AN INTELLIGENT SYSTEM BY FUZZY RELIABILITY ALGORITHM IN FAULT TREE ANALYSIS FOR NUCLEAR POWER PLANT PROBABILISTIC SAFETY ASSESSMENT

JULWAN HENDRY PURBA[a], JIE LU[b], GUANGQUAN ZHANG[b]

[a]*Center for Nuclear Reactor Safety and Technology*
National Nuclear Energy Agency of Indonesia (BATAN)
Gd. 80 Kawasan Puspiptek Setu, Tangerang Selatan
Banten – Indonesia 15310
purba-jh@batan.go.id

[b]*Decision Systems and e-Service Intelligence Laboratory*
Centre for Quantum Computation & Intelligent Systems
School of Software, Faculty of Engineering and Information Technology
University of Technology, Sydney (UTS)
P.O. Box 123, Broadway, NSW 2007, Australia
{Jie.Lu, Guangquan.Zhang}@uts.edu.au

Fault tree analysis for nuclear power plant probabilistic safety assessment is an intricate process. Personal computer-based software systems have therefore been developed to conduct this analysis. However, all existing fault tree analysis software systems only accept quantitative data to characterized basic event reliabilities. In real-world applications, basic event reliabilities may not be represented by quantitative data but by qualitative justifications. The motivation of this work is to develop an intelligent system by fuzzy reliability algorithm in fault tree analysis, which can accept not only quantitative data but also qualitative information to characterized reliabilities of basic events. In this paper, a newly-developed system called InFaTAS-NuSA is presented and its main features and capabilities are discussed. To benchmark the applicability of the intelligent concept implemented in InFaTAS-NuSA, a case study is performed and the analysis results are compared to the results obtained from a well-known fault tree analysis software package. The results confirm that the intelligent concept implemented in InFaTAS-NuSA can be very useful to complement conventional fault tree analysis software systems.

Keywords: Fault tree analysis; probabilistic safety assessment; nuclear power plant; fuzzy reliability algorithm; InFaTAS-NuSA.

1. Introduction

Fault tree analysis (FTA) 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.[1-3] It has been used in the last two decades to study the level I probabilistic safety assessment (PSA) of nuclear power plants (NPPs).[4-6]

Due to the complexity of FTA, a number of personal computer-based software systems have been developed. Two well-known FTA software packages in NPP PSA are

Probabilistic Safety Analysis PACKage (PSAPACK)[7-9] and Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE).[10-15] PSAPACK was developed by the International Atomic Energy Agency (IAEA) in cooperation with its Member States.[16] Meanwhile, SAPHIRE was developed by the U.S. Nuclear Regulatory Commission at the Idaho National Laboratory.[17] These two packages can only accept numerical values to represent basic event reliability characteristics.[16, 18] However, in real-world applications, reliabilities of some basic events may not be characterized by quantitative data but by qualitative linguistic terms.[19-21] Therefore, the motivation of this study is to develop an intelligent FTA system, which can accept qualitative linguistic terms to characterize reliabilities of basic events, to complement conventional FTA for NPP PSA. This intelligent system called InFaTAS-NuSA is realized by implementing a set of seven failure possibilities and a set of seven membership functions of triangular fuzzy numbers, which have been developed in Purba et al.[22], to deal with basic events whose reliabilities cannot be characterized by quantitative data. An area defuzzification technique, which has been developed in Purba et al.[23], is then used to decode triangular fuzzy numbers into a single numerical value. To benchmark the applicability of InFaTAS-NuSA, a case study on an NPP PSA is performed and the results are compared to the results of the same system generated by SAPHIRE. There are two aspects of originalities of InFaTAS-NuSA: (1) an introduction of the set of seven failure possibilities and the set of seven triangular fuzzy numbers into the quantitative analysis phase of conventional FTA; and (2) an implementation of a fuzzy reliability algorithm to integrate qualitative information with quantitative data. Furthermore, InFaTAS-NuSA exhibits two advantages: (1) it enables experts to qualitatively evaluate basic event reliability characteristics based on their expertise, working experiences and scientific intuition; and (2) it enables safety analysts to generate basic event probabilities from qualitative information provided by experts.

The rest of the paper is organized as follows. Section 2 describes new features implemented in InFaTAS-NuSA. The fuzzy reliability algorithm to generate basic event probabilities from qualitative information is given in Section 3. Section 4 describes a real-world application to be evaluated by InFaTAS-NuSA. The applicability of InFaTAS-NuSA for NPP PSA are then analyzed in Section 5. Finally, Section 6 summarizes the paper and briefly describes further research directions.

2. InFaTAS-NuSA New Features

The basic structure of InFaTAS-NuSA is shown in Fig. 1. It takes three different types of inputs and generates four different types of outputs.
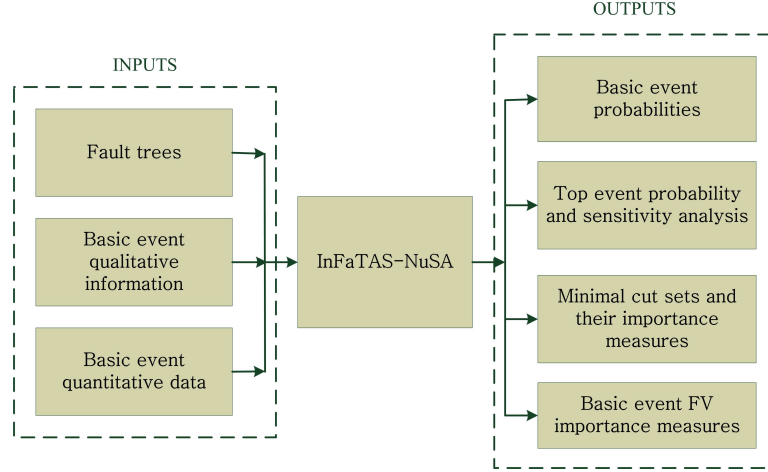
Fig. 1. Basic structure of InFaTAS-NuSA.

