International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 6 | ISSN : 2456-3307

A Need to Modify the Method of Failure Mode and Effect Analysis (FMEA) and Risk Management

[1]Nina Fadilah Najwa, [2]Apol Pribadi Subriadi
[1]Department of Information Systems, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia
[2]Department of Information Systems, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia

ABSTRACT

The proper using of FMEA method is proven to reduce the cycle of warranty costs and will certainly cost less to prevent than to fix the problems that have already occurred. FMEA also was suitable for assessing risk in information technology or systems aspect. Several studies criticized the FMEA limitation or weakness of using this method. The purpose of this paper is to provide a resume and critical analysis of previous research that discussed the development and limitation of FMEA. A systematic literature review methodology was conducted in order to review FMEA. As a result, 32 papers were obtained in the selection stage according to the criteria used and review based on quality content. Data collection and identification stage was carried out by the selected papers for further analysis and synthesis. The limitation FMEA was due to the subjectivity and caused inconsistent results. This paper provided the critical analysis about the point of weakness FMEA based on document FMEA, and also limitation FMEA based on risk management process. There were eight research questions that could be considered from the results. By conducting a literature review of the development and trending of FMEA research, it provided new research opportunities to proved the FMEA issues reviewed in this paper.

Keywords : FMEA, Subjectivity, Inconsistent, Risk Management, Critical Analysis.

I. INTRODUCTION

Risk management is one of the topics included in the scope of information systems research[1]. Risk management is a systematic strategic, procedural, and practical management application for identifying, analyzing, controlling, and monitoring risk processes. This was important to ensure good quality and reduce the risk of failure of a product or service[2]. Companies could manage common risks that exist in routine activities by risk management so that companies could run their activities more effectively and will get better results at a lower cost[3]. There were many methods that could be used for risk analysis such as those contained in ICH Q9 on quality risk management such as Failure Mode Effects and Analysis (FMEA), Failure Mode, Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Hazard Analysis and Critical Control Points (HACCP), Hazard Operability Analysis (HAZOP), Preliminary Hazard Analysis (PHA) and Risk Ranking and Filtering[4].

FMEA was one of the important techniques in managing risks related to what things should be understood and utilized. FMEA was built on environmental collaboration, including employees and overall aspects of the company's business process

activities [5]. FMEA provided a common structure and language that could be used by teams in manufacturing and services, profit and non-profit organizations, private organizations, public, or governmental organizations[6].

The proper of using FMEA method is proven to reduce the cycle of warranty costs and will certainly cost less to prevent than to fix the problems that have already occurred[7]. The using of FMEA might be applicable to the security, finance, software design, information technology or systems, marketing, human resources and purchasing[6]. In particular, the system or information technology section discussed the use of the FMEA method to determine the security of sensitive data. Selection of FMEA methods other than a commonly used method, since FMEA could be well-documented easily[4].

There were several studies that criticized the FMEA method, there was a limitation or weakness of using this method. Weakness occurred especially when performing RPN calculations because of the element of subjectivity, the potential value of RPN was not sustainable, there was a duplicate RPN value, practically mentioning RPN was not recommended to use[7]. Traditionally, FMEA only considered the impact of a failure of a system, so it was necessary to examine the strategy in defining risk and its calculation[8]. Thus, the result of risk analysis using FMEA was an issue of consistency and subjectivity[9][10][11][5].

This paper provided a resume of previous research that addresses the development of FMEA as well as FMEA limitation. There were 32 papers related FMEA was discussed and synthesized related to FMEA shortcoming. The synthesis was done by looking at risk management process that is identification, analysis, and risk evaluation. The discussion divided into perspectives in terms of FMEA such as critical perspective, FMEA limitation impact perspective, FMEA in Information security aspect. This paper also provided a critical analysis. The critical analysis was conducted by risk management process, the point of weakness FMEA based on FMEA methodology and document FMEA. Thus, by conducting a literature review of the development and trend of FMEA research, it provides new research opportunities to prove the FMEA issues reviewed in this paper.

II. THEORETICAL BACKGROUND

A. Risk Managemant

The concept of risk management was first introduced by Doug Bartlow in the USA around 1950 and in the UK in 1969[12]. According to Risk Management standard AS / NZS 4360 (1999)[13], the risk management process referred to covering the weaknesses in a method used in product development through a structured approach so that mitigation actions could be initiated to prevent risks, risk transfer, decrease the likelihood of risk or mitigate risk impacts. The management process proposed by AS / NZS 4360 was a related risk management process. The process consists of seven stages of sub-process iteration from the risk context of risk identification, risk analysis, risk evaluation, communication, and risk consulting with stakeholders, monitoring and managing risk events.

Meanwhile, according to Alexander (1992), the risk management process consists of four stages of risk identification using various techniques by filling out threat forms, analyzing by measuring the frequency and severity if possible threats occur, controlling by physical measure and conducting employee training to reduce acceptance threats and financial consequences, and calculate the cost of risk by planning the estimated losses if risks occur or the costs of handling and mitigating. The process of risk management is assumed to be an important strategy within the organization to plan for the reduction of risk from occurring or minimize the consequences of the event[14]. The risk management strategy generally consists of four strategies: risk prevention

(reducing possibilities), impact mitigation (mitigation), transfers (delegates risk to third parties as insurance insurers), and risk acceptance [15].

B. Information Security Risk

IT gave the big impact on business processes such as the company's products, business values, and other performance targets. The higher the intensity of IT usage in an industry, the higher company's dependence on IT. There was a positive and significant correlation between IT Resources with performance [16][17]. The better IT resources, the better company performance. Besides, not all exploration efforts on IT resources will have a significant impact on performance[16]. Thus, the higher level of dependence on IT then the relationship with performance will be the greater and also the existing IT risk higher.

