteria on weights for attributes, we discovered that all elements had a similar higher influence as in the genuine evaluation. The findings also show that quantitative outcomes are affected by weighted characteristics.

Table 10. Sensitivity Analysis.

Tryouts		A1	A2	A3	A4	A5	A6
Tryout-0	Satisfaction Degree (CC-i)	0.6445857	0.3366365	0.63565976	0.4669677	0.4463255	0.6236560
Tryout-1		0.6444452	0.3367587	0.63555669	0.4669697	0.4464576	0.6234576
Tryout-2		0.6445587	0.3377874	0.63885687	0.4669696	0.4463364	0.6239464
Tryout-3		0.6445523	0.3385691	0.63464579	0.4669789	0.4466658	0.6231346
Tryout-4		0.6444472	0.3314474	0.63546546	0.4666355	0.4466679	0.6236379
Tryout-5		0.6444526	0.3378898	0.63545794	0.4667458	0.4499776	0.6233469
Tryout-6		0.6444587	0.3377458	0.63445131	0.4666325	0.4415644	0.6237798
Tryout-7		0.6446589	0.3477758	0.63454697	0.4696345	0.4465467	0.6236577
Tryout-8		0.6458577	0.3563685	0.63445164	0.4662567	0.4444576	0.6236397
Tryout-9		0.6455869	0.3445784	0.63457846	0.4669646	0.4445677	0.6236599
Tryout-10		0.6455869	0.3365558	0.63454697	0.4661245	0.4464576	0.6238875
Tryout-11		0.6477587	0.3367895	0.63445796	0.4667435	0.4445465	0.6236397
Tryout-12		0.6456988	0.3355874	0.63445794	0.4664456	0.4463257	0.6236688

The author of the planned study chose six options to test. Comparing the outcomes of several approaches allows for a better understanding of the differences in numerical assessment in various ways. To assess the usefulness of the projected technique, the authors matched it to the other four MCDM techniques: fuzzy AHP-TOPSIS, classical AHP-TOPSIS, fuzzy ANP-TOPSIS, and classical ANP-TOPSIS [50–53]. Although hybrid procedures, such as fuzzy AHP-TOPSIS and fuzzy ANP TOPSIS produce noble outcomes, hesitant fuzzy AHP TOPSIS proves to be the most precise in the present example. The outcomes of the comparison were not as varied and dissimilar as they may have been, but the accuracy of the results varies.

When assigning values to attributes, the hesitant fuzzy AHP-TOPSIS technique offers the benefit of allocating hesitant fuzzy set evaluation. Web application durability estimation shows the calculated results in Table 11 and Figure 7. As a result, the authors employed the same six options for the sensitivity analysis as well. Table 10 depicts a well-established robustness assessment. Alternative 1 is the utmost effective factor for the industrial control system, according to the results of the robustness analysis. The principal row of the table signifies real-world computed findings in the context of robustness evaluation. By using robustness analysis criteria on weights for attributes, we discovered that all elements had the same higher influence as in the genuine evaluation. The findings also show that quantitative outcomes are affected by weighted characteristics.

Table 11. Comparative Analysis.

Procedures/Alternatives	A1	A2	A3	A4	A5	A6
Hesitant-Fuzzy-AHP-TOPSIS	0.6445857	0.3366365	0.63565976	0.4669677	0.4463255	0.6236560
Fuzzy-AHP-TOPSIS	0.6444526	0.3378898	0.63545794	0.4667458	0.4499776	0.6233469
Fuzzy-Delphi-AHP-TOPSIS	0.6446589	0.3477758	0.63454697	0.4696345	0.4465467	0.6236577
Classical-AHP-TOPSIS	0.6458577	0.3563685	0.63445164	0.4662567	0.4444576	0.6236397
Delphi-AHP-TOPSIS	0.6445587	0.3377874	0.63885687	0.4669696	0.4463364	0.6239464

Because of the added facility of the hesitant fuzzy set concept in the approach, findings measured by the hesitant fuzzy AHP TOPSIS procedure are more precise than the other four procedures, as shown in Table 11 and Figure 7. As a result, the method employed in this research work has more potential and produces better outcomes.

