# Fuzzy Temporal Fault Tree Analysis of Dynamic Systems

Sohag Kabir[a,*], Martin Walker[a], Yiannis Papadopoulos[a], Erich Rüde[b], Peter Securius[b]

[a]*Department of Computer Science, University of Hull, HU6 7RX, Hull, United Kingdom*
[b]*DNV GL SE, Hamburg, Germany*

---

## Abstract

Fault tree analysis (FTA) is a powerful technique that is widely used for evaluating system safety and reliability. It can be used to assess the effects of combinations of failures on system behaviour but is unable to capture sequence dependent dynamic behaviour. A number of extensions to fault trees have been proposed to overcome this limitation. Pandora, one such extension, introduces temporal gates and temporal laws to allow dynamic analysis of temporal fault trees (TFTs). It can be easily integrated in model-based design and analysis techniques. The quantitative evaluation of failure probability in Pandora TFTs is performed using exact probabilistic data about component failures. However, exact data can often be difficult to obtain. In this paper, we propose a method that combines expert elicitation and fuzzy set theory with Pandora TFTs to enable dynamic analysis of complex systems with limited or absent exact quantitative data. This gives Pandora the ability to perform quantitative analysis under uncertainty, which increases further its potential utility in the emerging field of model-based design and dependability analysis. The method has been demonstrated by applying it to a fault tolerant fuel distribution system of a ship, and the results are compared with the results obtained by other existing techniques.

*Keywords:* Reliability Analysis, Fault Tree Analysis, Dynamic Fault Trees, Temporal Fault Trees, Uncertainty Analysis, Fuzzy Set Theory

---

## 1. Introduction

Safety critical systems are widely used in many industries, e.g., aerospace, automotive, and energy sectors, and the failure of such systems has the potential to cause catastrophic effects on human life as well as the environment. An increasing amount of effort is now often devoted to ensuring that such failures cannot occur, and this can be achieved through dependability engineering techniques. One of the key goals in designing safety critical systems is to identify potential risks posed by such systems so that these risks can then be minimised. System safety and reliability are two key aspects of system dependability. Their estimation at design stage typically involves calculation of probabilities of system failures. In the case of safety, the focus is on failures that are potentially severe in their effects and therefore a low probability of occurrence must be demonstrated to keep risk at acceptable level. A wide variety of methods have been developed to perform safety analysis and reliability evaluation of systems. Fault tree analysis (FTA) is a well-established and widely used method for evaluating system safety and reliability. This is a graphical method to show the logical connection between different faults and their causes. Fault trees use Boolean logic and usually use AND and OR gates to show the combinations of component failures that are necessary and sufficient to cause the system failure.

Both qualitative and quantitative analysis can be performed using fault trees. The qualitative analysis is deductive in nature, i.e., the analysis starts with a system failure known as the top event and iteratively works backwards to identify the root causes of the top event. Afterwards, Boolean logic is used to minimise the

---

*Corresponding author. Tel: +44 (0)7405 024667
*Email address:* `s.kabir@2012.hull.ac.uk` (Sohag Kabir)

fault tree to obtain minimal cut sets (MCS) which are the smallest combination of the failure of components that can cause the system failure. Once the MCSs are obtained, by using probabilistic data about system components, quantitative analysis can be performed to estimate the probability of the system failure after a specified period of time. The quantification of fault trees are typically performed by calculating the probability of each MCS and by summing all the MCS probabilities. In addition to the top event probability, importance of the basic events, the intermediate events, and the minimal cut sets can be obtained from the fault tree quantification [1].

Increasingly, systems are growing more complex and their configurations becoming more dynamic, i.e., a system can operate in different functional modes. With the change of mode the interactions and data flow between components in the system architecture changes, and thus so does the propagation of faults through the system. Due to the dynamic nature of the system behaviour, assessing the effects of combinations of failure events is not enough by itself to fully capture the system failure behaviour; it is also necessary to understand the order in which they fail to obtain a more accurate and informative failure model. Despite the widespread use of FTA, the technique is not capable of capturing this sequence-dependent dynamic behaviour [2, 3]. A number of extensions to combinatorial fault trees such as dynamic fault trees (DFTs) [4] and Pandora temporal fault trees [5] have been introduced to address this limitation.

DFTs enable quantitative analysis of dynamic systems. They introduce a set of new dynamic gates, such as the SPARE (to model redundant spare components), FDEP (to model functional dependencies), and SEQ (to represent sequences) gates, and are usually evaluated by translating them into Markov chains. DFTs are explained further in section 2.2.1. Pandora likewise extends fault trees by introducing three temporal gates and a set of temporal laws to capture dynamic behaviour of systems. Temporal gates are used to determine the minimal cut sequences (MCSQs), which are the smallest sequences of events that are necessary and sufficient to cause the system failure.

The main idea behind introducing the Pandora temporal fault tree was to facilitate qualitative analysis of dynamic systems by minimising the temporal fault trees into MCSQs using the temporal laws. One of the advantages of Pandora is that by performing qualitative analysis, it can create useful insight into system failures with limited or absent quantitative failure data, e.g., in the case of new system components. Moreover, the technique is integrated well with model-based design and analysis. It has been shown in [3] that Pandora logical expressions can be used to describe the local failure behaviour of components and then enable compositional synthesis of TFTs from systems models using popular modelling languages, e.g. Matlab Simulink, EAST-ADL, or AADL, that have been annotated with Pandora expressions. Chen et al. [6] described an approach on dynamic fault tree analysis using temporal fault trees and Markov chains in the context of the EAST-ADL domain specific architecture description language.