IT risk is related to threats and harm due to intensive of using IT. Risks could cause unwanted or unexpected damage, misuse, loss in the overall business model and include its environment [18]. Threats are potential sources of certain threats to successfully implement certain vulnerabilities. The vulnerability is a weakness that is accidentally triggered or deliberately exploited. The source of the threat poses no risk if there is no vulnerability [19]. Assets in the IT security perspective are all valuable things that must be protected from harmful things. The information security aspects include confidentiality, integrity, and availability[20].

C. Failure Mode Effect and Analysis (FMEA)

Failure Modes Effect Analysis (FMEA) according to McCain (2006) is a risk management tool used to identify failures that will occur in a process, product or service. Before the failure occurs, proactive steps are to be designed and implemented. The FMEA implementation involved creating a risk factor called the Risk Priority Number (RPN) which is the result of assessing the severity of each potential failure of the customer (Severity), the possibility of occurrence of the failure (Occurrence) and the possibility of detection before the failure to reach the customer [21]. Preventing process and product issues before they occur was the goal of FMEA. Used in both design and manufacturing processes, substantively reducing costs by identifying products and processes increasing faster in the development process when changes were easy to make and less expensive to make. The result was a more assured process because it reduced or eliminated corrective action after the occurrence of problems and crisis changed[6].

The FMEA team determined, with failure mode analysis, the impact of each failure and identified every critical point of failure. Furthermore, each failure rating would be based on the most critical and possible failure impacts[22]. The results of this FMEA would help managers and technicians to identify failure modes, their causes and improvements while at the design and production stage[23]. FMEA had several common types, they were FMEA systems, FMEA design, and FMEA processes. The FMEA system can be used at the level of analysis of the entire system, which is built on many subsystems. The focus of this FMEA type for system security, system integration, interface or interaction between subsystems with other systems, interaction with the environment, human interaction, services, and various other issues that could cause the system could not work how it should be. The design of FMEA focused on product design, usually at the subsystem or component level. The focus was on design-related deficiencies, taking into account improvements in design and ensuring safe and reliable product operation during use of equipment. Meanwhile, the scope of the FMEA Process might include manufacturing and assembly operations, shipping, entry, material transport, storage, conveyors, tool maintenance, and labeling.

There were various FMEA types such as Failure Mode Effects and Criticality Analysis (FMECA) similar to FMEA, with additional steps of more

formal critical analysis. This additional step usually required objective data to support criticality calculations. It is recommended for practitioners who are required to conduct FMECA analysis to understand the basics of FMEA first, and then to study the FMECA procedure. Some other FMEA types include FMEA Concepts, FMEA Maintenance, Hazard Analysis, FMEA Software[7].

III. METHODOLOGY

In this stage would be described the steps undertaken in conducting a systematic review of the literature to several stages[24].

A. Determination of Research Objective

This literature review aimed to provide the reader with an overview of the topics of interest regarding the use of FMEA methods in risk management.

B. Search Process and Strategy

The literature search process that could answer research questions needs to be done by the search strategy. To obtain good quality journals, the sources used for literature searching are limited to international journals sites:

1. ScienceDirect (http://www.sciencedirect.com)
2. Emerald Insight (http://www.emeraldinsight.com)
3. IEEE (http://www.ieeexplore.ieee.org)

After determining the literature search database, then the next step was the determination of literature search keywords. The keywords used were as follows:

1. Failure Mode Effect and Analysis (FMEA)
2. FMEA in Risk Management
3. Modification of FMEA

C. Inclusion And Exclusion Criteria

The determination of inclusion and exclusion criteria is needed to provide a limitation in the selection of the literature to be reviewed, based on predetermined criteria. The inclusion criteria and exclusion criteria used in this literature review were as follows:

Inclusion Criteria:

1. The contents of the paper in accordance with what would be discussed by reading the research abstract.
2. Paper used in the form of journals or conferences.
3. Paper used in the language of instruction was English.
4. Included in the criteria topic (information system and risk management).
5. The paper used comes from the literature on the international journals provider site.

Exclusion Criteria:

1. The topic was not related to the discussion of the FMEA method and did not include research questions.
2. The introductory language of the paper did not use English.
3. Publications that were not accessible.

D. Inclusion And Exclusion Criteria

Preparation of paper quality measurement criteria is conducted to meet the research questions that have been formulated previously.

1. How the flow of thought (background, basic theory, things developed) in the paper discussed?
2. What keywords are used in the paper discussed?
3. How are solutions or problems raised in the paper discussed?

4. How the findings (theory denied or not and the relevance of previous research) in the paper discussed?
5. What are the limitations and opportunities for future research on the paper discussed?
6. What recommendations do the papers discuss both theoretically and practically?

E. Data Extraction And Synthesis

The purpose of data extraction was to obtain accurate and consistent information. The data included in the extraction is the identification, author name, year of publication, source, reference, data collection methodology, data analysis, and concepts. Additional paper searches are also obtained from references from main papers which form the basis for the idea of making this literature review.

IV. RESULT AND DISCUSSION

A. FMEA Topics In Statistic

FMEA has been used for more than 40 years. FMEA was formally used by the aviation industry in the mid-1960s and addressed to security or security issues. The objective of FMEA's defense was to remember to prevent safety threats and incidents of accidents. The FMEA approach standardized the process in a common language that could be used in many different areas of the organization. FMEA could also be used by technical and non-technical employees of various levels[6].