New features which are implemented in InFaTAS-NuSA to make it different from conventional FTA system are as follows.

2.1. *Basic Event Failure Possibility Distribution*

A set of seven qualitative linguistic terms has been developed in Purba et al.[22] to scale basic event failure possibilities from the less likely to the most likely occurrences as denoted in (1).

$$H = \{h_i \mid i = 1, 2, \ldots, 7\} = \{very\ low, low, reasonably\ low, moderate, reasonably\ high, high, very\ high\} \quad (1)$$

Those seven failure possibilities in (1) and their corresponding failure likelihood values are shown in Table 1.

Table 1. Basic event failure likelihood values.

Basic event failure possibilities	Failure likelihood values
very low	< 1.0E-8
low	1.0E-8 – 1.0E-7
reasonably low	1.0E-7 – 1.0E-6
moderate	1.0E-6 – 1.0E-5
reasonably high	1.0E-5 – 1.0E-4
high	1.0E-4 – 1.0E-3
very high	> 1.0E-3

2.2. *Failure Possibility Membership Functions*

A set of seven membership function of triangular fuzzy numbers has been developed in Purba et al.[22] to mathematically represent those seven basic event qualitative failure possibilities in (1) as denoted in (2-8).

$$\mu_{very\ low}(x) = \{0.00, 0.04, 0.08\} \tag{2}$$

$$\mu_{low}(x) = \{0.07, 0.13, 0.19\} \tag{3}$$

$$\mu_{reasonably\ low}(x) = \{0.17, 0.27, 0.37\} \tag{4}$$

$$\mu_{moderate}(x) = \{0.35, 0.50, 0.65\} \tag{5}$$

$$\mu_{reasonably\ high}(x) = \{0.63, 0.73, 0.83\} \tag{6}$$

$$\mu_{high}(x) = \{0.81, 0.87, 0.93\} \tag{7}$$

$$\mu_{very\ high}(x) = \{0.92, 0.96, 1.00\} \tag{8}$$

2.3. *Weighted Average Aggregation*

A weighted average aggregation in (9) is used to aggregate experts' subjective justifications.[24]

$$\mu_{b_k}(x) = \frac{w_{e_1} \cdot \mu_{e_1} \oplus w_{e_2} \cdot \mu_{e_2} \oplus w_{e_3} \cdot \mu_{e_3} \oplus \ldots \oplus w_{e_n} \cdot \mu_{e_n}}{w_{e_1} \oplus w_{e_2} \oplus w_{e_3} \oplus \ldots \oplus w_{e_n}} \tag{9}$$

where b_k is the kth basic event of a set of basic events (B) of a fault tree (FT) being evaluated as denoted in (10) and e_j is the jth expert of a set of experts (E) involved to evaluate B as denoted in (11). Meanwhile, μ_{e_j} is a membership function of triangular fuzzy numbers in (2-8) given by expert e_j to basic event b_k, w_{e_j} is a credibility weight of expert e_j as denoted in (12) and n is a number of experts.

$$B = \left\{b_i \mid i = 1, 2, 3, \ldots, l\right\} \text{ and } B \in FT \tag{10}$$

$$E = \left\{e_1, e_2, \cdots, e_n\right\} \tag{11}$$

$$W = \left\{w_1, w_2, \cdots, w_n; 0 \le w_i \le 1 \text{ and } \sum_{i=1}^{n} w_i = 1\right\} \tag{12}$$

2.4. *Area Defuzzification Technique*

An area defuzzification technique has been developed in Purba et al.[23] to decode a membership function of fuzzy numbers into a failure possibility score (R_s) in NPP PSA involving fuzzy concepts. R_s of a membership function of triangular fuzzy numbers is calculated as in (13).

$$R_s = ADT(\mu(x)) = \frac{1}{18}\left(4x_1 + x_2 + x_3\right) \tag{13}$$

where x_1, x_2 and x_3 are the numerical values of the parameters of the membership function $\mu(x) = (x_1, x_2, x_3)$

2.5. *Onisawa's Logarithmic Function*

An Onisawa's logarithmic function is to generate a failure probability (R) for each basic event in (10) as denoted in (14).[22, 24]

$$R = \begin{cases} \dfrac{1}{10^m}, & R_s \neq 0 \\ 0, & R_s = 0 \end{cases} \tag{14}$$

where $m = [(1 - R_s)/R_s]^{(1/3)} \times 2.301$ and R_s is a failure possibility score generated in (13).

2.6. *Minimal Cut Set Importance Measure*

A cut set of a fault tree is a set of fault events if they occur together can cause the top event to occur. Meanwhile, a minimal cut set is a cut set that has been reduced into the minimum number of fault events to cause the top event to occur.[25, 26] A minimal cut set importance measure is a measure used to assess how far a minimal cut set contributes to the failure of the top event[25, 27], which can be evaluated using (15).

$$\% mcs_i = \frac{P_{mcs_i}}{P_T} \times 100\% \tag{15}$$

where $\% mcs_i$ is the contribution percentage of the ith minimal cut set, P_{mcs_i} is the failure probability of the ith minimal cut set as in (16), and P_T is the overall probability of the top event as in (17).

$$P_{mcs_i} = \prod_{j=1}^{n} P_{b_j} \tag{16}$$

where b_j is a basic event in the mcs_i and n is the number of basic event in mcs_i.

$$P_T = 1 - \prod_{i=1}^{m} \left\{ 1 - P_{mcs_i} \right\} \tag{17}$$

where m is the number of minimal cut sets of the fault tree under evaluation.

