Methods

Sine Canbolat*, Ghada Elbez and Veit Hagenmeyer

A new hybrid risk assessment process for cyber security design of smart grids using fuzzy analytic hierarchy processes

Ein neues hybrides Risikobewertungsverfahren für die Gestaltung der Cybersicherheit von intelligenten Stromnetzen unter Verwendung Fuzzy-analytischer Hierarchieprozesse

https://doi.org/10.1515/auto-2023-0089
Received May 12, 2023; accepted August 9, 2023

Abstract: IT vulnerabilities, cyber threats, and resulting risks significantly impact the stability of current and future power grids. The results of a Risk Assessment process contribute to a better understanding of the causes and nature of the associated risks. The risks assessed by experts are available in both numerical and linguistic representations – this makes it beneficial to include a combination of linguistic and numerical analyses. In this paper, we propose a new Hybrid Risk Assessment method based on fuzzy logic, leading to more precise results. The presented approach specifies the variables and membership functions of fuzzy logic with reference to Smart Grids. For this propose, a case study with five risk events in a small-scale Smart Grid is carried out as an example. The results can then support decision-makers in ensuring grid stability.

Keywords: risk assessment process; energy systems; risk analysis; fuzzy logic

Zusammenfassung: IT-Schwachstellen, Cyber-Bedrohungen und die damit entstehenden Risiken haben erhebliche Auswirkungen auf die Stabilität aktueller und zukünftiger Stromnetze. Die Ergebnisse eines Risikobewertungsprozesses tragen zu einem besseren Verständnis der Ursachen und der Art der assozierten Risiken bei. Die von Experten bewerteten Risiken liegen sowohl in numerischer als auch in sprachlichen Darstellungen vor – dies macht ihre Kombination für die jeweilige komplexe Risikobewertung wünschenswert. Daher wird im vorliegenden Beitrag eine neue hybride Methode zur Risikobewertung vorgestellt, die auf Basis von Fuzzy-Logik zu präziseren Risikobewertungen führt. Der vorgestellte Ansatz spezifiziert die Variablen und Mitgliedschaftsfunktionen der Fuzzy-Logik mit Bezug auf das Smart Grid. Dafür wird beispielhaft eine Fallstudie mit fünf Risikofällen in einem Smart Grid durchgeführt. Die Ergebnisse können dann Entscheidungsträger bei der Sicherstellung der Netzstabilität unterstützen.

Schlagwörter: Risikobewertungsverfahren; Energiesysteme; Risikoanalyse; Fuzzy-Logik

List of abbreviations

AHP	Analytic Hierarchy Process.
CVE	Common Vulnerabilities and Exposures.
CVSS	Common Vulnerability Scoring System.
DoS	Denial-of-Service.
FAHP	Fuzzy Analytic Hierarchy Process.
HRA	Hybrid Risk Assessment.
IED	Intelligent Electronic Device.
IT	Information Technology.
MCDM	Multiple Criteria Decision-Making.
MF	Membership Function.
OT	Operational Technology.
PLC	Programmable Logic Controller.
RA	Risk Assessment.
RE	Risk Event.
RL	Risk Level.
SG	Smart Grid.
SIEM	Security Information and Event Management.
TCP	Transmission Control Protocol.
WF	Weight Factor.

***Corresponding author: Sine Canbolat**, Karlsruhe Institute of Technology (KIT), Institute for Automation and Applied Informatics (IAI), KASTEL Security Research Labs, Hermann-von-Helmholtz-Platz 1, 76344 Eggenstein-Leopoldshafen, Germany, E-mail: sine.canbolat@kit.edu. https://orcid.org/0000-0001-7292-7989
Ghada Elbez and Veit Hagenmeyer, Karlsruhe Institute of Technology (KIT), Institute for Automation and Applied Informatics (IAI), KASTEL Security Research Labs, Hermann-von-Helmholtz-Platz 1, 76344 Eggenstein-Leopoldshafen, Germany, E-mail: ghada.elbez@kit.edu (G. Elbez), veit.hagenmeyer@kit.edu (V. Hagenmeyer)

1 Introduction

Smart Grids (SGs) offer a promising technology to improve the reliability, resilience, quality of service and smart management of the future energy systems. They support generation, transmission, distribution and control of electricity in real-time. For instance, they play a vital role in managing the power balance across different voltage levels and providing energy effectively to the society. New concerns regarding security threats have emerged with the implementation of SGs. It is of utmost importance to secure SGs by carefully considering potential threats, vulnerabilities and risks. Enhancing cybersecurity measures to protect against Risk Events (REs) is crucial, especially given the reliance on electricity for the day-to-day operations of various facilities, including homes, businesses, hospitals, schools and more. For example, the interconnected nature of SGs through networks with a large number of access and control points can make them vulnerable to threats leading to cyber-attacks. Hence, a Risk Assessment (RA) process for supporting the overall grid stability and security should be conducted. The RA process contains five steps; context establishment, risk identification, risk analysis, risk evaluation and risk treatment [1]. We include the first four steps of the RA process in this paper, as shown in Figure 1, where the dashed rectangle presents the RA steps and the circle indicates the expected outcomes. The risk treatment step is out of the scope of the present paper.

