energies

Article

Fuzzy-Based Failure Modes, Effects, and Criticality Analysis Applied to Cyber-Power Grids

Andrés A. Zúñiga, João F. P. Fernandes and Paulo J. C. Branco *

IDMEC, Instituto Superior Técnico, University of Lisboa, 1049-001 Lisboa, Portugal; andres.zuniga@tecnico.ulisboa.pt (A.A.Z.); joao.f.p.fernandes@tecnico.ulisboa.pt (J.F.P.F.)
* Correspondence: pbranco@tecnico.ulisboa.pt

Abstract: Failure modes, effects, and criticality analysis (FMECA) is a qualitative risk analysis method widely used in various industrial and service applications. Despite its popularity, the method suffers from several shortcomings analyzed in the literature over the years. The classical approach to obtain the failure modes' risk level does not consider any relative importance between the risk factors and may not necessarily represent the real risk perception of the FMECA team members, usually expressed by natural language. This paper introduces the application of Type-I fuzzy inference systems (FIS) as an alternative to improve the failure modes' risk level computation in the classic FMECA analysis and its use in cyber-power grids. Our fuzzy-based FMECA considers first a set of fuzzy variables defined by FMECA experts to embody the uncertainty associated with the human language. Second, the "seven plus or minus two" criterion is used to set the number of fuzzy sets to each variable, forming a rule base consisting of 125 fuzzy rules to represent the risk perception of the experts. In the electrical power systems framework, the new fuzzy-based FMECA is utilized for reliability analysis of cyber-power grid systems, assessing its benefits relative to a classic FMECA. The paper provides the following three key contributions: (1) representing the uncertainty associated with the FMECA experts using fuzzy sets, (2) representing the FMECA experts' reasoning and risk perception through fuzzy-rule-based reasoning, and (3) applying the proposed fuzzy approach, which is a promissory method to accurately define the prioritization of failure modes in the context of reliability analysis of cyber-power grid systems.

Keywords: FMECA; fuzzy inference systems; fuzzy-based FMECA; risk assessment; cyber-power grids

Citation: Zúñiga, A.A.; Fernandes, J.F.P.; Branco, P.J.C. Fuzzy-Based Failure Modes, Effects, and Criticality Analysis Applied to Cyber-Power Grids. *Energies* **2023**, *16*, 3346. https://doi.org/10.3390/en16083346

Academic Editor: Luigi Fortuna

Received: 20 March 2023
Revised: 7 April 2023
Accepted: 7 April 2023
Published: 10 April 2023

1. Introduction

The *failure modes, effects, and criticality analysis* (FMECA) is a structured qualitative method for reliability analysis intended to identify failures that have significant consequences affecting the system performance in the application considered. FMECA is very useful for identifying potential failures in a system, understanding their causes and consequences, categorizing them, and using this information to help prioritize maintenance tasks [1,2].

The standard IEC 60812:2006, titled "Analysis Techniques for System Reliability: Procedure for *Failure Mode and Effects Analysis* (FMEA)", can be considered an official guide for the application of FMEA and the FMECA principles [3]. FMECA is an extension of FMEA that includes a *criticality analysis* through calculating risk metrics [3]. Although FMECA differs from FMEA because the first considers the calculation of criticality, both terms are commonly used as synonyms. In this work, we use the correct term FMECA.

The primary objective of an FMECA analysis is to improve design [1–3]. However, it can also be applied at any project stage (or process) to plan preventive maintenance actions. In FMECA, the potential failure modes for all components are analyzed, identifying the causes that originated the failure, the failure effects on the system, and the actions that must be executed to mitigate its effects before it occurs.

FMECA provides a risk level for each identified failure mode. A *Risk Priority Number* (RPN) assesses the risk level. It is computed based on the following three criteria called *risk factors*: the *Occurrence* (O), which represents the frequency of occurrence of the failure mode; the *Severity* (S), representing the impact of the failure mode on the system; the *Detection* (D), which represents a ranking of the level of detection of this failure mode. Numerical categories characterize risk factors. Each category is usually represented by a numerical scale that can be a 1–10 scale, as proposed in [4], or in a 1–5 scale, as proposed in [5], or scales specially defined according to the characteristics of the problem. For the *severity* and *occurrence* scales, the higher the effect or frequency, the higher its rating; conversely, for the detection scales, the lower the failure mode's detectability, the higher its *detection* rating.

In the classical FMECA context, the *risk priority number* (RPN) is calculated as in (1) as follows [3]:

$$RPN = S \circ O \circ D \tag{1}$$

The scalar multiplication is the most used operator where the symbol $\circ$ represents a composition between the risk factors. The higher the RPN for a specific failure mode, the higher its risk. The failure modes are ranked from higher to lower RPN, producing a failure mode's ordinal ranking.

FMECA is widely used in several industrial and commercial applications such as oil and gas, energy, mining, nuclear, chemical processes, and, lately, healthcare, among others. Concerning electrical power systems, FMECA analysis was applied in different contexts.

In [6], for example, the FMEA analysis was applied to the risk assessment in capacitor banks. The authors identified 17 failure modes from the following 3 main components: the capacitor unit, the support insulators, and the unit panel, and conducted a detailed explanation of failures and detection methods. The authors proposed four categories for the *severity*, five for the *occurrence*, and six for the *detection*. The FMEA was applied to capacitor banks installed in the Majan Electricity Company SAOC in Oman, where the capacitor banks are an important source of medium-voltage grid outages. The authors showed the FMEA worksheet with the failure modes ranked by their severity instead the RPN. However, they do not compute the RPN.

Reference [7] presents a risk analysis of power transformers for maintenance and replacement decision. The analysis uses the power transformers data published in 2015 by the *Conseil International des Grands Réseaux Électriques* (CIGRE). To conduct the analysis, the power transformer was divided into the following six main components: winding, core, insulation, bushings, tap changers, and tank. The authors develop a matrix that presents the relationships between the parameters that cause failures. In this analysis, some parameters included in the CIGRE data were used to assess the risk factors. The severity considers parameters related to the effects of failures in power transformers, the damage of the failures to the environment and themselves, their reparability, and the duration of the electricity interruptions. The occurrence considers parameters such as failure location, causes, and type. The detection considers parameters such as protection, monitoring, and inspection. In addition, the effect of aging in the power transformers is considered under the bathtub curve; the analysis considers the following three aging groups: ages from 0 to 5 years, ages from 5 to 20 years, and ages from 20 years and above. The RPN is computed for each of the three groups of ages, considering the failure modes with RPN greater than 100 as the top priority risk. The insulation defects appear as the riskiest failure modes in transformers with ages between 0 and 5 years; for ages between 5 and 20 years, the transformers achieve a stable operation, and the RPN value is low, and, not surprisingly, the RPN increases considerably for the FMECA analysis considering ages above 20 years. Unlike other applications of classical FMECA, this work considers additional factors to assess the risk factors and divides the analysis into three periods.

Reference [8] presents an approach to measure and collect data from remoter monitoring systems in high-voltage power transformers, whose alarms and alert conditions were identified through the FMEA analysis. Sensors for winding temperature, cooling-oil temperature, inner pressure, and electrical power were installed to measure the parameters.

A Simatic IoT2040, a Siemens open platform, user acquisition, processing, and data transfer to enable real-time monitoring and preventive maintenance applications, was also used. The FMEA analysis is used as an auxiliary method to detail and identify the transformer failures and their detection methods (alarms and alert conditions), defining alarm categories for different failures.

The first application of FMECA analysis in photovoltaic electrical systems (PV) is shown in [9], where the authors show a risk analysis for a photovoltaic array at the Northeast Solar Energy Research Center (NSERC) located at Brookhaven National Laboratory's (BNL). The system is composed of 1672 photovoltaic modules, and each one is rated at 310 Wp. To conduct the analysis, the PV system was simplified considering only the following three blocks: the source system composed of the photovoltaic modules, the rack and cable system; the string combiner composed of fuses, dc cables, and disconnect devices; the power conditioning system composed by the inverter, circuit breakers, transformers, protective relays, and grid interface. The implemented FMECA focuses on the failure modes of single components and considers less interest in their combination. The authors identified the following two main problems for the work development: the availability of specific photovoltaic systems failure databases and the outdated databases about failures in electric elements; finally, the author uses failure information from academic references. The five risk categories were defined based on the available information and experts' experience, represented by a 1–5 scale. Results show that inverter and lightning protection systems are the riskiest failure modes, followed by the cells and contacts. The author evidences a need for more publicly available FMEA analysis for PV systems. This makes it difficult to validate the obtained results. However, the analysis identified an important set of failure modes that will feed a probabilistic risk analysis.

Report [10] shows the results of the International Energy Agency Photovoltaic Power Systems Programme (IEA PVPS), specifically related to the Performance, Operation, and Reliability of Photovoltaic Systems (PVPS). The report considers the analysis of 191 maintenance tickets. Thirty failure modes related to the PV module, cables and connectors, mounting structure, and inverter were identified during the analysis; 11 detection methods were also identified. The failure mode impact is defined in terms of the following three safety categories: failure does not affect safety; failure may cause fire, electrical shock, or physical damage; failure can directly cause fire, electric shock, or physical damage. Five categories were defined to assess the failure mode impact on the system performance. The FMEA analysis is performed for each failure mode, and failure characteristics such as origin, detection method, impact on safety, and performance are assessed based on the expert's knowledge and opinion. The report also includes a quantitative analysis based on a cost priority number (CPN). The authors extract the following important conclusions from their analysis: the risk definitions are not fully structured, and event databases are not harmonized. In this case, they noted that standardization for the available metadata used in data analysis is necessary. Moreover, due to the large number of PV plants, the automation of the maintenance ticket is essential to extract key performance parameters efficiently, limiting human intervention.

Regarding wind electrical energy systems, the authors of [11] present a review of several FMECA applications in offshore wind power plant components and analyze a study case. The traditional risk categories represented the risk factors, as suggested in [3]. The FMECA identified 593 failure modes related to 83 components of the offshore wind turbine and 119 failure modes related to 23 components of the offshore wind substation. The tower and substructure, the blades, and the converter all achieve the higher RPN, and conversely, the blade bearings and the nacelle are ranked, respectively, as the less critical components [11]. In addition, the paper includes a quantitative comparative study using a simplified version of the components of the wind turbine system and the traditional FMEA methodology. The authors' analysis aims to verify possible differences between the obtained results and different wind turbine data and knowledge bases. The blades, generator, and converter all achieve a higher probability of *occurrence* for their failure modes.

The structural components, such as the blades and tower, achieve higher values for *severity*. This study applies the classical FMECA analysis, using the expert's knowledge to assess the risk factors subjectively.

The application of FMECA analysis in the cyber-power grid context still needs to be improved. Work [12] shows one of the first FMECA analysis applications in distribution grids combining power and cyber equipment. The traditional risk categories represented the risk factors, as suggested in [3]. The cyber-power grid test system was specially designed for this application. The generation system shown in Figure 1 consists of one conventional generation station (110 MW), one wind energy station (130 MW), one photovoltaic power plant (100 MW), and one energy storage system (50 MW). The power grid consists of four power transformers, fifteen circuit breakers, one residential load point (20 MW), one industrial load point (85 MW), and one commercial load point (40 MW). The storage facility and generation stations were not part of the FMECA analysis. The failure rate data for the power equipment were collected from statistical data from the Portuguese electrical utility and specialized databases and manufactured datasheets. The cyber network considers a ring topology for the *local area network* LAN-Ethernet network; the *wide area network* WAN-optical fiber network consisting of *human-machine interfaces* (HMI), ethernet switches, servers, energy boxes with smart metering functions, and *intelligent electronic devices* (IED). As indicated in Figure 1, the power grid architecture includes a control center consisting of an inter-control center communications protocol server, an applications server, an engineering server, an engineering database, and its respective backup. Finally, the test system considers a corporate center consisting of one business server, one corporate server, an e-mail server, a web apps server, and a file transfer protocol server. The reliability values for the cyber network were collected from reliability statistics and manufacturers' datasheets. The FMECA analysis identified 107 failure modes and fully analyzed the 42 riskiest ones. Results show that transformer explosions, IED control failures, and busbars' structural integrity loss achieve the highest RPN values.

On the other hand, the transformer tap-changer contacts' degradation, the optical fiber link fracture, and the optical fiber link humidity induced the lower RPN. The authors state an interesting conclusion regarding human interference in future smart grids, specifically the HMI's operational failure due to human error, which negatively impacts the grid. This human error is unintentional, and its high probability of occurrence and unpredictability makes it a high-risk failure cause. Among this application's main advantages was establishing a systematic process for failure identifications involving expert knowledge and technical data. However, the relative importance of the risk factors was not considered during the RPN computation, which the authors now consider for the same grid system in this paper.

Reference [13] shows innovative research related to smart grid technologies, where the authors introduce a novel application of chaotic systems in the context of an electrical energy distribution network's flow control. Chaos is introduced in the test circuits by implementing Chua's electronic circuit, which exhibits chaotic behavior. This application is also relevant for microgrids, where a decentralized strategy often improves performance. The paper proposes a mathematical model for a network of oscillators used for numerical and experimental analysis. The basic topology consists of N RLC oscillators coupled through a capacitor. In addition, the authors implemented a Chua circuit using operational amplifiers. The test results in evidence that the time constant of the energy flow can be effectively controlled by acting on the parameters of Chua's circuit [13]. The authors conclude that the effective implementation of chaotic signals is particularly valuable for some applications, particularly in cases where efficient energy management in electrical networks is necessary. One key benefit of utilizing this type of signal is the ability to control the time constant of energy distribution and regulate the direction of the energy flow by adjusting the parameters of the chaotic circuit considered.

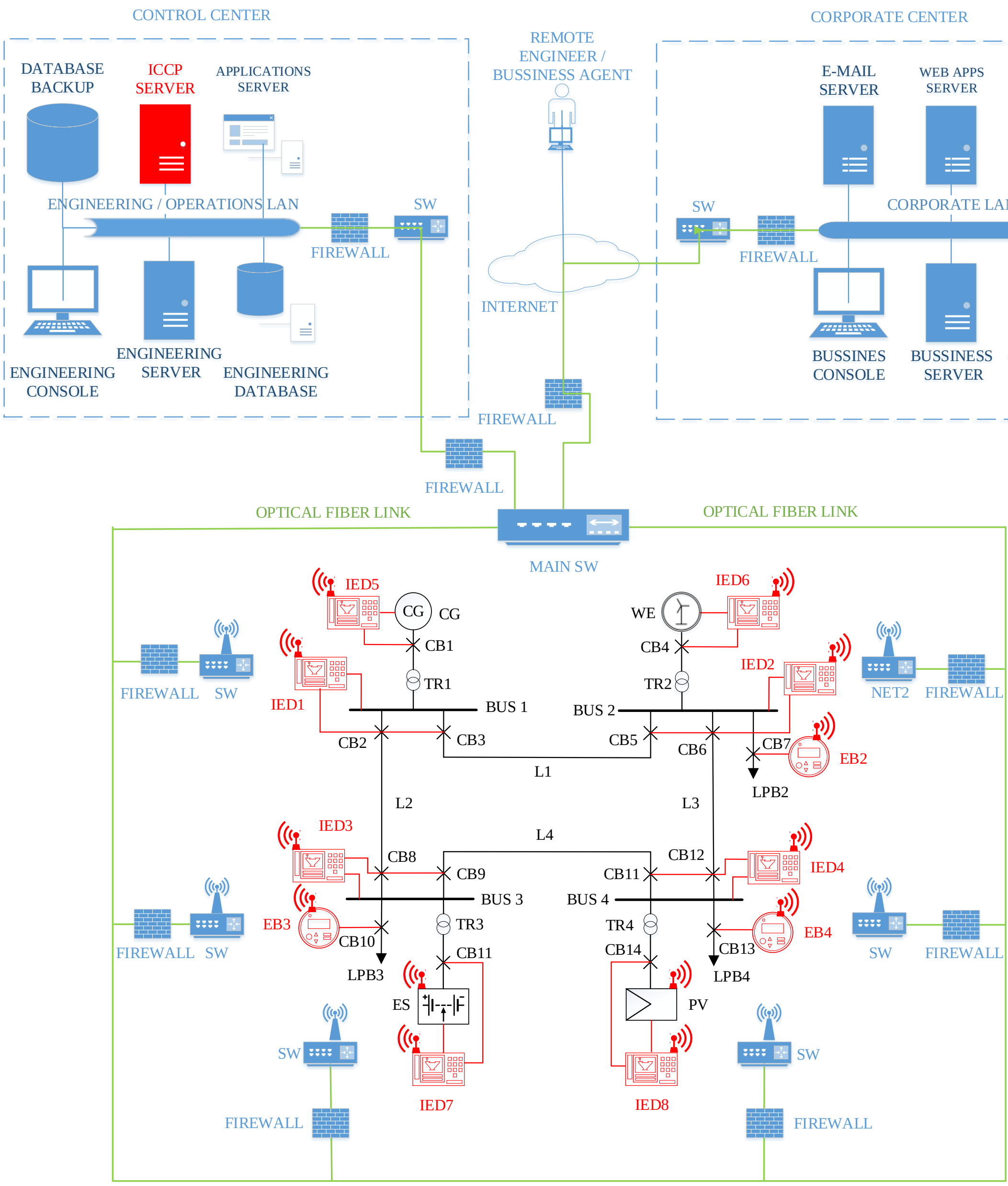

Figure 1. These authors in [12] applied FMECA analysis, combining power and cyber equipment in a distribution grid.