2.7. *Basic Event Fussell-Vesely Importance Evaluation*

A Fussell-Vesely importance is a measure to evaluate how far a basic event contributes to the failure of the top event, which can be evaluated using (18).

$$P_T = 1 - \prod_{i=1}^{m} \left\{ 1 - P_{mcs_i} \right\} \tag{18}$$

where b is the basic event to be evaluated, P_T is the overall probability of the top event as in (17), $P_{mcs_i(b)}$ is the probability of the ith minimal cut set containing the basic event b, and n is the number of minimal cut sets containing the basic event b.

2.8. *Top Event Sensitivity Analysis*

Top event sensitivity is analysed by generating a lower bound and an upper bound failure possibilities for each basic event. The lower bound failure possibility is generated using the lowest grade of failure possibility justified by the experts. Meanwhile, the upper bound failure possibility is generated using the highest grade of failure possibility justified by the experts. For example, if the failure possibilities of the basic event A are subjectively justified by five experts as {*low, reasonably low, low, moderate, low*}, then the lower bound failure possibility is generated using this set of failure possibilities "{*low, low, low, low, low*}" and the upper bound failure possibility is generated using this set of failure possibilities "(*moderate, moderate, moderate, moderate, moderate*}". Those lower and upper failure possibilities are then used to generate the failure probability range of the top event to find a sensitivity spectrum of the top event to the variations of the experts' subjective justifications.

3. Fuzzy Reliability Algorithm

A fuzzy reliability algorithm to generate a probability of a basic event of system fault trees from a qualitative failure possibility is as follows.

WHILE still basic event b_i

    IF b_i has historical failure probability distribution

        Enter its **lower bound**, **best estimate** and **upper bound** failure probabilities
    ELSE

        WHILE still experts e_j

            Read failure possibility $h_k^{e_j.b_i}$ given by the expert e_j

Find the left endpoint $x_{1k}^{e_j}$, the core $x_{2k}^{e_j}$ and the right endpoint $x_{3k}^{e_j}$ of the corresponding membership function μ_k

IF $h_k^{e_j.b_i} = h_1$ THEN $x_{1k}^{e_j} = 0.00; x_{2k}^{e_j} = 0.04; x_{3k}^{e_j} = 0.08$

ELSE IF $h_k^{e_j.b_i} = h_2$ THEN $x_{1k}^{e_j} = 0.07; x_{2k}^{e_j} = 0.13; x_{3k}^{e_j} = 0.19$

ELSE IF $h_k^{e_j.b_i} = h_3$ THEN $x_{1k}^{e_j} = 0.17; x_{2k}^{e_j} = 0.27; x_{3k}^{e_j} = 0.37$

ELSE IF $h_k^{e_j.b_i} = h_4$ THEN $x_{1k}^{e_j} = 0.35; x_{2k}^{e_j} = 0.50; x_{3k}^{e_j} = 0.65$

ELSE IF $h_k^{e_j.b_i} = h_5$ THEN $x_{1k}^{e_j} = 0.63; x_{2k}^{e_j} = 0.73; x_{3k}^{e_j} = 0.83$

ELSE IF $h_k^{e_j.b_i} = h_6$ THEN $x_{1k}^{e_j} = 0.81; x_{2k}^{e_j} = 0.87; x_{3k}^{e_j} = 0.93$

ELSE IF $h_k^{e_j.b_i} = h_7$ THEN $x_{1k}^{e_j} = 0.92; x_{2k}^{e_j} = 0.96; x_{3k}^{e_j} = 1.00$

END WHILE

Calculate the final membership function $\mu^{b_i}(x) = \left(x_1, x_2, x_3\right)$

FOR $l = 1$ to 3

$$x_l = \sum_{k=1}^{7} \sum_{j=1}^{j=n} \left(w_j \times x_{lk}^{e_j} \right)$$

END FOR

Calculate the b_i event failure possibility score $R_S^{b_i}$

$$R_s^{b_i} = \frac{1}{18}\left(4x_1 + x_2 + x_3\right)$$

Calculate the b_i event failure probability R^{b_i}

IF $R_S^{b_i} = 0$ THEN $R^{b_i} = 0$

ELSE $R^{b_i} = \dfrac{1}{10\left[\dfrac{1 - R_S^{b_i}}{R_S^{b_i}}\right]^{1/3} \times 2.301}$

END WHILE

4. A Real-World Application

The first model of a reactor protection system (RPS) of the Combustion Engineering pressurized water reactor (PWR) is applied to verify the effectiveness and applicability of the new features introduced into InFaTAS-NuSA to overcome the limitation of conventional FTA.

4.1. *Problem Description*

The RPS is one of many safety systems in nuclear power plants, which is designed to perform safe shutdown of the reactor by inserting control rod clusters into the reactor core to immediately terminate nuclear reaction, so that heat generation in the core can be eliminated. With the help of other safety systems, the integrity of the fuel and the reactor coolant pressure boundary can be maintained.

