The implementation of fault tree analysis approaches in nuclear power plant probabilistic safety assessment

Cite as: AIP Conference Proceedings **2180**, 020010 (2019); https://doi.org/10.1063/1.5135519
Published Online: 10 December 2019

Julwan Hendry Purba, Damianus Toersiwi Sony Tjahyani and Deswandri

The Implementation of Fault Tree Analysis Approaches in Nuclear Power Plant Probabilistic Safety Assessment

Julwan Hendry Purba[a], Damianus Toersiwi Sony Tjahyani[b], Deswandri[c]

Center for Nuclear Reactor Technology and Safety, National Nuclear Energy Agency of Indonesia (BATAN), Gd. 80 Kawasan Puspiptek Serpong, Tangerang Selatan – 15310, Indonesia.

[a]Corresponding author: purba-jh@batan.go.id
[b]dtsony@batan.go.id
[c]wandri@batan.go.id

Abstract. Probabilistic safety assessment (PSA) has been extensively implemented to assess the performance of nuclear power plant (NPP) safety systems. One well-known modeling approach in NPP PSA is a fault tree analysis (FTA). A fault tree is a graphical representation of possible failure scenarios of the system being evaluated. To estimate the top event failure probability, a quantitative analysis needs to be performed based on those scenarios. Prior to performing quantitative analysis, basic events' failure probabilities of the system fault tree need to be provided well in advance. Conventional FTA assumes that basic events always have precise probability distributions characterizing their lifetime to failure. However, in practical applications, this is not the case. For example, a new system will not have sufficient operating experiences to probabilistically estimate reliabilities of their components. To deal with this limitation, a number of approaches has been developed and proposed. Each approach offers advantageous but also has disadvantageous. Since the results of FTA will be used to verify NPP designs, it is necessary to select the most suitable approach. It is, therefore, essential to clearly understand the strengths and weaknesses of each approach. The purpose of this study is to review the implementation of various FTA approaches in NPP PSA. The strengths and weaknesses of each approach are also discussed. To achieve research objectives, this study classified those FTA approaches into conventional FTA and fuzzy FTA. Fuzzy FTA is further grouped into fuzzy hybrid FTA and fuzzy based FTA. This study concludes that safety analysts need to, firstly, confirm the type of reliability data at hands. Secondly, if epistemic uncertainty is essential and need to be considered in the study being performed, fuzzy based FTA should be applied. Otherwise, safety analysts should apply conventional FTA or fuzzy hybrid FTA depending on how the basic events' failure probabilities are generated.

Keywords: Fault tree analysis, nuclear power plant, probabilistic safety assessment, fuzzy fault tree analysis.

INTRODUCTION

The main objectives of nuclear power plant (NPP) safety systems are to ensure the normal operation of the plants without risk exposure to operators, publics, and environment; to prevent accidents when unexpected events happen; and to mitigate the consequences of accidents when they really occur. Over the past two decades, those objectives are achieved through probabilistic safety assessment (PSA). It is a comprehensive approach to evaluate significant plant vulnerabilities, to construct accident scenarios, to predict the safety level of the plant, and to numerically estimate potential risks. PSA evaluates safety and risk in NPPs by postulating potential initiating events that might initiate accidents [1]. Those initiating events could be internal and external hazards, component failures, and/or human errors. Designers, utilities as well as regulatory body utilize the results of PSA to verify NPP design, to propose new design, to adjust operation procedures, to improve the reliability of safety systems, and to potentially change regulation, or to license basic events.

One well-known modelling approach in NPP PSA is a fault tree analysis (FTA). It graphically represents parallel and/or sequential fault events, which could lead to the system failure. The system failure is defined as a top event of