From the previous literature review, we can conclude that the classical FMECA is a powerful tool for identifying potential failure modes and their effects in several applications because the risk assessment follows a systematic procedure that considers the knowledge of expert personnel and technical information about the system. Despite this FMECA advantage, an in-deep analysis of the available literature evidence the following weaknesses:

1. Computation of risk priority number (RPN) does not take into account the relative importance of *severity*, *occurrence*, and *detection* risk factors;
2. Different combinations of S, O, and D can produce the same RPN value;
3. The numerical scales used to represent the risk factors are usually attributed arbitrarily, being essentially qualitative scales;
4. Assessment of risk factors has a subjective character. Hence, an integer number may not represent the uncertainty associated with expert knowledge, and;

5. Although risk factors are represented as intervals, the RPN computing method is inappropriate for this kind of data.

FMECA technique is a team-based qualitative risk analysis method. Therefore, human reasoning plays an essential role during its development. An appropriate representation of expert knowledge in risk assessment is one of the main challenges of the classical FMECA method. Therefore, the criteria of the expert members constitute the principal source of uncertainty in the classical FMECA analysis. Moreover, FMECA experts use linguistic terms to represent risk categories, the second source of uncertainty in FMECA.

The mentioned five weaknesses in the classical FMECA analysis motivate us to find alternatives to integrate the uncertainty into the FMECA risk assessment when applied to the cyber-power grid perspective. Fuzzy logic appears as an appropriate approach to represent the natural language and the human reasoning mechanism, allowing us to deal with their intrinsic uncertainty. Employing fuzzy logic allowed us to represent each risk factor using a function with associated uncertainty instead of only an integer number. In addition, we can compute the failure modes risk through a reasoning mechanism instead of the simple arithmetic product between three integer numbers.

Considering that context, this paper's main objective is to evaluate using a type-I fuzzy inference system to improve risk prioritization in the FMECA analysis, considering a more natural risk definition based on expert knowledge. To test and apply the proposed fuzzy-based FMECA, we applied our approach to the cyber-power grid we studied in [12] using the power grid topology shown in Figure 1. In our approach, fuzzy membership functions represent risk categories, and the risk computation follows a rule-based inference mechanism.

Our results show that fuzzy sets and fuzzy rules adequately represent the expert knowledge and risk perception of the FMECA team members. Because our fuzzy-FMECA considered a different level of importance for each risk factor, the set of failure modes previously ranked as the riskiest by classical FMECA was relocated to the most correct priority. In addition, an in-deep analysis was included to explain how the fuzzy mechanism works to assess the risk in the proposed cyber-power grid case.

The paper has the following structure: Section 2 includes a literature review of the fuzzy-based methods used to improve the FMECA analysis. Section 3 presents a brief introduction to fuzzy sets and type-I fuzzy inference systems applied in the context of the FMECA analysis. Section 4 shows the implementation of the proposed fuzzy-FMECA approach, including detailed information about the membership functions representing the FMECA risk factors, fuzzy rules, and operators used for the fuzzy inference system. Section 5 presents the classical FMECA analysis case study in the cyber-power grid and the configuration of the fuzzy-FMECA test cases. Section 6 shows the results and a detailed discussion about the failure modes prioritization obtained by the classical and fuzzy-FMECA. Finally, Section 7 includes the paper's conclusions and significant points for future work.

2. Literature Review

As stated in the previous section, the FMECA analysis relies on the expert knowledge of analysis team members. These team members evaluate failure modes qualitatively, introducing uncertainty and vagueness into the process. The literature contains several approaches proposed to deal with uncertainties related to risk and safety analysis, especially in FMECA analysis.

In [14], the authors present an in-depth analysis of uncertainty sources in process safety analysis (PSA). The study identified three sources of uncertainty: *completeness uncertainty* refers to including all significant aspects within the analysis; *modeling uncertainty*, related to deficiencies in the accident scenario probabilities and consequences modeling; *parameter uncertainty*, related to incomplete available data. The paper includes an exhaustive identification of uncertainties associated with the different methods used in the following four PSA stages: hazard analysis, consequence assessment, frequency estimation, and risk estimation. The authors propose a hybrid approach consisting of the traditional qualitative hazard identification process and a quantitative model based on a fuzzy logic system (FLS) used to quantify the frequency, severity of consequences, and risk index. Authors propose a fuzzy logic-based "bow-tie" model to compute frequency; the consequence analysis is conducted by individual fuzzy logic models to deal with the consequence analysis complexity, showing an application for the *boiling liquid expanding vapor explosion* (BLEVE) calculation on a 600 m^3 tank with LPG. The risk index assessment model considers fuzzy frequency and severity input variables. Finally, to compute the risk correction index (RCI), which represents the effect of PSA quality on the overall risk index, the authors proposed an FLS approach consisting of three categories for complexity, three categories for experience, and nine fuzzy rules. The authors' main conclusion states that FLS is a promising approach to dealing with uncertainty in the PSA process.

Reference [15], the same authors present another innovative and recent fuzzy logic application to deal with uncertainty in the representative accident scenarios (RAS) identification as part of *Hazard and Operability* (HAZOP) analysis conducted by a team of experts. The study identified two main sources of uncertainty: uncertainties related to team member's knowledge and experience; uncertainties related to the effect of safety barriers [15]. To take into account the effects of the safety barriers, the authors propose a risk correction index (RCI); RCI is represented as a function of the quality index (QI), represented by the complexity of the system under analysis and the experience of the analysis team, and as a function of the efficacy index (EI) that represents the performance of the safety barriers qualitatively. The proposed approach for the RAS identification considers the following four stages: (1) The HAZOP analysis to identify the accident scenarios; (2) a traditional initial risk ranking and a fuzzy-based initial risk ranking that includes categories for classical and fuzzy frequency, and classical and fuzzy consequences; (3) a final risk ranking assessment, based on the traditional and fuzzy RCI, traditional and fuzzy QI and traditional and fuzzy EI; a final RAS selection between the traditional RAS or the fuzzy RAS. When applied to RAS identification in liquefied natural gas (LNG) storage tanks in a typical regasification terminal, the results show that the fuzzy initial risk and fuzzy final risk indices for each accident scenario were determined with more accuracy when compared to the traditional approach [15].

Several approaches have been applied in the last two decades to overcome the shortcomings mentioned above in classical FMECA. In [16], the author shows extensive bibliographic research on methods to improve the FMECA prioritization process from 1998 to 2018. The researchers used the following two-level keyword structure to conduct the bibliographic research: "FMEA" or "FMECA". Between the subordinate keywords, they propose "risk priority number", "risk evaluation", "risk assessment", "risk prioritization", "risk ranking", "risk factor weight", "reliability analysis", "criticality analysis", all these being determined based on published papers and experts' advice. Years from 2014 to 2018 account for 60% of the published papers, representing a significant growth in FMECA-oriented research in the last 25% of the analyzed period. China is the major contributor to the FMECA improvement. The methods of "gray theory" and "fuzzy inference systems" appear to be the most used in the last decade to improve the FMECA analysis, mainly in mechanical systems, aircraft systems, electronics, the automobile industry, and healthcare risk management [16]. The main issues were using weights for a certain quality judgment of each FMECA team member and the internal relationships among failure modes and associated correction actions. In our opinion, one of the main conclusions of this paper is related to the computational complexity of the proposed improvement methods, which makes it difficult for practitioners to adopt them. In this context, fuzzy inference systems appear as an appropriate methodology due to their conceptual simplification and the direct participation of practitioners in the implementation.

In [17], the authors compared the classical FMECA with two modified FMECA based on *Grey relational theory* (GRT) and *fuzzy rule base* (FRB). Five risk categories and triangular membership functions represent the linguistic terms related to risk factors. A 125-rule base was formulated, and the Mamdani FRB was used to assess the risk priority in the fuzzy rule base. The GRT is used to include experts' diverse opinions and to assign a relative weight to each assessment factor. The proposed approach assessed the risk of 27 failure modes in pipeline systems. When comparing the three methods in two failure modes having the same risk factors values, the classical and rule-based FMECA provided the same ranking. However, the GRT method pointed to a different ranking for both failure modes, thus not in agreement with the first two. The main advantages of using the rule-based and GRT-based FMECA are that both allow the expert's weighted experience to be better incorporated into FMECA when there is limited operational data.

In [18], the authors propose an FMECA method combining fuzzy set theory, *analytical hierarchy process* (AHP), and *data envelopment analysis* (DEA) to handle the uncertainty in risk analysis of aircraft landing systems. The fuzzy stage considers the risk factors of five categories, triangular and trapezoidal membership functions. The AHP assigns a weight for each FMECA risk factor associated with four experts. The DEA determines the optimum corrective actions for the riskiest failure modes. The authors applied their methodology to assess risk in a simple aircraft landing system, comparing it with the fuzzy-*developed FMEA* (FDFMEA). Authors conclude that their approach can provide much more information to make a better decision decreasing the risk level. However, the failure modes prioritization based on risk continued to remain subjective. A sensitivity analysis could provide more information about the proposed model's relationship between risk and cost.

Reference [19] shows an approach based on a combination of a modified fuzzy AHP method to obtain the weights attributed to each risk factor plus a modified fuzzy weighted *multi-objective optimization on the basis of a ratio analysis plus the full MULTIplicative form* (MULTIMOORA) methodology to determine priority weights for the decision-makers. The proposed approach includes the following three new risk factors: *time* T, *cost* C, and *profit* P. Each risk factor fuzzification considered seven risk categories formalized with triangular membership functions. The model was applied for risk assessment in a steel factory and compared with the traditional fuzzy-FMECA and weighted fuzzy-FMECA methods. The authors highlight some advantages of their proposed model, such as a more precise risk evaluation due to the simultaneous use of risk factors weighting and establishing a set of priority weights for the decision-maker's criteria and experience.

In [20], a type-II fuzzy system is applied to identify hazardous conditions in marine power systems applications. The method applied was a *general type-II fuzzy system* (GT2FS) decomposed into several *interval type-II fuzzy systems* (IT2FS) to reduce the computational complexity. The GT2FS considers five risk categories, type-II triangular membership functions, and thus 125 fuzzy rules. Compared with the type-I fuzzy-based FMECA and the classical FMECA, the authors state that their approach highlights the differences between different failure modes' rankings, becoming more robust and efficient for the RPN calculation and the prioritization process.

Reference [21] contains another application of improved FMECA in the marine context. The authors proposed a combined methodology based on fuzzy logic and the *decision-making trial and evaluation laboratory* (DEMATEL) for correlation between failure modes and their causes. The fuzzy system considered ten categories, trapezoidal membership functions for the risk factors S, O, and D, and five categories with triangular membership functions to represent risk factors weights. Before performing the risk assessment, an expert's total credibility weight also ponders the risk factor and its associated weights. The fuzzy RPN is then computed using the weighted geometric mean between risk factors, with the final RPN value obtained using the *Centroid of Area* COA. The DEMATEL method is applied in the next step to correlate the failure modes with their occurrence, computing a causal degree to rank the failure modes. When applied to the risk assessment in shipboard-integrated electric propulsion systems, the authors conclude that their approach is consistent with the practical engineering failure cases, and their approach considers the correlation effects between failure modes and causes, giving higher risk priority to common cause failure modes. In other words, a higher risk priority is achieved if the same cause induces multiple failure modes.

In [22], the authors proposed a new technique for fuzzy risk assessment in an FMECA analysis based on *D* numbers and multi-sensor information. The fuzzy stage considers seven risk categories with triangular and trapezoidal membership functions for risk factors. The weights for risk factors are computed, with them transformed into D numbers. Finally, the risk factors are ranked. When applying their approach to a case study that assesses the risk of the general anesthesia process, the proposed method overcomes the shortcomings of the traditional RPN approach to some degree, obtaining comparable performances relative to other MCDM technologies used in FMEA as the *Vise Kriterijumska Optimizacija I Kompromisno Resenje* VIKOR method. The proposed approach is especially suitable for the case that contains non-exclusive fuzzy evaluations.

Reference [23] introduces the notion of fuzzy relative importance for the FMECA risk factors. These were modeled by triangular membership functions, with authors including the failure modes priority through three trapezoidal-based linguistic terms (low, moderate, and high priority). In addition, two sets of fuzzy weights for the risk factors are computed. The authors apply the proposed approach to the manufacturing process. Their approach allows for establishing the relative importance of the risk factors by introducing a specific fuzzy variable. Using fuzzy weights allows representation of the perception of the experts from the FMECA team regarding each risk factor. The main limitation of this methodology is, however, the assignment of the parameters for the membership functions related to the importance and priority indices since they must be the result of consensus among the members of the FMECA team.

In [24], the authors use the FMECA method in the logistic environment facing the COVID-19 outbreak. The proposed approach considers a fuzzy-based FMECA to represent twelve process failures identified and an *Analytic Hierarchy Process* (AHP) method to obtain the weights for the three FMECA risk factors. The authors classified the failures into the following three main groups: business risks, safety risks, and special issues. Results show that failure mode, denoted by the *Exposure* of employees to high-risk groups with fever, is the riskiest, showing the influence of the COVID-19 pandemic on the logistical systems. The main advantage of the proposed approach combining the fuzzy-FMECA and AHP is the accuracy of the degree of risk computation. The limitation of this work is the dependence on the experts' knowledge because the results may vary for different groups of experts.

In [25], the authors present an approach combining the fuzzy-FMECA analysis and *Fault Tree Analysis* (FTA) to assess the riskiest failure modes quantitatively. The fuzzy-FMECA considers five risk categories, triangular membership functions, and a fuzzy inference system (FIS) to compute the risk priority number. When applied to a system with four failure modes, the authors concluded that their approach proves efficient because as the FTA only considers the riskiest failure modes, this allowed for reducing the tree size, concentrating on the most severe failures that affect the system.

Reference [26] introduces the application of fuzzy-based FMECA analysis for risk evaluation in power transformers. The proposed approach combines aggregation tools based on *hesitant fuzzy systems* (HFS) and the *Criteria Importance Through Inter-criteria Correlation* (CRITIC) technique. In the first step, an FMEA group, including three experts, is asked to offer their opinions on the risk evaluations for seven failure modes using the HFS. The second step considers the assignment of weights for each expert using the CRITIC weighting method. The global risk for each failure mode is computed using a novel *hesitant fuzzy weighted geometric average* (HFWGA), and finally, the failure modes are ranked. In addition, the authors conduct a comparison between their approach, the *Hesitant Fuzzy Vise Kriterijumska Optimizacija I Kompromisno Resenje* (HF-VIKOR), the *Hesitant Fuzzy Technique for Order Preference by Similarity to the Ideal Solution* (HF-TOPSIS), and extended generalized *TOmada de Decisao Interativa Multicriterio* (TODIM). The authors' results state that their rankings are consistent with the classical FMECA and the generalized TODIM, concluding that the proposed FMEA framework is valid for evaluating and ranking failure modes' risk prioritization. The proposed FMECA approach is flexible in handling risk assessment teams with multiple experts and includes a relative weighting among them. The three risk factors and the inherent relation between risk factors should be investigated to improve the method.