The Combustion Engineering RPS comprises numerous electronic and mechanical components to produce an automatic and manual rapid reactor trip. The first model of this RPS consists of four channels to measure parameter plants, six trip matrices to trip the reactor trip switch gear, trip breakers to interrupt power to the control element assembly drive mechanism (CEDM) allowing gravity to insert the control rod assembly into the reactor core, and a group of control rods, which will be de-energized on successful RPS actuation. The simplified diagram of the Combustion Engineering RPS is shown in Fig. 2. The failure of this system has been evaluated using SAPHIRE and the results are well documented in Wierman et al.[13].
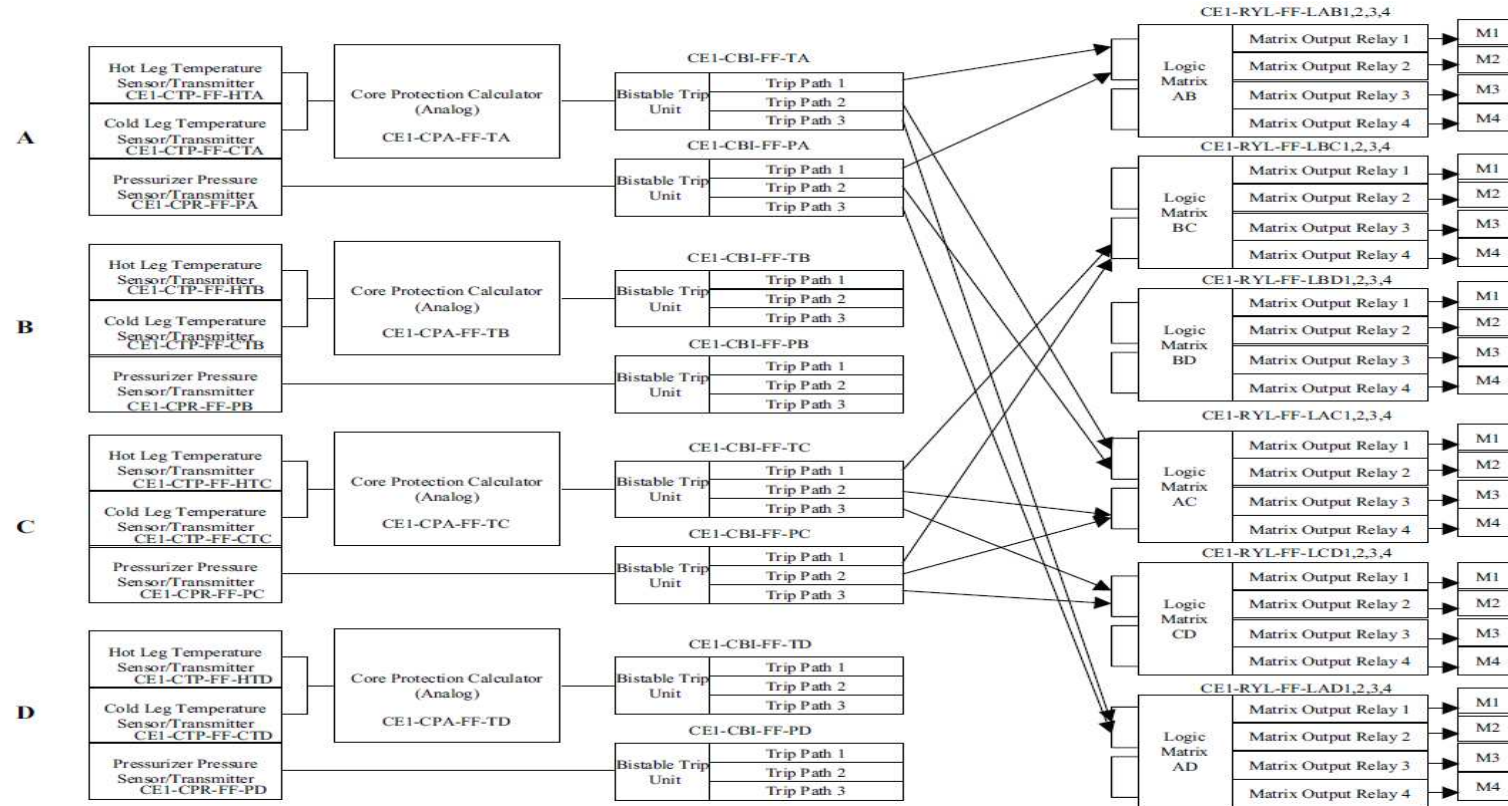
Fig. 2. Simplified diagram of the Combustion Engineering RPS Group 1.[13]

4.2. *Basic Event Failure Possibility Evaluation*

To demonstrate the integration of quantitative data with qualitative information, basic events of the Combustion Engineering RPS group 1 are classified into two groups. The first group is a set of basic events whose reliability characteristics are individually and subjectively evaluated by experts using the seven failure possibilities in (1). This set of basic events is shown in Table 2. To illustrate the quantification process of the algorithm described in Section 3, let us assume that seven experts of the same level of expertise about the Combustion Engineering RPS have been selected and their evaluations are given in Table 4. We need to note that those justification results shown in Table 4 are just of illustrative character of experts to obtain the closest matching failure probabilities to the known best estimate values, which are generated through simulation. Meanwhile, the second group is a set of basic events whose probabilities are available. This set of basic events is given in Table 3.

Table 2. A set of basic events whose reliability characteristics is evaluated by experts.