Carrying out an effective RA process is essential to provide a secure decision-making process in energy systems considering critical infrastructure and operations of Operational Technology (OT) aspects. In addition to data protection and cyber security risks in Information Technology (IT), OT related RAs have a broader scope, covering physical safety risks, operational disruptions and the potential impact on the related infrastructure. In the context of OT, there is a requirement for RA extension consequently. Our main contribution in the presented paper is to show the adaptation of fuzzy logic and Fuzzy Analytic Hierarchy Process (FAHP) in view of cyber security design for SGs. Moreover, the aim of our research is to understand the sources of risk, increase risk awareness, investigate which part of the network is under risk and at which level and assist engineers and/or operators in determining which risk should be considered first. Our Hybrid Risk Assessment (HRA) process enables an accurate representation of the levels and risk scores with respect to the REs.

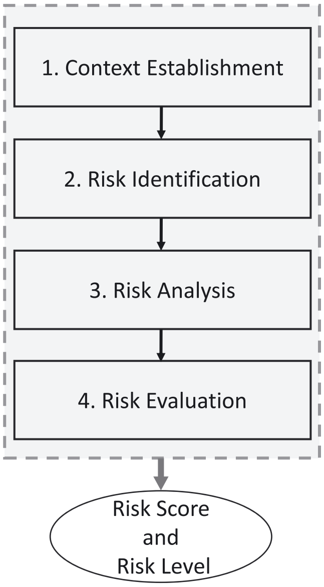

Figure 1: An overview of the risk assessment (RA) process in the presented paper.

The remainder of the paper is organized as follows. First, we begin with a brief statement of RA criticality in Section 2 presenting common approaches. Section 3 entails the main contribution of the present paper considering the HRA for SGs. This includes a representation of the HRA process with the Membership Functions (MFs) and FAHP. Moreover, in Section 4, we present a use case for a small-scale power grid to provide an application of the HRA process. Thereafter, a discussion regarding open research questions and also possible future work are addressed in Section 5. Finally, the conclusion is presented in Section 6.

2 Related work

Context establishment is the first step, which covers the scope, target and focus of the RA [1, 2]. It provides a basis for the definition of critical assets. The following step, risk identification, clarifies threats and vulnerabilities that may initiate unwanted events with respect to the predefined assets. This step entails determining potential events that could lead to harm or damage to assets [1]. Here, a threat is described as an initiator of events that may affect the system under assessment, while vulnerability is defined as a weakness or deficiency that triggers a threat scenario [1, 3]. Given the complex, interconnected nature of SGs and the rapid technological developments in this field, risk identification based on expert knowledge is critical. The third step, risk analysis, is an essential step in the RA process as it supports determining the Risk Level (RL). The final step of the present study, risk evaluation, is necessary to associate the results of the risk analysis with the risk evaluation criteria to consider if any action or treatment is required for the cyber-risks [1].

Risk analysis is one of the features of Security Information and Event Management (SIEM) systems [4] that play a crucial role in SGs, industrial automation and control systems by providing security threat monitoring and management particularly. These systems gather and examine data from different sources, such as network devices, servers and endpoints to detect and react to potential security incidents such as equipment damage, production downtime, or environmental harm. In a recent study [4], the risk analysis feature of the basic configuration of current SIEM solutions are evaluated as either low/basic or average in terms of implementation, but not as high/advanced. High/advanced, average and low/basic mean respectively the features are fully functioning, partially implemented and either poorly implemented or not implemented at all [4]. Given this situation, there is a need for improving risk analysis feature of current SIEM solutions [4, 5].

RA steps can be applied as qualitatively, quantitatively or hybrid to decide the likelihood, consequence and/or prioritization. While qualitative scale uses natural language expressions, quantitative scale is presented in numerical form, absolute scales and ratios. It can be also possible to use qualitative and quantitative RAs together [1]. In a nutshell, HRA supports investigation of which part of the grid is under risk and at which level.

To conduct an RA process, various approaches such as attack tree-based [6, 7], Bayesian attack graph-based [8], CORAS diagrams based [3], game theory [9] based and/or deep neural network-based [10] techniques are proposed in the literature. In an RA process, a risk matrix [1] is typically used to assign an RL based on the combination of the likelihood and impact of potential risks. Fuzzy logic [11] is a promising approach to conduct RA process. It is a mathematical modelling technique that enables the handling of uncertainties and imprecision in data. By allowing for the use of linguistic variables and fuzzy sets, fuzzy logic can capture the imprecision and uncertainty inherent in many RA. These linguistic values such as ‘Low’, ‘Medium’ or ‘High’ are allowed to be communicated more effectively with operators/experts. This can be useful for incorporating expert knowledge into the RA model. Fuzzy logic is a promising approach in SCADA RA process, but their current usage is limited [12]. The idea behind the Analytic Hierarchy Process (AHP) [13] is to deal with Multiple Criteria Decision-Making (MCDM) issues to reduce biases. An extension of fuzzy logic with AHP known as FAHP [14] can overcome uncertainty and subjectivity challenges. Due to the imprecise and uncertain nature of human decision-making, the FAHP is often utilized to tackle problems involving MCDM [15]. It has found effective adaptation in several domains for the RA process [16, 17]. Undoubtedly, when considering all relevant studies in the field, valuable information and useful methodologies have been provided. Nevertheless, there is still need for further development to support objectivity in the selection of parameters, considering more REs, accounting for variability of inputs, extending simplified risk analysis equations, presenting RL and prioritization. SG is still an open domain to demonstrate the applicability of RA process.