In [27], it is introduced the application of the fuzzy-FMECA analysis for the safety risk assessment in a water diversion infrastructure. Failure modes were classified into the following four main groups: social impact, operation management, engineering technology, and environmental impact. The fuzzy structure considers fives risk categories, triangular membership functions and Mamdani fuzzy inference system. The approach is applied to a strategic infrastructure in China, the Huixian section of the Middle Route Project of the South-to-North Water Diversion Project (MRP-SNWDP). To collect the data for the analysis, the authors asked twenty-four experts to fill out a questionary to determine the scores for *occurrence* and *detectability*, and the data for *severity* obtained from the inspection reports. In addition, a weight was associated with the experts' experience. Compared with the classical FMECA, the proposed approach can make a systematic risk prioritization, with the prioritization results obtained from both FMECA methods being very similar. This approach's main limitation is related to the subjectivity of the questionnaire survey and the use of qualitative indicators for the three risk factors.

A different application of fuzzy-based FMECA is found in [28], where the authors show its application in a quantifier prototype of methane gas (CH_4) and carbon dioxide (CO_2) specifically developed to measure the emissions generated by cattle. A group of specialists identified 30 failure modes through the classical FMECA analysis. The proposed fuzzy-FMECA architecture comprises five risk categories, trapezoidal membership functions for the three risk factors, seven categories and triangular membership functions for the RPN, and a Mamdani fuzzy inference system with 125 rules. From the results, the authors conclude that fuzzy logic is adequate for risk assessment, especially in the project or porotypes development stages, when no operational information is available to support the decisions. Although the fuzzy-based FMECA deals with the uncertainty associated with the expert's criteria, using classical ratings to assess the risk factors can disadvantage this methodology.

A recent application of adaptive neuro-fuzzy inference systems (ANFIS) and support vector machines (SVM) to improve the FMECA process is shown in [29]. FMECA analysis is a proactive diagnosis technique for this work's edible oil purification process. The authors propose an approach consisting of the following steps: (1) A process description where the authors define the system's main functions and the failure modes' causes, effects, and consequences; (2) A knowledge-based approach, where authors determine the risk parameters, defined the ANFIS and SVM structures; (3) A final step that includes the RPN computing and sensitive analysis. Four experts identified 67 failure modes from 14 components. The ANFIS approach considered 3 fuzzy categories with 27 rules, 5 fuzzy categories with 125 rules, and 10 categories with 1000 rules; in addition, the analysis considered a combination of eight membership functions for the risk factors triangular, trapezoidal, pi, gauss, gauss2, g-bell, p-sigmoid and d-sigmoid). The application of SVM considered the following two algorithms: Sequential Minimal Optimization (SMO) and Iterative Single Data Algorithm (ISDA), which classify the 67 failure modes into 67 risk clusters. The ANFIS network using hybrid training, specifically the 3-categories (27-rule) and the 5-categories (125-rule), showed high potential to create maximum risk number cluster failure modes. Regarding the SVM application, the ISDA algorithm has higher accuracy in predicting the actual values and classifying the failure modes with the lowest error compared to the other intelligent methods in this paper.

In [5], the authors show one of the first approaches that apply type-I Mamdani fuzzy systems for the FMECA analysis in the smart grid environment. The fuzzy-FMECA analysis was performed in the following two stages: first, an intermediate fuzzy variable called "impact" is computed using the fuzzy inference system between risk factor *Severity* and *Occurrence*. The fuzzy RPN is computed by applying the fuzzy inference system between the impact and the *Detection*. Risk factors were represented by triangular and Gaussian membership functions corresponding to five risk categories. The proposed approach was applied for risk assessment on eight smart grid components, showing that the fuzzy-based FMECA adequately prioritizes the failure modes. However, one must point out that this analysis does not consider any interdependency between the different components.

Reference [30] also shows the application of type-I fuzzy inference systems for improving the FMEA analysis in a smart grid distribution system. The fuzzy system considers 125 fuzzy rules, triangular membership functions for the risk factors *O*, *S*, and *D*, and Gaussian membership functions for the RPN. The Mamdani inference system and COA were used in the defuzzification process. When applied to a power grid test system shown in [12] consisting of 24 failure modes, authors conclude that their approach deal with the uncertainty in predicting failure modes where there is insufficient data or even knowledge to make accurate decisions, providing a way for dealing with multiple experts with conflicting opinions. The results proved that the method is more robust and accurate than classical FMECA. Moreover, the method developed can be improved by considering economic constraints.

Due to the limited applications of FMECA analysis in the context of cyber-power grids, this work aims to contribute to the prioritization of failure modes, introducing the application of fuzzy systems to represent the uncertainty associated with human language and the human logical reasoning mechanism.

The following section introduces type-I fuzzy inference systems and the FMECA risk factors representation in fuzzy logic terms.

3. Type-I Fuzzy Inference Systems

3.1. Fuzzy Sets and Fuzzy Logic

A fuzzy set can be viewed as an extension of a classical set that "introduces vagueness by eliminating the sharp boundary that defines when an object belongs to a set (or category) or not" [31]. In classical sets theory, a particular element belongs to a set or not; in fuzzy sets' terms, it is possible to say that this element belongs to a set with a certain *membership grade*. For example, the probability of occurrence for a particular failure mode is 5×10^{-2} occurrences per year. We state that it belongs to a risk category named *Occurrence Probable* (OP). To represent the risk category OP as a fuzzy set, one considers that the failure mode's probability of occurrence is *around* 5×10^{-2} occurrences per year. The term *around* means that fuzzy set OP will contain not only the failure modes with probability 5×10^{-2}, but also failure modes whose probability of occurrence is close to 5×10^{-2} within a predefined interval. Let us say that the fuzzy set OP (occurrence *around* 5×10^{-2}) is defined in the interval from 3×10^{-2} to 30×10^{-2}, as shown in Figure 2. All failure modes with a probability of occurrence within this interval will belong to the OP with a certain *membership grade*. This, in fuzzy sets, can be modeled through a *membership function*, denoted by $\mu(x)$ that assigns a membership grade between 0 and 1 to each element in the interval.

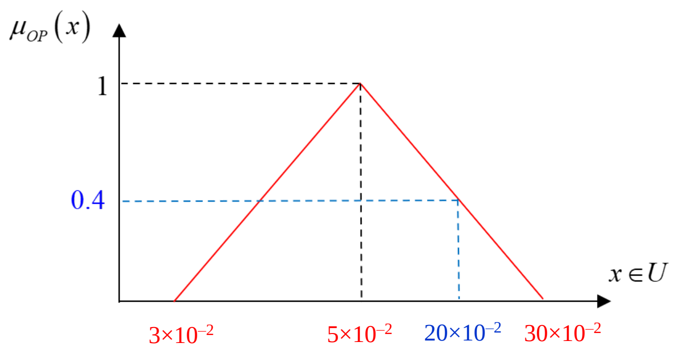

Figure 2. Example for a membership function for the category *Occurrence Probable* (OP).

Figure 2 shows a triangular-shaped membership function defined to represent the category OP on the interval [30×10^{-2}, 30×10^{-2}], and whose membership varies from 0 (non-membership) to 1 (full membership). When the probability of occurrence is 5×10^{-2}, it has a grade of membership equal to 1; when the probability of occurrence is 20×10^{-2}, it has a grade of membership equal to 0.4; when the probability of occurrence is 30×10^{-2}, it has a grade of membership equal to 0, and so on.

Formally, a fuzzy set $\widetilde{A}$ can be defined as a set of ordered pairs (2), where $\mu_A(x)$ is the "membership function" of x in the fuzzy set $\widetilde{A}$ (the degree that x belongs to $\widetilde{A}$). A letter U is called the *universe of discourse* and represents all the possible values for x [31]. This kind of fuzzy set is a standard or Type-1 fuzzy set [32,33] and is completely characterized by its membership function [34].

$$\widetilde{A} = \{(x, \mu(x))/x \in U\} \tag{2}$$

The membership function is considered a subjective representation of the human language [34,35]. It can be established using intuition or inference procedures, neural networks, genetic algorithms, soft partitioning, and other procedures found in the literature. In general, it is always preferable that the membership function represents the expert knowledge for a particular application if this knowledge is available.

In the context of FMECA, the three risk factors (S, O, and D) can also be represented in fuzzy terms as *linguistic variables* [35]. For example, linguistic values such as "Remote", "High", or "Moderate" can be used to define the occurrence, O, instead of using numerical values.

In a mathematically formal way, a *quintuple represents a linguistic value* $(x, T(x), U, G, M)$, where x is the variable, $T(x)$ is the term-set of x (collection of linguistic values for x), U is the universe of discourse for x (all possible values of x), G is a *syntactic rule* for generating terms $T(x)$, and M is a *semantic rule* that associates each linguistic value with is meaning $M(x)$, where $M(x)$ is a fuzzy set in U [35].

3.2. Fuzzy Membership Functions

The membership functions characterize the fuzziness in a fuzzy set. Usually, membership functions can be represented by mathematical formulae. The most common membership functions are the triangular and trapezoidal membership functions. The *triangular membership function* (tri), denoted by $tri(x; a, b, c)$, is specified by the following three parameters as shown in Equation (4) [34]:

$$tri(x; a, b, c) = \begin{cases} 0, & x < a \\ (x-a)/(b-a), & a \le x \le b \\ (c-x)/(c-b), & b \le x \le c \\ 0, & x > c^{+} \end{cases} \tag{3}$$

The *trapezoidal membership function* (trap), denoted by $trap(x; a, b, c, d)$, is specified by four parameters, as shown in the Equation (4) [34].

$$trap(x; a, b, c, d) = \begin{cases} (x-a)/(b-a), & a \le x \le b \\ 1 & b \le x \le c \\ (d-x)/(d-c), & c \le x \le d \\ 0, & otherwise \end{cases} \tag{4}$$

The two functions (3) will be used to represent the FMECA risk factors.

3.3. Fuzzy If-Then Rules

In fuzzy logic, approximate reasoning refers to a mode of reasoning in which the input-output relation of a system is expressed as a collection of fuzzy IF-THEN rules where the preconditions and consequents involve linguistic variables [31,34]. The fuzzy if-then rule is also known as a *fuzzy rule*, *fuzzy implication*, or *fuzzy conditional statement* [34].

A general structure of if-then rules is "IF x is A THEN y is B", where the expression "x is A" is called the antecedent or premise, and the expression "y is B" is called the consequent or conclusion [34]. Fuzzy if-then rules can be explained in detail using the context of fuzzy relations, but because this work is not a treatise on fuzzy relations, this topic was not covered in this section. An example in the FMECA context would be a fuzzy if-then rule associated with a particular failure mode expressed as follows:

IF (Severity **is** *hazardous*) **AND** (Occurrence **is** *remote*) **AND** (Detection **is** *high*) **THEN** (RPN **is** *moderate*).

The terms *hazardous*, *remote*, and *high* are fuzzy categories related to Severity, Occurrence, and Detection, respectively. *Moderate* is a fuzzy category related to the risk priority number (RPN). Usually, fuzzy rules are defined by a group of experts or using artificial intelligence mechanisms. In our context, one considers that the rule's antecedent is composed of the combination of the three risk factors, each represented linguistically by a fuzzy set.

3.4. Fuzzy Inference Systems

The *fuzzy inference system* (FIS) is a computational framework that formulates input/output mappings through fuzzy if-then rules and fuzzy reasoning mechanisms. The FIS consists of the following three stages, as shown in Figure 3 [34]:

- The input processing stage is called fuzzification, where the input variables are transformed into fuzzy sets;
- The reasoning mechanism, which performs the inference procedure based on the predefined fuzzy rules and the selected fuzzy inference mechanism to derive a reasonable output or conclusion and;
- In the output processing stage, defuzzification transforms the fuzzy sets resulting from the reasoning mechanism into a crisp value.

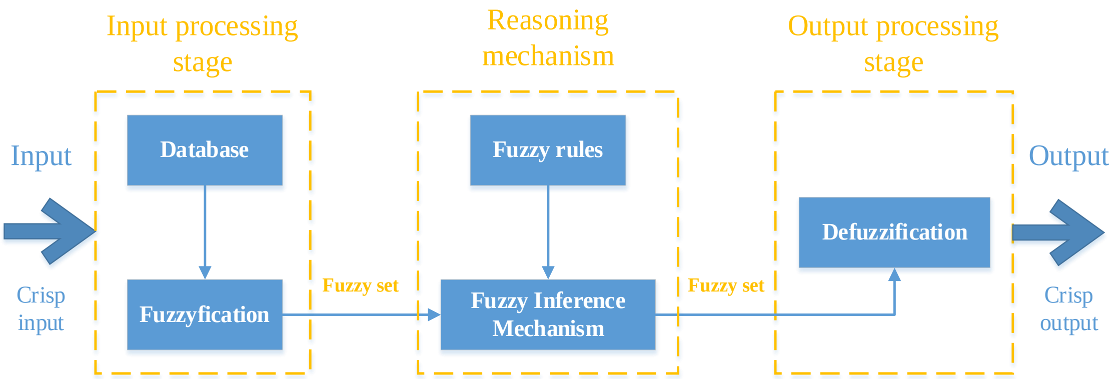

Figure 3. Type-I fuzzy inference system block diagram adapted from [34].

The inputs of a FIS can be either fuzzy or numerical values. In fuzzy logic, the numerical values are called *crisp* and can be represented as a fuzzy singleton function [31,34]. There are the following two main fuzzy inference systems: the Mamdani FIS and Takagi-Sugeno FIS [31,34]. To explain the fuzzy inference system block diagram shown in Figure 3, in the next paragraphs, we detail the Mamdani fuzzy inference system depicted in Figure 4 with the following two fuzzy rules:

$$\begin{aligned}
&\text{Rule1}: \text{ If } (x_{11} \text{ is } A_{11}) \textbf{ AND } \text{If } (x_{12} \textbf{ is } A_{12}) \textbf{ THEN } (z_1 \textbf{ is } C_1), \\
&\text{Rule2}: \text{ If } (x_{21} \text{ is } A_{21}) \textbf{ AND } \text{If } (x_{22} \textbf{ is } A_{22}) \textbf{ THEN } (z_2 \textbf{ is } C_2),
\end{aligned}$$

where the operator AND is represented by the *min(•)* (T-norm), the implication operator THEN is represented by the *min(•)* (T-norm), the aggregate operator is represented by *max(•)* (T-conorm), and the defuzzification is obtained by the *centroid of the area* (COA).

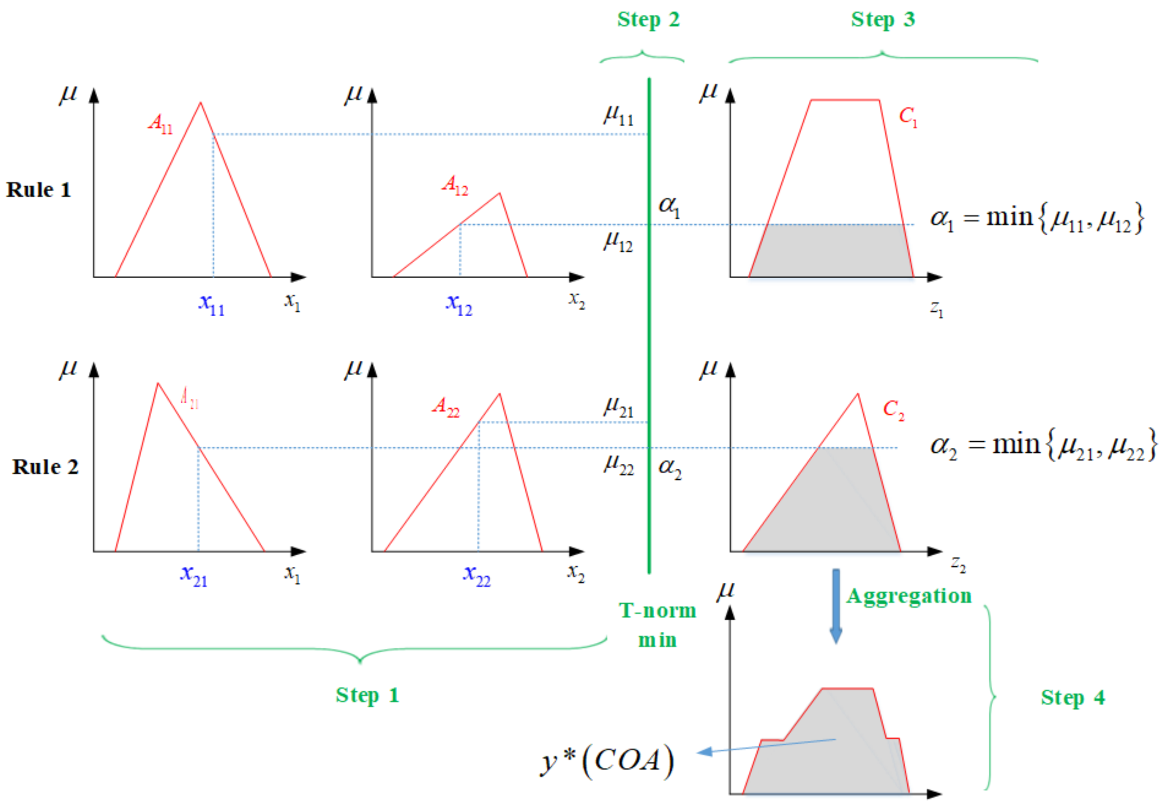

Figure 4. Structure of the Mamdani fuzzy inference system (adapted from [34]).