From the literature search process undertaken, the following was the search results from the database that has been determined:

TABLE 1: LITERATURE SEARCH RESULTS (PROCESS DATA: 2010-2017)

Keyword	Science Direct	Emerald	IEEE
Failure Method Effect Analysis (FMEA)	2811	427	250
FMEA in Risk Management	2499	364	147
Modification of FMEA	1316	224	15

It could be seen in Table 1, the paper related to FMEA was mostly in Science Direct. After getting the paper in accordance with the keyword, the selection of papers was done based on predetermined criteria of inclusion and exclusion, and to see duplicate searches. Then, the measurement of the quality of the paper has been selected. The paper that done by measurement, would go through final stages of selection of paper. The results of the paper selection can be seen in table 2.

TABLE 2: PAPER SELECTION RESULTS (PROCESS DATA: 2010-2017)

Database	Total Retrieved	inclusion (year)	Final Selection
Science Direct	6626	3741	8
Emerald Insight	1015	441	12
IEEE	412	270	8
Addition relevant reference	-	-	14

From Table 2, a paper was obtained that was in accordance with the theme and scope to be discussed in this paper. The paper has gone through the inclusion stages and eliminating the duplicate file. Thus, it was further discussed prior research related to FMEA methods and further research opportunities that need to be considered for discussion.

B. Current and Future Research

Unlike other quality improvement methods, FMEA did not provide complex statistical calculations. The foundations of FMEA were team members and input results from the FMEA process and the need for clear time estimation and division of tasks.[6] The following was the result of this literature review based on four perspectives.

1) FMEA critical perspective

The limitation of FMEA has an impact on the consistency of the results of risk assessment. The core stages of risk management start from identification of context that usually called as analyze the business process. The next step is to identify risks by listing risk based on FMEA parameters (severity, occurrence, and detection). After that, the risk analysis and evaluation stage are to provide risk assessment based on the criteria scale, calculation of RPN and sort the RPN value from the largest value to the smallest. Thus, the classification is based on a process of risk management to see the focus of prior research in criticizing the limitation of FMEA (Appendix). The following was the classification based on code (Table 4).

TABLE 4: CLASSIFICATION BASED ON CODE RISK MANAGEMENT

Code		
1	2	3
Identification failure[25],[26],[27],[23],[28]	Criteria scale/Rank [29],[30],[31]	Subjectivity[21]
Bias in identification risk[32],[22],[33],[34],[4]	Proved inconsistency Method[10]	Subjectivity and strategy[35],[33],[36]
Potential failure, cause, impacts.[37],[38],[39],[40],[36]	Risk Assessment[11],[41],[26],[28],[40]	Competence of Stakeholder[42],[36]
Irregularities [9]	RPN[43],[5],[44],[38],[27],[39],[23]	Team[34],[4]
Success factor[7]	Scale Criteria & RPN[45]	Irregularities[9]
	RPN evaluation[46],[22]	Success factor[7]
	FMEA Process[36],[4]	
	Irregularities[9]	
	Success factor[7]	

Code: [1]Risk Identification, [2]Risk Analysis, and Evaluation, [3]People

The table above was showed that the FMEA weakness points were in the FMEA parameter assignment process. It also identified the existence of problems in the criteria scale that caused the FMEA team's bias in measuring risk. These problems had an impact on prioritizing the RPN value. Thus, based on the stages of risk management using FMEA these aspects need to be considered. More specifically, the weak points of FMEA based on the FMEA document were described in Figure 1.

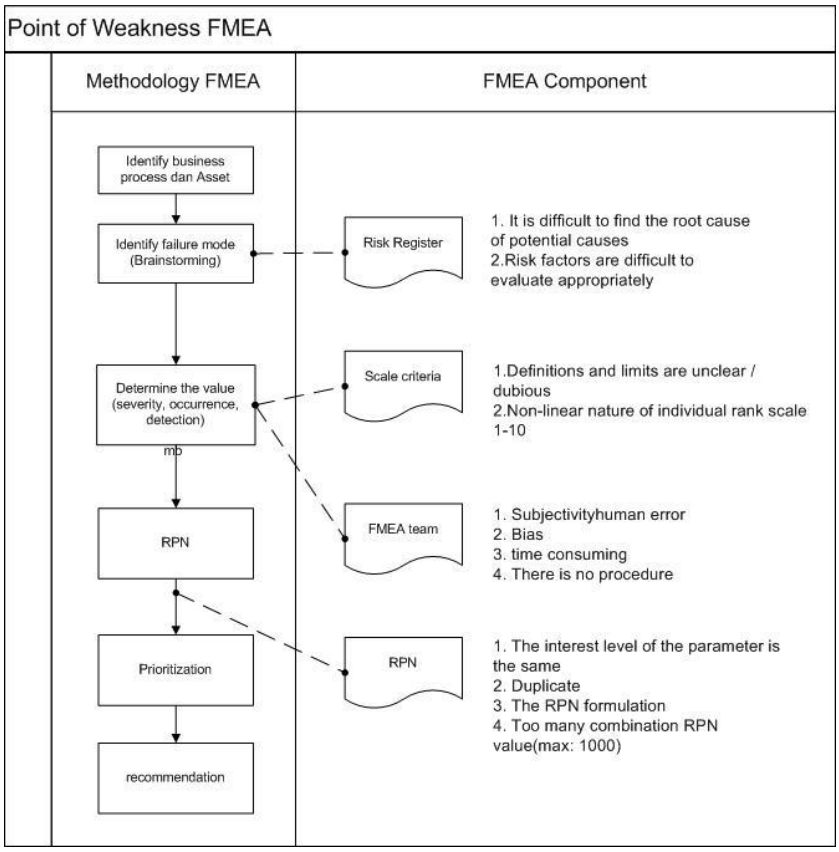

Figure 1: The point of Weakness FMEA

The proper use of FMEA could provide several benefits such as high product reliability, reduced design modifications, better quality of planning, continuous improvement of product and process design, and low production costs then can meet the needs of customers[5]. During the FMEA process, the RPN number of potential failures could support quantitative analysis of risk events, and this method not only finds high levels of risk appropriately and quickly but also addresses the concerns of loss and increases the reliability of a product[2]. Unlike other risk measurement procedures, FMEA could critically evaluate potential risks[42]. FMEA produced benefits, for prospective risk management and overall process improvement. It was used for management to continue to implement innovation management strategies by identifying the limits of risk priorities. FMEA was also useful for prospective risk management and overall process improvement[21].