3 Proposed hybrid risk assessment process

In the proposed HRA, the consideration of past occurrences of similar events is incorporated as a factor referred to as likelihood. The evaluation of the impact of RE is conducted, considering their implications for power subscribers and the wider society. This factor is referred to as consequence. The scales that are utilized to assess likelihood, consequences and RL in the present study are based on the study [18]. Our solution is more suitable to power grids in terms of inputs (likelihood and consequence) and the evaluation of the MFs. This is due to the fact that RA process may vary depending on the unique characteristics and requirements of each specific domain. Novelty lies in showing the application of fuzzy logic and FAHP in the domain of SGs. In the following part, we explain the flow of fuzzy logic and FAHP applications as a basis for the HRA process. We illustrate our HRA process in Figure 2.

Compared to [16], our approach is based on fuzzy logic and FAHP is adapted for SGs in terms of specific fuzzy logic’s

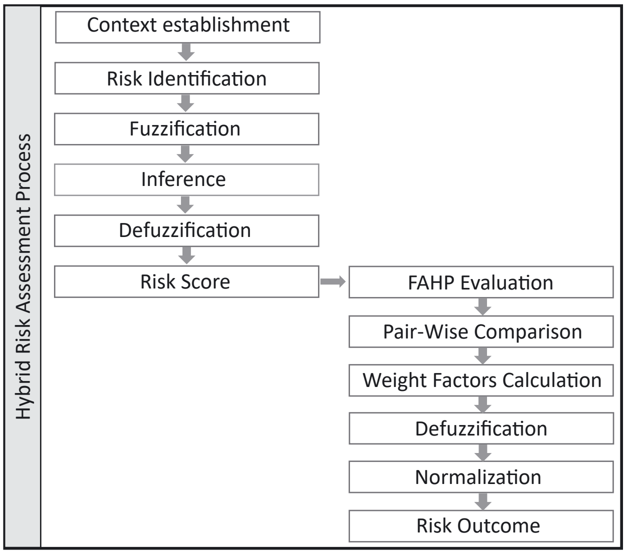

Figure 2: Flowchart of the hybrid risk assessment (HRA) process.

variables and MFs. In the grid related RA process, one of the challenges is to evaluate the precise values of risks. Due to the specific interconnected and complex nature of SGs, data used to calculate risk scores and levels can be uncertain, incomplete and subject to change over time. Fuzzy logic and FAHP are methods that can be used to overcome this difficulty. Fuzzy logic allows for the modeling of imprecise or uncertain information by using fuzzy sets to represent concepts or variables that have a degree of membership in a set, rather than being a fixed true or false value. Additionally, FAHP is a method that allows for the prioritization and the rank of risk factors based on their degree of importance. It involves the use of pairwise comparison matrices and a weighting system to determine the relative importance of different risk factors and the overall risk score. HRA starts with the context establishment step. It can be defined as substations in the transmission and the distribution domains. After evaluating the first outcomes within the present paper, the context can be extended in the future. For the risk identification, experts' opinion [18–20], MITRE ATT&CK [21] and NIST National Vulnerabilty database [22] be taken into account. These provide supportive definitions for our domain specific risks. After identifying risks, fuzzy logic provides the calculated risk scores and levels according to likelihood and consequences. Lastly based on these risk scores from fuzzy logic's outcome and pairwise comparison from FAHP, the overall risk score and RL at the grid are obtained for usage of decision-makers. While RL is the linguistic representation, risk score is the numerical representation of the risk involved. Fuzzy membership values are placed in the interval [0,1]. The MFs can be directly related to the linguistic terms used to describe the RL, such as 'High', 'Medium High', 'Medium Low' and 'Low'. While Gaussian MFs are used likelihood and consequence representations, the triangular and trapezoidal MFs are used for the RL representation to conduct fuzzy logic. To apply FAHP, a triangular fuzzy MF, $\widetilde{A} = (a,b,c)$, is used in the presented research. The identified risks will be the inputs to build the qualitative rules that are associated with the MFs. The mathematical formulation of a triangular MF is given by Equation (1):

$$\mu_{\widetilde{A}(x)} = \begin{cases} 0, & x \le a, \\ \dfrac{x-a}{b-a}, & a \le x \le b, \\ \dfrac{c-x}{c-b}, & b \le x \le c, \\ 0, & c \le x. \end{cases} \tag{1}$$

In our study, each risk is evaluated according to two factors, namely likelihood and consequence [1]. The columns of qualitative expressions and description in Tables 1–3 are based on a previous study [18]. These descriptions are extended with fuzzy logic MFs. A similar logic for generating the MFs' parameters is defined in the study [23].