The Mamdani FIS shown in Figure 4 comprises the following steps that represent the fuzzy inference system stages depicted in Figure 3 [34]:

- *Step 1*: Obtain the membership value for each input variable in the antecedent part of the fuzzy rule. In the example of Figure 4, for Rule 1, the membership value for the input x_{11} in the fuzzy set A_{11} is μ_{11}, and the membership value for the input variable x_{12} in the fuzzy set A_{12} is μ_{12}. The same analysis is valid for rule 2. This step is known as *fuzzification,* and the membership functions can be specially defined for the application or taken from a database; this step represents the Input Processing Stage depicted in Figure 3.

The reasoning mechanism shown in Figure 3 comprises the fuzzy rules and the fuzzy inference mechanism. This stage is conducted in the following two steps, the combination of membership values detailed in step 2 and the consequent generation detailed in step 3:

- *Step 2*: Combine the membership values on the antecedent part of each rule through a specific fuzzy operator, usually the *minimum* min(•) operator or the *maximum* max(•) operator, to obtain a fuzzy rule's weight (called *firing strength*). This step is equivalent to using the AND operator or the OR operator in Boolean logic. If the result of the combination is greater than zero, the rule is "fired," and its consequent will be computed using this *firing strength*. In the example of Figure 4, the operator *min(•)*, equivalent to the Boolean operator AND, is used to obtain the minimal value between μ_{11} and μ_{12}, resulting in the rule 1 firing strength α_1. The same analysis is valid for rule 2;
- *Step 3*: Generate the qualified consequents of each rule by weighting each consequent fuzzy set with the firing strength obtained in step 2. This step is equivalent to the implication (THEN) in Boolean logic. In the example of Figure 4, the fuzzy output rule 1 is weighted by the firing strength α_1. The implication operator, usually the *min* operator, truncates the consequent's fuzzy set at the α_1 value, obtaining the shaded area in set C1. The same analysis is valid for rule 2.

The output processing stage shown in Figure 3 corresponds to the conversion of the fuzzy consequent determined in step 3 into a crisp value:

- *Step 4*: Aggregate all the qualified consequents to produce the FIS fuzzy output, then this output is defuzzified to obtain the final crisp output. The aggregation process combines all rule's consequents to obtain a single fuzzy set through an *aggregation* operator, usually the operator *max(•)*. Defuzzification is the process of extracting a crisp representative value from a fuzzy set. This work considers the *centroid of the area, COA,* because it is the most popular defuzzification method [34]. In Figure 4, the application of the operator *max(•)* between the rule's outputs produces the shaded area, and the application of the operator COA produces the FIS crisp output $y*$.

3.5. FMECA Risk Factors Expressed in Fuzzy Terms

As stated in Section 1, the risk categories in the classical FMECA are represented by an integer numerical scale, being the most used on the 1–10 scale and the 1–5 scale. The selected scale usually determines the number of risk categories associated with each risk factor.

In this work, one considered the "seven plus or minus two" criterion defined by Miller in [33] to establish the number of fuzzy membership functions to each risk factor. According to Miller, the limit of the information processing capacity of human memory is seven units of information simultaneously, more or less two pieces of information. In [36], the authors used the Miller criterion to support their decision to fix the number of membership functions associated with a specific fuzzy category. Although the authors state that they do not have sufficient theoretical arguments to support their selection, they concluded that their decision to assign eight membership functions (seven plus one) is simple enough to be understood by the decision-maker and analyzed by the fuzzy system. Following this logic, we have selected five membership functions (exactly seven minus two terms) to represent the fuzzy categories associated with each risk factor.

FMECA must be conducted by human experts, who assign an integer value from 1 to 10 for each risk factor. Following, one considers the universe of discourse for each risk factor as the interval $U = [1, 10]$. The three risk factors (*Severity* S, *Occurrence* O, *Detection* D, and the *risk priority number* RPN) will be represented by fuzzy variables.

Regarding *Severity*, we consider the following assumptions:

- The Severity categories are as follows: Severity Minor (SMI), Severity Low (SL), Severity Moderate (SM), Severity Very High (SVH), and Severity Hazardous (SH);
- The term-set for Severity T(S) is as follows: $T(S) = \{$SMI, SL, SM, SVH, SH$\}$;
- The semantic rule M for the term set for Severity $T(S)$ is shown in Table 1.
- Regarding Occurrence, we consider the following assumptions:
- The Occurrence categories are the following: Occurrence Remote (OR), Occurrence Very Unlikely (OVU), Occurrence Occasional (OO), Occurrence Probable (OR), and Occurrence Frequent (OF);
- The term-set for Occurrence T(O) is as follows: $T(O) = \{$OR, OVU, OO, OP, OF$\}$;
- The semantic rule M for $T(O)$ is shown in Table 2.

Table 1. Semantic rules for term-set *Severity*.

Semantic Rule	Fuzzy Subset
M(SMI)	The effect of the failure mode is considered *Minor* when assessed as 1
M(SL)	The effect of the failure mode is considered *Low* when assessed between 2 and 3
M(SM)	The effect of the failure mode is considered *Moderate* when assessed between 4 and 6
M(SVH)	The effect of the failure mode is considered *Very High* when assessed between 7 and 8
M(SH)	The effect of the failure mode is considered *Hazardous* when assessed between 9 and 10

Table 2. Semantic rules for term-set *Occurrence*.

Semantic Rule	Fuzzy Subset
$M(\text{OR})$	The occurrence of the failure mode is considered *Remote* when assessed as 1
$M(\text{OVU})$	The occurrence of the failure mode is considered *Very Unlikely* when assessed between 2 and 3
$M(\text{OO})$	The occurrence of the failure mode is considered *Occasional* when assessed between 4 and 6
$M(\text{OP})$	The occurrence of the failure mode is considered *Probable* when assessed between 7 and 8
$M(\text{OF})$	The occurrence of the failure mode is considered *Frequent* when assessed between 9 and 10

Regarding the *Detection*, we consider the following assumptions:

- The categories for Detection are as follows: Detection Almost Certain (DAC), Detection High (DH), Detection Moderate (DM), Detection Low (DL), and Detection Absolutely Impossible (DAI);
- The term-set for Detection T(D) is as follows: $T(D) = \{\text{DAC, DH, DM, DL, DAI}\}$;
- The semantic rule M for $T(D)$ is shown in Table 3 as follows:

Table 3. Semantic rules for term-set *Detection*.

Semantic Rule	Fuzzy Subset
$M(\text{DAC})$	The detection of the failure mode is considered *Almost Certain* when assessed as 1
$M(\text{DH})$	The detection of the failure mode is considered *High* when assessed between 2 and 3
$M(\text{DM})$	The detection of the failure mode is considered *Moderate* when assessed between 4 and 6
$M(\text{DL})$	The detection of the failure mode is considered *Low* when assessed between 7 and 8
$M(\text{DAI})$	The detection of the failure mode is considered *Absolutely Impossible* when assessed between 9 and 10

In the classical FMECA, the RPN results from the product of S, O, and D have a range from 1 to 1000. The RPN also can be divided into risk categories in the fuzzy reasoning context to implement the reasoning mechanism. Therefore, the range or universe of discourse does not necessarily need to be equal to the classical RPN. In this work, the universe of discourse for RPN is considered as $U = [1, 10]$ with the following assumptions:

- The categories for the RPN were defined as follows: *Risk Minor* (RMI), *Risk Low* (RL), *Risk Moderate* (RM), *Risk High* (RH), and *Risk Extreme* (RE);
- The term-set for RPN *T(RPN)* is as follows: $T(RPN) = \{\text{RMI, RL, RM, RH, RE}\}$;
- The semantic rule M for $T(RPN)$ is shown in Table 4.

Table 4. Semantic rules for term-set for *RPN*.

Semantic Rule	Fuzzy Subset
$T(\text{RMI})$	The overall risk of the failure mode is considered *Minor* when assessed around 1
$T(\text{RL})$	The overall risk of the failure mode is considered *Low* when assessed between 2 and 3
$T(\text{RM})$	The overall risk of the failure mode is considered *Moderate* when assessed between 4 and 6
$T(\text{RH})$	The overall risk of the failure mode is considered *Very High* when assessed between 7 and 8
$T(RE)$	The overall risk of the failure mode is considered *Hazardous* when assessed between 9 and 10

In the next section, we apply the fuzzy framework depicted before to represent and process the risk categories in a fuzzy-FMECA analysis. More specifically, we propose a methodology to apply fuzzy inference systems to prioritize the failure modes, which are then applied to a cyber-power grid.

4. Implementation

Figure 5 shows a flowchart describing the proposed fuzzy-FMECA approach. The flowchart is divided into the following two stages:

- *Stage 1*: The classical FMECA is accomplished first. As a result, one obtains the value of the three risk factors for each failure mode, the failure mode overall risk represented by the RPN computed through the Equation (1), and the failure modes ranking according to Section 1. The steps taken are shown in blue in Figure 5;
- *Stage 2*: This stage comprises the fuzzy-FMECA. Its steps are shown now in orange in Figure 5. The fuzzy database (composed of the fuzzy sets) and the fuzzy rules are constructed considering the expert criteria of the FMECA team members. Following, using the information of the fuzzy database, the risk factors (S, O, D, and RPN) are fuzzified. The fuzzy risk factors and the fuzzy rules are the input for the fuzzy inference mechanism. Once the inference mechanism is executed, the fuzzy RPN and the failure mode's ranking are obtained.

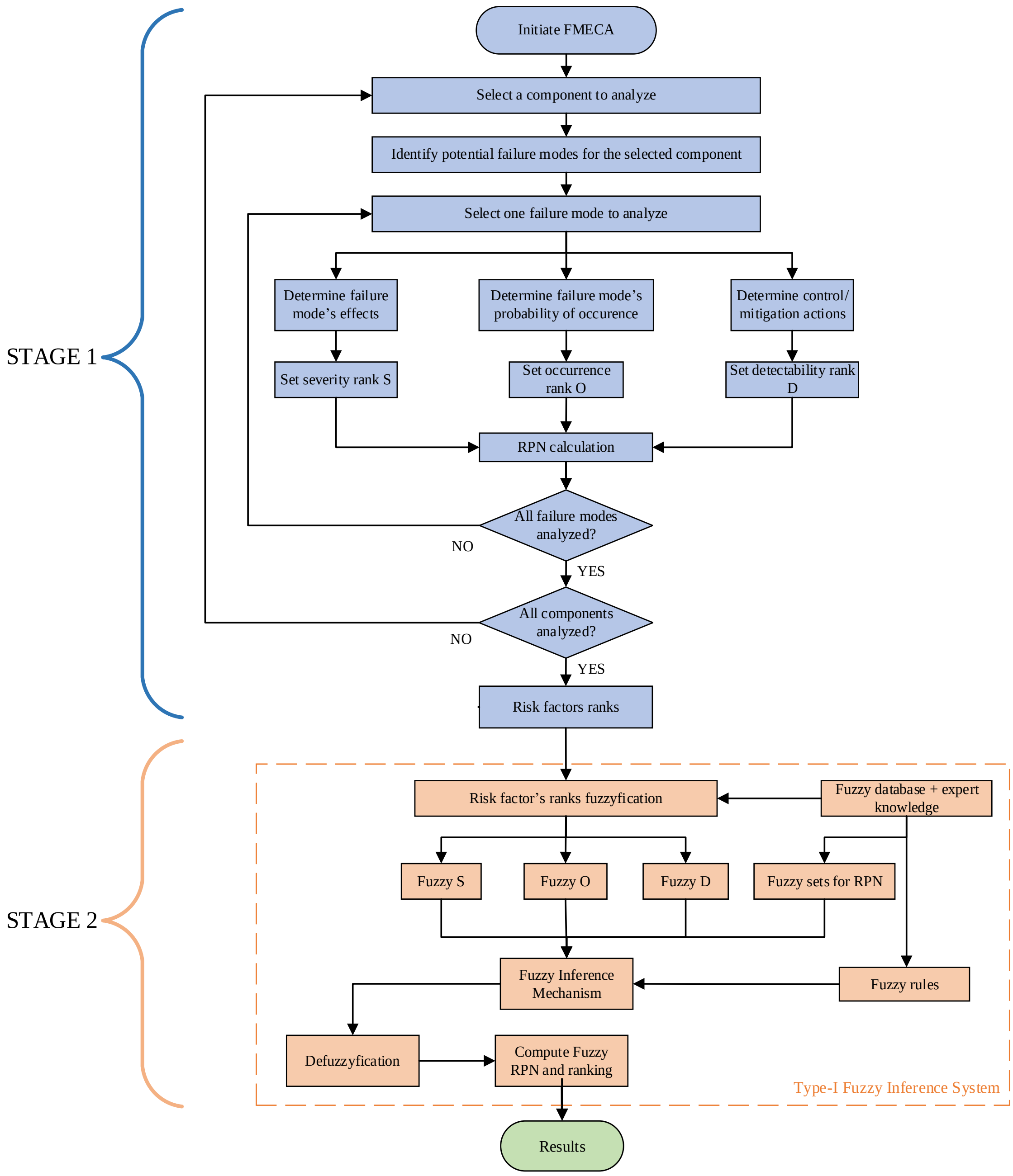

Figure 5. Flowchart for the proposed FMECA approach based on fuzzy systems.

To maintain the essence of the classical FMECA and for comparison purposes, we consider the rating for each risk factor as an integer number, resulting from the FMECA team members' consensus.

4.1. Fuzzy Categories for the FMECA Risk Factors

As stated in Section 3.5, the FMECA risk factors are assessed using integer numbers on a numerical scale from 1 to 10. This work considers five membership functions for each risk factor and the fuzzy RPN. Table 5 shows the proposed categories and their respective ratings. For example, when the rating for *Severity* is 4, 5, or 6, it belongs to the category *severity moderate* SM. The next section shows the proposed fuzzy membership functions used to represent each risk category in Table 5.

Table 5. Ratings for risk categories used as in the classical FMECA.

Severity (*S*)	Occurrence (*O*)	Detection (*D*)	FuzzyRPN [1]	Rating
Hazardous—SHA	*Frequent*—OF	*Absolutely impossible*—DAI	*Extreme*—RE	9, 10
Very High—SVH	*Probable*—OP	*Low*—DL	*High*—RH	7, 8
Moderate—SM	*Occasional*—OO	*Moderate*—DM	*Moderate*—RM	4, 5, 6
Low—SL	*Very unlikely*—OVU	*High*—DH	*Low*—RL	2, 3
Minor—SMI	*Remote*—OR	*Almost Certain*—DAC	*Minor*—RMI	1

[1] FuzzyRPN (Fuzzy Risk Priority Number) resulting from defuzzification is not always an integer number, and its value falls inside the limits of the corresponding rating.

The fuzzy risk priority number (FuzzyRPN) included in Table 5 results from defuzzification is not always an integer number, and its value falls inside the limits of the corresponding rating.

4.2. Membership Functions for the FMECA Risk Factors

The use of membership functions to represent the risk categories allows for the inclusion of the vagueness associated with the natural language used by the FMECA team members to classify the failure modes. While the classic FMECA considers strict membership for each category, the fuzzy-FMECA is flexible, and ratings may belong to two risk categories simultaneously with different membership values.

