Fuzzy Failure Modes Effect and Criticality Analysis of the Procurement Process of Artificial Intelligent Systems/Services

Khalid Alshehhi, Ali Cheaitou, Hamad Rashid
Department of Industrial Engineering and Engineering Management
University of Sharjah 27272 Sharjah, United Arab Emirates

***Abstract*—This study focuses on the ranking of risks associated with the procurement of Artificial Intelligent (AI) systems/services for UAE public Sectors. Considering the involvement of human-based reasoning, this study proposes to use Fuzzy Failure Mode Effect and Criticality Analysis (FMECA). The risks were identified from the literature and subsequently, using 40 interviews with practitioners, the final list is developed on the basis of the presence of risks in the AI procurement process. For Fuzzy FMECA, the input data is collected from fifteen experts. The values of Severity (S), and Detection (D) for each risk element are averaged to use as input. If-Then rule-based fuzzy inference system is employed to obtain the Fuzzy Risk Priority Numbers of risk elements. The traditional RPN and Fuzzy RPN numbers are compared and it is found that fuzzy RPN gives a realistic picture of the ranking of risks. Privacy and security risks, Integration Risks, Risk of Malfunction of systems/services, and Ethical risks are found to be high priorities. This study provides valuable insight to policymakers to develop strategies to mitigate these risks for smooth procurement and implementation of AI-related Projects.**

***Keywords*—Fuzzy Failure Mode Effect and Criticality Analysis (FMECA); procurement; Artificial Intelligent (AI) System; public sector; United Arab Emirates (UAE)**

I. INTRODUCTION

The United Arab Emirates (UAE) has been at the forefront of embracing technological advancements and digital transformation in the public sector. Artificial Intelligence (AI) systems have emerged as a critical enabler in the UAE public sector, transforming operations, improving decision-making, and delivering efficient and citizen-centric services [1]. The UAE government has led smart government programs aimed at leveraging AI's potential for improved service delivery. These programs are aimed at exploiting Artificial Intelligence (AI) technology in fields such as healthcare, transportation, education, public safety, and e-governance [2]. Artificial intelligence-powered platforms streamline administrative operations, provide personalized services, and enable data-driven decision-making. The UAE public sector hopes to increase operational efficiency, optimize resource allocation, and improve overall service quality by integrating AI technology.

Artificial Intelligence (AI) solutions have received much attention as part of this journey. However, the AI procurement process carries inherent risks that must be identified and handled efficiently [3]. If not adequately handled, these risks can negatively influence the successful adoption and use of AI technology. In addition, AI procurement risks can have financial implications such as operational disruption, Ethical and legal concerns, reputation damage, and missed opportunities [4]. Understanding the effects and putting appropriate risk mitigation measures in place is critical for public sectors looking to reap the advantages of AI while minimizing the negative outcomes. Failure Mode Effect and Criticality Analysis (FMECA) is a tool for identifying risks in complex systems.

FMEA may be used in various processes, including procurement (Skelton, 1997). In the process, it is also utilized to assure the safe functioning of complicated monitoring and control systems. FMEA methodically identifies the impact of risk elements on the system and assesses the importance of each failure mode in terms of system performance. The approach is primarily utilized in a wide range of technologies to investigate and comprehend component/system failure. FMEA is known as failure mode effect criticality analysis (FMECA) when it is used to prioritize failure modes. The failure modes are ranked using the Risk Priority Number (RPN) by FMECA. RPN is frequently computed as the product of failure mode occurrence (O), severity (S), and non-detection (D). According to Certa et al. (2017), O stands for the frequency of occurrence of the failure mode, S for the severity of the harm that particular failure modes with occurrences of O can cause to systems, processes, and the environment, and D stands for the likelihood that the failure modes with occurrences of O and S won't be detected.

Although there are various applications for FMEA, several researchers have highlighted the various shortcomings of the traditional Risk Priority Number (RPN) that is employed in FMEA. The most significant shortcoming is subjectivity and Lack of Consistency. The subjectivity and lack of consistency in the severity, occurrence, and detection ratings given to potential risks by RPN is one of its key issue. The same risk may be evaluated differently by various team members, resulting in variances in the final RPN ratings. This subjectivity can undermine the accuracy of the findings [5]. To overcome this limitation, fuzzy based FMEA was used by various researchers such as [6-9].

The approach for creating a fuzzy RPN (FRPN) is described in this study. It may partially address some of the

constraints mentioned in the literature. The fundamental inputs for producing FRPN are the fuzzified form of frequency, severity, and non-detection of the failure modes. The following stage in fuzzy FMECA is to establish the fuzzy rules. For this stage, the original classes of O, S, and D and the corresponding RPN class are used to establish the rules. The next stage is to use linguistic variables and membership functions to transform the crisp input data into fuzzy values. The assessment of the rule bases created during the study comes next. The last stage to transform the fuzzy output into crisp output is called defuzzification. The AI procurement process in UAE public sectors is subjected to this process. In addition, Comparisons are made between the outcomes of conventional and fuzzy FMECA.

The rest of the paper is as follows: Section II presents the literature review highlighting the rating of risks associated with procurements and tools and techniques for this purpose. Materials and Methods utilized in this study are presented in Section III. Section IV presents the results and discussions. Finally, Section V presents conclusions drawn from this study.

II. Literature Review

For the procurement process to be effective, risks must be identified and managed. The identification of risks and mitigation processes can be facilitated by a number of efficient tools and methods. The risk register is one such instrument, which entails methodically identifying possible hazards, evaluating their effect and likelihood, and developing suitable mitigation strategies. There are numerous methods/ techniques are employed for risk analysis [10]. Bathrinath, Bhalaji [11] used AHP-TOPSIS method for risk assessment and ranking in a Textile Industry. To analyze the risks in urban stormwater infrastructure systems, Shariat, Roozbahani [12] applied fuzzy spatial multi-criteria decision-making. Data analytics is also applied as a tool for the evaluation and improvement of procurement processes [13]. Delima, Santoso [14] applied a dynamic system development model for the development of purchasing model for agriculture e-commerce. Among all the tools and techniques, Failure Mode and Effect Analysis (FMEA) is a widely used tool for risk analysis.