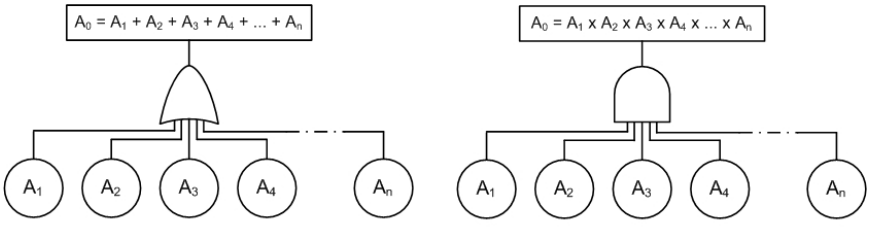
The 3rd International Conference on Nuclear Energy Technologies and Sciences (ICoNETS) 2019
AIP Conf. Proc. 2180, 020010-1–020010-7; https://doi.org/10.1063/1.5135519
Published by AIP Publishing. 978-0-7354-1927-8/$30.00

the tree. Through a fault tree, possible failure scenarios could be logically depicted using Boolean gates [2-4]. Based on those possible failure scenarios, a quantitative analysis is performed to estimate the failure probability of the top event. If the top event failure probability is greater than the objective probability, system designers should redesign the system or propose a more innovative design. These can achieved by utilizing better quality components, modifying maintenance policy, adjusting testing activities, and suggesting component redundancies [5]. To ensure that failure probability of the new proposed system is less than the objective probability, its reliability needs to be re-quantified.

To perform quantitative analysis, basic events of the fault tree of the evaluated system need to have corresponding failure probabilities [6, 7]. Conventional FTA assumes that basic events always have precise probability distributions describing their lifetime to failure. In practical engineering applications, this is not always the case. For example, a new system will not have sufficient operating experiences and historical failure data to assess reliabilities of their components [8]. To deal with the limitation of generating basic events' failure probabilities, a number of FTA approaches has been developed and proposed. Each approach offers advantageous but also has disadvantageous. Since the results of FTA will be used to verify NPP designs, it is necessary to select the most suitable approach to the study of interest. Therefore, clear understanding on the strengths and weaknesses of each approach is essential. The present paper aims to review the implementation of FTA approaches, which have been proposed and developed for generating basic events' failure possibilities in the quantitative analysis of FTA. The strengths and weaknesses of each approach are also discussed to help safety analysts properly select the most appropriate approach to their study. To achieve research objectives, the implementation of FTA approaches are classified into two groups, i.e. conventional FTA and fuzzy FTA. Fuzzy FTA is further grouped into fuzzy hybrid FTA and fuzzy based FTA.

METHODOLOGY

A fault tree is a graphical representation to depict logical interrelationships amongst basic events to the predefined undesired top event that is the failure of the system being investigated. In drawing a fault tree model, the process starts from the higher fault events to the more basic fault events. Boolean gates, then, denote the relationship between those fault events. The higher event is the output of the gate and the lower event is the input to the gate. The most common Boolean gates in a typical fault tree model are an OR Boolean gate and an AND Boolean gate. A typical fault tree model is graphically shown in Figure 1.



(a) Boolean OR gate (b) Boolean AND gate

Figure 1: A typical fault tree model [9].

The top event A_0 in Figure 1(a) will be failure if one of input events A_i fails. Meanwhile, the top event A_0 in Figure 1(b) will be failure if all input events A_i fails at the same time.

The top event failure probability is a function of the basic event reliability data. Based on how basic events' probabilities are generated to characterize their reliabilities, the implementation of FTA approaches in NPP PSA can be organized into two groups, i.e. conventional FTA and fuzzy FTA. Fuzzy FTA can be further categorized into two groups, i.e. fuzzy hybrid FTA and fuzzy based FTA. This classification is depicted in Figure 2.

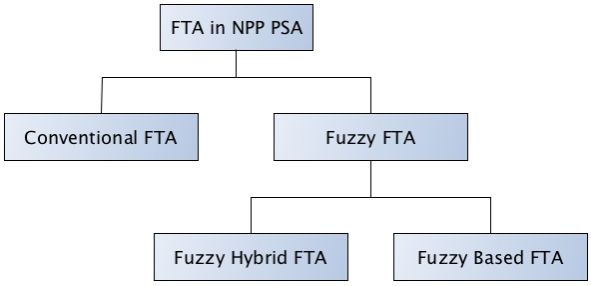


Figure 2: Classification of fault tree analysis implementation in NPP PSA.

This study reviews the implementation of each approach in Figure 2 using a number of accessible scientific publications. Strengths and weaknesses of each approach are discussed to help safety analysts decide which approach is the most relevant to their study.