This work uses the following two widely-used membership functions: triangular and trapezoidal; the FMECA team members selected these functions for their parameterization simplicity. To parameterize the membership functions, we considered the criteria of the FMECA team members who performed the FMECA analysis presented in [12]; they set the central point, limits, slope, and the overlapping of the functions. Table 6 shows the parameters for the triangular membership functions that represent the risk factors' *Occurrence* and *Detectability*. Figure 6 shows their shapes.

Table 6. Type-I triangular membership functions for the FMECA risk factors.

Category	Occurrence	Detection
1	tri(x; 0,1.5,2.5)	tri(x;0,1.5,2.3)
2, 3	tri(x; 0.8,2.8,4.2)	tri(x;1.1,2.9,4.5)
4, 5, 6	tri(x; 3.2,5.4,7.4)	tri(x;2.5,5.0,7.5)
7, 8	tri(x; 6.4,7.5,9.6)	tri(x;4.8,7.5,10.4)
9, 10	tri(x; 8.7,9.3,11.4)	tri(x;7.6,9.3,12.4)

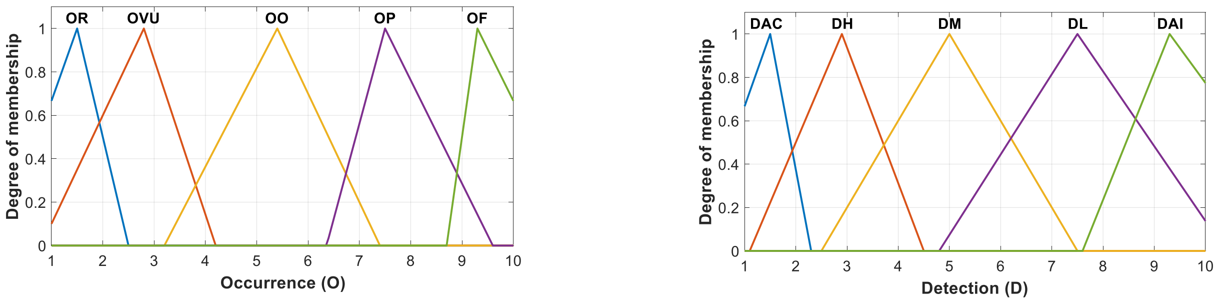

Figure 6. Triangular type-I FIS membership functions for the FMECA risk factors occurrence and detectability.

To parametrize the triangular membership functions were considered the following assumptions:

- The functions' shapes are non-symmetrical to allow different overlapping levels between categories;
- The triangular membership function OR has the lower limit at O = 0 and the upper limit at O = 2.5; the maximum membership value occurs at O = 1.5;
- The triangular membership function OVU has the lower limit at O = 0.8 and the upper limit at O = 4.2; the maximum membership value occurs at O = 2.8, that is, at the mid-point of its respective interval;
- Categories OR and OVU are superposed. When a failure mode's severity is rated as 1, we can say that it belongs to category OR with membership 0.667 and, simultaneously, to category OVU with membership 0.1. When a failure mode's occurrence is rated as 2, we can say that it belongs to category OR with a membership of 0.50, and at the same time, it belongs to category OVU with a membership of 0.60. The simultaneous membership of a particular failure mode into two different categories shows the flexibility of the system to represent the vagueness associated with the risk perception of the members of the FMECA team;
- The membership functions for detection were parametrized following the abovementioned criteria.

Table 7 shows the parameters for the trapezoidal membership functions to represent the risk factors *Severity* and *FuzzyRPN*, and Figure 7 shows their shapes.

Table 7. Type-I trapezoid membership functions for the FMECA risk factors.

Category	Severity	FuzzyRPN
1	trap(x; 0.1,0.6,1.5,2.4)	trap(x; 1.0,1.0,1.6, 2.5)
2,3	trap(x;0.9,2.0,3.0,3.5)	trap(x; 1.0,2.4,3.2,4.1)
4,5,6	trap(x;2.7,4.0,5.0,7.8)	trap(x;2.9,4.2,5.5,7.6)
7,8	trap(x;5.1,7.0,8.0,9.5)	trap(x;5.5,7.0,8.0,9.5)
9,10	trap(x;7.6,9.0,10.0,12.2)	trap(x;7.67,9.06,10,10)

To parametrize the trapezoidal membership functions were considered the following assumptions:

- Most functions are shaped as non-symmetrical to allow different overlapping levels between categories;
- The trapezoidal membership function SMI has the lower limit at S = 0 and the upper limit at S = 2.4; the maximum membership value occurs between S = 1 and S = 1.5;
- The trapezoidal membership function SL has the lower limit at S = 0.9 and the upper limit at S = 3.5; the maximum membership value occurs between S = 2 and S = 3;
- Categories SMI and SL are superposed. When a failure mode's severity is rated as 1, we can say that it belongs to category SMI with the maximum membership of 1.0 and, at the same time, it belongs to category SL with a membership of 0.09. When a

failure mode's severity is rated as 2, we can say that it belongs to category SM with the maximum membership of 1.0 and, at the same time, it belongs to category SL with a membership of 0.44;

- The membership functions for the *FuzzyRPN* consider the full membership around the mid-point of each category; as an example, for the risk category RM with limits between 4 and 6, the full membership is achieved when resulting fuzzy RPN are computed between 4.2 and 5.5, and for the risk category RH the full membership is achieved when the resulting RPN are computed between 7 and 8.

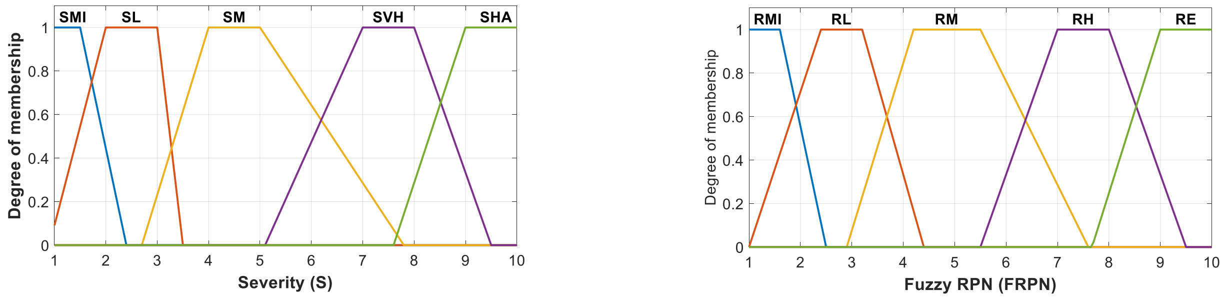

Figure 7. Trapezoidal type-I FIS membership functions for the FMECA risk factors *Severity* and *FuzzyRPN*.

4.3. Fuzzy If-Then rules for the Proposed Approach

The fuzzy rules used in this work were defined by the same team that conducted the classical FMECA analysis shown in [12], considering the combination of the five risk factor categories (the five membership functions) as premises. The respective consequent was then selected from the FuzzyRPN categories. The resulting 125 fuzzy rules are listed in Appendix A.

4.4. Operations for the Type-I Fuzzy Inference System

We select the same logical operators used for the Mamdani FIS example of Section 3.4. They are as follows:

- "AND" method—**min**;
- "IMPLICATION" method—**min**;
- "AGGREGATION" method—**max**;
- Defuzzification—**COA**;

5. Application of the Fuzzy-FMECA Approach to a Cyber-Power Grid

5.1. Cyber-Power Grid Test System

The proposed fuzzy-FMECA approach was applied to the cyber-power grid test system shown in Figure 1 and was previously used by these authors in [12]. The system comprises a four-bus 30 kV power system and a cyber network for monitoring and management. The main equipment considered was the busbar, cable, circuit breaker (CB), transformer, human-machine interface (HMI), switch (SW), intelligent electronic device (IED), and optical fiber.

One hundred and seven (107) *failure modes* (FM) were initially identified, but only the 42 riskiest failure modes were selected for further analysis, as listed in Table 8. It shows the classical FMECA worksheet for the cyber-power grid test system, where the values for each risk factor *S*, *O*, and *D* were considered obtained from the consensus of the FMCEA team members. This set will also be used as inputs for the proposed fuzzy-FMECA approach. Table 8 also shows the RPN value and the rank achieved for each failure mode.

Table 8. Classical FMECA applied to the cyber-power grid test system shown in Figure 1 (based on [12]).

Failure Mode	Equipment	Failure Mode(s)	*S*	*O*	*D*	RPN	Rank
FM01	Busbar	Loss of structural integrity	7	5	9	315	9
FM02	Busbar	Loss of structural integrity	7	6	9	378	3
FM03	Busbar	Loss of structural integrity	7	5	9	315	10
FM04	Busbar	Loss of electrical continuity	8	4	10	320	6
FM05	Busbar	Electrical disturbances	8	4	10	320	7
FM06	Bus-bar	Electrical disturbances	8	4	8	256	17
FM07	Cable	Cable integrity defect	8	7	5	280	15
FM08	Cable	Electrical operation failure	6	6	10	360	4
FM09	CB	Insulation failure	6	5	7	210	26
FM10	CB	Wrong operation	7	6	4	168	37
FM11	CB	Bushing breakdown	6	5	10	300	11
FM12	CB	Bushing terminal hot spot	6	4	8	192	29
FM13	CB	CB contacts degradation	6	5	9	270	16
FM14	Transformer	Bushing breakdown	6	4	10	240	22
FM15	Transformer	Bushing terminal hot spot	6	4	7	168	39
FM16	Transformer	Magnetic-core delamination	6	4	7	168	38
FM17	Transformer	Winding overheating	7	6	7	294	14
FM18	Transformer	Tap changer contacts degradation	6	3	9	162	40
FM19	Transformer	Tank rupture	8	3	9	216	23
FM20	Transformer	Winding isolation degradation or breakdown	6	4	10	240	21
FM21	Transformer	Distortion, loosening, or winding displacement	7	5	9	315	8
FM22	Transformer	Transformer explosion	9	5	10	450	1
FM23	Transformer	Cooling system failure	8	3	7	168	36
FM24	HMI	Operational failure	5	5	10	250	19
FM25	HMI	Security failure	9	2	10	180	33
FM26	SW	Performance decreased	6	7	6	252	18
FM27	SW	Operational failure (Switch blackout)	6	6	10	360	5
FM28	SW	Operational failure (Switch blackout)	6	5	10	300	13
FM29	SW	Network/Cyber storm	6	4	7	168	35
FM30	SW	Power outage	6	3	10	180	34
FM31	SV	Data errors	6	5	10	300	12
FM32	SV	Power outages	7	3	10	210	25
FM33	SV	Security failure	10	2	10	200	28
FM34	IED	Communication failure	6	5	8	240	20
FM35	IED	Communication failure	6	4	8	192	30
FM36	IED	Communication Failure	6	5	7	210	27
FM37	IED	Monitoring failure	6	5	6	180	32
FM38	IED	Control failure	8	7	7	392	2
FM39	IED	Power outages	7	3	10	210	24
FM40	IED	Security failure	9	3	7	189	31
FM41	Optical fiber	Fracture	4	3	10	120	41
FM42	Optical fiber	Humidity induced	4	3	10	120	42

5.2. Membership Functions for the FIS Implemented

We propose a fuzzy inference system for application in cyber-power grids that considers triangular and trapezoidal membership functions as detailed in Section 4.2. Table 9 shows the FIS configuration to test the proposed fuzzy-based FMECA approach.

Table 9. Membership functions for the tested FIS configuration.

Configuration	MF Severity	MF Occurrence	MF Detection	MF Fuzzy RPN
FIS	Trapezoidal	Triangular	Triangular	Trapezoidal

It considers trapezoidal membership functions for *Severity* and the FRPN and triangular membership functions for the *Occurrence* and *Detection* risk factors.

Table 5 identified that the risk level *Severity Minor* (SMI) has the lowest *Severity* category. It could represent an additional uncertainty source for the FMECA team. For this reason, one chose a trapezoidal function to represent it (see Figure 7), where *Severity* values between 1 and 1.5 correspond to full membership of their respective category. We consider full membership to the category *Severity Low* (SL) for ratings between its lower limit $S = 2$ and its upper limit $S = 3$. For the category *Severity Very High* (SVH), we considered full membership for ratings between $S = 4$ and $S = 6$, and for the category *Severity Hazardous* (SHA), we assigned full membership for ratings between $S = 9$ and $S = 10$.

The risk category *Severity Moderate* (SM) shows how fuzzy systems allow modeling the criteria elaborated by the FMECA team members. As detailed in Table 5, failure modes classified as 4, 5, or 6 belong to that category level named *Severity Moderate* (SM). However, we propose that failure modes classified between 4 and 5 must have full membership in the fuzzy category SM, and failure modes classified as 6 have a membership of 0.6428. The three ratings (4, 5, and 6) still belong to category SM but with different membership values.

The previous-mentioned criteria were also used to select the membership functions for the FuzzyRPN, as shown in Figure 7. In this work, the value of FRPN is computed as the centroid of the area (COA) of the membership function resulting from the fuzzy inference mechanism. So, the FuzzyRPN it is not always an integer number such as the risk factors ratings.

To represent more certainty around the midpoint of each risk category, notice that we used trapezoidal membership functions with the following characteristics: FRPN between 1 and 1.5 have full membership in the category *Risk Minor* (RMI), FRPN between 2.4 and 3.2 have full membership in category *Risk Low* (RL), FRPN between 4.2 and 5.5 have full membership in category *Risk Moderate* (RM), FRPN between 7 and 8 have full membership in category *Risk High* (RH), and FRPN between 9 and 10 have full membership in category *Risk Extreme* (RE).

6. Results and Discussion

This section shows the results of applying the FIS configuration shown in Table 9. Table 10 begins listing the 42 failure modes. It shows the classical RPN results and associated rank in two gray columns. Aside, one shows, for the same inputs, the fuzzy-FMECA results by its FRPN values and the new rank order.

To have a general overview of the ranks obtained with the two FMECA methodologies, Figure 8 shows a radar chart displaying the classical FMECA (red line) and the proposed fuzzy-FMECA (orange line). The radial axes represent the 42 failure modes, and the concentric circles represent the ranking. This kind of chart greatly simplifies the comparison between the FMECA rankings for small problems. Moreover, one can quickly detect failure modes with significant priority changes; for example, FM42 appears ranked as priority 42 by the classical FMECA (orange line) and ranked as priority 27 by the fuzzy-FMECA (blue line), or FM38 ranked as 2 by the classical FMECA and downgraded to priority 16 by the fuzzy-FMECA (orange line).

In the next sections, one conducts a detailed analysis of the results obtained for the fuzzy-FMECA compared with those from the classical FMECA. The following two situations need analysis and discussion: differences are higher concerning the prioritization rank for the riskiest failure modes, and the second analysis must analyze the failure modes with the same FRPN and what this means.

6.1. Classical FMECA $\times$ Fuzzy-FMECA: Higher Differences in Prioritization for the Riskiest Failure Modes

Table 11 summarizes the top ten failure modes (FM) indicated by the classical FMECA ranking (gray color column) and indicated by the fuzzy-FMECA ranking. According to the classical FMECA, the riskiest failure mode corresponds to FM22—transformer explosion by an internal short circuit. This failure mode was also ranked priority 1 by the fuzzy-FMECA.

Table 10. Rankings and risk priority number for the classical and the fuzzy-FMECA.