The FMEA approach, which was developed in the 1960s for the aerospace industry, is a powerful tool for assessing possible risks [15]. In complex systems, this method is very helpful in averting undesirable outcomes [16]. FMEA is widely utilized in a variety of industries, including those in the aerospace, automotive, nuclear, electronics, chemical, mechanical, and medical domains [17-22]. Aldenny, Kristian [23] applied FMEA analysis to determine possible risks with the government's electronic procurement process using the FMEA approach. To improve the purchasing process of public procurement in hospitals, Kumru and Kumru [24] applied the FMEA to indicate the levels of risks associated with potential issues. Nahavandi and Tavakoli [25] applied the FMEA combined with the TOPSIS method to identify the risks associated with procurement in the automotive supply chain. The Modified FMEA is also used for ranking risks associated with military weapons procurement [26]. Handayani [27] also applied the FMEA analysis to evaluate the risks associated with supplier-buyer transactions in a supply chain procurement. These studies infer that FMEA is an effective tool for analyzing the risks associated with the Procurement process.

There are some limitations of the traditional FMEA process which doesn't capture the subjectivity in a precise way. To overcome this difficulty, a variant of FMEA was developed using a fuzzy set theory known as fuzzy FMEA. Incorporating the criticality analysis in Fuzzy FMEA, the Fuzzy FMECA was developed as an advanced method for ranking the risks. Numerous fields, including engineering [28], manufacturing [29], healthcare [30], and more recently, new technologies like artificial intelligence [31], have found use for fuzzy FMECA. When working with complicated systems where it might be challenging to exactly quantify risk variables, fuzzy FMECA is particularly helpful. Fuzzy FMECA allows decision-makers to consider linguistic variations and subjective aspects by introducing fuzzy logic, making risk analysis more adaptable and understandable.

A crucial step in purchasing cutting-edge technology to improve organizations operations as well as decision-making is the procurement process for Artificial Intelligent (AI) systems or services. Predictive analytics, machine learning, and other disruptive features that AI systems provide have the ability to completely change a number of sectors. It takes strategic decision-making to choose the best AI solutions that fit an organization's objectives, requirements, and capabilities when purchasing AI systems or services. For effective AI integration, suppliers and technology providers must be properly evaluated and chosen [32]. In order to evaluate failure modes, their impacts, and criticality while procuring AI solutions, fuzzy FMECA (Failure Mode Effect and Criticality Analysis) is extremely important. By introducing fuzzy logic, which enables the management of uncertainties and ambiguity frequently found in AI systems, fuzzy FMECA expands classic FMECA approaches. The inherent complexity and changing nature of AI technology make this competence essential in the context of AI procurement [33]. Complex algorithms and learning models are used in AI systems, which might result in erratic and unexpected behavior. Fuzzy FMECA can manage ambiguous inputs and hazy data, providing a more accurate evaluation of likely risk mechanisms [34]. AI systems often produce results with varying degrees of ambiguity. Fuzzy FMECA utilizes linguistic variables to quantify the degree of criticality, providing a more nuanced evaluation of failure effects [35].

III. Materials and Method

FMECA typically consists of two steps: (i) Use failure mode and effect analysis to distinguish between various failure types and their impacts, (ii) group failure mode criticality analysis according to the likelihood of occurrence and impact [15]. Traditional FMEA calculations involve generating a risk priority number (RPN). Three main factors are needed when doing an FMEA: occurrence (O), which indicates the likelihood of accident occurrences. The term "severity" (S) refers to the seriousness of the consequences of failure modes not being detected. Non-detection (D) eliminates the possibility of detecting failures before they occur. The sum of the three

aforementioned operations yields a risk level known as the risk priority number (RPN).

The shortcomings of the traditional Risk Priority Number (RPN) employed in FMEA have been noted by several academics. The relative relevance of O, S, and D is not often considered in most FMEA analyses, according to Wang, Chin [36]. According to [37], different O, S, and D combinations may result in exactly the same RPN number, but their hidden risk implications may be quite different.

An intelligent framework that summarizes established multi-valued logic for problem-solving under vulnerability is referred to as fuzzy logic. Control designers may easily implement control methodologies used by human administrators thanks to fuzzy logic [38]. Its structure is based on the fact that some problems might be solved based on related knowledge or expert learning while others did not require the proper or accurate esteem. It is based on a likelihood hypothesis for the conversion of crisp to fuzzy input, which will be handled by referring to the state of the fuzzy rule base created by experts. Fuzzy rule base preparation, which converts fuzzy output to crisp output, might solve the problem. Fuzzy logic was a mechanism for making decisions when information was vulnerable and taking flexibility into account.

It is feasible to obtain a complete description of potential risk and its impact by using fuzzy logic in failure modes, effects, and criticality analysis (FMECA). This strategy might effectively address the problems and clearly identify any risks and implications. Furthermore, it could also build trust at the same time. It enables an assessor to directly assess the risks associated with failure by using language concepts in criticality evaluation. Ambiguity, subjective information, or data including quantitative information may be used in the evaluation and organization, although not always unambiguously. The combination of severity (S), occurrence (O), and non-detection (D) parameters had a more flexible structural design. The use of fuzzy logic in FMECA for ranking the risks associated with the procurement of AI systems/services is the main topic of this paper.

A. The Proposed Method

The proposed method is based on the work done by Makowski and Mannan [39]. Risk is normally evaluated using two components, severity, and occurrence, during the risk assessment process. Traditional risk predicts frequency and severity as discrete values/categories. Due to a number of uncertainties, frequency and severity values are non-crisp in nature [39]. When there are uncertainties in the parameters used for risk computation, fuzzy logic can be employed to estimate the risk. In the classification of these characteristics, fuzzy logic does not identify precise limits. The fuzzy risk matrix is created by combining a fuzzy frequency and a fuzzy severity.