FMEA had limitations or deficiencies based on the literature already reviewed and discrepancies found. Common problems that exist in FMEA based on experience[5], that lack of detailed information on product function or parts, potential failure modes, the potential impact of failures, potential causes of failure, and design of existing controls. Thus, with this lack of information, it led to misunderstanding, confusion or uncertainty in defining risk. Other issues were the integrity of FMEA documents that include the inconsistent issue of severity, occurrence, and detection issues, which some parts of the FMEA report were lost, the absence of high-risk recommendations based on the RPN, and the scale change of the rankings after correction.

Traditional FMEA used a linear-scale approach to determine severity, occurrence, and detection by numeric values. This scale criterion becomes a problem if unclear definitions and dubious constraints. The research was done by Paciarotti et al.[46] did modifications or improvements in terms of FMEA scales. This is done to minimize the shortcomings of FMEA. The study defines the scale

(1,3,9) in the assignment of S, O, D values (high, medium, low). Limiting the size of the parameter variables could make FMEA a faster method, more effective and produce strong results.

There was a subjective issue in prioritizing the risk, this was one of the limits obtained based on the review literature that had been done. Prioritization activities were performed on the basis of human emotions and thoughts, so there was doubt in the accuracy of the concept which also comes from the parameters used. The FMEA team would be difficult to determine the difference of opinion that occurred in the calculation, and the variables required in calculating the number of risks that were not appropriate and dubious[3]. Individual subjectivity and bias also impact on team dynamics. The error of defining risk depends on the experience of team members in analyzing the failures and familiarity of the system for members and known cognitive biases. Thus, the very possibility of human error in risk assessment. This situation often occurred when little data on the events and effects of failure are known, requiring subjectivity[29].

The inconsistent result caused by this subjectivity so there was a need for a strategy to overcome the subjectivity of FMEA team in doing a risk assessment. The time-consuming FMEA required multidisciplinary teams to understand well the process being analyzed. FMEA only help in identifying the possibility of a failed process, but not eliminating it, in addition to the need to establish an action plan and implement it[36]. Thus, not only capable of using FMEA but also implementing improvement actions.

The consistency of FMEA results could be improved by building the expertise of some facilitators who could assist the analyst team to use FMEA to be more effective and consistent by defining failure modes and severity, probability and indexes detected. Then, with experience, the facilitator would prove the value when evaluating the impact of the corrective action that had been done. The second possible strategy was always the presence of an expert member of a team, this had an impact on the value. There was at least two qualified personnel included in the FMEA team to balance significant individual differences in crucial risk decisions[11].

Another strategy was to combine FMEA with other methods. From the literature in the Fuzzy method could be the most widely used in FMEA modification. Using traditional FMEA and fuzzy based decision support systems eliminated uncertainty and subjective information[23]. In this literature was discussed studies combining FMEA with fuzzy. First, this research aims to make it easier for analysts, managers, and engineers to model, analyze and predict risk using FMEA with fuzzy combinations to be more realistic and consistent. In the phase of failure identification, this research used Root Cause Analysis (RCA). The using RCA was useful for deeper analysis to produce cause and risk detection. The theoretical contribution of this research was to integrate FMEA with qualitative (RCA and FMEA) approach as well as quantitative (fuzzy)[23]. Second, the research was done by Batbayar et al. [44] Based on his research that FMEA was not sufficient to measure different risks. The fuzzy approach was more accurately by involving the weight of the impact of different experts[27].

On the other hand, the use of fuzzy on the FMEA framework has its drawbacks[47]. First, it was difficult to define the relevant functions for risk factors because language or terms are difficult to understand easily. Secondly, it required a large cost and took a lot of time on fuzzy implementation. Third, complex calculations taking into consideration the loss of information in the risk analysis process. Thus, the implementation of fuzzy was in fact still

difficult and takes a long time in the process of risk analysis.

Further research is better to not eliminate the element of ease in FMEA, and look for other strategies to improve traditional FMEA performance in risk management. The combination is done from the approach to the mathematical model to the social approach of behavior. The relevance of the traditional FMEA is also an interesting subject for further investigation. Despite the many weaknesses of FMEA and the number of studies to minimize these weaknesses, it is still often used in various sectors. Thus, FMEA's reliability in risk management needs to be done critically.

Research questions were considered in this perspective are:

1. How consistency results from the use of FMEA?
2. What causes or affects the consistency of FMEA?
3. How does the strategy need to be done to overcome FMEA limitation?
4. How to synthesize FMEA framework to minimize FMEA consistency issues?
5. How relevant is the use of FMEA in the current period? Is it still relevant to use or not?
6. FMEA methods can be combined with various methods. Which is method best suits FMEA?