Failure Mode	Classic RPN	Classic Rank	FIS FRPN	FIS Rank
FM01	315	9	8.216	4
FM02	378	3	8.138	7
FM03	315	10	8.216	5
FM04	320	6	8.325	2
FM05	320	7	8.325	3
FM06	256	17	7.760	15
FM07	280	15	7.556	19
FM08	360	4	7.872	9
FM09	210	26	6.831	34
FM10	168	37	5.819	42
FM11	300	11	7.872	10
FM12	192	29	7.041	28
FM13	270	16	7.872	11
FM14	240	22	7.226	22
FM15	168	39	5.974	39
FM16	168	38	5.974	40
FM17	294	14	6.860	33
FM18	162	40	6.329	37
FM19	216	23	7.688	17
FM20	240	21	7.226	23
FM21	315	8	8.216	6
FM22	450	1	8.679	1
FM23	168	36	6.906	31
FM24	250	19	7.500	21
FM25	180	33	7.529	20
FM26	252	18	6.779	36
FM27	360	5	7.872	12
FM28	300	13	7.872	13
FM29	168	35	5.974	41
FM30	180	34	7.001	30
FM31	300	12	7.872	14
FM32	210	25	7.049	24
FM33	200	28	8.048	8
FM34	240	20	7.675	18
FM35	192	30	7.041	29
FM36	210	27	6.831	35
FM37	180	32	6.047	38
FM38	392	2	7.736	16
FM39	210	24	7.049	25
FM40	189	31	6.906	32
FM41	120	41	7.049	26
FM42	120	42	7.049	27

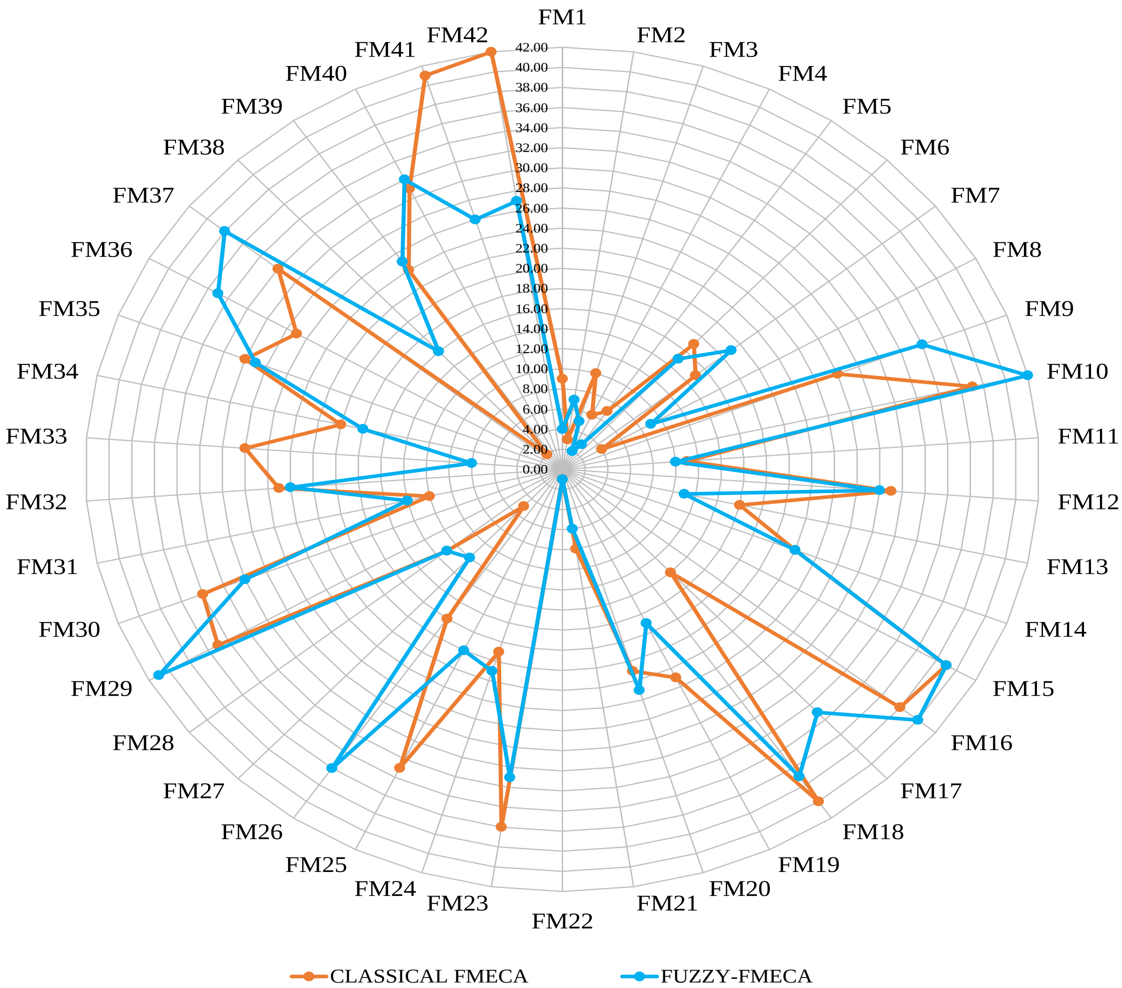

Figure 8. Radar chart showing the ranking for the classical FMECA ranking (red line) and the ranking for the fuzzy-FMECA proposed (blue line).

In this case, the *Severity* factor was rated as SHA (Severity Hazardous), and the *Detection* factor was rated as DAI (Detection Almost Impossible). Both risk factors were then considered the highest risk category. The *Occurrence* factor was rated as Occasional (OO) with O = 5 at the mid-point of the *Occurrence* interval (from 1 to 10). The risk perception for this failure mode is that it should be somewhat risky because two of the three risk factors were classified as somewhat risky in their respective categories. Concerning the failure mode FM38 in Table 11, the IED control failure was ranked as priority 2 by the classical FMECA. However, the fuzzy-based FMECA significantly decreased its priority to 16, as shown in Figure 8. Let us then analyze what caused this substantial difference. The classical RPN for FM38 is obtained using the single arithmetic product between $S = 8$, $O = 7$, and $D = 7$, giving an RPN = 392. Now, based on the membership functions established by the experts' team, Table 5 points that $S = 8$ belongs to the risk category *Severity Very High* (SVH) that $O = 7$ belongs to an *Occurrence Probable* (OP), and that $D = 7$ belongs to the risk category of *Detection Low* (DL). Unlike the crispy RPN, the FuzzyRPN was achieved from a more enlarged procedure. According to the fuzzy sets shown in Figures 6 and 7 that the FMECA team members defined, the rating $S = 8$ means that the failure mode can be considered simultaneously as being *Severity Very High SVH* with membership 1 and also as *Severity Hazardous SHA* with membership 0.2857. The rating $O = 7$ means that the failure mode can be considered simultaneously having an *Occurrence Occasional* (OO) with a membership of 0.2 and an *Occurrence Probable* (OP) with a membership of 0.5614. The rating $D = 7$ means that the failure mode can be considered as *Detection Moderate* (DM) with a membership of 0.2 and *Detection Low* (DL) with a membership of 0.8088.

Table 11. Comparison between the top ten classical FMECA rankings and those obtained using the proposed fuzzy-based FMECA.

Id	Equipment	Failure Mode	Failure Causes	Failure Effects	S	O	D	FMECA Rank	Fuzzy Rank
FM22	Transformer	Transformer explosion	Internal short circuit	Serious damage in the substation; personnel injuries or death	9	5	10	1	1
FM38	IED	Control failure	Defective data processing (software error)	Inability to control power system operation	8	7	7	2	16
FM02	Bus bar	Loss of structural integrity	Break of the support insulators	Bus bar break; no electrical connection	7	6	9	3	7
FM08	Cable	Electrical operation failure	Short circuits transients	Excessive heat (saturation)	6	6	10	4	9
FM27	SW	Operational failure (SW blackout)	SW is locked up	Incorrect SW function or SW malfunction	6	6	10	5	12
FM04	Bus bar	Loss of electrical continuity	Arc flash	Degradation of the physical structure	8	4	10	6	2
FM05	Bus bar	Electrical disturbances	Short circuits between bus bars	Short circuits	8	4	10	7	3
FM21	Transformer	Distortion, loosening, or displacement of the winding	Short circuits	Internal short circuits; transformer damage	7	5	9	8	6
FM01	Busbar	Loss of structural integrity	Fracture of the Cooper bar	Bus bar break; no electrical connection	7	5	9	9	4
FM03	Busbar	Loss of structural integrity	Cracking of connection welds	Bus bar break; no electrical connection	7	5	9	10	5

Figure 9 shows the "fired" fuzzy rules and the fuzzy inference mechanism for failure mode FM38. The fuzzy rules represent the FMECA team members' risk perception regarding the risk factors previously assessed for each failure mode. The ratings for failure mode FM38 (*Severity* $S = 8$, *Occurrence* $O = 7$ and *Detection* $D = 7$) activated the following eight fuzzy rules:

Rule 88: If (S is SVH) and (O is OO) and (D is DM,) then (RPN is RH)
Rule 89: If (S is SVH) and (O is OO) and (D is DL), then (RPN is RH)
Rule 93: If (S is SVH) and (O is OP) and (D is DM), then (RPN is RH)
Rule 94: If (S is SVH) and (O is OP) and (D is DL), then (RPN is RH)
Rule 113: If (S is SHA) and (O is OO) and (D is DM), then (RPN is RH)
Rule 114: If (S is SHA) and (O is OO) and (D is DL), then (RPN is RH)
Rule 118: If (S is SHA) and (O is OP) and (D is DM), then (RPN is RH)
Rule 119: If (S is SHA) and (O is OP) and (D is DL), then (RPN is RE)

The fuzzy sets of the risk factors and the eight fuzzy rules represent, respectively, the uncertainty and the logical reasoning of the FMECA team members. The classical RPN calculation does not include these human reasoning characteristics and their uncertainty. So, the fuzzy-FMECA combines them to produce the output. Notice that the failure mode FM04, loss of electrical continuity in busbar caused by arc flash, replaced the FM38 in priority 2. The severity for both failure modes is 8. The *Occurrence* weight to FM04 was 4. Despite being less than the *Occurrence* weight attributed to FM38 having been 7, the *Detection* factor of FM04 was 10, much higher than that attributed to FM38 being 7. In this case, the inference mechanism gave more relative importance to *Severity* and *Detection* factors when computing the FRPN due to its more defined memberships for higher values. As shown in Figure 9, rules 94 and 119 completely define the resulting FIS area, concluding that both rules completely explain the FRPN results. We consider that the new priority for FM04 is most appropriate considering the impact of the failure mode and the almost impossible chance of detecting it, as established by the FMECA experts.

Figure 9. Fired fuzzy rules and associated fuzzy RPN (Centroid) for the FM38—IED control failure by defective data processing ("software error").

The FMECA team members consider that the severity and detection of failure mode FM01, caused by fracture of the cooper bar, have high values (7 and 9, respectively). The classical FMECA classified FM01 as priority 9, but the fuzzy-FMECA assigned it priority 4, replacing the failure mode FM08 “electrical operational failures in cables caused by transient short circuits”. We consider that fuzzy-FMECA risk priority is more appropriate because it ponders the strong impact and the low detection of FM01 and because a busbar failure impact can be more significant than a cable failure impact.

Another busbar-type failure mode, the FM03 “loss of structural integrity of busbar caused by cracking of connection welds”, has the same severity, occurrence, and detection as FM01. Classical FMECA ranked FM03 as priority 10, but fuzzy-FMECA increased its classification to 5, replacing the failure mode FM27, "switch operational failure by locked up"; this priority change is evident in Figure 8. As in the previous analysis, we consider the new ranking appropriate because the causes of failure mode FM03, its impact, and low detectability increase the overall failure mode risk.

In addition, a busbar failure directly affects the system operation and can affect its integrity; instead, an ethernet switch failure comprises the system’s remote communication and control, but the grid can continue functioning using the local control and monitoring functions.

Regarding busbar failure mode FM02 “loss of structural integrity of busbar caused by break of the support insulators,” the classical FMECA ranked it as priority three, while the fuzzy-FMECA decreased its classification to 7, replacing FM05. In the same way, the classical FMECA ranked the failure mode FM05 “electrical disturbances caused by short circuits between busbars,” as priority 7, while the fuzzy-FMECA ranked it as priority 3, replacing FM02. FM02 has its Severity classified as 7, the occurrence classified as 6, the Detection classified as 9, and the RPN equal to 378; FM05 has its Severity rated as 8, the Occurrence rated as 4, the Detection rated as 10, and the RPN is equal to 320. Although the RPN for FM02 is higher than the PRN for FM05, the risk perception of FM05 is different. FM05 has a higher Severity and Detection than FM02, while the Occurrence of FM02 is higher than FM05. The impact of both failures on the system is significant; however, the perception of risk represented by severity and detection is higher for FM05, although FM02 can occur more frequently. From the previous analysis, we consider that fuzzy-FMECA more appropriately ranked the failure mode FM05 as priority 3 instead of FM02 because the fuzzy inference system allows it to better represents the FMECA team members’ risk perception.

It is clear that all failure modes associated with busbars had their priority augmented by the fuzzy-FMECA. This is foreseeable since the busbars, being the strongest connecting element in the cyber-power grids test system, its relevance must be put in evidence of what was made by the fuzz-based FMECA.

Since the FRPN includes the abovementioned characteristics, we can consider that the ranking obtained using the fuzzy-FMECA is much more adequate than the classical FMECA regarding the assumptions the FMECA team members introduced into the fuzzy mechanism.

6.2. Classical FMECA $\times$ Fuzzy-FMECA: Failure Modes with the Same FRPN

Table 10 shows that when using the fuzzy-FMECA, failure modes FM32, FM39, FM41, and FM42 achieved the same FRPN = 7.049 despite being ranked with priorities as 24, 25, 26, and 27, respectively. Let us analyze first the failure modes FM32 and FM39 that have the same ratings for *Severity* with $S = 7$, *Occurrence* with $O = 3$, and *Detection* with $D = 10$. These ratings activate the following four fuzzy rules:

Rule 59: If (S is SM) and (O is OVU) and (D is DL), then (RPN is RM)
Rule 60: If (S is SM) and (O is OVU) and (D is DAI), then (RPN is RH)
Rule 84: If (S is SVH) and (O is OVU) and (D is DL), then (RPN is RH)
Rule 85: If (S is SVH) and (O is OVU) and (D is DAI), then (RPN is RH)

Considering the four fuzzy rules and the membership functions in Figures 6 and 7, the rating $S = 7$ implies that the failure mode can be considered *Severity Moderate* (SM) with a membership of 0.286 and *Severity Very High* (SVH) with a membership 1. Moreover, the rating O = 3 means that the failure mode can be considered an *Occurrence Very Unlikely* (OVU) with a membership of 0.857. At last, the rating D = 10 means that the failure mode can be considered a *Detection Low* (DL) with a membership of 0.1379 but has a *Detection Almost Impossible* (DAI) with a membership of 0.7742. Figure 10 shows the "fired" fuzzy rules and the resulting output (fuzzy and defuzzified) for FM32 and FM39. For FM32 with S = 7, O = 3, and D = 10, the resulting output for rules 60, 84, and 85 is the fuzzy set RH fired at α = 0.857, α = 0.138, and α = 0.774, respectively, as shown in Figure 9. If we apply the *max(●)* operator to aggregate these three outputs, one obtains the same area under the fuzzy set RH resulting from rule 85. The conclusion of this is that rule 59 and rule 85 determine the shape of aggregated output, thus defining the FRPN = 7.049 for failure modes FM32 and FM39.

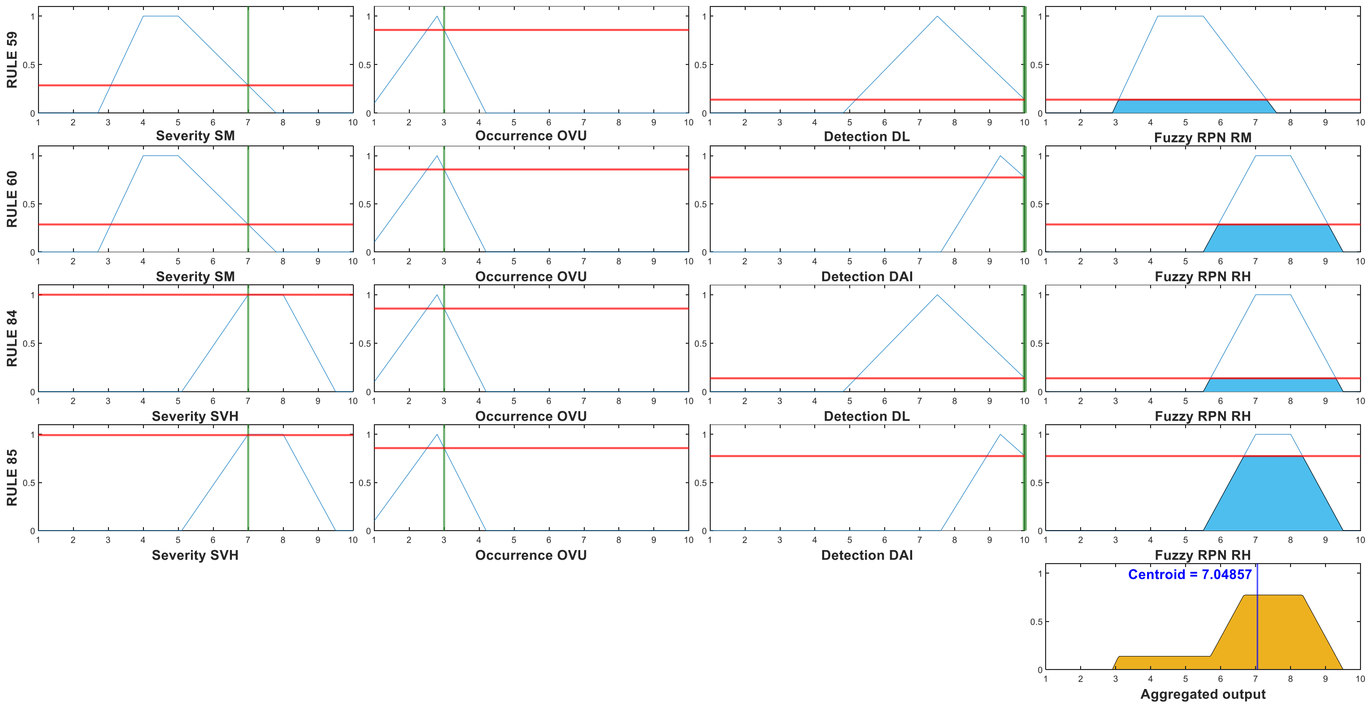

Figure 10. Fired fuzzy rules and aggregated output for failure modes FM32 and FM39.