The RPN in the FMECA research makes use of three parameters: O, S, and D. O, S, and D crisp input data are generally quantified on a ten-point scale (see Tables I to III). Using linguistic expressions and membership functions, they are turned into fuzzy values. Similarly, the output's membership function (RPN) is constructed. In this study, 1000 rules were designed to govern the output value. As an example (rule No. 996), if the occurrence is definite (10), the severity is substantial (6), and the detection is not possible, RPN is calculated conventionally by multiplying O, S, and D (10*6*6) = 360. The standard RPN, which corresponds to class 9, has been improved by integrating the linguistic phrase "high" matching to this class. A Mamdani fuzzy inference technique is used to convert qualitative rules into quantitative results. The fuzzy set for each rule is aggregated once the rules have been assessed. The centre of area approach is utilised for defuzzification in this work.

TABLE I. OCCURRENCE SCALES USED IN FMECA OCCURRENCE 'O'

Rank	Probability of failures	Human error occurrence Probability	Linguistic Variable
1	< 1:20000	< every 5 years	Unlikely
2	1:20000	In 3–5 years	Very remote
3	1:10000	In 1–3 years	remote
4	1:2000	Per year	Very low
5	1:1000	In every 6 months	Low
6	1:200	In every 3 months	Moderate
7	1:100	Per months	Moderately high
8	1:20	Per Week	High
9	1:10	Every few days	Very high
10	1:2	Per Day	Almost certain

(Courtesy:M. Giardina, M. Morale/Journal of Loss Prevention in the Process Industries 35(2015),35–45).

TABLE II. SEVERITY SCALES USED IN FMECA SEVERITY 'S'

The severity of Each risk	Effect	Rank
No reason to expect risk to have any effect on safety, health, environment, or mission	None	1
Very minor effect on product or system performance to have any effect on safety or health. The system does not require repair / restart.	Very Minor	2
Minor effect on product or system performance to have any effect on safety or health. The system can require repair/ restart.	Minor	3
Very low effect on system performance. A failure is not serious enough to cause injury, property damage, or system damage, but can result in unscheduled maintenance or repair	Low	4
Moderate effect on system performance. The system requires repair. A failure may cause moderate injury, moderate property damage, or moderate system damage which will result in delay or loss of system availability or mission degradation. 100% of the mission may need to be reworked or process delayed.	Moderate	5
System performance is degraded. Some safety functions may not operate. A failure causes injury, property damage, or system damage. Some portion of mission is lost. High delaying restoring function.	Significant	6
System performance is severely affected but functions (reduced level of safety performance). The system may not operate. Risk does not involve noncompliance with government regulations or standards.	Major	7
System is inoperable with loss of primary function. Risk can involve hazardous outcomes and/or noncompliance with government regulations or standards.	Extreme	8

Risk involves hazardous outcomes and/or noncompliance with government regulations or standards. Potential safety, health or environmental issue. Risk will occur with warning.	Very Extreme	9
Risk is hazardous and occurs without warning. It affects safe operation. A Risk is serious enough to cause injury, property damage, or system damage. Risk will occur without warning.	Serious	10

TABLE III. DETECTION SCALES USED IN FMECA DETECTION 'D'

Likelihood of detection of risk	Degree of Importance	Probability of failure of detection	rating
Current control(s) almost certainly will detect a potential risk.	Almost certain	0-10	1
Very likelihood system will detect risk.	Very High	10-20	2
High chance the system will almost certainly detect a potential risk.	High	20-30	3
Moderately high likelihood system will detect risk.	Moderately High	30-40	4
Moderate chance that the system will detect a risk.	Moderate	40-50	5
Low likelihood system will detect risk.	Low	50-60	6
Very low likelihood system will detect risk.	Very Low	60-70	7
Remote chance that the system will detect a risk.	Remote	70-80	8
Risk most likely remains undetected.	Very Remote	80-90	9
Risk is not detectable.	Almost Impossible	90-100	10

TABLE IV. RISK CLASSIFICATION ON BASICS OF FUZZY RPN

Trapezium Membership function	Linguistic Variable	Rank
[0,0,100,200]	None	1
[100,200,200,300]	Very low	2
[200,300,300,400]	Low	3
[300,400,400,500]	High low	4
[400,500,500,600]	Low medium	5
[500,600,600,700]	Medium	6
[600,700,700,800]	High medium	7
[700,800,800,900]	Low high	8
[800,900,900,1000]	High	9
[900,900,1000,1000]	Very high	10

The main purpose of the AI procurement process in the public sector is to fulfil the requirements of public administration, such as government modernization and digitalization (Wegener & Müller, 2018). It can also be regarded as a means to promote good governance (Mehr, 2017; Solihati & Indriyani, 2021). The AI procurement process involves managing materials, purchasing transactions, and activities to ensure the quality of purchased AI products based on the requirements set for them (Karlsson, 2020). It involves all functions, from identifying needs to the selection of sources and awarding and administration of contracts as shown in Fig. 1.

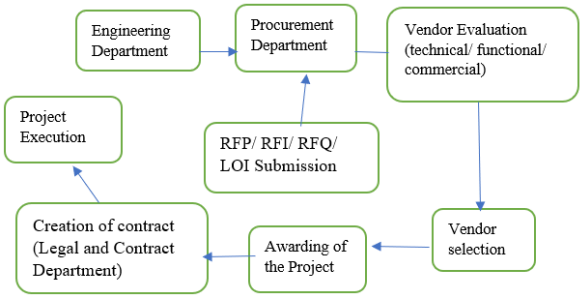


Fig. 1. AI procurement process common to the UAE Public Sectors.