Since Gaussian MFs can be useful for smooth and continuously differentiable fuzzy model [24], they can be applicable for likelihood and also for consequence variables. Here Gaussian MFs are used for likelihood and consequences in Tables 1 and 2. These Gaussian MFs were created with the help of tune fuzzy inference system using fuzzy logic designer from MATLAB. Triangular and trapezoidal MFs are applied for RL in Table 3. The MFs' parameters presented via the help of Fuzzy Logic tool box of MATLAB.

As depicted in Figure 2, the step following the decision about the fuzzy MFs, is to clarify the inference process to set conclusions from a set of fuzzy rules. The number of fuzzy rules in the fuzzy rule base depends on the number of qualitative expressions adopted for representing likelihood and consequence. For example, in the current research, there

Table 1: Likelihood representation.

Qualitative expressions	Description	Rate	Gaussian MFs
Unlikely	Expected to occur less than every 10th year	1	0.39375, 1
Less likely	Expected to occur once a year	2	0.26875, 1.90625
Possible	Expected to occur several times a year	3	0.428906, 3.5
Likely	Expected to occur several times a month	4	0.486523, 4.5

Table 2: Consequence representation.

Qualitative expressions	Description	Rate	Gaussian MFs
Minor	Minor or insignificant impact on the subscribers	1	0.39375, 1
Moderate	Local impact affecting a small number of subscribers	2	0.26875, 1.90625
Major	Serious consequences on local community	3	0.428906, 3.5
Critical	Essential services are affected	4	0.486523, 4.5

Table 3: Risk level (RL) representation.

Qualitative expressions	Description	Parameters MFs
Low	Acceptable risk	0, 0, 3, 6 (trapezoid)
Medium low	Tolerable risk	3, 6, 9 (triangular)
Medium high	Reduced risk with reasonable controls	6,9,12 (triangular)
High	Unacceptably high risk	9, 12, 16, 16 (trapezoid)

are 4 qualitative expressions for likelihood and 4 qualitative expressions for consequences which make up 16 rules in total. These rules are listed in Table 4 considering likelihood and consequence. In the present fuzzy rules, a total number of 16 if–then rules were created based on the size of the risk matrix of 4 × 4.

After the step of inference, the defuzzification process is completed which leads to a risk score of a given index. This process is fundamental for converting the output of a fuzzy system from a fuzzy set into a crisp value that can be used to support the decision-making process. The centroid method is applied for defuzzification in the case study. The evaluated risk scores of REs feed the FAHP process. It starts with pairwise comparison to determine the relative importance of the risk factors. Then the process continues with usage of triangular MFs to represent the degree of membership of the risk factors in different sets. Table 5 presents the importance with the help of the triangular fuzzy numbers to create the pairwise comparison matrix in the FAHP.

As depicted in Figure 2, to construct fuzzy pairwise comparison matrix that will lead to FAHP, the arithmetic operations for two triangular fuzzy numbers $\widetilde{a}_p\left(t_p^l, t_p^m, t_p^u\right)$ and $\widetilde{a}_q\left(t_q^l, t_q^m, t_q^u\right)$ are taken into account. The operations for fuzzy logic addition (⊕), multiplication (⊗), division (∅) and exponential (exp) can be found in [16]. Geometric mean can be used to calculate Weight Factor (WF) [16]. $DF_{\widetilde{w}_i}$ is defuzzified mean value of fuzzy WF [16].

$$\begin{aligned}\widetilde{f}_i &= (\widetilde{a}_{i,1} \otimes \widetilde{a}_{i,2} \otimes \ldots \widetilde{a}_{i,j} \ldots \otimes \widetilde{a}_{i,n})^{1/n} \\ &= \left(\left(t_{i,1}^l \, x \, t_{i,2}^l \, x \, \ldots \, t_{i,j}^l \, \ldots \, x \, t_{i,n}^l\right)^{1/n},\right. \\ &\quad \left(t_{i,1}^m \, x \, t_{i,2}^m \, x \, \ldots t_{i,j}^m \, \ldots \, x \, t_{i,n}^m\right)^{1/n}, \\ &\quad \left.\left(t_{i,1}^u \, x \, t_{i,2}^u \, x \, \ldots \, t_{i,j}^u \, \ldots \, x \, t_{i,n}^u\right)^{1/n}\right)\end{aligned} \tag{2}$$

$$\widetilde{w}_i = \frac{\widetilde{f}_i}{\widetilde{f}_1 \oplus \widetilde{f}_2 \ldots \oplus \widetilde{f}_j \ldots \oplus \widetilde{f}_n} \tag{3}$$

$$DF_{\widetilde{w}_i} = \frac{\left[\left(t_i^u - t_i^l\right) + \left(t_i^m - t_i^l\right)\right]}{3 + t_i^l} \tag{4}$$

$$w_i = \frac{DF_{\widetilde{w}_i}}{\sum DF_{\widetilde{w}_i}} \tag{5}$$

$$RL = \sum_{i=1}^{n} RL_i w_i \tag{6}$$

Table 4: Fuzzy rules.