RESULTS AND DISCUSSION

The main difference between conventional FTA and fuzzy FTA is in the data used to represent the occurrence likelihood of individual basic events constructing the fault tree of the system being interest. In conventional FTA, basic events' reliabilities are probabilistically estimated using their historical failure data. Meanwhile, in fuzzy FTA, basic events' reliabilities are characterized using fuzzy probabilities. In the sequel, each approach is elaborated and its strengths and weaknesses are also discussed.

Conventional Fault Tree Analysis

In conventional FTA, basic event lifetime to failure is characterized by a probability distribution. It is a mathematical representation of the occurrence probabilities of various possible outcomes within a specified event. It characterizes a random phenomenon about the event probabilities. Basic event failure probability is represented in the form of conventional probability of, for example, 1.8E-5.

In this FTA approach, Boolean algebras are used to quantify the output of every Boolean gate. The output of the OR Boolean gate and the AND Boolean gate depicted in Figure 1 can be respectively quantified using (1-2) [9, 10].

$$P(A_0) = 1 - \prod_{i=1}^{n}\{1 - P(A_i)\} \quad (1)$$

$$P(A_0) = \prod_{i=1}^{n} P(A_i) \quad (2)$$

where n is the number of fault events and $P(A_i)$ is the probability of event A_i. Various data sources have been used by scholars to generate probability distributions of basic events $P(A_i)$ in (1-2). Each source offer advantageous but also has disadvantageous.

To obtain the most actual results of FTA, basic event probability distributions should be collected from operating experiences of the system being evaluated [11, 12]. The Living PSA paradigm is then applied to reflect changes in the plants during their lifetime [13]. Those collected data will represent the real performance of the system being investigated. The probability of the undesired top event calculated from basic event probabilities using (1-2) will represent the real reliability of the system. Hence, system designers can be much confident to redesign the system or to propose a more innovative design in order to improve system reliability. Unfortunately, basic events do not always have probability distributions to characterize their lifetime to failure. For example, when an accident occurs infrequently or a system design is new, sufficient operating experiences will not be available. Therefore, reasonable historical failure data are not sufficient to statistically estimate the component reliability characteristics.

When historical failure data are still not available or insufficient, it is therefore unavoidable to apply generic data taken from operating experiences of other nuclear facilities and non-nuclear facilities [3, 14-17]. However, the results of FTA will not actually describe the real performance of the system being evaluated. Should system need to be redesigned or a more innovative design needs to be proposed to improve reliability; system designers cannot directly rely on the results. They have to evaluate uncertainties and imprecision caused by those generic data. For this purpose, Monte Carlo simulation (MCS) is widely used. It can calculate the overall uncertainties of

conventional fault tree analysis [18, 19]. MCS has been commonly used to solve real engineering problems in many fields for reliability analysis. It allows to realistically modelling the behavior of complex engineering systems. However, MCS is appropriate only for quantifying aleatory uncertainty. It is not suitable for quantifying epistemic uncertainty [18, 20].

Fuzzy Fault Tree Analysis

In fuzzy FTA approach, fuzzy probabilities are applied to characterize basic event reliabilities. A fuzzy probability is defined as a membership function of a fuzzy set. It is expressed in the space of probabilities to characterize event reliability. This membership functions are usually defined in a real unit interval [0, 1]. Trapezoidal and triangular fuzzy numbers are the most common membership functions to represent fuzzy probabilities [20]. Basic event fuzzy probability is represented in the form of membership function of triangular fuzzy number of, for example, (0.25, 0.37, 0.49), or in the form of membership function of trapezoidal fuzzy number of, for example, (0.15, 0.2, 0.3, 0.35).

Two different approaches have been proposed to generate basic events' fuzzy probabilities. The first approach utilizes limited historical failure data [21, 22]. In this approach, the membership functions describing fuzzy probabilities are generated using the lower bound, the middle and the upper bound values, which are statistically calculated from the available limited historical failure data [9]. The second approach utilizes experts' judgments. In this second approach, a group of experts are asked to subjectively justify reliabilities of basic events using qualitative failure possibilities. These qualitative assessments already have predefined corresponding quantitative fuzzy probabilities [23, 24]. In this second approach, it is essential to select members of the expert team who have expertise and experiences on the system being studied to avoid bias in their judgment. It is also necessary to weight selected experts to confirm their credibility. Kumaraningrum et al. weighted selected experts based on professional experience, education background, technical qualifications, and the involvement in the design, construction as well as commissioning of the reactor being evaluated [25].