AI procurement risks refer to those risks which are associated with the purchase of AI technologies/systems. The increased visibility of associated risks in AI projects led to a more strident clamour for ethical, legal, and secure adoption. Based on the literature and subsequent interviews with practitioners from UAE public sectors, the participants identified the following risks in the procurement of AI projects in their respective organizations: privacy and security risks, integration risk, skills risk, risk of time frame, the risk of financial economic loads, and risk regarding vendors. They also identified other risks such as risk of miscommunication and the risk of system malfunction. The list of risks was also validated by a focus group discussion. The risks and their definitions are represented in Table V.

TABLE V. BRIEF DESCRIPTION OF RISKS ASSOCIATED WITH AI PROCUREMENT PROCESS

Risk	Definition
Privacy and security risk	Privacy risk refers to the likelihood of experiencing problems arising from data processing and the impact that it may bring. Security risk deals with the possibility of losses resulting from information security concerns.
Ethical risk	It is associated with the possibility of reputational or moral harm to individuals or organizations. In AI procurement, this risk involves moral dilemmas due to the process of AI-driven dehumanization and displacement of human control
Integration Risk	In AI procurement, it refers to the probability of failure of the integration of systems, technologies, or information due to system incompatibility.
Skill-related Risk	It deals with the likelihood of lack of or inadequate skills that the workforce may encounter by introducing new technology to the organization.
Legal risk	It refers to the potential failure of an organization to comply with regulations or terms of the contract. In AI procurement, AL algorithms or data misuse can lead to legal liability risks.
Risk of Environmental Sustainability influencing Hazards	It refers to the probability of hazards posed against maintaining an ecological balance in the natural environment and against conserving natural resources for the utilization of current and future generations.
Financial Load risk	It refers to the probability of losing money or danger than can lead to the loss of capital. In AI procurement, financial load risk may be due to exceeding allocated budget.

Time frame-related risk	It deals with the possibility of time impacting the project, such as delay. In AI procurement, this risk can lead to cost overruns.
Vendor related risk	It refers to risks associated with vendors, such as delays caused by vendors, overpricing of technology provided, security breaches, and unforeseen vendor in capabilities, amongst others, which can cause reputational damage to the organization.
Risk of Miscommunication	It refers to the likelihood of the personnel or workforce to fail to communicate adequately (including top-bottom and bottom-up channels of information flow). In AI procurement, this can lead to bias in decision-making.
Risk of System Malfunction	It deals with the probability of system failure, error, or malfunctioning. In AI procurement, this may arise from not being able to regularly update the system's network.

Fuzzy FMECA was performed for AI Procurement process (see Fig. 1). To identify the risk elements, Literature review, Interviews with experts and Focus group discussion were employed. The validated list of risks is presented in Table V. In the proposed study fuzzy logic is used to address the issues in prioritization of these risks. In expert elicitation, the experts, from UAE public sector with extensive understanding of the AI procurement process, used fuzzy language phrases to define the risk variables O, S, and D. The O, S, D values for each risk are collected from the experts using an online survey. In total, 22 responses were recorded. The seven responses were discarded as data were missing or non-serious inputs are seen. Finally, we have taken the average value of O, S, and D for each risk elements and traditional RPN was calculated as shown in Table VI. RPN is a class based on the classes of O, S, and D assigned by the expert, rather than a product of multiplied values of O, S, and D.

TABLE VI. RPN AND PRIORITISATION OF RISKS

Sl. No.	Risks	Occurrence ranking	Severity Ranking	No-Detection Ranking	RPN	Priority
1	Privacy and Security Risk	8	8.1	5.3	343	1
2	Ethical Risk	5.7	6.9	5.8	228	3
3	Integration Risk	7	7.1	4.8	239	2
4	Skill Related Risk	6.1	5.9	4.8	173	7
5	Legal Risks	5.2	6.3	6.2	203	5
6	Environmental Risk	4	6.3	5.7	144	11
7	Financial Risk	6.2	6.2	4.3	165	9
8	Time Frame Related Risk	6	5.6	4.9	165	9
9	Vendor Related Risk	6.3	5.8	4.6	168	8
10	Miscommunication Risks	5.7	6.7	5.3	202	6
11	System Malfunction Risk	6.2	6.9	5	214	4

The different scales used to measure the two components O and S are shown in Tables I and II. The scale used to measure the parameter D is shown in Table III. These measures assess the likelihood of occurrence, severity, and likelihood of non-detection (see Table IV). The risks data came from a survey based on experts' opinion for AI procurement Process risk analysis. 11 risk elements were identified and prioritized based on the appropriate RPN score (see Table VI).

Fig. 2 depicts an overview of the fuzzy logic method. The study consists of three primary steps: (i) Fuzzification employing linguistic variables to turn the three risk factors S, O, and D into fuzzy membership functions. (ii) Rule assessment based on expert knowledge of the relationships between various risks and the effect, as represented by fuzzy if-then rules. (iii) A de-fuzzification technique generates a crisp ranking from the fuzzy RPN to provide the failure mode prioritization level.

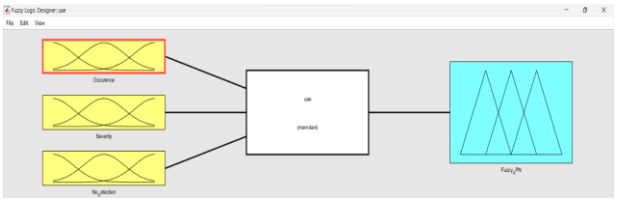
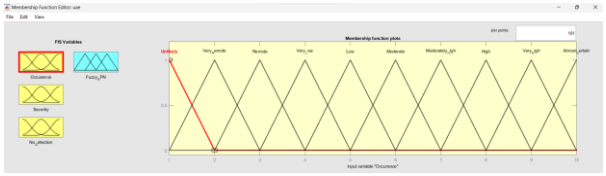
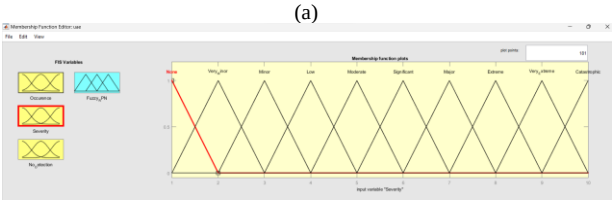


Fig. 2. Schematic of fuzzy logic process for FMECA Using Matlab FIS editor.

