Annals of Nuclear Energy 70 (2014) 21–29

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

A fuzzy-based reliability approach to evaluate basic events of fault tree analysis for nuclear power plant probabilistic safety assessment

Julwan Hendry Purba *

Reactor Safety Analysis and Assessment Division, Centre for Reactor Technology and Nuclear Safety, National Nuclear Energy Agency (BATAN), Gd. 80 Kawasan Puspiptek Serpong Tangerang, Banten 15310, Indonesia

ARTICLE INFO

Article history:
Received 31 July 2013
Received in revised form 23 February 2014
Accepted 26 February 2014
Available online 20 March 2014

Keywords:
Reliability
Failure possibility
Failure probability
Fuzzy sets
Fault tree analysis
Nuclear power plant

ABSTRACT

Fault tree analysis has been widely utilized as a tool for nuclear power plant probabilistic safety assessment. This analysis can be completed only if all basic events of the system fault tree have their quantitative failure rates or failure probabilities. However, it is difficult to obtain those failure data due to insufficient data, environment changing or new components. This study proposes a fuzzy-based reliability approach to evaluate basic events of system fault trees whose failure precise probability distributions of their lifetime to failures are not available. It applies the concept of failure possibilities to qualitatively evaluate basic events and the concept of fuzzy sets to quantitatively represent the corresponding failure possibilities. To demonstrate the feasibility and the effectiveness of the proposed approach, the actual basic event failure probabilities collected from the operational experiences of the David–Besse design of the Babcock and Wilcox reactor protection system fault tree are used to benchmark the failure probabilities generated by the proposed approach. The results confirm that the proposed fuzzy-based reliability approach arises as a suitable alternative for the conventional probabilistic reliability approach when basic events do not have the corresponding quantitative historical failure data for determining their reliability characteristics. Hence, it overcomes the limitation of the conventional fault tree analysis for nuclear power plant probabilistic safety assessment.

1. Introduction

Safety issues for engineering systems are the most concern for many analysts and researchers. These issues become more significant for complex engineering systems such as nuclear power plants (NPPs), which could release radioactive materials into the environment. NPP safety system evaluation provides safety arguments to convince public that their health and safety are protected from possible radiation hazards during the NPP lifetime. Fault tree analysis (FTA) has been used in the last two decades to evaluate the safety systems of NPPs in studies of the level I probabilistic safety assessment (PSA) (Guimaraes and Lapa, 2008; Guimaraes et al., 2011). It provides a comprehensive and structured approach to identify and understand key plant vulnerabilities, to develop accident scenarios, to assess the level of plant safety, and to derive numerical estimates of potential risks (Delaney et al., 2005; Kishi et al., 2004; Liu et al., 2008). In conventional FTA, it is assumed that components always have precise probability distributions of their lifetime to failure. However, this is not the case in real applications. If a system under evaluation is new, there will be insufficient statistical data for probabilistically estimating component reliabilities. When FTA applies this limited data to assess system reliabilities, uncertainties contained in the data have to be quantified. A number of researchers have developed and proposed methodologies to deal with and quantify uncertainties due to these imprecise probability distributions (Sankararaman and Mahadevan, 2013; Volkanovski and Cepin, 2011; Xu et al., 2012). Therefore, it is necessary to develop new techniques, which could effectively determine component failure probabilities without the need to resort to the precise failure probability distributions.

Fuzzy set theory was first introduced as a useful tool to complement conventional reliability theories in 1989 (Onisawa). Since then, there have been a number of researchers tempted to develop techniques involving fuzzy set theory to evaluate system reliabilities. Based on how fuzzy sets are implemented, the fuzzy reliability approaches have two types of models.

The first type of fuzzy reliability models only implements a fuzzification module to assess system reliability. Fuzzification is a process of converting a crisp value into fuzzy subsets to deal with uncertainty (Klir and Yuan, 2001). For example, in Di Maio et al. (2011), a fuzzy *C*-means clustering was used to classify accident

* Tel.: +62 81212330661; fax: +62 217560913.
E-mail address: purba-jh@batan.go.id

http://dx.doi.org/10.1016/j.anucene.2014.02.022
0306-4549/

scenario of a nuclear power plant equipped with a digital instrumentation and control system. Dai et al. (2011) combined fuzzy logic with the multivariate decision diagram and neural network to diagnose and heal computer system problems. Ding et al. (2010, 2008) proposed a membership function of fuzzy numbers to represent a sub-system state to assess the reliability of multi-state weighted *k*-out-of-*n* systems. Meanwhile, fuzzy rule based is combined with Bayesian reasoning to obtain failure priority values for criticality analysis in the failure mode and effect analysis (Yang et al., 2008).

In the second type of fuzzy reliability models, the fuzzy reliability approach implements both a fuzzification module and a defuzzification module. Defuzzification is a process of mapping membership functions of fuzzy numbers into a crisp form or value (Klir and Yuan, 2001). For example, in Wang et al. (2011), a fuzzy model is developed to deal with the drawbacks of the rule-based quantified cognitive reliability and error analysis method (CREAM) for power system safety assessment. In this model, the fuzzification unit decomposes input variables into fuzzy sets and the defuzzification unit generates a crisp score from the output generated by the fuzzy inference module. In Gargama and Chaturvedi (2011), the membership functions of fuzzy numbers are used to represent linguistic variables and a defuzzification technique has been used to generate a crisp score for prioritising failure modes to overcome the limitation of the traditional FMEA. Moreover, Ke et al. (2008) has used the membership functions for the mean time to failure of the repairable systems and the crisp value to characterize of the system availability.