The advantage offered by these two approaches is their capabilities to characterize basic event reliabilities without being confined to probability distributions. Based on how basic event fuzzy probabilities utilized in FTA approaches, fuzzy FTA is further organized into two sub-groups, i.e. fuzzy hybrid FTA and fuzzy based FTA. In the sequel, each sub-group is elaborated and discussed in details.

Fuzzy Hybrid Fault Tree Analysis

In fuzzy hybrid FTA approach, fuzzy probabilities are only applied to characterize basic event reliabilities. The reliability of intermediate events and the top event are still represented by conventional probability. Therefore, the probabilities of the top event A_0 in Figures 1(a) and 1(b) are still quantified using Boolean algebras in (1-2) [26-28]. To integrate basic events' fuzzy probabilities into Boolean algebra quantification, they need to be, firstly converted, into the form of conventional probability, for example, from the form of (0.25, 0.37, 0.49) into the form of 1.8E-5. To convert basic event fuzzy probabilities into their corresponding conventional probabilities, two algorithms are needed, i.e. a defuzzification technique and an Onisawa's logarithmic function.

The defuzzification technique is to decode a fuzzy probability into a single scalar quantity. For example, from the form of (0.35, 0.50, 0.65) into the form of 0.102619. Various defuzzification techniques have been proposed for a number of different applications and purposes. Huang, Chen and Wang [29] acknowledged that no one single defuzzification technique could be applied in any applications. An area defuzzification technique developed and proposed by [9] has been confirmed to be suitable for NPP PSA.

The Onisawa's logarithmic function [30] is to convert the single scalar quantity generated by the defuzzification technique into a conventional probability. For example, from the form of 0.102619 into the form of 1.8E-5. This generated conventional probability is then used to quantify the probabilities of intermediate events and the top event based on Boolean algebras in (1-2).

Since fuzzy probabilities are applied to only characterize basic event reliabilities, epistemic uncertainty raised in the basic events' fuzzy probabilities will not be propagated into the top event failure probability. Furthermore, MCS is also not suitable for quantifying epistemic uncertainty. However, this FTA approach can integrate two types of basic events' failure probabilities, i.e. fuzzy probabilities and conventional probabilities. In the case of basic events do have their corresponding lifetime to failure; conventional probability can be statistically generated. On the other

hand, in the case of basic events do not have their corresponding lifetime to failure; fuzzy probabilities can be generated from expert judgments.

Fuzzy Based Fault Tree Analysis

In fuzzy based FTA, fuzzy probabilities are used to not only characterize basic event reliabilities but also intermediate event reliabilities and the top event reliability as opposed to fuzzy hybrid FTA. While the fuzzy probabilities of basic events are collected either from experts' qualitative judgments or limited available data, the fuzzy probability of the intermediate events and the top event are quantified using fuzzy combination rules instead of Boolean algebras as in conventional FTA and fuzzy hybrid FTA.

In this approach, two fuzzy combinations rules substitute the OR and AND Boolean gates. The OR Boolean gate is quantified using a fuzzy complementation rule. Meanwhile, the AND Boolean gate is calculated using a fuzzy multiplication rule. Therefore, the probability of the top event A_0 in Figures 1(a) and 1(b) can be quantified using (3-4), respectively [9, 23].

$$\mu_{A_0}(x) = 1 - \prod_{i=0}^{n}\{1 - \mu_{A_i}(x)\} \quad (3)$$

$$\mu_{A_0}(x) = \prod_{i=0}^{n} \mu_{A_i}(x) \quad (4)$$

where $\mu_{A_i}(x)$ is the fuzzy probability of basic event A_i and $\mu_{A_0}(x)$ is the fuzzy probability of the top event A_0 in Figure 1.

This approach offers another advantage of propagating epistemic uncertainty raised in basic event fuzzy probabilities into the top event. However, this approach cannot be partially applicable when some of basic events come with their corresponding lifetime to failure.