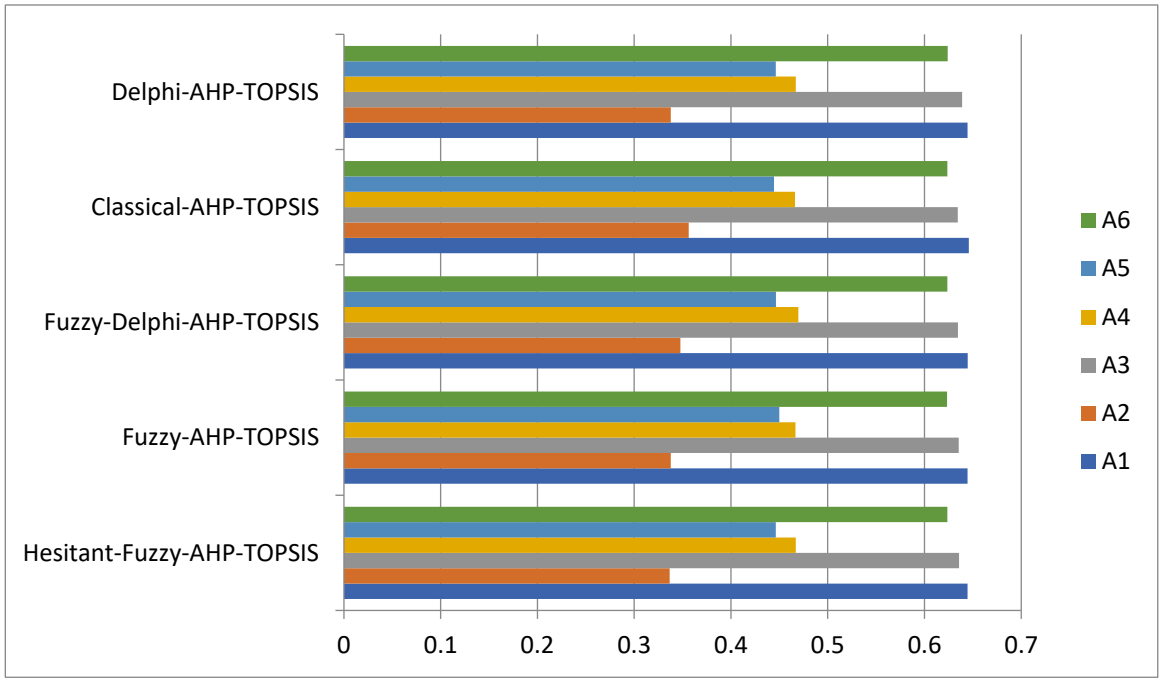

Figure 7. Graphical representation of comparative analysis.

7. Conclusions

We feel that it is critical to developing a hybrid dataset using several main datasets that are accessible online, as well as datasets gathered through the testbed simulation setup or at power industry campuses, as future work. To verify the accuracy of machine learning approaches from the perspective of industrial control systems, we plan to extend our early work from the viewpoint of industrial control systems with hybrid datasets, including the one described in [28–35]. Intrusion detection, on the other hand, has not been substantially researched in the collected works. As a result, it can be employed as an impeccable benchmark for future work to verify and validate the built ML algorithms. The simplified framework of the TE process, which is mentioned, can be employed to analyze the consequences of attacks in the procedure control domain. We feel that an industrial control systems simulation testbed can be employed for the following purposes:

- To serve as a prototype for a shared technical platform for the establishment of future industrial control systems cybersecurity test centers.
- To give businesses a cost-effective test platform that lowers simulation and testing costs while delivering more noteworthy outcomes than a standard testbed.
- To perform cyber-attacks against a hybrid framework of real-world monitoring and control systems in the energy sector.
- To create an easy-to-use testbed that is more realistic than simulations and less expensive.
- To prepare hybrid datasets for machine learning frameworks to train on in order to develop robust intrusion detection systems for industrial control systems.