Although the primary goal of Pandora was to perform qualitative analysis of failure behaviour of dynamic systems, a number of recent efforts [7, 8] have been made to probabilistically evaluate the Pandora TFTs. Similar to other probabilistic reliability evaluation methods, such as classical FTA, the quantification methods for Pandora TFTs also assume that the components of a system are non-repairable, basic events are statistically independent, and failure behaviour of components are described by precise probability distributions, i.e., these methods take it as guaranteed that precise probabilistic failure data of components are always available. However, for many complex systems, it is often very difficult to estimate precise failure data of components from past occurrences due to lack of knowledge, scarcity of statistical data, and changes in operating environments of the systems [9, 10]. This situation is especially relevant in the early design stages because at that time analysts may have to consider new or partially defined components which have no available quantitative failure data, and thus precise failure data could not possibly be known. Therefore, in the absence of precise failure data, it may be necessary to work with rough estimates of probabilities. The existing evaluation methods for the Pandora TFTs are not capable of working with uncertain data of this sort.

Fuzzy set theory has been proven effective in solving problems where precise data are not available and in making decisions from vague information [11, 12, 13]. Fuzzy set theory was firstly used in FTA by Tanaka et al. [10], where failure probabilities of the basic events of the fault tree were represented as trapezoidal fuzzy numbers and the fuzzy extension principle was used to estimate the probability of the top event. Further extensive research on fuzzy fault tree analysis was performed by Misra and Weber [12] and

Liang and Wang [14] based on the work presented in [10]. At the same time, Gmytrasiewicz et al. [15] and Singer [16] have also analysed fault trees based on fuzzy set theory. Fuzzy set theories and the expert elicitation have been combined in [17] to evaluate the reliability of a robot drilling system. Some of the early work on investigating the use of fuzzy logic on safety includes work on post-hoc deductive accident investigation [18]. Fuzzy set theory based FTA (FFTA) has been used to analyse the reliability of a variety of systems, for example, Yuhua and Datao [19] have used FFTA to evaluate the failure probability of oil and gas transmission system. An intuitionistic fuzzy sets based method has been used in [20] for the failure analysis of the printed circuit board assembly. Ferdous et al. [21] have proposed a computer-aided fuzzy fault tree analysis method. Tyagi et al. [22] have applied FFTA in reliability analysis of an electric power transformer. Recently, FFTA has been used to evaluate the probability of the fire and explosion in crude oil tanks [23] and Rajakarunakaran et al. [24] have applied FFTA for risk evaluation of an LPG refuelling station.

Although a significant amount of research has investigated how to use fuzzy set theory in classical FTA to enable it to perform quantitative analysis with limited quantitative data, very limited research, such as [25, 26, 27, 28] has been undertaken to allow the same in dynamic fault tree analysis. Recently, some preliminary ideas on fuzzy set theory based Pandora temporal fault tree analysis were presented in [29]. Given the increasing importance of model-based design and analysis, and the potential benefits of Pandora in this context, we believe that it is both theoretically and practically useful to explore possible ways to incorporate uncertainty aspects in the quantitative analysis of Pandora TFTs. This could yield significant advantages when analysing systems at early stages in the design process, for example, when firm quantitative failure data is not available. It would allow the design to be refined on the basis of the results and then further quantitative analysis can be conducted later on to confirm the results once solid data is available. Therefore, in this paper, we propose a fuzzy set theory based quantification methodology for Pandora TFTs. The proposed methodology is demonstrated by applying it to evaluate the dependability of a fault tolerant fuel distribution system of a ship.

The rest of the paper is organised as follows: Section 2 presents some preliminary ideas on fuzzy fault tree analysis, dynamic extensions of classical fault trees, more specifically, the fundamental basis of Pandora temporal fault trees and the ways of quantifying Pandora TFTs. Section 3 describes the proposed methodology. The method is then illustrated by applying it to a case study in section 4. Finally, our concluding remarks are presented in section 5.

## 2. Background

### 2.1. Fuzzy Set Theory and Fuzzy Fault Tree Analysis

Fuzzy set theory has been developed to deal with imprecise, vague or partially true information [11]. A fuzzy number $A$ can be thought of as a set of real numbers where each possible value has a weight between 0 and 1. This weight is referred to as degree of membership defined by a membership function. Let us consider a function $\mu_A(x) : \mathbb{R} \to [0,1]$ as:

$$\mu_A(x) = \begin{cases} \mu_A^l(x), & for\ a_1 < x \le b_1 \\ \mu_A^r(x), & for\ b_1 \le x < c_1 \\ 0, & otherwise. \end{cases} \tag{1}$$

Note that $\mu_A(x)$ has a left region $\mu_A^l(x)$ and a right region $\mu_A^r(x)$ connected at maximum, $\mu_A^l(b_1) = \mu_A^r(b_1)$. Now we can define a fuzzy number $A$ by the function in equation (1) which is called the membership function of the fuzzy number $A$, and write

$$A \triangleq \mu_A(x) \tag{2}$$

where $\triangleq$ means *is defined as*.

Fuzzy set theory has been used in fault tree analysis in different ways. The basic idea of fuzzy fault tree analysis is to use fuzzy representations of component failure data instead of the crisp representations used in classical FTA. Among different forms of fuzzy numbers, the triangular fuzzy number (TFN) and

3

the trapezoidal fuzzy number (TZFN) are widely used in reliability analysis to represent fuzzy failure rates or probabilities of components. The triangular representation of the basic event failure probabilities can be denoted by a triplet $(a_1, b_1, c_1)$ and the corresponding membership function is written as:

$$\mu_A(x) = \begin{cases} \dfrac{x - a_1}{b_1 - a_1}, & for\ a_1 < x \le b_1 \\ \dfrac{c_1 - x}{c_1 - b_1}, & for\ b_1 < x < c_1 \\ 0, & otherwise. \end{cases} \tag{3}$$