Now, one advance for the other failure modes, FM41 and FM42. These have the same ratings for *Severity* S = 4, *Occurrence* O = 3, and *Detection* D = 10. These ratings activate the following two fuzzy rules:

Rule 59: If (S is SM) and (O is OVU) and (D is DL), then (RPN is RM);
Rule 60: If (S is SM) and (O is OVU) and (D is DAI), then (RPN is RH).

Considering these rules, the rating S = 4 implies that the failure mode can be considered *Severity Moderate* (SM) with membership 1. Rating O = 3 means that the failure mode can be considered as having an *Occurrence Very Unlikely* (OVU) with membership 0.857. At last, rating D = 10 means that the failure mode can be considered a *Detection Low* (DL) with a membership of 0.138 and activating the risk factor of a *Detection Almost Impossible* (DAI) with a membership of 0.774.

Figure 11 shows the fired fuzzy rules and the resulting output (fuzzy and defuzzified). Notice that the resulting output of rule 59 stays the same for FM32 and FM41. That is, the fuzzy set RM is fired at α = 0.138. For FM41 with S = 4, O = 3, and D = 10, the resulting output for rule 60 is the fuzzy set RH fired at α = 0.774. When comparing rule 85 (Figure 10) and rule 60 (Figure 11), we can verify that the fuzzy set DAI with D = 10 determines the resulting output for both rules. Hence, the shape of the aggregated output and the FRPN = 7.049 becomes the same for FM32 and FM41.

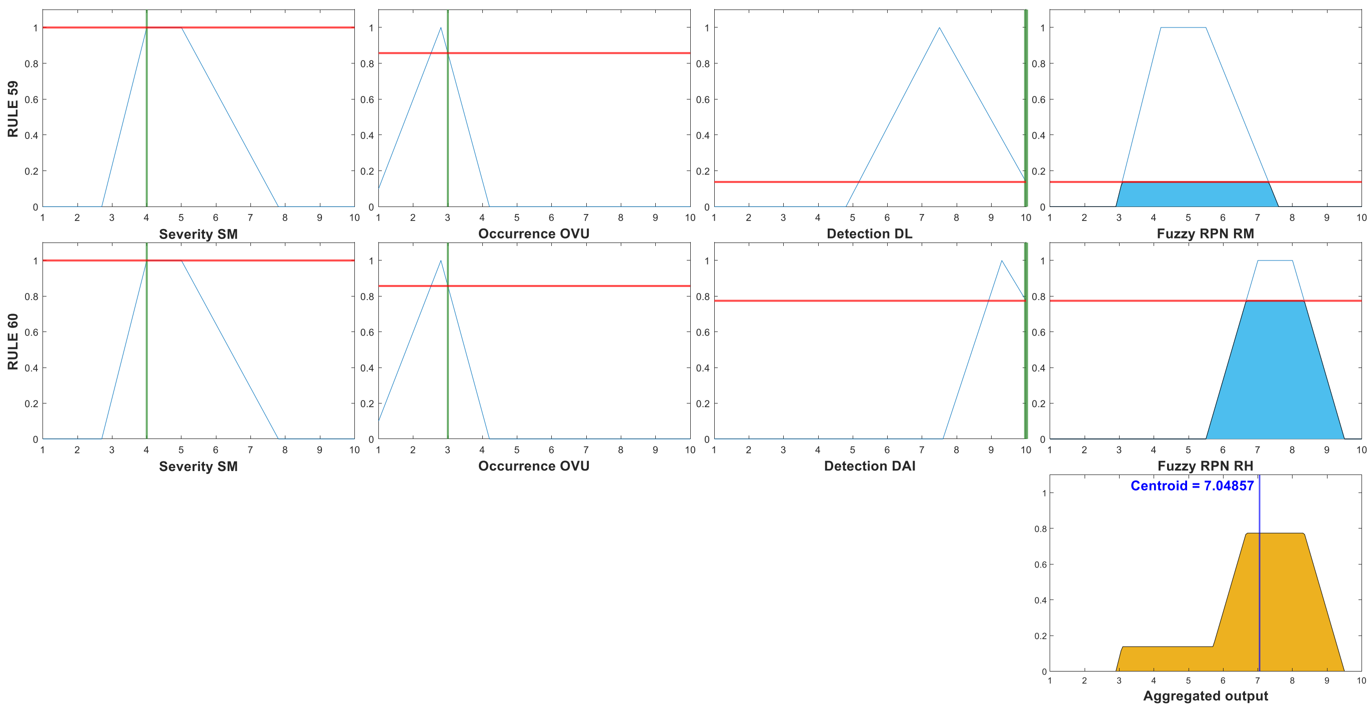

Figure 11. Fired fuzzy rules and aggregated output for failure modes FM41 and FM42.

Figure 12 shows the aggregated fuzzy output for the failure modes FM32 (FM39) and FM41 (FM42), with the same FRPN = 7.049. This explains this equality in the FRPN values and the equality obtained for other failure modes with equal FRPN and similar ratings.

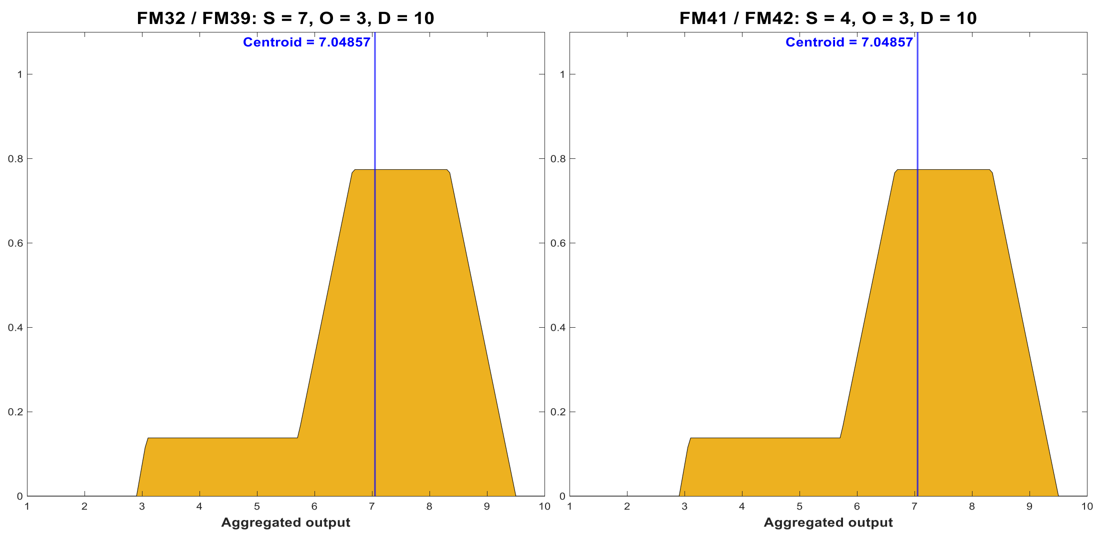

Figure 12. Fuzzy output for the failure modes FM32 (FM39) and FM41 (FM42) with the same FRPN = 7.049.

It is then vital to reduce the existence of failure modes with equal FRPN. One proposal then considers the following procedures:

- Establish individual categories for the risk factors rankings, that is, ten categories instead of 5;
- Adjusting the overlapping between fuzzy categories and;
- Adjust the membership function parameters or use non-linear membership functions.

7. Conclusions

This paper used a type-I fuzzy inference system to improve risk prioritization in classical FMECA analysis, now considering a more natural risk definition based on expert knowledge, the fuzzy-based FMECA. The proposed approach is relevant since the classical approach does not consider any relative importance between the risk factors to obtain the failure modes' risk level. In general, it does not necessarily represent the real risk perception of the FMECA expert members expressed using linguistic terms. Hence, the criteria of the expert members will constitute the principal source of uncertainty in the classical FMECA analysis.

This weakness related to the classical FMECA analysis motivated us to find the first alternatives to integrate the uncertainty into FMECA risk assessment. Fuzzy membership functions were used to represent the risk categories, and a rule-based inference mechanism was applied for the risk computation value or the fuzzy RPN. While the classic FMECA considers strict membership for each category, the fuzzy FMECA is flexible, and ratings may belong to two risk categories simultaneously, with different membership values. Because our fuzzy-based FMECA considered a different level of importance for the risk factors, the failure modes previously ranked as the riskiest by classical FMECA could reallocate to the correct priority levels.

The proposed fuzzy-FMECA approach was tested on a cyber-power grid test system composed of a four-bus 30kV power system and a cyber network. This was previously used by authors using the classical FMEA. Hence, one can compare which better information can be obtained concerning the risk priority number. From the initial 107 *failure modes* (FM) identified, the fuzzy-based FMECA indicates that only 42 failure modes represent the riskiest values. These were selected for further analysis.

The proposed fuzzy-based FMECA still has the following limitations that need to be addressed:

1. The use of integers-based classical rankings to assess the three risk factors restricts the exploitation of all fuzzy features of the proposed method;
2. The limits of the risk categories of the classic FMECA analysis were taken from IEC standards. They may not adequately represent the risk thresholds in real cases and should be calibrated with experimental data, and;
3. The use of 5 risk categories can constrain the diversity to represent the risk criteria of the experts.

Additional aspects are under development by this group and are intended to be included in future works. The main aspects are as follows:

- Definition of tailor-made risk categories and scales for the FMECA risk factors in the context of cyber-power grids;
- The use of ten risk categories to represent the risk factors;
- A sensibility analysis of the overlapping between the membership functions;
- The use of non-linear membership functions;
- The application of Type-II fuzzy inference systems for the fuzzy-FMECA analysis in cyber-power grids and;
- The proposal for a statistical-based comparison method for different FMECA approaches.

Author Contributions: Conceptualization, A.A.Z., J.F.P.F. and P.J.C.B.; methodology, A.A.Z. and P.J.C.B.; validation, A.A.Z., J.F.P.F. and P.J.C.B.; formal analysis, A.A.Z.; investigation, A.A.Z.; writing—original draft preparation, A.A.Z.; writing—review and editing, A.A.Z., J.F.P.F. and P.J.C.B.; supervision, J.F.P.F. and P.J.C.B.; funding acquisition, J.F.P.F. and P.J.C.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research is financed by SENESCYT-Ecuador through the postgraduate fellowship CZ05-000291-2017, and by national funds through FCT—Foundation for Science and Technology, I.P., through IDMEC, under LAETA, project UIDB/50022/2020.

Data Availability Statement: The data used in this study are available within the article.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

This appendix describes the 125 fuzzy if-the rules defined for the Type-I fuzzy-based FMECA proposed in this work.

1. If (S is SMI) and (O is OR) and (D is DAC), then (RPN is RMI)
2. If (S is SMI) and (O is OR) and (D is DH), then (RPN is RMI)
3. If (S is SMI) and (O is OR) and (D is DM,) then (RPN is RL)
4. If (S is SMI) and (O is OR) and (D is DL), then (RPN is RL)
5. If (S is SMI) and (O is OR) and (D is DAI,) then (RPN is RM)
6. If (S is SMI) and (O is OVU) and (D is DAC), then (RPN is RMI)
7. If (S is SMI) and (O is OVU) and (D is DH), then (RPN is RMI)
8. If (S is SMI) and (O is OVU) and (D is DM), then (RPN is RL)
9. If (S is SMI) and (O is OVU) and (D is DL), then (RPN is RL)
10. If (S is SMI) and (O is OVU) and (D is DAI), then (RPN is RM)
11. If (S is SMI) and (O is OO) and (D is DAC), then (RPN is RMI)
12. If (S is SMI) and (O is OO) and (D is DH), then (RPN is RL)
13. If (S is SMI) and (O is OO) and (D is DM), then (RPN is RL)
14. If (S is SMI) and (O is OO) and (D is DL), then (RPN is RM)
15. If (S is SMI) and (O is OO) and (D is DAI), then (RPN is RH)
16. If (S is SMI) and (O is OP) and (D is DAC), then (RPN is RMI)
17. If (S is SMI) and (O is OP) and (D is DH), then (RPN is RL)
18. If (S is SMI) and (O is OP) and (D is DM), then (RPN is RL)
19. If (S is SMI) and (O is OP) and (D is DL), then (RPN is RM)
20. If (S is SMI) and (O is OP) and (D is DAI), then (RPN is RH)
21. If (S is SMI) and (O is OF) and (D is DAC), then (RPN is RL)
22. If (S is SMI) and (O is OF) and (D is DH), then (RPN is RL)
23. If (S is SMI) and (O is OF) and (D is DM), then (RPN is RM)
24. If (S is SMI) and (O is OF) and (D is DL), then (RPN is RH)
25. If (S is SMI) and (O is OF) and (D is DAI), then (RPN is RH)
26. If (S is SL) and (O is OR) and (D is DAC), then (RPN is RMI)
27. If (S is SL) and (O is OR) and (D is DH), then (RPN is RMI)
28. If (S is SL) and (O is OR) and (D is DM), then (RPN is RL)
29. If (S is SL) and (O is OR) and (D is DL), then (RPN is RL)
30. If (S is SL) and (O is OR) and (D is DAI), then (RPN is RM)
31. If (S is SL) and (O is OVU) and (D is DAC), then (RPN is RMI)
32. If (S is SL) and (O is OVU) and (D is DH), then (RPN is RL)
33. If (S is SL) and (O is OVU) and (D is DM), then (RPN is RL)
34. If (S is SL) and (O is OVU) and (D is DL), then (RPN is RM)
35. If (S is SL) and (O is OVU) and (D is DAI), then (RPN is RH)
36. If (S is SL) and (O is OO) and (D is DAC), then (RPN is RMI)
37. If (S is SL) and (O is OO) and (D is DH), then (RPN is RL)
38. If (S is SL) and (O is OO) and (D is DM), then (RPN is RL)
39. If (S is SL) and (O is OO) and (D is DL), then (RPN is RM)
40. If (S is SL) and (O is OO) and (D is DAI), then (RPN is RH)
41. If (S is SL) and (O is OP) and (D is DAC), then (RPN is RL)
42. If (S is SL) and (O is OP) and (D is DH), then (RPN is RL)
43. If (S is SL) and (O is OP) and (D is DM), then (RPN is RM)
44. If (S is SL) and (O is OP) and (D is DL), then (RPN is RH)
45. If (S is SL) and (O is OP) and (D is DAI), then (RPN is RH)
46. If (S is SL) and (O is OF) and (D is DAC), then (RPN is RL)
47. If (S is SL) and (O is OF) and (D is DH), then (RPN is RM)