Previous cyber security incidents demonstrate the significance of conducting security assessments on industrial control systems, especially to detect and close system weaknesses. Not only this, but a threat assessment is included in the cyber security assessment. Because most energy firms place a premium on system availability, cyber security evaluations should not affect the day-to-day operations of industrial control systems. The problems of conducting cyber security assessments in control systems are discussed in this paper, as well as the impact they have had on industrial control systems in general. We believe that a cyber-security assessment can be carried out by setting up a virtual lab that mimics the real-world environment of industrial control systems. Energy firms that own or administer

industrial control systems should be able to take the necessary steps to ensure that their systems are secure and dependable, based on the challenges stated in this article. Because of the complexity of new malware targeting control systems, such as zero-day rootkits and attacks, attacks at the component level of control systems are exceedingly difficult to avoid and detect. As a result, at the procedure control level, new intrusion detection algorithms for industrial control systems are necessary. In this case, machine learning technologies have proven to be quite beneficial. The key consequences of the proposed work are as follows.

- By focusing on industrial control system cyber security factors, security approaches will be improved, analyzed, identified, and prioritized.
- To analyze the security evaluation of industrial control systems, MCDM methodologies, such as the hesitant fuzzy sets-based AHP-TOPSIS procedure are employed.
- Hesitant fuzzy sets based on the AHP method and hesitant fuzzy sets based on the TOPSIS procedure are well-known and widely employed for resolving multi-criteria decision-making issues, and they produce accurate and effective answers.

This research work could serve as a model for similar future research activities and policy initiatives aimed at securing the energy industries. The target for the future is to implement similar research activities with other powerful MCDM methodology on internet-based channels. The real-world dataset will be assessed, and final findings will be obtained easily by involving broad-level energy industries.

Funding: Deanship of Scientific Research at Shaqra University, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The author would like to thank Shaqra University, Saudi Arabia to support him in this work.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Stouffer, K.A.; Pillitteri, V.Y.; Lightman, S.; Abrams, M.; Hahn, A. *Guide to Industrial Control Systems (ICS) Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2015.
2. Alosaimi, W.; Ansari, T.J.; Alharbi, A.; Alyami, H.; Ali, S.; Agrawal, A.; Khan, R.A. Toward a Unified Model Approach for Evaluating Different Electric Vehicles. *Energies* **2021**, *14*, 6120. [CrossRef]
3. Bonandir, N.A.; Jamil, N.; Nawawi, N.A.; Jidin, R.; Rusli, M.E.; Yan, L.K.; Maudau, L.L.A.D. A Review of Cyber Security Assessment (CSA) for Industrial Control Systems (ICS) and Their Impact on The Availability of the ICS Operation. *J. Phys. Conf. Ser.* **2021**, *1860*, 012015. [CrossRef]
4. Toshiba Energy Systems & Solutions Corporation. Power System Monitoring and Control Systems that Contribute to Improving the Supply-Demand Adjustment Performance. Product/Technical Services: Transmission & Distribution. Available online: https://www.toshiba-energy.com/en/transmission/product/power-stabilization.htm (accessed on 9 November 2021).
5. Bhamare, D.; Zolanvari, M.; Erbad, A.; Jain, R.; Khan, K.; Meskin, N. Cybersecurity for industrial control systems: A survey. *Comput. Secur.* **2020**, *89*, 101677. [CrossRef]
6. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* **2016**, *56*, 1–27. [CrossRef]
7. Knowles, W.; Prince, D.; Hutchison, D.; Disso, J.F.P.; Jones, K. A survey of cyber security management in industrial control systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *9*, 52–80. [CrossRef]
8. Sajid, A.; Abbas, H.; Saleem, K. Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. *IEEE Access* **2016**, *4*, 1375–1384. [CrossRef]
9. Ding, D.; Han, Q.L.; Wang, Z.; Ge, X. A Survey on Framework based Distributed Control and Filtering for Industrial Cyber Physical Systems. *IEEE Trans. Ind.* **2019**, *15*, 2483–2499. [CrossRef]
10. Molina, E.; Jacob, E. Software-defined networking in cyber-physical systems: A survey. *Comput. Electr. Eng.* **2018**, *66*, 407–419. [CrossRef]
11. Zeng, P.; Zhou, P. *Intrusion Detection in SCADA System: A Survey*; Springer: Singapore, 2018; pp. 342–351.