From the results and discussion elaborated above, it can be summarized that it is necessary to select the most suitable fault tree analysis for NPP PSA. It is critical for safety analysts to, firstly, know the type of the available reliability data of the system being investigated. If basic events sufficiently have their own probability distribution of their lifetime to failures, conventional FTA should be applied. The results will actually represent the real safety performance of the system being investigated. When available historical failure data is not sufficient to statistically estimate basic events' failure probabilities or expert judgments are the only means to generate basic events' failure probabilities, fuzzy FTA should be used. Secondly, if epistemic uncertainty is essential and need to be considered in the study being performed, fuzzy based FTA should be applied. Otherwise, safety analysts should apply conventional FTA or fuzzy hybrid FTA. The decision, which one of these two approaches to be used, depends on how basic event probabilities of the system being studied are generated or collected.

CONCLUSIONS

In conventional FTA, reliabilities of basic events, intermediate events, and the top event are characterized by conventional probabilities. Meanwhile, in fuzzy FTA, reliabilities of basic events are characterized using fuzzy probabilities. Different from fuzzy hybrid FTA in which reliabilities of intermediate events and the top event are still in the form of conventional probabilities, reliabilities of intermediate events and the top events in fuzzy based FTA are also characterized by fuzzy probabilities. Prior to the selection of the most appropriate FTA approaches in NPP PSA, safety analysts need to, firstly, confirm the type of reliability data at hands. If basic events have their own probability distribution of their lifetime to failures, conventional FTA should be applied. When available historical failure data is not sufficient or expert judgments are the only means to generate basic events' failure probabilities, fuzzy FTA should be used. Secondly, if epistemic uncertainty is essential, fuzzy based FTA should be applied. Otherwise, safety analysts should apply conventional FTA or fuzzy hybrid FTA depending on how basic event probabilities are generated.

ACKNOWLEDGMENTS

The work presented in this paper was funded by the government of Indonesia through DIPA of the Center for Nuclear Reactor Technology and Safety, National Nuclear Energy Agency of Indonesia (BATAN).