2) FMEA limitation impact perspective

According to Backlund dan Hannu (2002), FMEA had many a number of subjective approaches to risk management, but all had such limitations as not being able to produce consistent and relevant decision support. Not that a purely quantitative approach was free from problems. The subjective risk management, of course, was clearly a limitation that needs attention. Including FMEA's existing limitation was one of the approaches to risk management. Every organization wants supporters in the product and process in terms of security, trouble-free during business activities. When FMEA is used appropriately, FMEA could anticipate and prevent problems, reduce costs, shorten production times, and achieve safe and reliable products or services[7].

If FMEA was improperly used or inconsistent results exist, it will certainly harm the organization. This was because should the risk priority require a higher cost at the highest risk of ranking, but with the difference of risk ranking then the organization could make mistakes in the prevention or focus on handling. However, not always inconsistent risk results in FMEA indicated a poor weakness in risk analysis procedures. FMEA conducted by two different teams would provide valuable information that other teams did not identify[11]. This distinction raised a new definition of risk that did not exist previously. Thus, each FMEA team would be given the freedom to use this FMEA approach flexibly to define the risks found.

The research question that needs to consider was:

(g) What is the impact of FMEA consistency results?

3) FMEA in information security risk aspect

Organizations need information security that protected critical assets. The organization did the investment of IT to increase their performance. Thus, the organization was needed to consider the software estimation. This estimation was very important to be able to know how much the relevant value of software generated. The estimation purposed to predict the output of a project to review the schedule, cost, risk and also the effort in the project[48]. Investment of IT was need considering what product or specific application that suitable for the organization requirements. A poor investment product will increase the risk of IT[49]. One of the techniques for understanding the organization requirements was elicitation technique. Requirement

divided into a functional and nonfunctional requirement. If these requirements did not define at the early stages of software development then it affected the quality of the software and would take a lot of repair costs after the implementation of the system. Security was one of the aspects of non-functional requirements[50].

Information security was based on aspects of confidentiality, integrity, and availability. These information security risks will be affected both financially and non-financially. Thus, if the organization did not know the risks to be faced then the organization could not take effective preventive. FMEA was suitable for assessing risk in IT aspect[26]. Based on his research, the using of FMEA widely used in the industry sector, that is why this research objective to exploration FMEA in Information Technology sector. As the result, FMEA that had been modification more effective than traditional FMEA. The modification based on ISO 27001 (information security standard) that synthesize FMEA steps into PDCA cycle that was called as Infosec FMEA cycle. Another research of using FMEA in information technology was researched by Silva et al.[27] This research combined FMEA with the Fuzzy method. Based on the result of this research was the communication security dimension is the most important aspect of information security.

FMEA could use as a protected critical asset in IT [6]. In the real application, FMEA still not used widely in IT aspect[27][26]. This gap could be considered by academic researcher and practitioner for using FMEA in IT sector.

The research question that needs to consider was:

(h) How is the use of effective FMEA in IT Information Security Risk?

V. CONCLUSION

FMEA could anticipate and prevent problems, reduce costs, shorten production times, and achieve reliable security and products/services. However, there were several studies that criticized the FMEA method. Limitations were due to the subjectivity in risk management using FMEA and result in inconsistent results. FMEA limitation was due to the lack of detailed information on the function of a product or part, potential failure mode, potential impacts of failure, the potential causes failure, and the design of control. So that, this has led to a misconception, confusion or uncertainty in risk identification. Other problems was the integrity of the problem FMEA documents including the inconsistencies rank, which some part of the report FMEA missing, the absence of recommendations for the risk that height based on an RPN, change the scale of the rank after making any amendments, and activities prioritisation was done based on the human emotion and mind.

FMEA only helped in identifying the possibility of the process by which failed to, but not eliminated. In addition, there was an effort to build strategy and action plans to implement it. Based on the limitation FMEA issue, there were eight research questions that could be further study was for research to come. So that, the future research can analyze the consistency of FMEA, known the impact of consistency of FMEA, find out the cause of the issue of the consistency of FMEA, formulation the new strategy for FMEA, which is adjusted to synthesize FMEA, analyzes relevance FMEA with the present cases, know the right combination of other methods suitable for FMEA, and more exploration the using of FMEA in IT sector. In particular, the system or information technology section discussed the use of the FMEA method to determine the security of sensitive data.

VI. REFERENCES

[1] Sidorova, Evangelopoulos, Valacich, and Ramakrishnan, "Uncovering the Intellectual Core of the Information Systems Discipline," MIS Q., vol. 32, no. 3, p. 467, 2008.

[2] X. Zhao and X. Bai, "The application of FMEA method in the risk management of medical device during the lifecycle," 2010 2nd Int. Conf. E-bus. Inf. Syst. Secur. EBISS2010, pp. 455–458, 2010.

[3] M. Kakvan, M. A. Mohyeddin, and H. Gharaee, "Risk evaluation of IT service providers using FMEA model in combination with Multi-Criteria Decision-Making Models and ITIL framework," 2014 7th Int. Symp. Telecommun. IST 2014, pp. 873–878, 2014.

[4] J. F. van Leeuwen et al., "Risk analysis by FMEA as an element of analytical validation," J. Pharm. Biomed. Anal., vol. 50, no. 5, pp. 1085–1087, 2009.

[5] S. Gary Teng, S. M. Ho, D. Shumar, and P. C. Liu, "Implementing FMEA in a collaborative supply chain environment," Int. J. Qual. Reliab. Manag., vol. 23, no. 2, pp. 179–196, 2006.

[6] R. E. McDermott, R. J. Mikulak, and M. R. Beauregard, The Basic of FMEA, 2nd ed. New York: Taylor & Francis Group, 2009.

[7] C. S. Carlson, "Understanding and Applying the Fundamentals of FMEAs," 2014 Annu. Reliab. Maintainab. Symp., p. 12, 2014.