12. Krotofil, M.; Cárdenas, A.A. Resilience of Process Control Systems to Cyber-Physical Attacks. In Proceedings of the Nordic Conference on Secure IT Systems, Ilulissat, Greenland, 18–21 October 2013; pp. 166–182.
13. Stefanidis, K.; Voyiatzis, A.G. An HMM-Based Anomaly Detection Approach for SCADA Systems. In Proceedings of the IFIP International Conference on Information Security Theory and Practice, Crete, Greece, 26–27 September 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 85–99.
14. Byres, E.; Lowe, J. The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems. In Proceedings of the VDE Kongress, Berlin, Germany, 8–20 October 2004; Volume 116, pp. 213–218.
15. Alfakeeh, A.S.; Almalawi, A.; Alsolami, F.J.; Abushark, Y.B.; Khan, A.I.; Bahaddad, A.A.S.; Agrawal, A.; Kumar, R.; Khan, R.A. Hesitant Fuzzy-Sets Based Decision-Making Model for Security Risk Assessment. *CMC-Comput. Mater. Contin.* **2022**, *70*, 2297–2317. [CrossRef]
16. Pollet, J. Developing a solid SCADA security strategy. In Proceedings of the 2nd ISA/IEEE Sensors for Industry Conference, Houston, TX, USA, 19–21 November 2002; pp. 148–156.
17. Igure, V.M.; Laughter, S.A.; Williams, R.D. Security issues in SCADA networks. *Comput. Secur.* **2006**, *25*, 498–506. [CrossRef]
18. Nicholson, A.; Webber, S.; Dyer, S.; Patel, T.; Janicke, H. SCADA security in the light of Cyber-Warfare. *Comput. Secur.* **2012**, *31*, 418–436. [CrossRef]
19. Wang, C.; Fang, L.; Dai, Y. A Simulation Environment for SCADA Security Analysis and Assessment. In Proceedings of the 2010 International Conference on Measuring Technology and Mechatronics Automation, Changsha, China, 13–14 March 2010; Volume 1, pp. 342–347.
20. Ansari, T.J.; Pandey, D.; Alenezi, M. STORE: Security Threat Oriented Requirements Engineering Methodology. *J. King Saud Univ.-Comput. Inf. Sci.* **2018**. in press.
21. Queiroz, C.; Mahmood, A.; Hu, J.; Tari, Z.; Yu, X. Building a SCADA Security Testbed. In Proceedings of the 2009 Third International Conference on Network and System Security, Gold Coast, QLD, Australia, 19–21 October 2009; pp. 357–364.
22. Ansari, T.J.; Pandey, D. An Integration of Threat Modeling with Attack Pattern and Misuse Case for Effective Security Requirement Elicitation. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 16–20.
23. Shahzad, A.; Musa, S.; Aborujilah, A.; Irfan, M. Industrial control systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption. In Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication—ICUIMC '14, Siem Reap, Cambodia, 9–11 January 2014; ACM Press: New York, NY, USA, 2014; pp. 1–6.
24. Qin, Y.; Cao, X.; Liang, P.; Hu, Q.; Zhang, W. Research on the Analytic Factor Neuron Framework Based on Cloud Generator and Its Application in Oil & Gas SCADA Security Defense. In Proceedings of the 2014 IEEE 3rd International Conference on Cloud Computing and Intelligence Systems, Shenzhen, China, 27–29 November 2014; pp. 155–159.