Rule	Explanation
R1	If likelihood is unlikely and consequence is minor, THEN RL is low
R2	If likelihood is unlikely and consequence is moderate, THEN RL is low
R3	If likelihood is unlikely and consequence is major, THEN RL is low
R4	If likelihood is unlikely and consequence is critical, THEN RL is medium low
R5	If likelihood is less likely and consequence is minor, THEN RL is low
R6	If likelihood is less likely and consequence is moderate, THEN RL is medium low
R7	If likelihood is less likely and consequence is major, THEN RL is medium low
R8	If likelihood is less likely and consequence is critical, THEN RL is medium high
R9	If likelihood is possible and consequence is minor, THEN RL is low
R10	If likelihood is possible and consequence is moderate, THEN RL is medium low
R11	If likelihood is possible and consequence is major, THEN RL is medium high
R12	If likelihood is possible and consequence is critical, THEN RL is high
R13	If likelihood is likely and consequence is minor, THEN RL is medium low
R14	If likelihood is likely and consequence is moderate, THEN RL is medium high
R15	If likelihood is likely and consequence is major, THEN RL is high
R16	If likelihood is likely and consequence is critical, THEN RL is high

Table 5: Risk level (RL) representation for FAHP.

Qualitative expressions	Triangular fuzzy numbers	Triangular fuzzy reciprocals
Equal importance	(1,1,2)	(1/2,1,1)
Intermediate value	(1,2,3)	(1/3,1/2,1)
Moderate importance	(2,3,4)	(1/4,1/3,1/2)
Intermediate value	(3,4,5)	(1/5,1/4,1/3)
Important	(4,5,6)	(1/6,1/5,1/4)
Intermediate value	(5,6,7)	(1/7,1/6,1/5)
Very important	(6,7,8)	(1/8,1/7,1/6)
Intermediate value	(7,8,9)	(1/9,1/8,1/7)
Extreme importance	(8,9,9)	(1/9,1/9,1/8)

The total RL of the SGs is calculated by Equation (6) [16]. In the last step, we aggregate the results of pairwise comparison according to the equations from 2 to 6 to present the risk outcome as an overall risk score and RL.

4 Use case: HRA process of small-scale power grid

Conducting HRA process for SGs can be helpful to support stability and security as introduced in [25]. The proposed HRA process in Figure 2 is applied and tested considering a case study with five REs in a small-scale SG. Due to the safety concerns associated with using large-scale and in-action SGs for experimentation, the case study incorporates smaller-scale version of an SG, referred to as test-beds or demonstrators. Our chosen subject of study is a small-scale SG. A prototypical configuration of such a grid includes both Programmable Logic Controllers (PLCs) and Intelligent Electronic Devices (IEDs). PLCs can be programmed to perform diverse tasks such as monitoring equipment conditions, regulating the flow of electricity and retrieving data from sensors. IEDs are specialized devices designed specifically for power systems. They are used to detect and isolate electrical faults, manage power system parameters and monitor power quality. Simulating these devices allows researchers and engineers to experiment with novel control techniques, communication protocols and protection measures in order to enhance the dependability and efficiency of power systems. In Figure 3, an overview of a small-scale SG from the “KASTEL Security Lab Energy” is illustrated. The different PLCs are responsible for the control of a simulated physical system including a wind turbine, photovoltaic generator and battery system. As depicted in Figure 3, the simulated models are based on MATLAB. By comparing the power generated and the power required, the PLC determines whether to charge

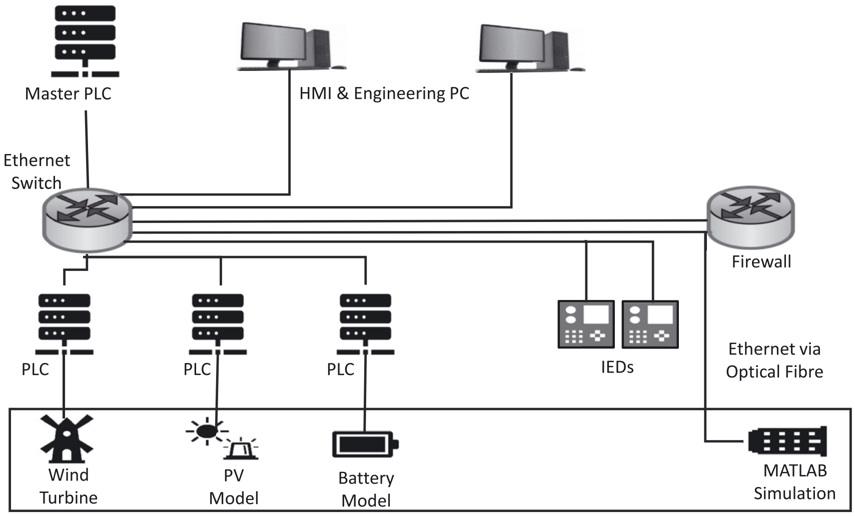

Figure 3: Small-scale smart grid (SG) architecture at the “KASTEL Security Lab Energy”.

Table 6: Risk events (REs).