A trapezoidal form of the failure probability can be denoted by a quadruple $(a_1, b_1, c_1, d_1)$, and the membership function is defined as:

$$\mu_A(x) = \begin{cases} \dfrac{x - a_1}{b_1 - a_1}, & for\ a_1 < x < b_1 \\ 1, & for\ b_1 \le x \le c_1 \\ \dfrac{d_1 - x}{d_1 - c_1}, & for\ c_1 < x < d_1 \\ 0, & otherwise. \end{cases} \tag{4}$$

Fuzzy operators for the fault tree gates are defined to quantify the output probabilities of the gates based on the fuzzy representation of the failure probabilities of input basic events. For example, if the probability of a basic event $BE_i$ is represented as $Pr\{BE_i\}(t) = \{a_i(t), b_i(t), c_i(t)\}$ then for all statistically independent basic events, the fuzzy operators for the AND and the OR gate are defined as follows:

$$P_{AND} = \left\{ \prod_{i=1}^{N} a_i(t), \prod_{i=1}^{N} b_i(t), \prod_{i=1}^{N} c_i(t) \right\} \tag{5}$$

$$P_{OR} = \left\{ 1 - \prod_{i=1}^{N} (1 - a_i(t)), 1 - \prod_{i=1}^{N} (1 - b_i(t)), 1 - \prod_{i=1}^{N} (1 - c_i(t)) \right\} \tag{6}$$

where $b_i(t)$ is the most likely value of the probability of the basic event $BE_i$ at time $t$ and $a_i(t)$ and $c_i(t)$ are the lower and upper bound of the basic event probability respectively.

After the minimal cut sets (MCSs) in sum-of-products form are obtained from the qualitative analysis of a fault tree, the fuzzy failure rates are provided for the basic events constituting the MCSs. Subsequently, all the MCSs are quantified using equation (5) and the top event probability is quantified using equation (6). As fuzzy representations of the basic event failure probabilities are used in the quantification process, the top event probability is also obtained as fuzzy number. However, sometimes the fuzzy top event probability is mapped to a crisp (non-fuzzy) value.

## 2.2. Dynamic Extensions of Classical Fault Trees

### 2.2.1. Dynamic Fault Trees

Dynamic Fault Trees (DFTs) [4] are an extension of static fault trees that enable a fault tree to capture sequence dependent dynamic behaviour. To represent the dynamic behaviour of the systems, DFT introduces two special gates: the Functional Dependency (FDEP) gate and SPARE gate. The FDEP gate helps to model a scenario when functionalities of some system components are dependent on the operation of a single component. For example, if a single power supply is used to provide power to many of the system components then failure of the power supply would cause all the dependent components to fail as well. In the FDEP gate there is only one trigger event (either a basic event or an intermediate event) but there could be multiple functionally dependent events (see Fig.1(a)). The occurrence of the trigger event would force the dependent events to occur; by contrast, the occurrence of a dependent event would affect neither the trigger event nor the other dependent events. This gate is particularly convenient for modelling networked systems

4

where communication between connected components take place through a common network element and the failure of the common element isolates the other connected elements.



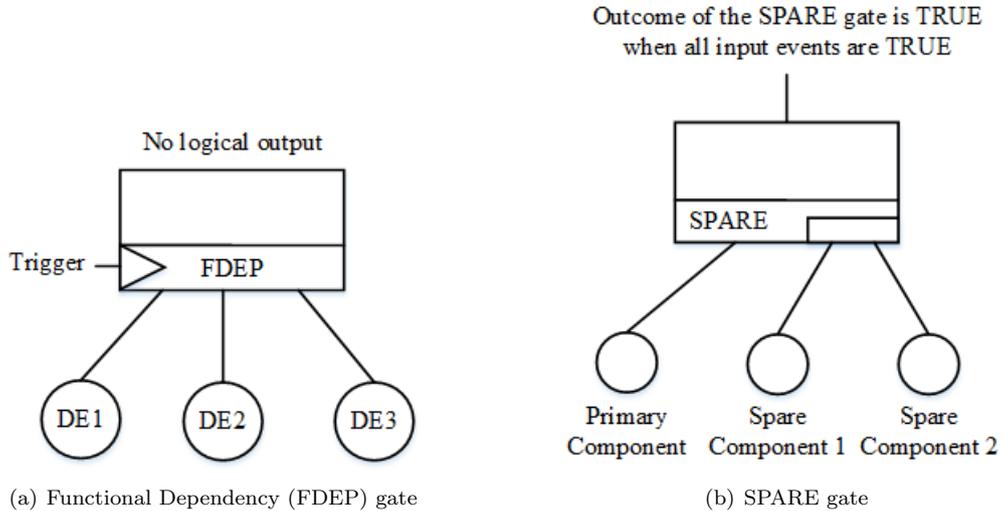(a) Functional Dependency (FDEP) gate          (b) SPARE gate

Figure 1: Dynamic fault tree gates

A SPARE gate is shown in Fig.1(b), with three basic event inputs. One of the basic events (left most) acts as a primary component and other events act as secondary backup components. This gate models a scenario where the spare components are activated in a sequence, i.e., if there are two spare components then when the primary component fails, the leftmost spare component will be activated; if the first spare fails then the second spare will be activated and so on. The SPARE gate can model three types of spares: cold spares, warm spares, and hot spares. In the cold spare mode the spare components are deactivated until they are required in any sort of system operation. In contrast, in the hot spare mode, the spare components are always kept active but only serve their function when the primary fails. In warm spare mode, the spare components are neither on nor off, instead they are kept in-between these two states, i.e., components are kept in a reduced readiness state until required. Multiple SPARE gates can share a pool of spare components. In this case, if the primary component of any of the SPARE gates fails, it is then replaced by the first available spare component (i.e., neither failed nor already occupied by another SPARE gate). DFTs also use two other gates to model sequences of events: the Priority-AND (PAND) gate, which is true only if its input events occur in a particular sequence (typically left to right), and the Sequence-Enforcing gate (SEQ), which imposes a sequence on its events such that they must occur in that order. This latter gate can be viewed as a type of cold SPARE gate and so is not often used.