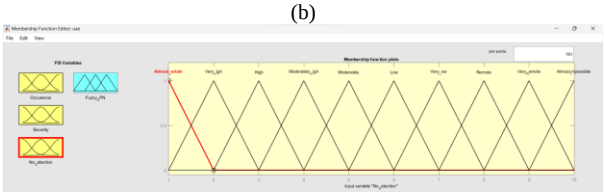
The complete fuzzification procedure was carried out in MATLAB using the fuzzy toolbox, with the triangular membership function representing the inputs O, S, and D as shown in Fig. 3(a), 3(b), and 3(c). The triangular membership function was also employed to depict the FRPN output membership functions (see Fig. 4).



(a)



(b)



(c)

Fig. 3. (a): Membership functions for input variable 'Occurrence', (b): Membership functions for input variable 'Severity', (c): Membership functions for input variable 'Detection'.

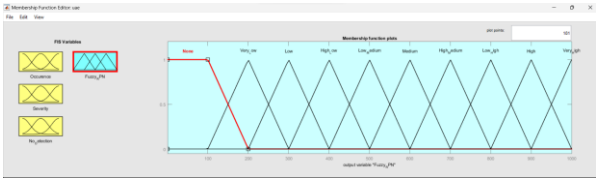
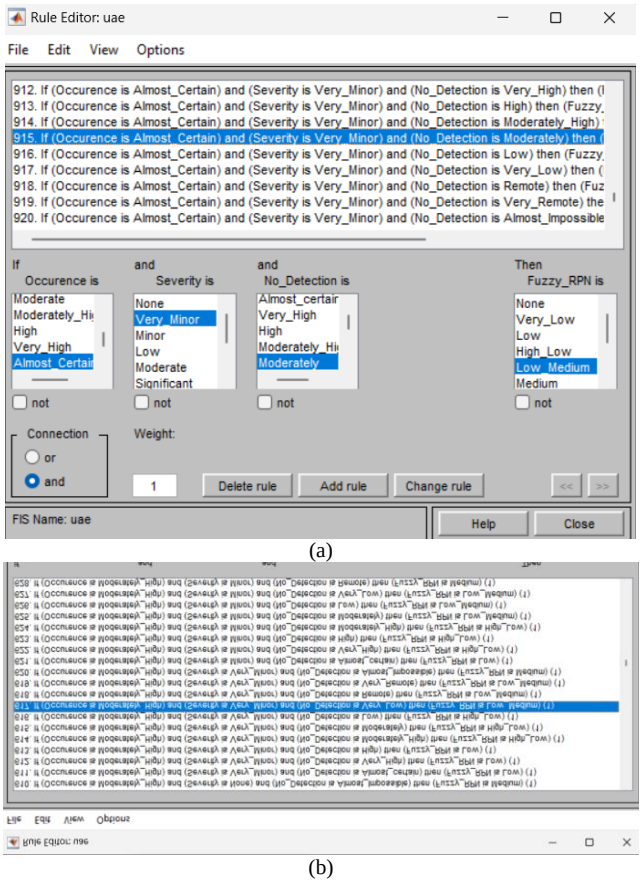


Fig. 4. Membership functions for Output variable 'Fuzzy RPN'.



(a)

(b)

Fig. 5. (a): Rule base developed for relating O, S &D to FRPN using expert elicitation, (b): Rule base developed for relating O, S &D to FRPN using expert elicitation.

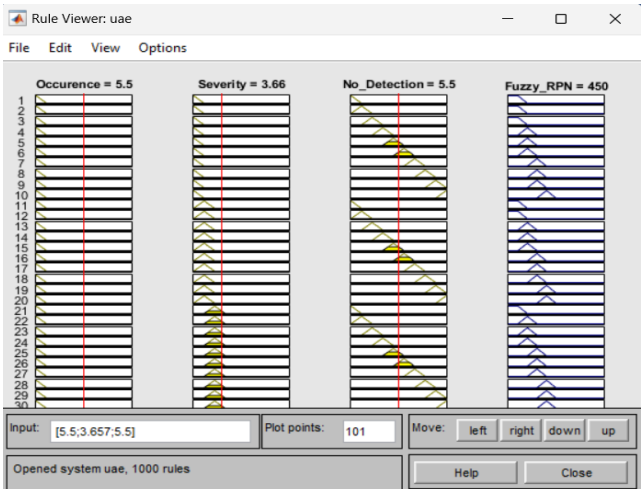
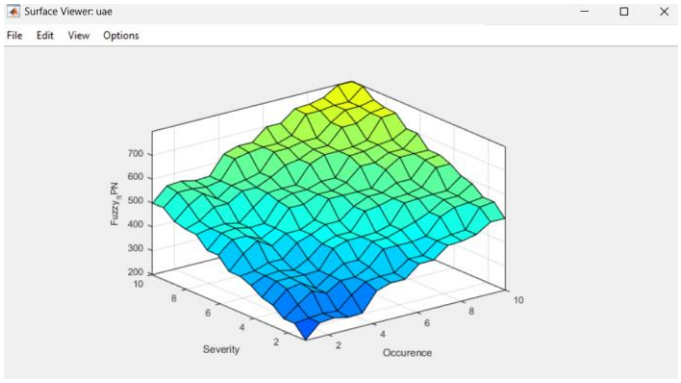


Fig. 6. Defuzzification at the rule plot in Matlab.