Name	Explanation	Condition	Likelihood	Consequence
RE1	An unauthorised entity tampers, the measurement of the wind turbine PLC	It affects integrity. Data from wind turbine to the PLC can be manipulated	2	1
RE2	Reporting of inaccurate electrical signals to the master PLC	It affects integrity. Can promote changes that may cause damage to the SG	3	3
RE3	An attacker with network access can inject malicious data to modbus transmission control protocol (TCP) port 502	It affects integrity. Can result on affecting the control algorithm by sending malicious data	4	1
RE4	Denial-of-service (DoS) attack against the master PLC	It affects availability. Can cause reduced overview of the SG (the need to send technician intervention)	3	4
RE5	The inability of IEDs to recognize authorised users due to the attacker sending an excessive number or size of GOOSE (generic object oriented substation event) messages in the network	It affects availability. This can cause a certain number of subscribers to be disconnected	2	4

or discharge the batteries. The IEDs receive and process data from sensors and other equipment to issue protection and control commands such as tripping circuit breakers to identify and isolate electrical faults.

Five REs are defined in Table 6. The Common Vulnerability Scoring System (CVSS) and Common Vulnerabilities and Exposures (CVE) in the NIST National Vulnerabilty database [22] were taken into account. Moreover, the presented likelihood and consequence are interpreted considering the literature studies [18–20]. The results of fuzzy logic are shown in Table 7. After the fuzzy logic is proceeded, FAHP is conducted. To start with FAHP, pairwise comparison is shared in Table 8. It serves as an analysis for evaluating the relative significance of various risks during the decision-making process by contrasting each risk with all the others in a matrix format.

These calculations from Tables 7 and 8 are performed with the help of the Fuzzy Logic tool box of MATLAB. According to these calculations, RE4 has the highest risk with the level of '80 % High'. Considering these outcomes and Table 3, RE2 and RE4 must be treated initially. The overall RL is calculated for the grid by the arithmetical operation 6 and it is 11.28 with '24 % Medium High' and '76 % High'. The risk outcome is evaluated on the basis of fuzzy logic and arithmetical operations equations from 2 to 6. Considering the risk outcome, it can be understood that the treatment actions RE4, RE2, RE5, RE3 and RE1 will be carried out sequentially.

Table 7: Risk scores and risk levels (RLs) gained by fuzzy logic and risk matrix for five risk events (REs).

Name	Fuzzy logic		Risk matrix	
	Risk score	Risk level (RL)	Risk score	Risk level (RL)
RE1	2.34	Low: 100 %	2	Low
RE2	9.07	Medium high: 97 % high: 3 %	9	Medium high
RE3	4.2	Low: 60 %, medium low: 40 %	4	Medium low
RE4	11.4	Medium high: 20 % high: 80 %	12	High
RE5	7.41	Medium low: 53 % medium high: 47 %	8	Medium high

Table 8: Pairwise comparison for FAHP.

	RE1	RE2	RE3	RE4	RE5
RE1	1,1,1	1/2,1,1	1/4,1/3,1/2	1/5,1/4,1/3	1/4,1/3,1/2
RE2	1,1,2	1,1,1	2,3,4	1/5,1/4,1/3	2,3,4
RE3	2,3,4	1/4,1/3,1/2	1,1,1	1/3,1/2,1	1/3,1/2,1
RE4	3,4,5	3,4,5	1,2,3	1,1,1	3,4,5
RE5	2,3,4	1/4,1/3,1/2	1,2,3	1/5,1/4,1/3	1,1,1

5 Discussion and future work

In this section, the result of the proposed HRA process is discussed with possible enhancements to be addressed in the future work. Regarding IT domain, there are various existing RA approaches to calculate the risk outcome. Most of them estimate the impact and likelihood with the help of risk matrix [1]. Risk scores of five REs are represented at Table 7 in Section 4 by using a risk matrix with multiplication of the likelihood and the consequence. According to the findings obtained from Table 7, it is observed that the risk scores calculated using the fuzzy logic and risk matrix are close to each other.

The RLs obtained from fuzzy logic can belong to more than one linguistic set such as the REs from 2 to 5. Since the linguistic scales such as 'Medium High' and 'High' are shared with the decision-makers, an outcome from fuzzy logic can provide more detailed information about the risk than a risk matrix. For instance, as indicated in Table 7, the RLs of RE2 and RE5 are obtained from the risk matrix as 'Medium High', while from fuzzy logic they are '97 % Medium High', '3 % High' for RE2 and '53 % Medium Low', '47 % Medium High' for RE5. According to the presented study, fuzzy logic provides more detailed information than the risk matrix to decide on the treatment sequence. These detailed information can be helpful to the decision-makers in implementing mitigation strategies that are tailored to the unique characteristics of each risks. This outcome can increase the likelihood of successfully reducing the impact of risks. Risk matrices may encounter challenges in adequately representing the multidimensional aspects of risks and their interdependencies in the dynamic and evolving nature of SG technologies. From this perspective, fuzzy logic is capable of effectively addressing the uncertainties, complexities and interdependencies inherent in RAs specific to SGs. Based on these insights, the case study supports that the suggested HRA process is a promising approach. Our proposed approach can be applicable in different RA processes for SGs use cases when expert knowledge is available. Expert knowledge can provide insights into potential uncertainties of the assessment process for example identify possible attacker intentions or threat consequences. A comparison in terms of quality is suggested for future work. This contains the inclusion of more REs that could help qualify and quantify limitations across the different approaches. As a future work, we may consider the potential of expanding the fuzzy logic by incorporating fuzzy trees to accommodate a broader range of input variables.