DFTs are intended to perform quantitative reliability analysis of dynamic systems, and consequently they have limited support for qualitative analysis. For probabilistic evaluation, DFTs are typically transformed into equivalent Markov chains and quantified based on exponential distribution of failure behaviour of components [30, 31]. Alternatives have also been proposed, such as an algebraic framework to model dynamic gates of DFTs; this allows qualitative [32] and quantitative [33, 34] analysis of DFTs. Moreover, Petri Nets based approaches [35, 36] and Bayesian Networks based approaches [37, 38, 39] are also developed to quantify DFTs.

*2.2.2. Pandora Temporal Fault Trees*

As with DFTs, Pandora is intended to enable analysts to more readily capture sequence-related failure behaviour in fault trees. Pandora extends conventional fault trees by defining three temporal gates: Priority-AND (PAND), Priority-OR (POR), and Simultaneous-AND (SAND) (see Fig. 2). These gates allow analysts to represent sequences or simultaneous occurrence of events as part of a fault tree.

5

The PAND gate is not a new gate and has been used in FTA as far back as the 1970s [40]; it is also used in the Dynamic Fault Tree methodology, as mentioned above. However, the semantics of the PAND gate were not fully defined, particularly with regard to what happens when input events occur simultaneously or when contradictory sequences are used (e.g. a PAND with repeated input events, suggesting an input occurring before itself), and this ambiguity limited its usefulness in qualitative analysis. Later techniques such as Pandora have defined its semantics in more depth. In Pandora, therefore, the PAND gate is used to represent a particular sequence of events and is defined as being true only if:

- all input events occur;

- input events occur in sequence from left to right;

- and no input events occur simultaneously.

In this paper, for clarity, the symbol '$\lhd$' is used to represent the PAND gate in logical expressions, i.e., $X \lhd Y$ means $X \ PAND \ Y$ where $X$ and $Y$ are both failure events.
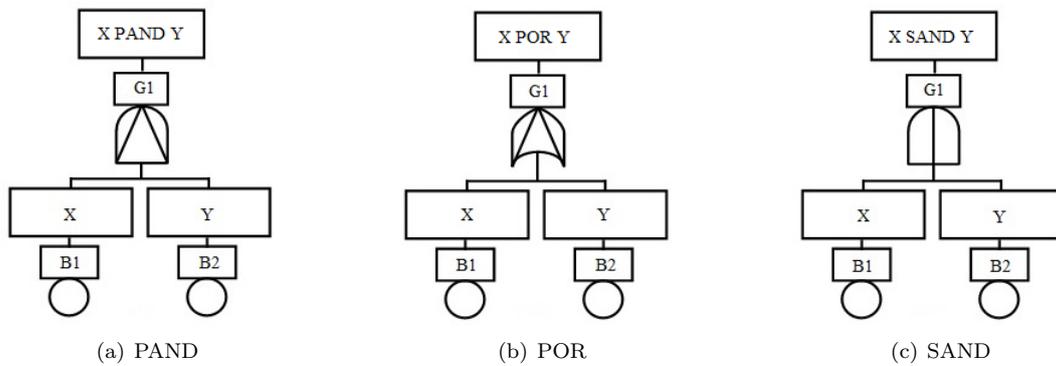


(a) PAND          (b) POR          (c) SAND

Figure 2: Pandora temporal gates

Like the PAND gate, the POR gate also defines a sequence. It is used to indicate that one input event has priority and must occur first for the POR to be true, but unlike PAND does not require all other input events to occur as well. It can be used to represent trigger conditions where the occurrence of the priority event means that subsequent events may have no effect. The POR is true only if its left-most (priority) input event occurs and no other input event occurs before or at the same time as the left-most input event. The symbol '$\wr$' is used to represent the POR gate in logical expressions, thus $X \wr Y$ means $X \ POR \ Y$.

The SAND gate is used to define situations where an outcome is only triggered if two or more events occur approximately simultaneously, e.g., because of a common cause, or because the events have a different effect if they occur approximately simultaneously as opposed to in a sequence. It is true only if all input events occur and all events occur at the same time. The symbol '&' is used to represent the SAND gate in logical expressions. Pandora temporal fault trees also use the Boolean AND and OR gate. '$\vee$' and '$\wedge$' are used to represent OR and AND gate in logical expressions respectively. The priority of the gates is as follows: SAND is highest, then PAND, POR, AND, and OR.

Pandora considers events (failure of components) as persistent, i.e., once an event occurs, it remains in the 'true' state indefinitely. It also considers that the transition from one state to another state occurs instantly, i.e., there is no delay to go from 'false' to 'true' state. In addition to three temporal gates, Pandora also defines a set of temporal laws that describe the behaviour of the gates and how they relate to each other and to the standard Boolean AND and OR gates. The most important of these laws are the Completion Laws [5], which relate the temporal gates to the Boolean gates:

- Conjunctive Completion Law: $\qquad X \wedge Y \qquad \Leftrightarrow \qquad X \lhd Y \vee X \& Y \vee Y \lhd X$

6

- Disjunctive Completion Law: $\qquad X \vee Y \qquad \Leftrightarrow \qquad X \wr Y \vee X \& Y \vee Y \wr X$

- Reductive Completion Law: $\qquad X \qquad \Leftrightarrow \qquad Y \lhd X \vee X \& Y \vee X \wr Y$

These laws allow us to reduce and minimise the temporal expressions to obtain minimal cut sequences (MCSQs), which are analogous to minimal cut sets in classical fault trees. Temporal laws form the basis for qualitative analysis of Pandoras temporal fault trees and can be proved with temporal truth tables [5].