Basic event name	Description
CE1-CBI-FF-PA,B,C,D CE1-CBI-FF-TA,B,C,D	Channel trip unit (bi-stable) fails to trip at its set point
CE1-CPA-FF-TA,B,C,D	Channel analog core protection calculator fails to send a signal to the trip unit
CE1-CPR-FF-PA,B,C,D	Channel reactor vessel pressure sensor/ transmitter fails to detect a high pressure and sends a signal to the trip unit
CE1-CTP-FF-CTA,B,C,D CE1-CTP-FF-HTA,B,C,D	Channel reactor vessel temperature/ transmitter (cold or hot leg) fails to detect a low level and sends a signal to the trip unit
CE1-MSW-FF-MT1,2	Manual scram switch fails to operate upon demand
CE1-RYL-FF-LA,B,C,D–1,2,3,4	Channel logic relay fails to de-energize upon demand
CE1-RYT-FF-ICM1,2,3,4	Trip system trip relay fails to de-energize upon demand
CE1-CBI-CF-P(T)2OF3TM	Common cause failure specific 2 of 3 bi-stables associated with either a pressure (P) or temperature (T) signal (T&M)
CE1-CBI-CF-P(T)3OF4	Common cause failure specific 3 of 4 bi-stables associated with either a pressure (P) or temperature (T) signal
CE1-CBI-CF-4OF6TM	Common cause failure specific 4 of 6 bi-stables (T&M)
CE1-CBI-CF-6OF8	Common cause failure specific 6 of 8 bi-stables
CE1-CPA-CF-T2OF3TM	Common cause failure 2 of 3 analog core protection calculators (T&M)
CE1-CPA-CF-T3OF4	Common cause failure 3 of 4 analog core protection calculators
CE1-CPR-CF-P2OF3TM	Common cause failure 2 of 3 pressure sensor/ transmitters (T&M)
CE1-CPR-CF-P3OF4	Common cause failure 3 of 4 pressure sensor/ transmitters
CE1-CTP-CF-C(H)T2OF3TM	Common cause failure 2 of 3 temperature sensor/ transmitters (T&M)
CE1-CTP-CF-C(H)T3OF4	Common cause failure 3 of 4 temperature sensor/ transmitters
CE1-ROD-CF-RODS	Common cause failure 20% or more CRD/rods fail to insert
CE1-RYL-CF-LM6OF12TM	Common cause failure specific 6 of 12 logic relays (T&M)
CE1-RYL-CF-LM12OF24	Common cause failure specific 12 of 24 logic relays
CE1-RYL-CF-1,2,3,4LM3OF3TM	Common cause failure 3 of 3 logic relays (T&M)
CE1-RYL-CF-1,2,3,4LM6OF6	Common cause failure 6 of 6 logic relays
CE1-RYT-CF-TR2OF4 CE1-RYT-CF-2OF4	Common cause failure 2 of 4 trip relays

Table 3. A set of basic events whose probabilities is available.

Basic event name	Description	Failure probabilities		
		Lower bound	Best estimate	Upper bound
/CE1-RPS-TM-CHA	RPS channel A NOT in test and maintenance	9.68E-1	9.8E-1	1.0
CE1-RPS-TM-CHA	RPS channel A in test and maintenance	0.0	1.6E-2	3.2E-2
CE1-XHE-XE-SCRAM	Operator fails to initiate manual scram	1.0E-2	1.0E-2	1.0E-2

Table 4. Expert subjective evaluation results.

Basic event name	Basic event failure possibilities justified by the experts						
	e_1	e_2	e_3	e_4	e_5	e_6	e_7
CE1-CBI-FF-PA,B,C,D CE1-CBI-FF-TA,B,C,D	*Reasonably High*	*High*	*Reasonably High*	*High*	*Reasonably High*	*High*	*Reasonably High*
CE1-CPA-FF-TA,B,C,D	*Very High*	*Very High*	*Very High*	*Very High*	*Very High*	*Very High*	*Very High*
CE1-CPR-FF-PA,B,C,D	*Reasonably High*	*Moderate*	*Moderate*	*Moderate*	*Moderate*	*Moderate*	*Reasonably High*
CE1-CTP-FF-CTA,B,C,D CE1-CTP-FF-HTA,B,C,D	*High*	*Very High*	*High*	*Very High*	*High*	*Very High*	*High*
CE1-MSW-FF-MT1,2	*Moderate*	*Reasonably High*	*Moderate*	*Moderate*	*Moderate*	*Moderate*	*High*
CE1-RYL-FF-LA,B,C,D–1,2,3,4	*Reasonably High*	*Reasonably High*	*Reasonably High*	*Reasonably High*	*Moderate*	*Reasonably High*	*Reasonably High*
CE1-RYT-FF-ICM1,2,3,4	*Reasonably High*	*Moderate*	*Reasonably High*	*Moderate*	*Moderate*	*Moderate*	*Moderate*
CE1-CBI-CF-P(T)2OF3TM	*Reasonably Low*	*Low*	*Reasonably Low*	*Low*	*Low*	*Very Low*	*Low*
CE1-CBI-CF-P(T)3OF4	*Reasonably Low*	*Reasonably Low*	*Moderate*	*Reasonably Low*	*Reasonably Low*	*Reasonably Low*	*Reasonably Low*
CE1-CBI-CF-4OF6TM	*Low*	*Low*	*Low*	*Reasonably Low*	*Low*	*Reasonably Low*	*Moderate*
CE1-CBI-CF-6OF8	*Reasonably Low*	*Reasonably Low*	*Reasonably Low*	*Low*	*Low*	*Low*	*Low*
CE1-CPA-CF-T2OF3TM	*Reasonably High*	*Reasonably High*	*Reasonably High*	*High*	*Reasonably High*	*Reasonably High*	*Reasonably High*
CE1-CPA-CF-T3OF4	*Moderate*	*Moderate*	*Moderate*	*Reasonably High*	*Reasonably High*	*Moderate*	*High*
CE1-CPR-CF-P2OF3TM	*Low*	*Reasonably Low*	*Low*	*Low*	*Moderate*	*Reasonably Low*	*Moderate*
CE1-CPR-CF-P3OF4	*Reasonably Low*	*Reasonably Low*	*Reasonably Low*	*Reasonably Low*	*Low*	*Reasonably Low*	*Very Low*
CE1-CTP-CF-C(H)T2OF3TM	*Moderate*	*Reasonably Low*	*Moderate*	*Reasonably Low*	*Moderate*	*Moderate*	*Moderate*
CE1-CTP-CF-C(H)T3OF4	*Low*	*Reasonably Low*	*Reasonably Low*	*Reasonably Low*	*Reasonably Low*	*Moderate*	*Moderate*
CE1-ROD-CF-RODS	*Low*	*Low*	*Reasonably Low*	*Reasonably Low*	*Low*	*Reasonably Low*	*Low*
CE1-RYL-CF-LM6OF12TM	*Very Low*	*Low*	*Reasonably Low*	*Reasonably Low*	*Low*	*Very Low*	*Low*
CE1-RYL-CF-LM12OF24	*Low*	*Low*	*Very Low*	*Low*	*Low*	*Low*	*Low*
CE1-RYL-CF-1,2,3,4LM3OF3TM	*Low*	*Reasonably Low*	*Low*	*Reasonably Low*	*Low*	*Very Low*	*Reasonably Low*
CE1-RYL-CF-1,2,3,4LM6OF6	*Low*	*Low*	*Reasonably Low*	*Low*	*Low*	*Low*	*Low*
CE1-RYT-CF-TR2OF4 CE1-RYT-CF-2OF4	*Reasonably Low*	*Reasonably Low*	*Reasonably Low*	*Reasonably Low*	*Reasonably Low*	*Reasonably Low*	*Reasonably Low*