25. Zhang, W.W.; Cao, X.D.; Hu, Q.C.; Liang, P.; Qin, Y. Research on FPN-Based Security Defense Framework of Oil and Gas SCADA Network. In Proceedings of the Computational Intelligence in Industrial Application: The 2014 Pacific-Asia Workshop on Computer Science in Industrial Application (CIIA 2014), Singapore, 8–9 December 2014; CRC Press: Boca Raton, FL, USA, 2015; p. 31.
26. Colombo, A.W.; Bangemann, T.; Karnouskos, S.; Delsing, J.; Stluka, P.; Harrison, R.; Lastra, J.L. Industrial Cloud-Based Cy-ber-Physical Systems. *IMC-AESOP Approach* **2014**, *22*, 4–5.
27. Stouffer, K.; Falco, J.; Scarfone, K. *Guide to Industrial Control Systems (ICS) Security—Rev. 2*; NIST Special Publication: Gaithersburg, MD, USA, 2014.
28. Morris, T.; Thornton, Z.; Turnipseed, I. Industrial Control System Simulation and Data Logging for Intrusion Detection System Research. In Proceedings of the 7th Annual Southeastern Cyber Security Summit, Huntsville, AL, USA, 3–4 June 2015.
29. Simmhan, Y.; Aman, S.; Kumbhare, A.; Liu, R.; Stevens, S.; Zhou, Q.; Prasanna, V. Cloud-Based Software Platform for Big Data Analytics in Smart Grids. *Comput. Sci. Eng.* **2013**, *15*, 38–47. [CrossRef]
30. Khan, A.I.; ALGhamdi, A.S.A.M.; Alsolami, F.J.; Abushark, Y.B.; Almalawi, A.; Ali, A.M.; Agrawal, A.; Kumar, R.; Khan, R.A. Integrating Blockchain Technology into Healthcare Through an Intelligent Computing Technique. *CMC-Comput. Mater. Contin.* **2022**, *70*, 2835–2860. [CrossRef]
31. Abushark, Y.B.; Khan, A.I.; Alsolami, F.J.; Almalawi, A.; Alam, M.; Agrawal, A.; Kumar, R.; Khan, R.A. Usability Evaluation Through Fuzzy AHP-TOPSIS Approach: Security Requirement Perspective. *Comput. Mater. Contin.* **2021**, *68*, 1203–1218. [CrossRef]
32. Coffey, K.; Smith, R.; Maglaras, L.; Janicke, H. Vulnerability Analysis of Network Scanning on SCADA systems. *Secur. Commun. Netw.* **2018**, *2018*, 3794603. [CrossRef]
33. Samtani, S.; Yu, S.; Zhu, H.; Patton, M.; Matherly, J.; Chen, H. Identifying SCADA Systems and Their Vulnerabilities on the Internet of Things: A Text-Mining Approach. *IEEE Intell. Syst.* **2018**, *33*, 63–73. [CrossRef]
34. Alosaimi, W.; Alharbi, A.; Alyami, H.; Ahmad, M.; Pandey, A.K.; Kumar, R.; Khan, R.A. Impact of Tools and Techniques for Securing Consultancy Services. *Comput. Syst. Sci. Eng.* **2021**, *37*, 347–360. [CrossRef]
35. Roy, B.; Misra, S.K. An Integrated Fuzzy ANP and TOPSIS Methodology for Software Selection under MCDM Perspective. *Int. J. Innov. Res. Comput. Commun. Eng.* **2018**, *6*, 492–501.
36. Tavana, M.; Zandi, F.; Katehakis, M.N. A hybrid fuzzy group ANP–TOPSIS framework for assessment of e-government readiness from a CiRM perspective. *Inf. Manag.* **2013**, *50*, 383–397. [CrossRef]