### 2.2.3. Quantitative Evaluation of Pandora TFTs

Quantitative analysis of Pandora TFTs helps to estimate the probability of the top event occurring from the given failure rates of basic failure modes (events) of the system. Quantification of TFTs requires quantifying the gates, and various techniques are available for probabilistic evaluation of TFT gates. These techniques include analytical solutions [40, 1, 33, 7, 34]; a Markov chain based solution [30]; Bayesian network based solutions [41, 39, 8]; and Petri net based solutions [35, 36]. However, this paper considers analytical solutions only as they are most compatible with the fuzzy set based approach. Note that the analytical solutions above work based on the fixed value of components' failure data and consider that the system components have exponentially distributed failure rates.

The probability of an AND gate with $N$ statistically independent events can be evaluated as [42]:

$$Pr\{E_1 \wedge E_2 \wedge E_3 \wedge \ \cdots \ \wedge E_{N-1} \wedge E_N\}(t) = \prod_{i=1}^{N} P_r\{E_i\}(t) \tag{7}$$

where $Pr\{E_i\}(t)$ is the probability of failure of basic event $E_i$ at time $t$.

If an OR gate has $N$ input events, the probability of the OR gate is frequently approximated using the following equation [43]:

$$Pr\{E_1 \vee E_2 \vee E_3 \vee \cdots \vee E_{N-1} \vee E_N\}(t) = 1 - \prod_{i=1}^{N} \left(1 - P_r\{E_i\}(t)\right) \tag{8}$$

In a minimal cut sequence (MCSQ), if there are $N$ statistically independent input events in a PAND gate and they occur sequentially, i.e., event 1 occurs first, then event 2, $\cdots$, event $N-1$, and finally event $N$, then the probability of that PAND gate can be evaluated as [33]:

$$Pr\{E_1 \lhd E_2 \lhd E_3 \lhd \ \cdots \ \lhd E_{N-1} \lhd E_N\}(t) = \prod_{i=1}^{N} \lambda_i \sum_{k=0}^{N} \left[\frac{e^{(u_k t)}}{\prod_{\substack{j=0 \\ j \neq k}}^{N} (u_k - u_j)}\right] \tag{9}$$

where $u_0 = 0$ and $u_m = -\sum_{j=1}^{m} \lambda_j \ for \ m > 0$.

For any minimal cut sequence of $N$ statistically independent events in a POR gate with the expression $E_1 \wr E_2 \wr E_3 \wr \cdots \wr E_{N-1} \wr E_N$, the probability of that POR gate can be evaluated as [7]:

$$Pr\{E_1 \wr E_2 \wr E_3 \wr \cdots \wr E_{N-1} \wr E_N\}(t) = \frac{\lambda_1 \left(1 - \left(e^{-(\sum_{i=1}^{N} \lambda_i)t}\right)\right)}{\sum_{i=1}^{N} \lambda_i} \tag{10}$$

In a continuous time domain, the probability of two exponentially distributed statistically independent events occurring at the same time can be treated as zero [33]. For this reason, any minimal cut sequence containing the SAND operator are usually ignored during the quantitative evaluation of Pandora TFTs. As the MCSQs can contain any number of gates from AND, PAND, SAND and POR gates, although SAND gate is quantified as zero, they are probabilistically evaluated using equation (7), (9), and (10) depending on the nature of the gates the MCSQs contain. The top event of the TFTs is represented as the disjunction of the MCSQs and hence the top event probability can be approximated closely using equation (8).

7

### 3. Fuzzy Temporal Fault Tree Analysis

The main idea behind fuzzy temporal fault tree analysis is to use a fuzzy representation of the failure data instead of single values and then evaluate the top event as a range of possible values. In this way, important quantitative information about the dependability of a system can be obtained even if the exact data about the system components are not known. To be able to use the fuzzy representation of the failure data we have to define the fuzzy operators for the temporal fault tree gates. After the temporal fault tree is obtained using qualitative analysis, the following steps are required to be able to use the fuzzy representation of failure data in the quantitative analysis:

- Obtain fuzzy possibility of component failure data.

- Use fuzzy possibility values and the fuzzy operators of the TFT gates to obtain fuzzy top event possibility and importance measures.

- Determine the crisp top event probability from the top event possibility.

#### 3.1. Process of obtaining fuzzy failure data for system components

Before we can use the fuzzy set theory based methodology, we need to decide what form of the fuzzy representation of the numbers we are going to use to represent the failure data for the components. After that, we have to obtain the fuzzy failure possibility of components in the prespecified format. There are different methods available to obtain fuzzy numbers such as expert knowledge elicitation or $3\sigma\sigma$ expression [9]. In this paper, we use the triangular form of the fuzzy number to represent the failure possibilities of basic events and use the expert elicitation method to obtain the fuzzy failure possibility of components. However, the users have the flexibility to use any other method to obtain the data.

#### 3.1.1. Domain expert evaluation and fuzzification of the opinion

In this evaluation step, a set of qualitative data representing the failure possibility of basic events is obtained. To obtain this, a set of experts is provided with a set of basic events from the TFT representing the failure behaviour of the system and the mission time $t$. The experts will then subjectively evaluate the failure possibility of the components after the specified mission time. An expert is a person who is familiar with the system under consideration, have knowledge about the working environment of the system, and have considerable training and knowledge of the system operation. The experts can be selected from different fields like design, operation, maintenance, and management of the system.

As experts are human beings, they may have different levels of expertise, working experience and obviously their background may vary widely. The experts make decisions about different basic events based on their experiences and their knowledge about the system. As a result, the opinions obtained from different experts are subjective due to the varying perceptions of the experts about the system. In a real world scenario, the opinion of an expert with higher experience and expertise should be given higher priority over the opinion of the expert with relatively low expertise and experience. To facilitate this, a weighting factor is used to define the relative quality of the opinion of the experts.