5. Result Analysis

To show the effectiveness and the applicability of the new features implemented in InFaTAS-NuSA to overcome the limitation of conventional FTA, we compare four types of outputs generated by InFaTAS-NuSA to the ones generated by SAPHIRE, i.e. basic event probabilities as in Table 5, top event failure probability as in Table 6, minimal cut set importance measures as in Table 7, and basic event Fussell-Vesely importance measures as in Table 8.

Table 5. Comparison of basic event probabilities.

Basic event name	Basic event probabilities in		Relative error
	SAPHIRE	InFaTAS-NuSA	
CE1-CBI-FF-PA,B,C,D	5.0E-4	4.8E-4	0.045884
CE1-CBI-FF-TA,B,C,D			
CE1-CPA-FF-TA,B,C,D	**7.6E-3**	**1.0E-3**	**0.864983**
CE1-CPR-FF-PA,B,C,D	1.1E-4	1.1E-4	0.040376
CE1-CTP-FF-CTA,B,C,D	8.4E-4	8.3E-4	0.009576
CE1-CTP-FF-HTA,B,C,D			
CE1-MSW-FF-MT1,2	1.3E-4	1.3E-4	0.035225
CE1-RYL-FF-LA,B,C,D–1,2,3,4	2.6E-4	2.8E-4	0.092713
CE1-RYT-FF-ICM1,2,3,4	1.2E-4	1.1E-4	0.046322
CE1-CBI-CF-P(T)2OF3TM	2.6E-7	2.6E-7	0.004218
CE1-CBI-CF-P(T)3OF4	7.2E-6	7.5E-6	0.047039
CE1-CBI-CF-4OF6TM	1.7E-6	1.8E-6	0.047185
CE1-CBI-CF-6OF8	7.7E-7	7.6E-7	0.013927
CE1-CPA-CF-T2OF3TM	3.8E-4	3.8E-4	0.012703
CE1-CPA-CF-T3OF4	1.7E-4	1.7E-4	0.007939
CE1-CPR-CF-P2OF3TM	5.0E-6	5.0E-6	0.006601
CE1-CPR-CF-P3OF4	1.5E-6	1.5E-6	0.000282
CE1-CTP-CF-C(H)T2OF3TM	3.7E-5	3.6E-5	0.019914
CE1-CTP-CF-C(H)T3OF4	1.0E-5	9.2E-6	0.076792
CE1-ROD-CF-RODS	8.4E-7	7.6E-7	0.096100
CE1-RYL-CF-LM6OF12TM	1.6E-7	1.5E-7	0.031932
CE1-RYL-CF-LM12OF24	4.3E-8	4.3E-8	0.010018
CE1-RYL-CF-1,2,3,4LM3OF3TM	4.7E-7	5.1E-7	0.090759
CE1-RYL-CF-1,2,3,4LM6OF6	2.0E-7	2.0E-7	0.013905
CE1-RYT-CF-2OF4	4.8E-6	4.4E-6	0.089537

It can be seen from Table 5 that the greatest relative error of the basic event probabilities generated by InFaTAS-NuSA is less than 10%, which means that the generated probabilities are very close to the known probabilities, except for the basic event **CE1-CPA-FF-TA, B, C, D**. This exception might be caused by the incapability of the fuzzy reliability algorithm implemented in InFaTAS-NuSA to generate basic event probabilities greater than 1.03E-03. To confirm and verify this incapability, two important issues need to be raised in future studies, i.e. the failure possibility distribution as well as their membership function definitions and the defuzzification technique.

Nevertheless, in general, the results have confirmed that the new features introduced into InFaTAS-NuSA are effective to deal with basic events whose reliabilities are characterized by qualitative justifications to overcome the limitation of conventional FTA for NPP PSA. These results also confirm that expert subjective evaluations can be in good agreement with the real quantitative probabilities collected from nuclear power plant operating experiences.