37. Li, B.Z.; Bi, R. The Application of Fuzzy-ANP in Evaluation Index System of Computer Security. *Key Eng. Mater.* **2010**, *439–440*, 754–759. [CrossRef]
38. Kumar, R.; Khan, A.I.; Abushark, Y.B.; Alam, M.; Agrawal, A.; Khan, R.A. An Integrated Approach of Fuzzy Logic, AHP and TOPSIS for Estimating Usable-Security of Web Applications. *IEEE Access* **2020**, *8*, 50944–50957. [CrossRef]
39. Attaallah, A.; Ahmad, M.; Ansari, T.J.; Pandey, A.K.; Kumar, R.; Khan, R.A. Device Security Assessment of Internet of Healthcare Things. *Intell. Autom. Soft Comput.* **2020**, *27*, 593–603. [CrossRef]
40. Alosaimi, W.; Ansari, T.J.; Alharbi, A.; Alyami, H.; Seh, A.; Pandey, A.; Agrawal, A.; Khan, R. Evaluating the Impact of Different Symmetrical Models of Ambient Assisted Living Systems. *Symmetry* **2021**, *13*, 450. [CrossRef]
41. Kumar, R.; Ansari, M.T.J.; Baz, A.; Alhakami, H.; Agrawal, A.; Khan, R.A. A multi-perspective benchmarking framework for esti-mating usable-security of hospital management system software based on fuzzy logic, ANP and TOPSIS methods. *KSII Trans. Internet Inf. Syst.* **2021**, *15*, 240–263.
42. Chong, C.Y.; Lee, S.P.; Ling, T.C. Prioritizing and fulfilling quality attributes for virtual lab development through application of fuzzy analytic hierarchy process and software development guidelines. *Malays. J. Comput. Sci.* **2014**, *27*, 1–19.
43. Onar, S.C.; Oztaysi, B.; Kahraman, C. Strategic Decision Selection Using Hesitant fuzzy TOPSIS and Interval Type-2 Fuzzy AHP: A case study. *Int. J. Comput. Intell. Syst.* **2014**, *7*, 1002–1021. [CrossRef]
44. Wang, C.N.; Thanh, N.V.; Su, C.C. The Study of a Multicriteria Decision Making Model for Wave Power Plant Location Se-lection in Vietnam. *Processes* **2019**, *7*, 650. [CrossRef]
45. Kahraman, C. (Ed.) *Fuzzy Multi-Criteria Decision Making: Theory and Applications with Recent Developments*; Springer Science & Business Media: Berlin, Germany, 2008; Volume 16.
46. Ansari, T.J.; Baz, A.; Alhakami, H.; Alhakami, W.; Kumar, R.; Khan, R.A. P-STORE: Extension of STORE Methodology to Elicit Privacy Requirements. *Arab. J. Sci. Eng.* **2021**, *46*, 8287–8310. [CrossRef]
47. Ansari, M.T.J.; Khan, N.A. Worldwide COVID-19 Vaccines Sentiment Analysis through Twitter Content. *Electron. J. Gen. Med.* **2021**, *18*, 10. [CrossRef]
48. Kumar, R.; Alenezi, M.; Ansari, M.T.J.; Gupta, B.K.; Agrawal, A.; Khan, R.A. Evaluating the Impact of Malware Analysis Techniques for Securing Web Applications through a Decision-Making Framework under Fuzzy Environment. *Int. J. Intell. Eng. Syst.* **2020**, *13*, 94–109. [CrossRef]
49. Torra, V.; Narukawa, Y. On hesitant fuzzy sets and decision. In Proceedings of the 2009 IEEE International Conference on Fuzzy Systems, Jeju, Korea, 20–24 August 2009; pp. 1378–1382.
50. Zarour, M.; Alenezi, M.; Ansari, T.J.; Pandey, A.K.; Ahmad, M.; Agrawal, A.; Kumar, R.; Khan, R.A. Ensuring data integrity of healthcare information in the era of digital health. *Health Technol. Lett.* **2021**, *8*, 66–77. [CrossRef] [PubMed]
51. AlHakami, W.; Binmahfoudh, A.; Baz, A.; AlHakami, H.; Ansari, T.J.; Khan, R.A. Atrocious Impinging of COVID-19 Pandemic on Software Development Industries. *Comput. Syst. Sci. Eng.* **2021**, *36*, 323–338. [CrossRef]
52. Alyami, H.; Nadeem, M.; Alharbi, A.; Alosaimi, W.; Ansari, T.J.; Pandey, D.; Kumar, R.; Khan, R.A. The Evaluation of Software Security through Quantum Computing Techniques: A Durability Perspective. *Appl. Sci.* **2021**, *11*, 11784. [CrossRef]
53. Kumar, R.; Baz, A.; Alhakami, H.; Alhakami, W.; Agrawal, A.; Khan, R.A. A hybrid fuzzy rule-based multi-criteria framework for sustainable-security assessment of web application. *Ain Shams Eng. J.* **2021**, *12*, 2227–2240. [CrossRef]