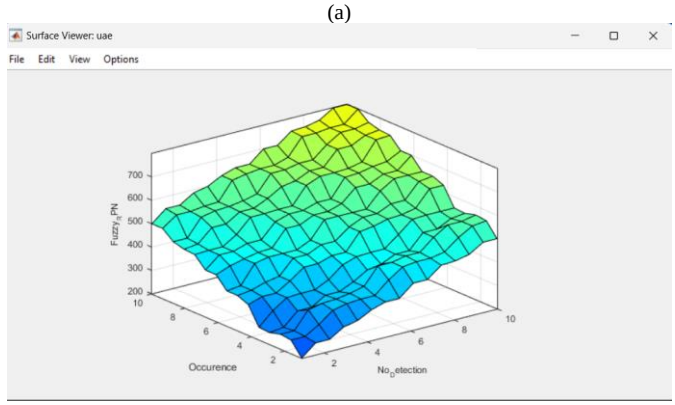
The input values of O, S, and D were provided by experts. As 15 experts' opinions were considered, an average value of O, S and D were taken into consideration. For the analysis, 1000 if then rules were developed as shown in Fig. 5(a) and (b). These criteria are intended to cover all conceivable O, S, and D combinations. The Mamdani min/max inference mechanism is utilised (input method: min; aggregate method: max), and the results are defuzzied using the centre of gravity approach (see Fig. 6).

IV. Results and Discussion

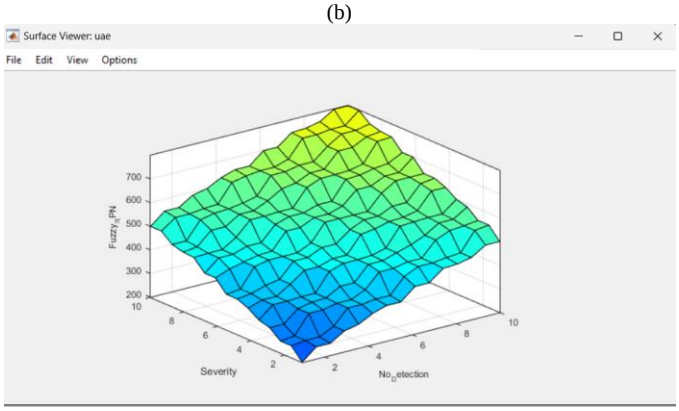
A basic condition for fuzzy inference applications is that the fuzzy system's output be monotonic with regard to its inputs [40]. The suggested model's rule base is nondecreasing as can be seen from the output surface plots as shown in Fig. 7(a), (b), (c).



(a)



(b)



(c)

Fig. 7. (a): Surface plot of Occurrence and severity vs. FRPN in Matlab Surface viewer., (b): Surface plot of Occurrence and No-Detection vs. FRPN in Matlab Surface viewer. (c): Surface plot of Severity and No-Detection vs. FRPN in MATLAB Surface viewer

The values of the inputs (O, S, and D) from the data collecting process are supplied to the FIS system during implementation and result extracted to produce the Fuzzy RPN. The Fuzzy RPN values associated with each risk is shown in Table VII along with priority. It can be seen that the

distribution of output value of Fuzzy RPN is more uniform compared to traditional RPN. It can be also seen that Fuzzy RPN numbers obtained are more realistic to interpret. For example, using conventional process, RPN is calculated conventionally by multiplying O, S, and D (10*6*6) = 360. The standard RPN, which corresponds to class 7, has been improved by integrating the linguistic phrase "high medium" matching to this class. In order to compare and validate, the ranking of risk elements based on Fuzzy RPN, As demonstrated in Table VII, a focus group discussion was conducted. The experts from public sector of UAE government were invited and provided with the ranking obtained by this study. Majority of experts expressed their agreement with the ranking obtained by this method.

TABLE VII. FUZZY RPN AND PRIORITISATION OF RISKS

Sl. No.	Risks	Occurrence ranking	Severity Ranking	No-Detection Ranking	Fuzzy RPN	Priority
1	Privacy and Security Risk	8	8.1	5.3	700	1
2	Ethical Risk	5.7	6.9	5.8	578	4
3	Integration Risk	7	7.1	4.8	600	2
4	Skill Related Risk	6.1	5.9	4.8	511	9
5	Legal Risks	5.2	6.3	6.2	531	7
6	Environmental Risk	4	6.3	5.7	500	10
7	Financial Risk	6.2	6.2	4.3	522	8
8	Time Frame Related Risk	6	5.6	4.9	500	10
9	Vendor Related Risk	6.3	5.8	4.6	532	6
10	Miscommunication Risks	5.7	6.7	5.3	569	5
11	System Malfunction Risk	6.2	6.9	5	589	3

The results obtained suggest that Privacy and Security risk is predominant in the case of AI Procurement Process. Various studies also suggested that the privacy and security risk is very important compared to others [41, 42]. The privacy and security risks involved with data privacy concerns, data security vulnerabilities, algorithm biasness, lack of transparencies, adversarial attacks on the system, dependency of third-party vendors and so on. Considering the stakes involved, this risk is considered as most important and having highest impact among all risks.

The next risk of major concern is the integration risk. The integration risk may be faced due to various issues such as data compatibility, system compatibility, customization requirements, skill gaps, user adoption, performance and scalability and vendor reliability. The integration risk is also found to be very important [43]. Considering the importance of integration for example even a city-level law enforcement agency, for example, may not be aware of all the systems utilised across its many departments, how data is linked, and how the outputs shape their practises and policies. Sanchez-Graells, A. [3] highlighted that integration risk makes it difficult for the public and civil society to engage with the appropriate partners, gather information, and hold anybody accountable.