Table 6. Top event failure probability and its sensitivity

Failure probability	SAPHIRE	InFaTAS-NuSA
Lower bound value (5%)	8.8E-7	4.5E-6
Mean value	5.7E-6	5.2E-6
Upper bound value (95%)	1.7E-5	9.0E-6

Meanwhile, the mean value generated by InFaTAS-NuSA is very much closer to the mean value generated by SAPHIRE as shown in Table 6. The difference of these values is caused by the difference in the basic event probabilities generated by InFaTAS-NuSA and the data directly input to SAPHIRE. However, the top event failure probability range generated by InFaTAS-NuSA is still inside the acceptable range of the system failure probability calculated by SAPHIRE.

Table 7. Minimal cut set importance measures.

Minimal cut sets	SAPHIRE		InFaTAS-NuSA	
	Failure probability	Contribution percentage	Failure probability	Contribution percentage
CE1-RYT-CF-2OF4	4.80E-06	84.5%	4.37E-6	84.6%
CE1-ROD-CF-RODS	8.40E-07	14.9%	7.59E-7	14.7%
CE1-RYT-FF-ICM2*CE1-RYT-FF-ICM1	1.40E-08	0.3%	1.31E-8	0.3%
CE1-RYT-FF-ICM4*CE1-RYT-FF-ICM3	1.40E-08	0.3%	1.31E-8	0.3%
/CE1-RPS-TM-CHA*CE1-CBI-CF-6OF8*CE1-XHE-XE-SCRAM	7.50E-09	0.1%	7.44E-9	0.1%
/CE1-RPS-TM-CHA*CE1-RYL-CF-LM12OF24*CE1-XHE-XE-SCRAM	4.20E-10	0.0%	4.17E-10	0.0%
CE1-CBI-CF-4OF6TM*CE1-RPS-TM-CHA*CE1-XHE-XE-SCRAM	2.80E-10	0.0%	2.85E-10	0.0%
/CE1-RPS-TM-CHA*CE1-CBI-CF-6OF8*CE1-MSW-FF-MT1	9.80E-11	0.0%	1.00E-10	0.0%
/CE1-RPS-TM-CHA*CE1-CBI-CF-6OF8*CE1-MSW-FF-MT2	9.80E-11	0.0%	1.00E-10	0.0%
CE1-RPS-TM-CHA*CE1-RYL-CF-LM6OF12TM*CE1-XHE-XE-SCRAM	2.50E-11	0.0%	2.48E-11	0.0%

Furthermore, Table 7 shows that the importance measures of the minimal cut sets generated by InFaTAS-NuSA are in the same order with the ones generated by SAPHIRE. The fact that the contribution percentage shown in this table equals to zero

does not mean that it is zero but that it is very small due to the round-off in the algorithm used.

Table 8. Basic event Fussell-Vesely importance measures.

Basic events	InFaTAS-NuSA
CE1-RYT-CF-2OF4	8.46E-1
CE1-ROD-CF-RODS	1.47E-1
CE1-RYT-FF-ICM1	2.54E-3
CE1-RYT-FF-ICM2	2.54E-3
CE1-RYT-FF-ICM3	2.54E-3
CE1-RYT-FF-ICM4	2.54E-3
CE1-XHE-XE-SCRAM	1.58E-3
/CE1-RPS-TM-CHA	1.56E-3
CE1-CBI-CF-6OF8	1.48E-3
CE1-RYL-CF-LM12OF24	8.30E-5

Table 8 shows the top ten basic events which contribute the most to the failure of the RPS of the Combustion Engineering PWR Group 1. Unfortunately, the details of this evaluation generated by SAPHIRE are not provided in Wierman et al.[13], but it was mentioned that the trips of CE1-RYT-FF-ICM1, CE1-RYT-FF-ICM2, CE1-RYT-FF-ICM3, and CE1-RYT-FF-ICM4 are four dominant contributors to the failure of this RPS, as also can be seen in Table 8. In this important measure, the ranking of the basic events is more important than the FV scores.

6. Conclusion and Further Research

This study has developed InFaTAS-NuSA to overcome the limitations of the conventional fault tree analysis by introducing new features to deal with basic events whose reliability characteristics are represented by qualitative justifications. The introduction of the failure possibility distribution enables safety analysts to qualitatively characterize basic event reliabilities when they are not provided with quantitative probability distributions, which is needed in conventional fault tree analysis. Furthermore, the introduction of the fuzzy reliability algorithm enables safety analysts to evaluate reliability of a system by integrating qualitative information with quantitative data, which cannot be done in conventional fault tree analysis. The first model of the reactor protection system of the Combustion Engineering pressurized water reactor has been used to verify the effectiveness and applicability of the new features introduced into InFaTAS-NuSA. Four types of outputs, i.e. basic event probabilities, top event failure probability, minimal cut set importance measures, and basic event Fussell-Vesely importance measures, generated by InFaTAS-NuSA are benchmarked to the ones of the same system generated by SAPHIRE. The results of the benchmarking confirm that new features introduced into InFaTAS-NuSA can overcome the limitations of the conventional fault tree analysis for nuclear power plant probabilistic safety assessment.

Based on the current results, we need to conduct more experiments to explore InFaTAS-NuSA's features and enable future improvements and/or find new directions for development.