Due to the complexity of the systems and the vagueness of the events, the experts cannot provide the exact numerical values regarding the failure possibility of components; instead they give their opinion in linguistic terms. The values of linguistic variables are words or sentences in natural languages and they play an important role in dealing with situations which are too complex or vague in nature, i.e., very difficult to describe using conventional quantitative expressions. For instance, we can consider *"failure possibility of component"* as a linguistic variable consisting of fuzzy sets like *very low, low, fairly low, medium, fairly high, high, very high* as shown in the example Fig. 3.

Once an expert provides his/her opinion about the failure possibility of an event in linguistic terms, then this must be mapped to corresponding quantitative data in the form of a membership function of fuzzy numbers. As mentioned earlier, the membership functions could be of triangular or trapezoidal form. For example, Fig. 3 shows membership functions of the linguistic variables in the triangular form. The system analysts have to define the failure possibility distribution (values for membership functions) for different

8

Table 1: Weighting scores for different experts [24]

| Constitution | Classification | Score |
|---|---|---|
| Professional Position | Professor, GM/DGM, Chief Engineer, Director | 5 |
| | Assistant Professor, Manager, Factory Inspector | 4 |
| | Engineer, Supervisors | 3 |
| | Foreman, Technician, Graduate apprentice | 2 |
| | Operator | 1 |
| Professional Experience (years) | $\geq 20$ | 5 |
| | 15 to 19 | 4 |
| | 10 to 14 | 3 |
| | 5 to 9 | 2 |
| | $< 5$ | 1 |
| Educational or Technical qualification | Ph.D or M.Tech. | 5 |
| | MSc or B.Tech. | 4 |
| | Diploma or BSc | 3 |
| | ITI | 2 |
| | Secondary school | 1 |
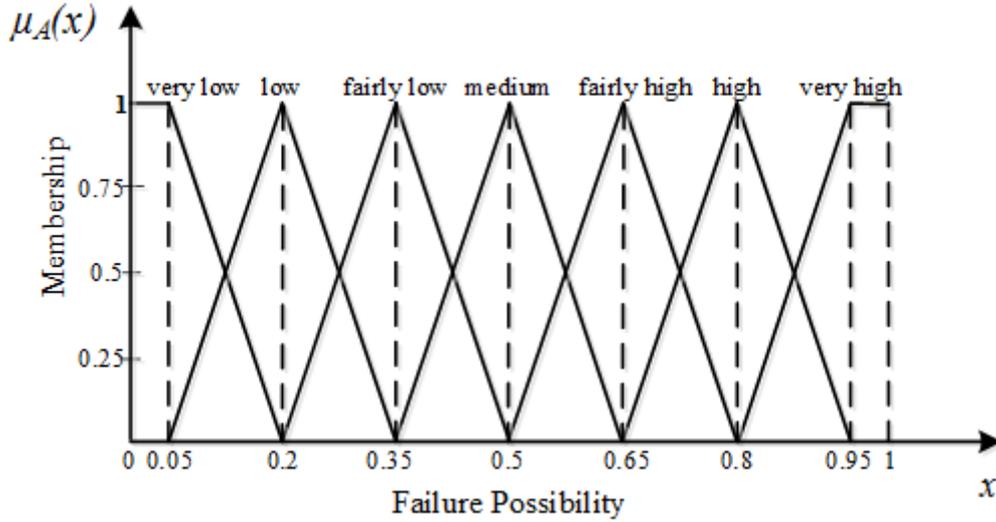


Figure 3: Fuzzy numbers representing linguistic variables

linguistic variables based on the nature of the system they want to analyse. However, this is a subjective task and results may vary from analyst to analyst. Ross [44, 45] described six different methods – intuition, inductive reasoning, inference, genetic algorithm, neural networks, and rank ordering to form membership functions of fuzzy sets. Analysts can choose any of the above mentioned methods to define the values for membership functions of the failure possibility of the basic events.

3.1.2. Aggregation of the opinions of the experts

In the domain expert evaluation process, failure possibility data for each basic event is obtained from a set of $M$ different experts. Since each expert may have different view about an event, their opinion about

9

the event may be different. In order to achieve an agreement among the conflicted views of the experts, their opinion should be aggregated into a single opinion. The aggregation could be done by simply taking the arithmetic average of different opinions, but it will give all the experts equal weight and thus overlooks the knowledge, expertise and experience of the experts. On the other hand, if we take the weighted average of the opinions to obtain a single opinion then the opinion of the experienced experts (with higher score) would dominate the result, and consequently the opinion of the less experienced experts (with a low score) will not be properly reflected. To ensure that the expertise and experience of experts are taken into account and at the same time the opinions of the less experienced experts are properly accommodated in the aggregated opinion, the aggregation process is done in six different steps, described below:

**Step 1: Similarity Measures**
In this step, a matrix known as the *similarity matrix* (SM) is obtained in the following form by calculating similarities between the opinions of different experts.

$$SM = \begin{bmatrix} 1 & s_{12} & s_{13} & \ldots & s_{1M} \\ s_{21} & 1 & s_{23} & \ldots & s_{2M} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{M1} & s_{M2} & s_{M3} & \ldots & 1 \end{bmatrix} \tag{11}$$

If there are M experts then $SM$ will be a $M \times M$ matrix and each entry in the matrix will represent the similarity between the opinions of two particular experts. For example, an entry $s_{ij}$ in this matrix represents the similarity between the opinions of experts $Ex_i$ and $Ex_j$.