Our study presents the applicability of fuzzy logic and FAHP based RA for SG. Circumstances may change or new threats may emerge, requiring adjustments to the RA process. Automating the RA process with effective techniques and tools like machine learning algorithms and simulation models can be a beneficial way to support the expert knowledge in the HRA process in a further step. To have a better understanding for risk sources and naturally enhance a secure decision-making process, future work will focus on increasing the number of REs and conducting the HRA process in a larger scale and heterogeneous substation. Additionally, this will enhance our understanding of the risks arising from communication protocols utilized by various manufacturers. Future work will focus on integrating expert knowledge with data-driven insights gathered from cyber-attacks launched against the IEC 61850 substation at "KASTEL Security Lab Energy" to improve decision-making process. Further endeavors are required to focus on the collection of real-world data from IEC 61850 Substations during cyber-attacks, with the aim of validating and enhancing calculated risk values under realistic scenarios. Moreover, potential future applications are explored for integrating this approach into SIEM systems to enhance their risk analysis feature.

The RA findings play a crucial role in effectively communicating information to relevant stakeholders, which can be valuable in demonstrating aspects such as policy adherence or compliance with directives and regulations [1]. For instance, we presume that through gaining an understanding of the risk outcomes generated by the HRA process and taking into consideration the identified risks and their potential impact, organizations and policymakers can appropriately align their compliance measures to effectively address the most significant threats. Moreover, they can establish more targeted measures to address cybersecurity challenges. Therefore, future efforts will be dedicated to expand IEC 61850 substation related REs. Overall, this will offer valuable support to decision-makers to design a list of action based prioritized risks and evaluating their acceptability.

6 Conclusions

The RA process is influenced by human decisions that can be ambiguous, blurred and hard to express with absolute numerical values. In the presented work, we propose an HRA process by using fuzzy logic and FAHP. Our main contribution is to provide a framework, based on fuzzy logic and FAHP to support comprehensive HRA process for the domain of SG. Using the presented approach, risk scores and levels are investigated. The outcomes will be beneficial for demonstrating a policy adherence with cyber-security recommendations in future energy systems since they provide a detailed understanding of an SG's security posture. This information can be used to demonstrate that one has conducted a thorough RA and has implemented appropriate security controls to address the identified risks. The RA process can help the decision-makers implement appropriate measures to address these issues.

Acknowledgment: We would like to thank the anonymous reviewers who provided valuable remarks that considerably improved the quality of the present paper. We would like to thank Dr. Mohammed Ramadan for his insightful comments and careful editing suggestions.
Research ethics: Not applicable.
Informed consent: Not applicable.
Author contributions: All the authors have accepted responsibility for the entire content of this submitted manuscript and approved submission.
Competing interests: The authors state no conflict of interest.
Research funding: This work was supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs (structure 46.23.02).
Data availability: Not applicable.

References

[1] A. Refsdal, B. Solhaug, K. Stølen, A. Refsdal, B. Solhaug, and K. Stølen, *Cyber-Risk Management*, Cham, Springer, 2015.

[2] A. Omerovic, H. Vefsnmo, G. Erdogan, O. Gjerde, E. Gramme, and S. Simonsen, "A feasibility study of a method for identification and modelling of cybersecurity risks in the context of smart power grid," in *COMPLEXIS 2019-Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk 2019*, SciTePress, 2019.

[3] M. S. Lund, B. Solhaug, and K. Stølen, *Model-Driven Risk Analysis: The CORAS Approach*, Berlin, Heidelberg, Springer Science & Business Media, 2010.

[4] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (siem): analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, p. 4759, 2021.

[5] P. Radoglou-Grammatikis, P. Sarigiannidis, E. Iturbe, et al., "Spear siem: a security information and event management system for the smart grid," *Comput. Netw.*, vol. 193, p. 108008, 2021.

[6] E. J. Byres, M. Franz, and D. Miller, "The use of attack trees in assessing vulnerabilities in scada systems," in *Proceedings of the International Infrastructure Survivability Workshop*, Citeseer, 2004, pp. 3–10.

[7] E. Rios, A. Rego, E. Iturbe, M. Higuero, and X. Larrucea, "Continuous quantitative risk management in smart grids using attack defense trees," *Sensors*, vol. 20, no. 16, p. 4404, 2020.

[8] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using bayesian attack graphs," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 61–74, 2011.

[9] D. Lu, C. Xu, L. Zhang, L. Wang, and Y. Sun, "Comprehensive risk assessment method of power grid based on grey relational weight game theory," in *IOP Conf. Ser. Earth Environ. Sci.*, vol. 453, no. 1, p. 012068, 2020.

[10] Z. Zeng, S. Yao, and T. Zhang, "Risk assessment method for smart substation secondary system based on deep neural network," in *Proceedings of PURPLE MOUNTAIN FORUM 2019-International Forum on Smart Grid Protection and Control*, Springer, 2020, pp. 443–454.

[11] L. A. Zadeh, "Fuzzy logic," *Computer*, vol. 21, no. 4, pp. 83–93, 1988.

[12] Y. Cherdantseva, P. Burnap, A. Blyth, et al., "A review of cyber security risk assessment methods for scada systems," *Comput. Secur.*, vol. 56, pp. 1–27, 2016.