48. If (S is SL) and (O is OF) and (D is DM), then (RPN is RH)
49. If (S is SL) and (O is OF) and (D is DL), then (RPN is RH)
50. If (S is SL) and (O is OF) and (D is DAI), then (RPN is RE)
51. If (S is SM) and (O is OR) and (D is DAC), then (RPN is RMI)
52. If (S is SM) and (O is OR) and (D is DH), then (RPN is RL)
53. If (S is SM) and (O is OR) and (D is DM), then (RPN is RL)
54. If (S is SM) and (O is OR) and (D is DL), then (RPN is RM)
55. If (S is SM) and (O is OR) and (D is DAI), then (RPN is RH)
56. If (S is SM) and (O is OVU) and (D is DAC), then (RPN is RMI)
57. If (S is SM) and (O is OVU) and (D is DH), then (RPN is RL)
58. If (S is SM) and (O is OVU) and (D is DM), then (RPN is RL)
59. If (S is SM) and (O is OVU) and (D is DL), then (RPN is RM)
60. If (S is SM) and (O is OVU) and (D is DAI), then (RPN is RH)
61. If (S is SM) and (O is OO) and (D is DAC), then (RPN is RL)
62. If (S is SM) and (O is OO) and (D is DH), then (RPN is RL)
63. If (S is SM) and (O is OO) and (D is DM), then (RPN is RM)
64. If (S is SM) and (O is OO) and (D is DL), then (RPN is RH)
65. If (S is SM) and (O is OO) and (D is DAI), then (RPN is RH)
66. If (S is SM) and (O is OP) and (D is DAC), then (RPN is RL)
67. If (S is SM) and (O is OP) and (D is DH), then (RPN is RM)
68. If (S is SM) and (O is OP) and (D is DM), then (RPN is RH)
69. If (S is SM) and (O is OP) and (D is DL), then (RPN is RH)
70. If (S is SM) and (O is OP) and (D is DAI), then (RPN is RE)
71. If (S is SM) and (O is OF) and (D is DAC) then (RPN is RL)
72. If (S is SM) and (O is OF) and (D is DH), then (RPN is RM)
73. If (S is SM) and (O is OF) and (D is DM), then (RPN is RH)
74. If (S is SM) and (O is OF) and (D is DL), then (RPN is RH)
75. If (S is SM) and (O is OF) and (D is DAI), then (RPN is RE)
76. If (S is SVH) and (O is OR) and (D is DAC), then (RPN is RMI)
77. If (S is SVH) and (O is OR) and (D is DH), then (RPN is RL)
78. If (S is SVH) and (O is OR) and (D is DM) then (RPN is RL)
79. If (S is SVH) and (O is OR) and (D is DL), then (RPN is RM)
80. If (S is SVH) and (O is OR) and (D is DAI), then (RPN is RH)
81. If (S is SVH) and (O is OVU) and (D is DAC), then (RPN is RL)
82. If (S is SVH) and (O is OVU) and (D is DH), then (RPN is RL)
83. If (S is SVH) and (O is OVU) and (D is DM), then (RPN is RM)
84. If (S is SVH) and (O is OVU) and (D is DL), then (RPN is RH)
85. If (S is SVH) and (O is OVU) and (D is DAI), then (RPN is RH)
86. If (S is SVH) and (O is OO) and (D is DAC), then (RPN is RL)
87. If (S is SVH) and (O is OO) and (D is DH), then (RPN is RM)
88. If (S is SVH) and (O is OO) and (D is DM,) then (RPN is RH)
89. If (S is SVH) and (O is OO) and (D is DL), then (RPN is RH)
90. If (S is SVH) and (O is OO) and (D is DAI), then (RPN is RE)
91. If (S is SVH) and (O is OP) and (D is DAC), then (RPN is RL)
92. If (S is SVH) and (O is OP) and (D is DH), then (RPN is RM)
93. If (S is SVH) and (O is OP) and (D is DM), then (RPN is RH)
94. If (S is SVH) and (O is OP) and (D is DL), then (RPN is RH)
95. If (S is SVH) and (O is OP) and (D is DAI), then (RPN is RE)
96. If (S is SVH) and (O is OF) and (D is DAC), then (RPN is RM)
97. If (S is SVH) and (O is OF) and (D is DH), then (RPN is RH)
98. If (S is SVH) and (O is OF) and (D is DM), then (RPN is RH)
99. If (S is SVH) and (O is OF) and (D is DL), then (RPN is RE)
100. If (S is SVH) and (O is OF) and (D is DAI), then (RPN is RE)
101. If (S is SHA) and (O is OR) and (D is DAC), then (RPN is RL)

102. If (S is SHA) and (O is OR) and (D is DH), then (RPN is RL)
103. If (S is SHA) and (O is OR) and (D is DM), then (RPN is RM)
104. If (S is SHA) and (O is OR) and (D is DL), then (RPN is RH)
105. If (S is SHA) and (O is OR) and (D is DAI), then (RPN is RH)
106. If (S is SHA) and (O is OVU) and (D is DAC), then (RPN is RL)
107. If (S is SHA) and (O is OVU) and (D is DH), then (RPN is RM)
108. If (S is SHA) and (O is OVU) and (D is DM), then (RPN is RH)
109. If (S is SHA) and (O is OVU) and (D is DL), then (RPN is RH)
110. If (S is SHA) and (O is OVU) and (D is DAI), then (RPN is RE)
111. If (S is SHA) and (O is OO) and (D is DAC), then (RPN is RL)
112. If (S is SHA) and (O is OO) and (D is DH), then (RPN is RM)
113. If (S is SHA) and (O is OO) and (D is DM), then (RPN is RH)
114. If (S is SHA) and (O is OO) and (D is DL), then (RPN is RH)
115. If (S is SHA) and (O is OO) and (D is DAI), then (RPN is RE)
116. If (S is SHA) and (O is OP) and (D is DAC), then (RPN is RM)
117. If (S is SHA) and (O is OP) and (D is DH), then (RPN is RH)
118. If (S is SHA) and (O is OP) and (D is DM), then (RPN is RH)
119. If (S is SHA) and (O is OP) and (D is DL), then (RPN is RE)
120. If (S is SHA) and (O is OP) and (D is DAI), then (RPN is RE)
121. If (S is SHA) and (O is OF) and (D is DAC), then (RPN is RM)
122. If (S is SHA) and (O is OF) and (D is DH), then (RPN is RH)
123. If (S is SHA) and (O is OF) and (D is DM), then (RPN is RH)
124. If (S is SHA) and (O is OF) and (D is DL), then (RPN is RE)
125. If (S is SHA) and (O is OF) and (D is DAI), then (RPN is RE)

References

1. Rausand, M.; Høyland, A. *System Reliability Theory: Models, Statistical Methods and Applications*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2004; ISBN 3-17-572399-3.
2. Stamatis, D.H. *Failure Mode and Effect Analysis: FMEA from Theory to Execution*, 2nd ed.; ASQ Quality Press: Milwaukee, VI, USA, 2003; ISBN 0-87-389598-3.
3. *IEC 60812:2006*; Analysis Techniques for System Reliability—Procedure for Failure Mode and Effects Analysis (FMEA). International Electrotechnical Commission: London, UK, 2018.
4. *SAE J1739_202101*; Potential Failure Mode and Effects Analysis (FMEA) Including Design FMEA, Supplemental FMEA-MSR, and Process FMEA. SAE International: Warrendale, PA, USA, 2021.
5. Zúñiga, A.A.; Fernandes, J.F.P.; Branco, P.J.C. A Fuzzy-Based Failure Modes and Effects Analysis (FMEA) in Smart Grids. In *Advances in Intelligent Systems and Computing, Proceedings of the International Conference on Information Technology & Systems ICITS 2019, Quito, Ecuador, 6–8 February 2019*; Rocha, Á., Ferrás, C., Paredes, M., Eds.; Springer: Cham, Switzerland, 2019; Volume 918, pp. 507–516. ISBN 978-3-03011-890-7.
6. Pourramazan, A.; Saffari, S.; Barghandan, A. Study of Failure Mode and Effect Analysis (FMEA) on Capacitor Bank Used in Distribution Power Systems. *Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng. IJIREEICE* **2017**, *5*, 113–118. [CrossRef]
7. Eyuboglu, O.H.; Dindar, B.; Gul, O. Risk Assessment by Using Failure Modes and Effects Analysis (FMEA) Based on Power Transformer Aging for Maintenance and Replacement Decision. In Proceedings of the 2020 2nd Global Power, Energy and Communication Conference, GPECOM 2020, Izmir, Turkey, 20–23 October 2020; pp. 251–255. [CrossRef]
8. Asadi, F.; Phumpho, S.; Pongswatd, S. Remote Monitoring and Alert System of HV Transformer Based on FMEA. *Energy Rep.* **2020**, *6*, 807–813. [CrossRef]
9. Colli, A. Failure Mode and Effect Analysis for Photovoltaic Systems. *Renew. Sustain. Energy Rev.* **2015**, *50*, 804–809. [CrossRef]
10. Herz, M.; Friesen, G.; Jahn, U.; Köntges, M.; Lindig, S.; Moser, D. *Quantification of Technical Risks in PV Power Systems*; IEA PVPS: Paris, France, 2021.
11. Díaz, H.; Guedes Soares, C. Failure Mode Identification and Effect Analysis of Offshore Wind Turbines and Substations. In *Developments in Renewable Energies Offshore, Proceedings of the 4th International Conference on Renewable Energies Offshore, RENEW 2020, Lisbon, Portugal, 12–15 October 2020*; Taylor & Francis: Abingdon, UK, 2021; pp. 444–460. [CrossRef]
12. Zúñiga, A.A.; Baleia, A.; Fernandes, J.; da Costa Branco, P.J. Classical Failure Modes and Effects Analysis in the Context of Smart Grid Cyber-Physical Systems. *Energies* **2020**, *13*, 1215. [CrossRef]
13. Bucolo, M.; Buscarino, A.; Famoso, C.; Fortuna, L. Chaos Addresses Energy in Networks of Electrical Oscillators. *IEEE Access* **2021**, *9*, 153258–153265. [CrossRef]

14. Markowski, A.S.; Mannan, M.S.; Kotynia (Bigoszewska), A.; Siuta, D. Uncertainty Aspects in Process Safety Analysis. *J. Loss Prev. Process Ind.* **2010**, *23*, 446–454. [CrossRef]
15. Markowski, A.S.; Siuta, D. Fuzzy Logic Approach for Identifying Representative Accident Scenarios. *J. Loss Prev. Process Ind.* **2018**, *56*, 414–423. [CrossRef]
16. Huang, J.; You, J.X.; Liu, H.C.; Song, M.S. Failure Mode and Effect Analysis Improvement: A Systematic Literature Review and Future Research Agenda. *Reliab. Eng. Syst. Saf.* **2020**, *199*, 106885. [CrossRef]
17. Hassan, S.; Wang, J.; Kontovas, C.; Bashir, M. Modified FMEA Hazard Identification for Cross-Country Petroleum Pipeline Using Fuzzy Rule Base and Approximate Reasoning. *J. Loss Prev. Process Ind.* **2022**, *74*, 104616. [CrossRef]
18. Daneshvar, S.; Yazdi, M.; Adesina, K.A. Fuzzy Smart Failure Modes and Effects Analysis to Improve Safety Performance of System: Case Study of an Aircraft Landing System. *Qual. Reliab. Eng. Int.* **2020**, *36*, 890–909. [CrossRef]
19. Fattahi, R.; Tavakkoli-Moghaddam, R.; Khalilzadeh, M.; Shahsavari-Pour, N.; Soltani, R. A Novel FMEA Model Based on Fuzzy Multiple-Criteria Decision-Making Methods for Risk Assessment. *J. Enterp. Inf. Manag.* **2020**, *33*, 881–904. [CrossRef]
20. Bahrebar, S.; Blaabjerg, F.; Wang, H.; Vafamand, N.; Khooban, M.H.; Rastayesh, S.; Zhou, D. A Novel Type-2 Fuzzy Logic for Improved Risk Analysis of Proton Exchange Membrane Fuel Cells in Marine Power Systems Application. *Energies* **2018**, *11*, 721. [CrossRef]
21. Liu, S.; Guo, X.; Zhang, L. An Improved Assessment Method for FMEA for a Shipboard Integrated Electric Propulsion System Using Fuzzy Logic and DEMATEL Theory. *Energies* **2019**, *12*, 3162. [CrossRef]
22. Deng, X.; Jiang, W. Fuzzy Risk Evaluation in Failure Mode and Effects Analysis Using a D Numbers Based Multi-Sensor Information Fusion Method. *Sensors* **2017**, *17*, 2086. [CrossRef] [PubMed]
23. Komatina, N.; Aleksic, A.; Banduka, N. Determination of Failures Priority Based on FMEA, Fuzzy Sets, and Fuzzy Logic Rules. In Proceedings of the 8th International Conference on Industrial Engineering—SIE 2022, Belgrade, Serbia, 29–30 September 2022.
24. Jin, G.; Meng, Q.; Feng, W. Optimization of Logistics System with Fuzzy FMEA-AHP Methodology. *Processes* **2022**, *10*, 1973. [CrossRef]
25. Mazdak Khodadadi-Karimvand; TaheriFar, S. Safety Risk Assessment; Using Fuzzy Failure Mode and Effect Analysis. *Trans. Fuzzy Sets Syst.* **2022**, *1*, 90–98. [CrossRef]
26. Zhou, B.; Chen, J.; Wu, Q.; Pamučar, D.; Wang, W.; Zhou, L. Risk Priority Evaluation of Power Transformer Parts Based on Hybrid Fmea Framework Under Hesitant Fuzzy Environment. *Facta Univ. Ser. Mech. Eng.* **2022**, *20*, 399–420. [CrossRef]
27. Li, H.; Liang, M.; Li, F.; Zuo, J.; Zhang, C.; Ma, Y. Operational Safety Risk Assessment of Water Diversion Infrastructure Based on FMEA with Fuzzy Inference System. *Water Supply* **2022**, *22*, 7513–7531. [CrossRef]
28. Cruz-Rivero, L.; Méndez-Hernández, M.L.; Mar-Orozco, C.E.; Aguilar-Lasserre, A.A.; Barbosa-Moreno, A.; Sánchez-Escobar, J. Functional Evaluation Using Fuzzy FMEA for a Non-Invasive Measurer for Methane and Carbone Dioxide. *Symmetry* **2022**, *14*, 421. [CrossRef]
29. Soltanali, H.; Khojastehpour, M.; De Almeida, E. Sustainable Food Production: An Intelligent Fault Diagnosis Framework for Analyzing the Risk of Critical Processes. *Sustainability* **2022**, *14*, 1083. [CrossRef]
30. Akula, S.K.; Salehfar, H.; Behzadirafi, S. Comparision of Traditional and Fuzzy Failure Mode and Effects Analysis for Smart Grid Electrical Distribution Systems. In Proceedings of the 2022 North American Power Symposium (NAPS), Salt Lake City, UT, USA, 9–11 October 2022.
31. Lin, C.-T.; Lee, G. *Neural Fuzzy Systems: A Neuro-Fuzzy Synergism to Intelligent Systems*; Prentice Hall, Inc.: Upper Saddle River, NJ, USA, 1996; ISBN 0-13-235169-2.
32. Castillo, O.; Melin, P.; Kacprzyk, J.; Pedrycz, W. Type-2 Fuzzy Logic: Theory and Applications. In Proceedings of the 2007 IEEE International Conference on Granular Computing (GRC 2007), Fremont, CA, USA, 2–4 November 2007; p. 145. [CrossRef]
33. Mendel, J.M.; Hagras, H.; Tan, W.-W.; Melek, W.W.; Ying, H. *Introduction to Type-2 Fuzzy Logic Control: Theory and Applications*; Wiley-IEEE Press: Hoboken, NJ, USA, 2014; ISBN 978-1-11827-839-0.
34. Jang, J.-S.R.; Sun, C.-T.; Mizutani, E. *Neuro-Fuzzy and Soft Computing: A Computational Approach to Learning and Machine Intelligence*; Prentice Hall, Inc.: Upper Saddle River, NJ, USA, 1997.
35. Zadeh, L.A. The Concept of a Linguistic Variable and Its Application to Approximate Reasoning-I. *Inf. Sci.* **1975**, *8*, 199–249. [CrossRef]
36. Chen, S.-J.; Hwang, C.-L.; Hwang, F.P. *Fuzzy Multiple Attribute Decision Making: Methods and Applications*; Springer: Berlin/Heidelberg, Germany, 1992; ISBN 978-3-54055-820-0.