To determine similarity between the opinions of two experts, we use the concept described in [46]. Hsu and Chen [46] used the following equation to obtain the similarity between two fuzzy sets.

$$S(\tilde{A}_i, \tilde{A}_j) = \frac{\int_x \left( min\{\mu_{\tilde{A}_i}(x), \mu_{\tilde{A}_j}(x)\} \right) dx}{\int_x \left( max\{\mu_{\tilde{A}_i}(x), \mu_{\tilde{A}_j}(x)\} \right) dx} \tag{12}$$

where $S(\tilde{A}_i, \tilde{A}_j)$ is known as the similarity measure function introduced in [47]; and $\tilde{A}_i$, and $\tilde{A}_j$ are the opinion of expert $i$ and $j$ respectively. The formula in equation (12) calculates the ratio of the consistent area (overlapped area) to the whole area for any form of fuzzy set.

As seen in the matrix SM, the diagonal entries are 1, because these entries represent, $S(\tilde{A}_i, \tilde{A}_i)$, i.e., similarity of one expert opinion with itself. If the two opinions do not overlap at all, then the similarity between them would be 0. As mentioned earlier, in this paper, we use the triangular form of the fuzzy set, therefore we have to derive specific formulae for different cases of triangular fuzzy set with the help of the formula of equation (12).
If two experts $Ex_i$ and $Ex_j$ provide their opinion as triangular fuzzy numbers $\tilde{A}_i$ and $\tilde{A}_j$ respectively, then four possible scenarios can occur:

1. The two sets completely overlap each other.
2. Two sets do not overlap at all.
3. Two sets partially overlap where $\tilde{A}_i$ starts before $\tilde{A}_j$ (see Fig. 4(a)).
4. Two sets partially overlap where $\tilde{A}_j$ starts before $\tilde{A}_i$ (see Fig. 4(b))

In the first scenario, both the sets (opinions are same), i.e., similarity between them is 1. In the second case, as the sets do not overlap at all, that means similarity between them is 0. In the other two cases, the opinions partially overlap and the overlapped area is another triangular fuzzy set. Let us consider the opinion of two experts $Ex_i$ and $Ex_j$ as $\tilde{A}_i = \{a_i, b_i, c_i\}$ and $\tilde{A}_j = \{a_j, b_j, c_j\}$ then the similarity between the opinions can be calculated as follows:

1. If $c_i \leq a_j$ *or* $c_j \leq a_i$ then

$$S(\tilde{A}_i, \tilde{A}_j) = 0 \tag{13}$$

10

(a) $\tilde{A}_i$ precedes $\tilde{A}_j$        (b) $\tilde{A}_j$ precedes $\tilde{A}_i$
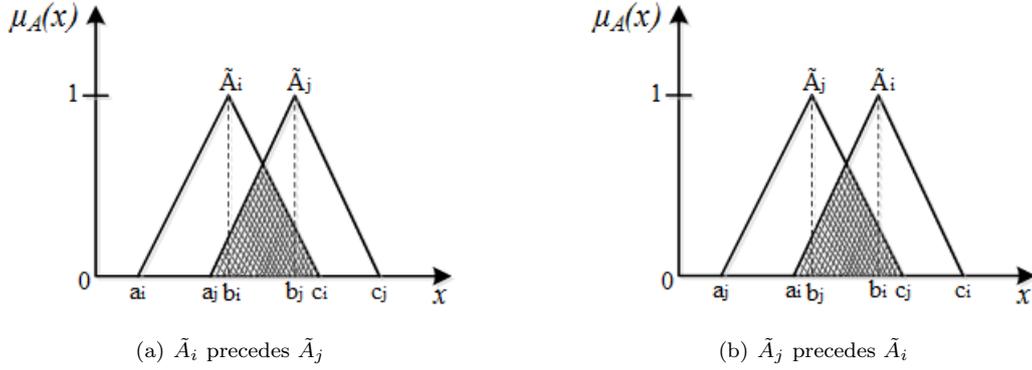
Figure 4: Overlapping between two opinions in triangular form

2. If $a_i \leq a_j$ and $c_i > a_j$ then

$$S(\tilde{A}_i, \tilde{A}_j) = \frac{(c_i - a_j)^2}{a_i(b_i - b_j - c_i) + a_j(a_i + b_i - b_j - c_j) + b_i(-c_i - c_j) + c_j(b_j + c_i) + b_j c_i} \tag{14}$$

3. If $a_j \leq a_i$ and $c_j > a_i$ then

$$S(\tilde{A}_i, \tilde{A}_j) = \frac{(c_j - a_i)^2}{a_j(b_j - b_i - c_j) + a_i(a_j + b_j - b_i - c_i) + b_j(-c_j - c_i) + c_i(b_i + c_j) + b_i c_j} \tag{15}$$

**Step 2: Average agreement calculation**
Once the similarity matrix is obtained, then the average agreement, $AA(Ex_i)$, for each of the experts is obtained as:

$$AA(Ex_i) = \frac{1}{M-1} \sum_{\substack{j=1 \\ j \neq i}}^{M} SM(i,j) \tag{16}$$

**Step 3: Relative agreement calculation**
After the average agreement for all the experts are calculated, then the relative agreement, $RAD(Ex_i)$, for all the experts is calculated as:

$$RAD(Ex_i) = \frac{AA(Ex_i)}{\sum_{i=1}^{M} AA(Ex_i)} \tag{17}$$

**Step 4: Weighting factor calculation**
Weighting scores for experts are defined in Table 1 based on their professional positions, years of working experience and their educational qualifications. As a result, when we select $M$ experts, each of them may have different weighting score (WS). For example, if we choose a professor with a PhD degree and 20 years of work experience, then his/her weighting score would be 15 (5+5+5=15). On the other hand, the weighting score for an engineer with a MSc degree and 11 years of work experience would be 10 (3+3+4). So the weighting factor for each of the experts is calculated as:

$$WF(Ex_i) = \frac{WS(Ex_i)}{\sum_{i=1}^{M} WS(Ex_i)} \tag{18}$$

where $WS(Ex_i)$ is the weighting score of expert $i$ and $WF(Ex_i)$ is weighting factor for expert $i$.