In the meantime, previous studies also indicate that qualitative natural languages are more appropriate for system reliability assessment when quantitative data is unavailable or inadequate for the probabilistic reliability approach (Celik et al., 2010; Coletti and Scozzafava, 2004; Gupta and Bhattacharya, 2007; Hryniewicz, 2007). In addition, experts are also more comfortable to justify event failure likelihood using qualitative natural languages rather than quantitative judgment (Ferdous et al., 2011a; Mentes and Helvacioglu, 2011; Yu and Park, 2000). However, due to the limitation of knowledge and experience, expert elicitation is often ambiguous and uncertain. Rao et al. (2007) acknowledged that uncertainties in reliability studies raised in the expert opinions need to be properly treated. Previous researchers have confirmed that possibilistic distributions can be used to deal with these problems (Baraldi and Zio, 2008; Flage et al., 2013). Theory of possibility, which is proposed by Zadeh (1978), can be mathematically represented by a membership function of the fuzzy sets (Cho et al., 2002; Dumitrescu et al., 2006; Vencheh and Allame, 2010; Wolkenhauer, 2001; Yang et al., 2008).

Those approaches in the second type of fuzzy reliability models and the fact that experts are more comfortable to assess the reliability of the system qualitatively rather quantitatively when they are provided with inadequate, improper and inaccurate data become the motivation of this study to overcome the limitation of the conventional reliability approach. This study aims to propose a fuzzy-based reliability approach to generate probabilities of basic events of fault trees whose probability distributions of their lifetime to failures are not available. The approach implements the concept of failure possibility to qualitatively evaluate basic event failure likelihoods and the concept of fuzzy sets to mathematically represent basic event failure possibilities. The involvement of experts in this proposed approach is different from expert elicitation techniques in probabilistic reliability approaches. While experts in probabilistic approaches are asked to provide probability density functions or cumulative probability functions of events which are expressed in numerical values (Ayyub, 2001; Boring et al., 2005; Hammitt and Zhang, 2013; Sankararaman and Mahadevan, 2013), experts in the proposed approach individually assess the failure likelihood of basic events by choosing one failure possibility from a number of predefined failure possibilities which are expressed in qualitative linguistic terms. In addition, while uncertainties in probabilistic approach are evaluated using Monte Carlo simulation (Ferdous et al., 2011b; Hanss and Turrin, 2010), uncertainties in the proposed approach are captured in the fuzzy membership functions. Therefore, the proposed approach offers two main advantages over expert elicitation techniques: (1) experts can provide their judgements in qualitative words without being confined with historical failure data and (2) uncertainties within the experts' judgement are directly captured through the implementation of membership functions of fuzzy sets.

To mathematically demonstrate the feasibility and the effectiveness of the proposed approach, basic event failure probabilities generated by the approach are compared to the known reliability data taken from the actual nuclear power plant operating experiences. The rest of the paper is organized as follows. Section 2 briefly defines basic event failure possibility distribution and their corresponding membership functions, an area defuzzification technique, and an Onisawa's logarithmic function. The proposed fuzzy-based reliability approach is described in Section 3. In Section 4, an illustrative case study is given to validate the proposed approach. Result analysis to verify the proposed approach is described in Section 5. Finally, Section 6 summarizes the study and provides further research directions.

2. Definition

This section briefly defines the concepts used in the proposed fuzzy-based reliability approach to generate basic event failure probabilities of fault trees of nuclear power plant safety systems from qualitative failure possibilities.

Definition 2.1 (Basic event failure possibility distribution). A basic event failure possibility distribution is a set of qualitative linguistic terms used to scale the failure likelihood of the basic events of fault trees of nuclear power plant safety systems. Based on the range of the component failure data collected from nuclear power plant operating experiences, i.e. from 10^{-13} to 10^{-2} (IAEA, 1997; Papazoglou et al., 1984; Wierman et al., 2001a,b), seven qualitative linguistic terms have been defined to grade basic event failure likelihoods from the less likely to the most likely occurrences. For example, a *very low* represents basic events whose failure probabilities predicted to be less than 10^{-8}. Meanwhile, a *very high* represents basic events whose failure probabilities predicted to be greater than 10^{-3}. Basic events with *low*, *reasonably low*, *moderate*, *reasonably high*, and *high* failure possibilities are up-graded from *very low* to *very high* failure possibilities. Those seven linguistic terms in (1) and their corresponding failure likelihood values are shown in Table 1 (Purba et al., 2013).

$$H = \{h_i | i = 1, 2, \ldots, 7\} = \{Very\ Low, Low, Reasonably\ Low, Moderate, Reasonably\ High, High, Very\ High\} \quad (1)$$

Table 1
Basic event failure likelihood values (Purba et al., 2013).

Basic event failure possibilities	Failure probabilities
Very low (h_1)	<1.0E−8
Low (h_2)	1.0E−8 – 1.0E−7
Reasonably low (h_3)	1.0E−7 – 1.0E−6
Moderate (h_4)	1.0E−6 – 1.0E−5
Reasonably high (h_5)	1.0E−5 – 1.0E−4
High (h_6)	1.0E−4 – 1.0E−3
Very high (h_7)	>1.0E−3