Acknowledgments

References

1. M.J. Delaney, G.E. Apostolakis, and M.J. Driscoll, Risk-informed design guidance for future reactor systems. *Nucl. Eng. Des.* **235** (2005) 1537-1556.
2. T. Kishi, H. Kikuchi, S. Miura, M. Fukuda, M. Hirano, and N. Watanabe, Application of probabilistic safety assessment to the pipe rupture incident at Hamaoka Unit-1. *J. Nucl. Sci. Technol.* **41** (2004) 77-85.
3. L.P. Davies, Risk assessment in the UK nuclear power industry. *Saf. Sci.* **40** (2002) 203-230.
4. A.C.F. Guimaraes and C.M.F. Lapa, Parametric fuzzy study for effects analysis of age on PWR containment cooling system. *Appl. Soft Comput.* **8** (2008) 1562–1571.
5. B.J. Garrick and R.F. Christie, Probabilistic risk assessment practices in the USA for nuclear power plants. *Saf. Sci.* **40** (2002) 177-201.
6. C. Kirchsteiger, A new approach to quantitative assessment of reliability of passive systems. *Saf. Sci.* **43** (2005) 771-777.
7. P.V. Suresh, A.K. Babar, and V. Venkat Raj, Uncertainty in fault tree analysis: A fuzzy approach. *Fuzzy Sets Syst.* **83** (1996) 135-141.
8. A.J. Arul, C.S. Kumar, S. Athmalingam, O.P. Singh, and K.S. Rao, Reliability analysis of safety grade decay heat removal system of Indian prototype fast breeder reactor. *Ann. Nucl. Energy*. **33** (2006) 180-188.
9. G. Vinod, H.S. Kushwaha, A.K. Verma, and A. Srividya, Importance measures in ranking piping components for risk informed in-service inspection. *Reliab. Eng. Syst. Saf.* **80** (2003) 107-113.
10. E.A. Harvego, S.M.M. Reza, M. Richards, and A. Shenoy, An evaluation of reactor cooling and coupled hydrogen production processes using the modular helium reactor. *Nucl. Eng. Des.* **236** (2006) 1481-1489.
11. F. Faghihi, E. Ramezani, F. Yousefpour, and S.M. Mirvakili, Level-1 probability safety assessment of the Iranian heavy water reactor using SAPHIRE software. *Reliab. Eng. Syst. Saf.* **93** (2008) 1377-1409.
12. J.H. Bickel, Risk implications of digital reactor protection system operating experience. *Reliab. Eng. Syst. Saf.* **93** (2008) 107-124.
13. T.E. Wierman, S.T. Beck, M.B. Calley, S.A. Eide, C.D. Gentillon, and W.E. Kohn, Reliability study: Combustion engineering reactor protection system, 1984–1998, in *NUREG/CR-5500, Vol. 10*. 2001: , USNRC, Washington DC.

14. S.S. Arshi, M. Nematollahi, and K. Sepanloo, Coupling CFAST fire modeling and SAPHIRE probabilistic assessment software for internal fire safety evaluation of a typical TRIGA research reactor. *Reliab. Eng. Syst. Saf.* **95** (2010) 166-172.

15. T.E. Wierman, S.T. Beck, M.B. Calley, S.A. Eide, C.D. Gentillon, and W.E. Kohn, Reliability study: Babcock and Wilcox reactor protection system, 1984–1998, in *NUREG/CR-5500, Vol. 11*. 2001: , USNRC, Washington DC.

16. L. Lederman, H. Vallerga, and A. Bojadjiev, IAEA activities on extending PSAPACK as a tool for use in NPP safety management. *Reliab. Eng. Syst. Saf.* **30** (1990) 447-454.

17. C. Smith, J. Knudsen, K. Kvarfordt, and T. Wood, Key attributes of the SAPHIRE risk and reliability analysis software for risk-informed probabilistic applications. *Reliab. Eng. Syst. Saf.* **93** (2008) 1151-1164.

18. M. Hamada, H.F. Martz, C.S. Reese, T. Graves, V. Johnson, and A.G. Wilson, A fully Bayesian approach for combining multilevel failure information in fault tree quantification and optimal follow-on resource allocation. *Reliab. Eng. Syst. Saf.* **86** (2004) 297-305.

19. R. Ferdous, F. Khan, R. Sadiq, P. Amyotte, and B. Veitch, Fault and event tree analyses for process systems risk analysis: Uncertainty handling formulations. *Risk Anal.* **31** (2011) 86-107.

20. M. Celik, S.M. Lavasani, and J. Wang, A risk-based modelling approach to enhance shipping accident investigation. *Saf. Sci.* **48** (2010) 18-27.

21. O. Hryniewicz, in *Computational Intelligence in Reliability Engineering New Metaheuristics, Neural and Fuzzy Techniques in Reliability*, ed. G. Levitin (Springer-Verlag, Berlin Heidelberg, 2007), p. 363-386.

22. J.H. Purba, J. Lu, G. Zhang, and W. Pedrycz, A fuzzy reliability assessment of basic events of fault trees through qualitative data processing. *Fuzzy Sets Syst.* **243** (2014) 50-69.

23. J.H. Purba, J. Lu, D. Ruan, and G. Zhang, An area defuzzification technique to assess nuclear event reliability data from failure possibilities. *Int. J. Comput. Intell. Appl.* **11** (2012) 1250022 (16 pp).

24. J.H. Purba, J. Lu, and G. Zhang, in *Computational Intelligence Systems in Industrial Engineering*, ed. C. Kahraman (Atlantis Press, Paris, France, 2012), p. 131-154.

25. C.A. Ericson, in *Hazard Analysis Techniques for System Safety*, ed. Ericson (John Wiley & Sons, Virginia, 2005), p. 183-221.

26. Y.Y. Haimes, in *Risk Modeling, Assessment, and Management* (John Wiley & Sons, New Jersey, 2004), p. 525-569.

27. E. Borgonovo, Differential, Criticality and Birnbaum Importance Measures: An Application to Basic Event, Groups and SSCs in Event Trees and Binary Decision Diagrams. *Reliab. Eng. Syst. Saf.* **92** (2007) 1458-1467.