REFERENCES

1. Zubair, M., A. Ababneh, and A. Ishag, *Station black out concurrent with PORV failure using a Generic Pressurized Water Reactor simulator.* Ann. Nucl. Energy, 2017. **110**: p. 1081-1090.
2. Khakzad, N., F. Khan, and P. Amyotte, *Risk-based design of process systems using discrete-time Bayesian networks.* Reliab. Eng. Syst. Saf., 2013. **109**: p. 5-17.
3. Kamyab, S. and M. Nematollahi, *Evaluating the core damage frequency of a TRIGA research reactor using risk assessment tool software.* Nucl. Eng. Des., 2011. **241**(8): p. 2942-2947.
4. Song, H., H.Y. Zhang, and C.W. Chan, *Fuzzy Fault Tree Analysis Based on T–S Model With Application to INS/GPS Navigation System.* Soft Computing - A Fusion of Foundations, Methodologies and Applications, 2009. **13**(1): p. 31-40.
5. Contini, S., L. Fabbri, and V. Matuzas, *A novel method to apply Importance and Sensitivity Analysis to multiple Fault-trees.* J. Loss Prev. Process Ind., 2010. **23**: p. 574-584.
6. Yang, G., *Potential Failure Mode Avoidance*, in *Life Cycle Reliability Engineering*. 2007, John Wiley & Sons: Hoboken, New Jersey. p. 194-235.
7. Verma, A.K., A. Srividya, and D.R. Karanki, eds. *Reliability and Safety Engineering*. 2010, Springer-Verlag: London.
8. Kabir, S., *An overview of fault tree analysis and its application in model based dependability analysis.* Expert Syst. Appl., 2017. **77**: p. 114-135.
9. Purba, J.H., *Fuzzy probability on reliability study of nuclear power plant probabilistic safety assessment: A review.* Prog. Nucl. Energy, 2014. **76**: p. 73-80.
10. Verma, A.K., A. Srividya, and D.R. Karanki, *System Reliability Modeling*, in *Reliability and Safety Engineering*. 2010, Springer-Verlag: London. p. 71-168.
11. Liu, T., J. Tong, and J. Zhao. *Probabilistic risk assessment framework development for nuclear power plant*. in *IEEE International Conference on Industrial Engineering and Engineering Management*. 2008. Singapore.
12. Delaney, M.J., G.E. Apostolakis, and M.J. Driscoll, *Risk-informed design guidance for future reactor systems.* Nucl. Eng. Des., 2005. **235**(14): p. 1537-1556.
13. Di Maio, F., F. Antonello, and E. Zio, *Condition-based probabilistic safety assessment of a spontaneous steam generator tube rupture accident scenario.* Nucl. Eng. Des., 2018. **326**: p. 41-54.
14. Abdelgawad, M., A.R. Fayek, and F. Martinez. *Quantitative assessment of horizontal directional drilling project risk using fuzzy fault tree analysis* in *Construction Research Congress 2010: Innovation for Reshaping Construction Practice*. 2010. American Society of Civil Engineers.
15. Bickel, J.H., *Risk implications of digital reactor protection system operating experience.* Reliab. Eng. Syst. Saf., 2008. **93**(1): p. 107-124.
16. Kamyab, S., M. Nematollahi, and G. Shafiee, *Sensitivity analysis on the effect of software-induced common cause failure probability in the computer-based reactor trip system unavailability.* Ann. Nucl. Energy, 2013. **57**: p. 294-303.
17. Borges, D.S., et al., *Nondeterministic method to analysis of the aging effects in PWR power plants components.* Ann. Nucl. Energy, 2015. **81**: p. 249-256.
18. Hanss, M. and S. Turrin, *A Fuzzy-Based Approach to Comprehensive Modeling and Analysis of Systems with Epistemic Uncertainties.* Struct. Saf., 2010. **32**: p. 433-441.
19. Ferdous, R., et al., *Fault and event tree analyses for process systems risk analysis: Uncertainty handling formulations.* Risk Anal, 2011. **31**(1): p. 86-107.
20. Ferdous, R., et al., *Fault and event tree analyses for process systems risk analysis: Uncertainty handling formulations.* Risk Anal., 2011. **31**(1): p. 86-107.
21. Guimaraes, A.C.F. and C.M.F. Lapa, *Parametric fuzzy study for effects analysis of age on PWR containment cooling system.* Appl. Soft Comput., 2008. **8**(1): p. 1562–1571.
22. Guimaraes, A.C.F., et al., *Fuzzy uncertainty modeling applied to AP1000 nuclear power plant LOCA.* Ann. Nucl. Energy, 2011. **38**(8): p. 1775-1786.
23. Purba, J.H., et al., *Fuzzy probability based fault tree analysis to propagate and quantify epistemic uncertainty.* Ann. Nucl. Energy, 2015. **85**: p. 1189-1199.
24. Purba, J.H., et al., *α-Cut method based importance measure for criticality analysis in fuzzy probability – Based fault tree analysis.* Ann. Nucl. Energy, 2017. **110**: p. 234-243.

25. Kumaraningrum, A.R., H. Hermansyah, and J.H. Purba. *Experts' selection in the application of fuzzy fault tree analysis to evaluate an RSG – GAS primary cooling system*. in *The 8th Annual Basic Science International Conference (BaSIC 2018)*. 2018. East Java, Indonesia: American Institute of Physics.
26. Yuhua, D. and Y. Datao, *Estimation of Failure Probability of Oil and Gas Transmission Pipelines by Fuzzy Fault Tree Analysis.* J. Loss Prev. Process Ind., 2005. **18**: p. 83-88.
27. Gupta, S. and J. Bhattacharya, *Reliability Analysis of a Conveyor System Using Hybrid Data.* Qual. Reliab. Eng. Int., 2007. **23**(7): p. 867-882.
28. Pan, N.F. and H. Wang. *Assessing failure of bridge construction using fuzzy fault tree analysis*. in *IEEE International Conference on Fuzzy Systems and Knowledge Discovery*. 2007. Haikou.
29. Huang, D., T. Chen, and M.J.J. Wang, *A Fuzzy Set Approach for Event Tree Analysis.* Fuzzy Sets and Systems, 2001. **118**(1): p. 153-165.
30. Onisawa, T., *An approach to human reliability in man-machine systems using error possibility.* Fuzzy Sets Syst., 1988. **27**(2): p. 87-103.