[13] T. Saaty, *The Analytic Hierarchy Process: Planning, Priority Setting, Resources Allocation*, New York, McGraw-Hill, 1980.

[14] P. J. Van Laarhoven and W. Pedrycz, "A fuzzy extension of saaty's priority theory," *Fuzzy Sets Syst.*, vol. 11, nos 1–3, pp. 229–241, 1983.

[15] S. Kubler, J. Robert, W. Derigent, A. Voisin, and Y. Le Traon, "A state-of the-art survey & testbed of fuzzy ahp (fahp) applications," *Expert Syst. Appl.*, vol. 65, pp. 398–422, 2016.

[16] M. An, S. Huang, and C. Baker, "Railway risk assessment-the fuzzy reasoning approach and fuzzy analytic hierarchy process approaches: a case study of shunting at waterloo depot," *Proc. Inst. Mech. Eng. F J. Rail Rapid Transit*, vol. 221, no. 3, pp. 365–383, 2007.

[17] M. M. Silva, A. P. H. de Gusmão, T. Poleto, L. C. e Silva, and A. P. C. S. Costa, "A multidimensional approach to information security risk management using fmea and fuzzy theory," *Int. J. Inf. Manage.*, vol. 34, no. 6, pp. 733–740, 2014.

[18] K. Bernsmed, M. G. Jaatun, and C. Frøystad, "Is a smarter grid also riskier?" in *International Workshop on Security and Trust Management*, Springer, 2019, pp. 36–52.

[19] A. Elgargouri and M. Elmusrati, "Analysis of cyber-attacks on iec 61850 networks," in *2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT)*, IEEE, 2017, pp. 1–4.

[20] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in *ISGT 2014*, IEEE, 2014, pp. 1–5.

[21] MITRE: ICS Matrix, 2022 [Online]. Available at: https://attack.mitre.org/matrices/ics/ [accessed: Dec. 1, 2022].

[22] National Vulnerability Database, 2022 [Online]. Available at: https://nvd.nist.gov/ [accessed: Dec. 1, 2022].

[23] N. Abdussamie, M. Daboos, I. Elferjani, C. Shuhong, and A. Alaktiwi, "Risk assessment of lng and flng vessels during manoeuvring in open sea," *J. Ocean Eng. Sci.*, vol. 3, no. 1, pp. 56–66, 2018.

[24] R. Babuška, *Fuzzy Modeling for Control*, vol. 12, Dordrecht, Springer, 2012.

[25] S. Canbolat, G. Elbez, and V. Hagenmeyer, "Hybrid risk assessment process for smart grids," in *Poster präsentiert auf 10th KIT-Zentrum Energie Promovierenden-Symposium//KIT Energy Center Doctoral Symposium (2023)*, Karlsruhe, Deutschland, 10. Mai 2023, 2023, 46.23.02; LK 01.

Bionotes

Sine Canbolat
Karlsruhe Institute of Technology (KIT), Institute for Automation and Applied Informatics (IAI), KASTEL Security Research Labs, Hermann-von-Helmholtz-Platz 1, 76344 Eggenstein-Leopoldshafen, Germany
sine.canbolat@kit.edu
https://orcid.org/0000-0001-7292-7989

Sine Canbolat is a research associate at the Institute for Automation and Applied Informatics at the Karlsruhe Institute of Technology (KIT) while pursuing a Ph.D. at the KIT, Germany. Her research interests include risk assessment, security information and event management (SIEM) systems and alarm correlation.

Ghada Elbez
Karlsruhe Institute of Technology (KIT), Institute for Automation and Applied Informatics (IAI), KASTEL Security Research Labs, Hermann-von-Helmholtz-Platz 1, 76344 Eggenstein-Leopoldshafen, Germany
ghada.elbez@kit.edu

Ghada Elbez is head of the Secure Energy Systems (SES) research group at Karlsruhe Institute of Technology (KIT), Germany and coordinator of the KASTEL Security Lab Energy at the Institute for Automation and Applied Informatics (IAI). She received her M.Sc. degree in Electrical Engineering and Computer Science in 2016 from the Ecole Polytechnique de Lille, France and her PhD in 2022 from the Informatics Faculty at KIT. Her research interests include cyber-security of energy systems, defense mechanisms for early detection of attacks and security standards. She serves as reviewer and chair in different IEEE and ACM conferences. She actively contributes to some German standardization groups within VDI/VDE on the topics of cyber-security in energy systems.

Veit Hagenmeyer
Karlsruhe Institute of Technology (KIT), Institute for Automation and Applied Informatics (IAI), KASTEL Security Research Labs, Hermann-von-Helmholtz-Platz 1, 76344 Eggenstein-Leopoldshafen, Germany
veit.hagenmeyer@kit.edu

Veit Hagenmeyer is currently the Professor of Energy Informatics with the Faculty of Informatics, and the Director of the Institute for Automation and Applied Informatics, Karlsruhe Institute of Technology, Karlsruhe, Germany. His research interests include modeling, optimization and control of sector-integrated energy systems, machine learning based forecasting of uncertain demand and production in energy systems mainly driven by renewables, and integrated cyber-security of such systems.