The risk of system malfunction is also found to be a risk of high impact especially in areas where human life at stake such as healthcare sector [44]. The AI system malfunction can be happening due to various factors such as system complexity and maturity, data quality and biasness, model transparency, improper testing and validation, lack in robustness of model, integration issues with existing system, security measures which prevent unauthorised use. During the procurement phase, due care to be taken so that system malfunction cannot happen.

Another risk that is categorized of moderately high impact is ethical risk which associated with raise ethical concerns and may result in harm to individuals, communities, or society as a whole. Kuziemski, M. et al. [45] also support that as AI technologies grow more prevalent, organisations must address the ethical implications during the purchase process.

Risk of miscommunication is also found to be of moderately high impact. In AI procurement, miscommunication risks relate to the possibility of misunderstandings, misinterpretations, or imprecise communication between the parties engaged in the procurement process. As per Grewal and Sridhar [46], these risks might develop at any point during the procurement process, from early planning and needs collection to contract negotiations and implementation. Miscommunication can result in a variety of obstacles and issues, including unclear requirements, misaligned expectations, inaccurate scope and cost estimation, lack of understanding of technical specifications, data access and ownership, and vendor capabilities.

Other risk elements that are vendor related risks are found to be of moderate impact. In the AI procurement process, vendor-related risks refer to potential obstacles or concerns that result from the selection and engagement of an AI vendor or service provider. Choosing the correct vendor is critical since it has a direct influence on the success of the AI project and the organization's ability to meet its goals. Chopra A. [47] has identified several vendor-related concerns in artificial intelligence procurement such as vendor reputation and reliability, Vendor’s financial stability, lack of expertise and experience, Vendor lock-in, intellectual property issues, cultural fit, etc..

The legal risks involved in procurement of AI system or services are found to be moderate impact. This risk consists of issues arising due to intellectual property rights, data ownership and usage, data compliance, regulatory requirements, etc. Other risk elements are found to be of low to moderately low impacts are risk associated with time frame, finances, skill related and environmental risks. It should be noted that from the perspective of UAE public sectors, finance is not considered to be a major concern as well as skills. Further, timeframe and environmental related risks are also found to be of low impact on the AI procurement Process.

V. CONCLUSION

The proposed Fuzzy FMECA method was applied to rank the risks involved in the procurement of AI Services/ Systems in UAE Public Sectors. The study was carried out by employing fuzzy linguistic variables for occurrence, severity, and non-detection, and then combining these variables using an if-then rule base to achieve Fuzzy RPN or FRPN. The outcomes of traditional FMECA and fuzzy FMECA approaches are compared. Fuzzy FMECA has been proven to be an excellent approach for prioritizing the risks associated with AI procurement Process. The Privacy and security risk are found to be most important, then, Integration risk and system malfunction risks. Other Moderately impact risks are ethical risk, miscommunication risk, vendor related risk and legal risks. The risk associated with finances, skills, environment and time frame were found be of moderate or low impact. The ranking of these risks is validated by a focus group study. This method can be extended to rank the risks involved in other complex systems or prioritizing the different alternatives for decision making.

REFERENCES

[1] Halaweh, M., Artificial intelligence government (Gov. 3.0): the UAE leading model. Journal of Artificial Intelligence Research, 2018. 62: p. 269-272.

[2] AE, U., UAE national strategy for artificial intelligence 2031. 2018.

[3] Hickok, M., Public procurement of artificial intelligence systems: new risks and future proofing. AI & society, 2022: p. 1-15.

[4] Sanchez-Graells, A., Governing the Assessment and Taking of Risks in Digital Procurement Governance. To be included in A Sanchez-Graells, Digital Technologies and Public Procurement. Gatekeeping and experimentation in digital public governance (OUP, forthcoming), 2022.

[5] Mikulak, R.J., R. McDermott, and M. Beauregard, The basics of FMEA. 2017: CRC press.

[6] Chin, K.-S., A. Chan, and J.-B. Yang, Development of a fuzzy FMEA based product design system. The International Journal of Advanced Manufacturing Technology, 2008. 36: p. 633-649.

[7] Chanamool, N. and T. Naenna, Fuzzy FMEA application to improve decision-making process in an emergency department. Applied Soft Computing, 2016. 43: p. 441-453.

[8] Balaraju, J., M.G. Raj, and C.S. Murthy, Fuzzy-FMEA risk evaluation approach for LHD machine–A case study. Journal of Sustainable Mining, 2019. 18(4): p. 257-268.

[9] Baykasoğlu, A. and İ. Gölcük, Comprehensive fuzzy FMEA model: a case study of ERP implementation risks. Operational Research, 2020. 20: p. 795-826.

[10] Tixier, J., et al., Review of 62 risk analysis methodologies of industrial plants. Journal of Loss Prevention in the process industries, 2002. 15(4): p. 291-303.

[11] Bathrinath, S., R. Bhalaji, and S. Saravanasankar, Risk analysis in textile industries using AHP-TOPSIS. Materials Today: Proceedings, 2021. 45: p. 1257-1263.

[12] Shariat, R., A. Roozbahani, and A. Ebrahimian, Risk analysis of urban stormwater infrastructure systems using fuzzy spatial multi-criteria decision making. Science of the Total Environment, 2019. 647: p. 1468-1477.

[13] TAN, M.H. and W.L. LEE, Evaluation and improvement of procurement process with data analytics. International Journal of Advanced Computer Science and Applications, 2015. 6(8): p. 70.

[14] Delima, R., et al., Development of purchasing module for agriculture e-Commerce using Dynamic System Development Model. International Journal of Advanced Computer Science and Applications, 2018. 9(10).

[15] Bowles, J.B. and C.E. Peláez, Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis. Reliability engineering & system safety, 1995. 50(2): p. 203-213.

[16] Sankar, N.R. and B.S. Prabhu, Modified approach for prioritization of failures in a system failure mode and effects analysis. International Journal of Quality & Reliability Management, 2001. 18(3): p. 324-336.