[8] N. Xiao, H. Z. Huang, Y. Li, L. He, and T. Jin, "Multiple failure modes analysis and weighted risk priority number evaluation in FMEA," Eng. Fail. Anal., vol. 18, no. 4, pp. 1162–1170, 2011.

[9] C. Estorilio and R. K. Posso, "The reduction of irregularities in the use of 'process FMEA,'" Int. J. Qual. Reliab. Manag., vol. 27, no. 6, pp. 721–733, 2010.

[10] D. M. Barends, M. T. Oldenhof, M. J. Vredenbregt, and M. J. Nauta, "Risk analysis of analytical validations by probabilistic modification of FMEA," J. Pharm. Biomed. Anal., vol. 64–65, pp. 82–86, 2012.

[11] M. T. Oldenhof et al., "Consistency of FMEA used in the validation of analytical procedures," J. Pharm. Biomed. Anal., vol. 54, no. 3, pp. 592–595, 2011.

[12] T. Simister, "Risk Management: The Need to Set Standards," Balanc. Sheet, vol. 8, no. 4, pp. 2–4, 2000.

[13] A. Ahmed, B. Kayis, and S. Amornsawadwatana, "A review of techniques for risk management in projects," Benchmarking An Int. J., vol. 14, no. 1, pp. 22–36, 2008.

[14] K. Alexander, "Facilities Risk Management," Facilities, vol. 10, no. 4, pp. 14–18, 1992.

[15] J. Emblemsvag, "The Augmented Subjective Risk Management Process," Manag. Decis., vol. 48, no. 2, pp. 248–1747, 2010.

[16] A. P. Subriadi, D. Hadiwidjojo, Djumahir, M. Rahayu, and R. Sarno, "Firm age, Firm Size and Information Technology intencity industry factors in influencing Information Technology contribution to improve performance," J. Theor. Appl. Inf. Technol., vol. 55, no. 1, pp. 126–136, 2013.

[17] A. P. Subriadi, D. Hadiwidjojo, Djumahir, M. Rahayu, and R. Sarno, "Information technology productivity paradox: A resource-based view and information technology strategic alignment perspective for measuring information technology contribution on performance," J. Theor. Appl. Inf. Technol., vol. 54, no. 3, pp. 541–552, 2013

[18] M. Spremic and P. D, "Emerging issues in IT Governance : implementing the corporate IT risks management model," Wseas Trans. Syst., vol. 7, no. 3, pp. 219–228, 2008.

[19] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems Recommendations of the

National Institute of Standards and Technology," Nist Spec. Publ. 800, vol. 30, no. July, 2002.

[20] M. E. Whitman and H. J. Mattord, "Principles of information security," Course Technol., pp. 1–617, 2012.

[21] K. Claxton and N. M. Campbell-Allen, "Failure modes effects analysis (FMEA) for review of a diagnostic genetic laboratory process.," Int. J. Qual. Reliab. Manag., vol. 34, no. 2, pp. 265–277, 2017.

[22] L. S. Lipol and J. Haq, "Risk analysis method : FMEA / FMECA in the organizations.," Int. J. Basic Appl. Sci., vol. 11, no. 5, pp. 5–74, 2011.

[23] R. K. Sharma and P. Sharma, "System failure behavior and maintenance decision making using, RCA, FMEA and FM," J. Qual. Maint. Eng., vol. 16, no. 1, pp. 64–88, 2010.

[24] B. Kitchenham, Procedures for performing systematic reviews. Keele, UK: Keele University, 2004.

[25] I. Cameron et al., "Process hazard analysis, hazard identification and scenario definition: Are the conventional tools sufficient, or should and can we do much better?," Process Saf. Environ. Prot., vol. 110, pp. 53–70, 2017.

[26] L. K. H. Lai and K. S. Chin, "Development of a Failure Mode and Effects Analysis Based Risk Assessment Tool for Information Security," Ind. Eng. Manag. Syst., vol. 13, no. 1, pp. 87–100, 2014.

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

[28] C. M. Thurnes, F. Zeihsel, S. Visnepolschi, and F. Hallfell, "Using TRIZ to invent failures - Concept and application to go beyond traditional FMEA," Procedia Eng., vol. 131, pp. 426–450, 2015.

[29] M. Banghart, "Utilizing Confidence Bounds in Failure Mode Effects Analysis (FMEA) Hazard Risk Assessment," 2014.

[30] R. N. Sankar and B. S. Prabhu, "Modified approach for prioritization of failures in a system failure mode and effects analysis," Int. J. Qual. Reliab. Manag., vol. 18, no. 3, pp. 324–336, 2001.

[31] A. Sutrisno, I. Gunawan, I. Vanany, and H. A. Khorshidhi, "A maintenance waste risk appraisal model based on modified failure mode and effect analysis (FMEA)," 2016 IEEE Int. Conf. Ind. Eng. Eng. Manag., pp. 1422–1425, 2016.

[32] F. Mason-Blakley and R. Habibi, "Prospective Hazard Analysis for Information System," Healthc. Informatics (ICHI), 2014 IEEE Int. Conf., pp. 256–265, 2014.

[33] L. Y. Zheng, K. S. Chin, and L. Wei, "Knowledge-Enriched Process FMEA Model For Process Planning," Asian J. Qual., vol. 3, no. 1, pp. 12–27, 2013.

[34] P. Jacob, "Failure analysis and reliability on system level," Microelectron. Reliab., vol. 55, no. 9–10, pp. 2154–2158, 2015.