[17] Putcha, C.S., et al., A case study on FMEA applications to system reliability studies. International Journal of Reliability, Quality and Safety Engineering, 2008. 15(02): p. 159-166.

[18] Vinodh, S. and D. Santhosh, Application of FMEA to an automotive leaf spring manufacturing organization. The TQM Journal, 2012. 24(3): p. 260-274.

[19] Mirghafoori, S.H., H. Sayyadi Tooranloo, and S. Saghafi, Diagnosing and routing electronic service quality improvement of academic libraries with the FMEA approach in an intuitionistic fuzzy environment. The Electronic Library, 2020. 38(3): p. 597-631.

[20] Wu, Z., et al., Nuclear product design knowledge system based on FMEA method in new product development. Arabian Journal for Science and Engineering, 2014. 39: p. 2191-2203.

[21] Ho, C.-C. and M.-S. Chen, Risk assessment and quality improvement of liquid waste management in Taiwan University chemical laboratories. Waste management, 2018. 71: p. 578-588.

[22] Chiozza, M.L. and C. Ponzetti, FMEA: a model for reducing medical errors. Clinica chimica acta, 2009. 404(1): p. 75-78.

[23] Aldenny, M., et al. The Implementation of Failure Mode and Effects Analysis (FMEA) of the Information System Security on the Government Electronic Procurement Service (LPSE) System. in Pervasive Computing and Social Networking: Proceedings of ICPCSN 2021. 2022. Springer.

[24] Kumru, M. and P.Y. Kumru, Fuzzy FMEA application to improve purchasing process in a public hospital. Applied soft computing, 2013. 13(1): p. 721-733.

[25] Nahavandi, N. and P. Tavakoli, RISK MANAGEMENT OF PROCUREMENT PROCESSES IN AUTOMOTIVE SUPPLY CHAIN; BAHMAN MOTOR COMPANY. International Journal of Industrial Engineering, 2022. 29(1).

[26] Rai, R.N., Select study of procurement process and availability improvement in military aviation. 2013, IIT Delhi.

[27] Handayani, D.I., Risk Management Of Supplier-Buyer In Procurement Of Raw Materials For Improving Supply Chain Performance. Jurnal Manajemen, 2018. 22(3): p. 293-309.

[28] Ahmed, S. and X.-C. Gu, Accident-based FMECA study of Marine boiler for risk prioritization using fuzzy expert system. Results in Engineering, 2020. 6: p. 100123.

[29] Erozan, İ., A fuzzy decision support system for managing maintenance activities of critical components in manufacturing systems. Journal of Manufacturing Systems, 2019. 52: p. 110-120.

[30] Iadanza, E., et al., Fuzzy FMECA Process Analysis for Managing the Risks in the Lifecycle of a CBCT Scanner. IEEE Access, 2021. 9: p. 135723-135741.

[31] Zúñiga, A.A., J.F. Fernandes, and P.J. Branco, Fuzzy-Based Failure Modes, Effects, and Criticality Analysis Applied to Cyber-Power Grids. Energies, 2023. 16(8): p. 3346.

[32] Renjith, V., P.H. Kumar, and D. Madhavan, Fuzzy FMECA (failure mode effect and criticality analysis) of LNG storage facility. Journal of loss prevention in the process industries, 2018. 56: p. 537-547.

[33] Kinkel, S., M. Baumgartner, and E. Cherubini, Prerequisites for the adoption of AI technologies in manufacturing–Evidence from a worldwide sample of manufacturing companies. Technovation, 2022. 110: p. 102375.

[34] Wan, N., et al., Risk assessment in intelligent manufacturing process: a case study of an optical cable automatic arranging robot. Ieee Access, 2019. 7: p. 105892-105901.

[35] Sarwar, M., G. Ali, and N.R. Chaudhry, Decision-making model for failure modes and effect analysis based on rough fuzzy integrated clouds. Applied Soft Computing, 2023. 136: p. 110148.

[36] Wang, Y.-M., et al., Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean. Expert systems with applications, 2009. 36(2): p. 1195-1207.

[37] Liu, H.-C., L. Liu, and N. Liu, Risk evaluation approaches in failure mode and effects analysis: A literature review. Expert systems with applications, 2013. 40(2): p. 828-838.

[38] Yen, J., Fuzzy logic: intelligence, control, and information. 1999: Pearson Education India.

[39] Makowski, A. and S. Mannan, Fuzzy logic for piping risk assessment. Journal of Loss Prevention in the Process Industries, 2009. 22(6): p. 921-927.

[40] Kouikoglou, V.S. and Y.A. Phillis, On the monotonicity of hierarchical sum–product fuzzy systems. Fuzzy sets and systems, 2009. 160(24): p. 3530-3538.

[41] Dilmaghani, S., et al. Privacy and security of big data in AI systems: A research and standards perspective. in 2019 IEEE International Conference on Big Data (Big Data). 2019. IEEE.

[42] Gopalan, S.S., A. Raza, and W. Almobaideen. IoT security in healthcare using AI: A survey. in 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA). 2021. IEEE.

[43] Spreitzenbarth, J.M., H. Stuckenschmidt, and C. Bode, The state of artificial intelligence: Procurement versus sales and marketing, in Supply Management Research: Aktuelle Forschungsergebnisse 2022. 2022, Springer. p. 173-193.

[44] Ayling, J. and A. Chapman, Putting AI ethics to work: are the tools fit for purpose? AI and Ethics, 2022. 2(3): p. 405-429.

[45] Kuziemski, M. and G. Misuraca, AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. Telecommunications policy, 2020. 44(6): p. 101976.

[46] Grewal, R. and S. Sridhar, Commentary: Toward formalizing social influence structures in business-to-business customer journeys. Journal of Marketing, 2021. 85(1): p. 98-102.

[47] Chopra, A. AI in supply & procurement. in 2019 Amity International Conference on Artificial Intelligence (AICAI). 2019. IEEE.