[35] R. Sawhney, K. Subburaman, C. Sonntag, P. Rao Venkateswara Rao, and C. Capizzi, "A modified FMEA approach to enhance reliability of lean systems," Int. J. Qual. Reliab. Manag., vol. 27, no. 7, pp. 832–855, 2010.

[36] K. Jain, "use of Failure Mode Effect Analysis (FMEA) to Improve Medication Management Process," Int. J. Health Care Qual. Assur., vol. 30, no. 2, 2017.

[37] D. C. de Aguiar, V. A. P. Salomon, and C. H. P. Mello, "An ISO 9001 based approach for the implementation of process FMEA in the Brazilian automotive industry," Int. J. Qual. Reliab. Manag., vol. 32, no. 6, pp. 589–602, 2015.

[38] F. Lolli et al., "A revised FMEA with application to a blow moulding process," Int. J.

Qual. Reliab. Manag., vol. 33, no. 7, pp. 900–919, 2016.

[39] D. Chang, "Applying DEA to enhance assessment capability of FMEA," Int. J. Qual. Reliab. Manag., vol. 26, no. 6, pp. 629–643, 2009.

[40] P. Chemweno, L. Pintelon, A. Van Horenbeek, and P. Muchiri, "Development of a risk assessment selection methodology for asset maintenance decision making: An analytic network process (ANP) approach," Int. J. Prod. Econ., vol. 170, pp. 663–676, 2015.

[41] H. Liu, "Improving risk evaluation in FMEA with a hybrid multiple criteria decision making method," Int. J. Qual. Reliab. Manag., vol. 32, no. 7, pp. 763–782, 2015.

[42] M. Murphy, G. Heaney, and S. Perera, "A methodology for evaluating construction innovation constraints through project stakeholder competencies and FMEA," Constr. Innov., vol. 11, no. 4, pp. 416–440, 2011.

[43] N. Sellappan, D. Nagarajan, and K. Palanikumar, "Evaluation of risk priority number (RPN) in design failure modes and effects analysis (DFMEA) using factor analysis," Int. J. Appl. Eng. Res., vol. 10, no. 14, pp. 34194–34198, 2015.

[44] K. Batbayar, M. Takács, and M. Kozlovszky, "Medical device software risk assessment using FMEA and fuzzy linguistic approach : case study," Int. Sysmposium Appl. Comput. Intell. Informatics, 12-14 May 2016. Rimisoara, Rom., pp. 197–202, 2016.

[45] A. Shahin, "Integration of FMEA and the Kano model," Int. J. Qual. Reliab. Manag., vol. 21, no. 7, pp. 731–746, 2004.

[46] C. Paciarotti, G. Mazzuto, and D. D'Ettorre, "A revised FMEA application to the quality control management," Int. J. Qual. Reliab. Manag., vol. 31, no. 7, pp. 788–810, 2014.

[47] H. Liu, L. Liu, and N. Liu, "Expert Systems with Applications Risk evaluation approaches in failure mode and effects analysis : A literature review," Expert Syst. Appl., vol. 40, no. 2, pp. 828–838, 2013.

[48] A. P. Subriadi, Sholiq, and P. A. Ningrum, "Critical review of the effort rate value in use case point method for estimating software development effort," J. Theroretical Appl. Inf. Technol., vol. 59, no. 3, pp. 735–744, 2014.

[49] N. Ningsi and A. P. Subriadi, "Mapping Portfolio IT Investment by Perception Level Management and IT investments toward Organization Performance (Case study : BPR Mustika Utama Kolaka Southeast Sulawesi)," 2nd Int. Semin. Sci. Technol., 2016.

[50] N. F. Najwa, M. A. Furqon, and F. Mahananto, "Literature Review on Extended Use case in Modeling Non- functional Requirement," Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 3, no. 3, pp. 1832–1844, 2018.

APPENDIX. REVIEW PAPER RESULTS

code	Focus Aspect, author	Background/Problem	Result
1	Identification failure[25]	The hazard identification process and possible definitions of scenarios on failure.	Improving the effectiveness, efficiency, and possibility of hazard risk using HAZOP and FMEA.
1	Bias in identification risk[29]	Synthesizing FMEA from looking at qualitative weaknesses.	Disadvantages of qualitative: consistent scope of analysis, consistent process modeling, and model completeness.

code	Focus Aspect, author	Background/Problem	Result
1	Potential failure, cause, impacts.[32]	Comparison of conventional FMEA applications with proposed concepts	Considered the sequence of events in the failure analysis to understand the cause and effect, based on ISO 9001.
2	Criteria scale/Rank[37]	Focus on potential errors in FMEA ranking. Human error and bias and data concerns affect the inaccuracies of the FMEA process.	Applying a confidence interval for risk qualification
2	Proved inconsistency Method[10]	Criticized the FMEA method by comparing results obtained by 2 different teams due to the consistency FMEA. Then, looking at opportunities from the results obtained.	FMEA's Both teams contain valuable information not identified by other teams. Inconsistency was not always a weakness.
2	Risk Assessment[11]	Modification FMEA by synthesizing also FMECA in which there was the probability of occurrence. Then compared the results of traditional FMEA risk assessments with the developed FMEA.	The improved modification is made to not only RPN but also category scores of severity and frequency estimates of undetected failure modes.
2	Scale criteria[38]	A new scale was defined by a combination of severity, occurrence, and detection called the Risk Priority Ranks (RPRs).	The failure model had a high RPR value assumed to be more important and gave high priority that had a low RPR value.
2	RPN[41]	Provided a new approach to evaluate RPNs and failure modes to improve traditional FMEA techniques.	The usefulness of the proposed methodology in the following conditions: FMEA teams did not agree with the scale of index ratings S, O and D.
2	RPN[5]	Issues of limitations of FMEA, and a tool that can be used in all parts of the collaborative environment for FMEA processes.	Provided examples of inconsistent results in rank S, D, and O that cause delayed in an implementation of FMEA in the supply chain.
2	Scale Criteria and RPN[43]	Severity calculation was not from the view of the customer. Increased FMEA capability with KANO Model	The gap between customer and manager in prioritizing a set of failures and differences between RPN and Cr prioritization due to frequency occurrence error.
2	RPN evaluation[44]	FMEA modification and adaptation to fit the quality control features and needs	Completed procedure and evaluation of the most important RPN values.
2	Assessment Risk[40]	Combining VIKOR, DEMATEL and AHP are used to assess the risk of failure modes identified in FMEA.	The new risk-priority model could be effective in helping analysts find high-risk failure modes and create appropriate maintenance strategies.
2	RPN[42]	The combination of fuzzy and FMEA in evaluating the risks in software tools in the health field.FMEA was not sufficient to measure different risks.	The fuzzy approach was more accurately more accurate by involving the weight of the impact of different experts
2	Risk	A new method that could directly	The proposed method has been

code	Focus Aspect, author	Background/Problem	Result
	Assessment[8]	analyze many failures for complex systems.	successfully combined with traditional FMEA to measure system reliability in many failure models.
2	Scale Criteria[39]	FMEA modification to calculate risk from waste maintenance. Additional indications, prevention and control scale to overcome FMEA limitation.	The shortcomings of the proposed model, and repaired with the addition of extended dimensions.
3	Subjectivity[21]	Many health organizations faced limitations and increased complexity. So it was necessary to risk management for preventive action before the occurrence.	FMEA produces benefits, for prospective risk management and overall process improvement.
3	Subjectivity and strategy[45]	Modified FMEA so that lean practitioners understand and improve the reliability of the lean system.	The practical methodology for improving lean system reliability was non-existent.
3	Competence of Stakeholder[46]	Methodology for extracting innovation constraints from project development through competent stakeholder management and FMEA.	There was no project boundary that required management to innovate, but a failure on the competence of stakeholders.
1,2	Potential Failure, severity, detection, occurrence, and RPN[33]	FMEA modification to make the value of event factors more reliable, and to connect FMEA charts directly to maintenance activities. K-means and the approach of normalization, applied and compared to fill the value of events.	Improving standards due to tighter mathematical formulations and careful application in the actual operating environment.
1,2	Risk Assessment process[26]	FMEA widely used in the industry sector. So, Exploration FMEA in Information Technology sector.	FMEA that had been modification more effective than traditional FMEA.
1,2	Identification risk and RPN[27]	Minimizing limitation FMEA with Fuzzy.	Communication security is the most important aspect of information security
1,2	Improve analysis failure and RPN[34]	A new approach to improve FMEA assessment capability. Data Envelopment Analysis (DEA) and investigate SOD instead of RPN.	The proposed approach supports the proposition that DEA can not only complement traditional FMEA to improve assessment capabilities.
1,2	RPN and Subjectivity in identification [23]	Model, analyze and predict the behavior of industrial systems in realistic and consistent measurement and plan appropriate maintenance in accordance with the strategy. Integration framework RCA, FMEA dan Fuzzy	Using traditional FMEA and fuzzy based decision support systems eliminated uncertainty and subjective information.
1,2	Risk assessment[28]	Combination Anticipatory Failure Determination (AFD)-FMEA or called Failure Mode and Effects Anticipation and Analysis (FMEAA).	New ways to identify the structure and system failures are similar to the usual way.
1,2	Procedure	FMEA / FMECA risk analysis methods	FMEA was more familiar than FMECA in

code	Focus Aspect, author	Background/Problem	Result
	risk assessment[22]	used by industry. Used of FMEA or FMECA and its differences within the organization	industry.
1,2	Risk measurement (severity, occurrence, detection)[35]	The organization might choose risk measurement techniques that vary depending on the factors of the type of technique, application domain, and the number of ratings given. There were still fewer generalizable techniques.	Selection methodologies form the basis for comparing the company's intrinsic competencies in general towards prioritizing competencies. a more complex alternative methodology.
1,3	Strategies[30]	Most FMEA processes used ineffective forms of expressing, organizing, and disabling knowledge of failures from the production process during process planning.	Effectively describe the knowledge of FMEA processes rather than specific processes of failure or data.
1,3	Procedure risk measurement, team[31]	Increased root-cause find of electronic component failure from system-related failure anamnesis approach.	The procedure was used, but it also displayed important things, such as processes, interdisciplinary team needs, guides, and so on.
1,2,3	FMEA process[36]	Used FMEA in the management process of health agencies. Testing the many FMEAs proves to be an effective method.	There were FMEA limits such as time-consuming, multidisciplinary teams, etc. FMEA is proven to improve management processes in accordance with strategies and procedures.
1,2,3	FMEA process[4]	Near Infrared (NIR) procedures used to filter drugs on FMEA, including technical risks, risk factors for human failure.	FMEA could improve the NIR method, and pay attention to human factors.
1,2,3	Irregularities [9]	Inconsistent FMEA results.The problem of irregularities and aims to propose strategies to minimize.	There were 7 factors that could contribute to inconsistencies. the strategy could improve the FMEA process significantly.
1,2,3	Success factor[7]	Provided a brief explanation of the fundamental concepts and procedures for an effective FMEA and provides the success of FMEA factors	When FMEA is used appropriately, it anticipates and prevents problems, reduces costs, lowers production time, and obtains security and high reliability of products and processes.

Code: [1]Risk Identification, [2]Risk Analysis, and Evaluation, [3]People