**Step 5: Aggregation weight calculation**
Now we have relative agreement degree ($RAD(Ex_i)$) and weighting factor ($WF(Ex_i)$) for all the experts. To

11

make balance between relative agreement and weighting factor, we calculate aggregation weight as follows:

$$AW(Ex_i) = \alpha \cdot WF(Ex_i) + (1 - \alpha)RAD(Ex_i) \tag{19}$$

where $\alpha$ ($0 \leq \alpha \leq 1$) is a relaxation factor which represents the importance of $WF(Ex_i)$ over $RAD(Ex_i)$. If $\alpha$ is set to zero, then no importance is paid on the $WF(Ex_i)$; on the other hand, if $\alpha$ is set to 1, then no importance is paid to $RAD(Ex_i)$. If no importance is paid to $RAD(Ex_i)$ by setting $\alpha$ to 1, then steps 1 to 3 are not required.

**Step 6: Aggregation of opinions**
This is the step where the opinions of the experts are aggregated to obtain a single opinion. The aggregation is performed using the following formula.

$$\tilde{A} = \sum_{i=1}^{M}(AW(Ex_i) \times \tilde{A}_i) \tag{20}$$

where $\tilde{A}$ is the aggregated opinion (a fuzzy set) and $\tilde{A}_i$ is the opinion of expert $i$.

*3.2. Defuzzification and top event probability calculation*

As the fuzzy possibilities of basic events are used in the quantification of the TFTs, the possibilities of the minimal cut sequences as well as the top event possibility would be obtained as fuzzy numbers. In order to provide a single possibility instead of a range of possibilities, we need to map the fuzzy failure possibilities to a crisp value known as the fuzzy failure possibility score (FFPS) through defuzzification. A number of methods, e.g., the weighted average method, the centre of area method, mean max membership method, the centre of maxima method, the mean of maxima method, centroid method, and so on are available to perform the defuzzication operation [44, 48]. For simplicity, in this paper, we use the centre of area method for defuzzification.
Defuzzication of a triangular fuzzy number, $\tilde{A} = (a_1, b_1, c_1)$ can be obtained using the following equation.

$$X = \frac{\int x\mu_{\tilde{A}}(x)dx}{\int \mu_{\tilde{A}}(x)dx} = \frac{\displaystyle\int_{a_1}^{b_1} \frac{x-a_1}{b_1-a_1}x\ dx + \int_{b_1}^{c_1} \frac{c_1-x}{c_1-b_1}x\ dx}{\displaystyle\int_{a_1}^{b_1} \frac{x-a_1}{b_1-a_1}dx + \int_{b_1}^{c_1} \frac{c_1-x}{c_1-b_1}dx} = \frac{1}{3}(a_1 + b_1 + c_1) \tag{21}$$

Using equation (21), we can obtain the top event possibility as a crisp value. However, in classical FTA, the top event is quantified as a single probability value. So, we have to map the possibility value into a probability value. Onisawa [49] has proposed a function to convert a crisp failure possibility value into a probability value. Failure probability from failure possibility can be obtained as follows.

$$FP = \begin{cases} \dfrac{1}{10^K}, & FFPS \neq 0, \\ 0, & FFPS = 0. \end{cases} \tag{22}$$

where $FP$ is the failure probability, $FFPS$ is fuzzy failure possibility score and

$K = \left( \dfrac{1-FFPS}{FFPS} \right)^{\frac{1}{3}} \times 2.301$ [49].

*3.3. Fuzzy operators for TFT gates*

Once the fuzzy failure possibilities of all the basic events are obtained, then we can use these values to quantify the top event possibility. However, we first need to define the fuzzy operators for all the TFT gates. One thing to note is that all the fuzzy operators for the TFT gates are defined for a continuous time domain

12

and for exponential distribution of failure rates.

**Fuzzy operator for the AND gate:**
The outcome of an AND gate becomes true when all the input events are true. The output probability of an AND gate with $N$ inputs can be obtained as a probability of all $N$ inputs occurring using equation (7). Now, we do not have the probability values for the basic events, rather we have fuzzy possibility values for the basic events. So, if the failure possibility of an event $i$ is presented by a triangular fuzzy number as $P_i(t) = \{a_i(t), b_i(t), c_i(t)\}$, then the fuzzy operator for the AND gate for triangular representation of the failure possibilities can be defined as:

$$P_{ANDF} = AND_F\{P_1(t), P_2(t), \cdots, P_N(t)\} = \prod_{i=1}^{N} P_i(t) = \left\{\prod_{i=1}^{N} a_i(t), \prod_{i=1}^{N} b_i(t), \prod_{i=1}^{N} c_i(t)\right\} \quad (23)$$

**Fuzzy operator for the OR gate:**
The formula to probabilistically evaluate the OR gate with $N$ statistically independent events is shown in equation (8). This formula takes probability as input and returns probability as an output. In the absence of the failure probability, if the failure possibility of an event $i$ is presented by a triangular fuzzy number as $P_i(t) = \{a_i(t), b_i(t), c_i(t)\}$, then the OR gate fuzzy operator for the triangular representation of the failure possibilities can be defined as:

$$P_{ORF} = OR_F\big(P_1(t), P_2(t), \cdots, P_N(t)\big) = 1 - \prod_{i=1}^{N} \big(1 - P_i(t)\big)$$

$$= \left(1 - \prod_{i=1}^{N} \big(1 - a_i(t)\big), 1 - \prod_{i=1}^{N} \big(1 - b_i(t)\big), 1 - \prod_{i=1}^{N} \big(1 - c_i(t)\big)\right) \quad (24)$$

Formulae for probabilistic evaluation of the PAND and the POR gate are shown in equation (9) and (10) respectively. As seen in these equations, to obtain probability of the PAND and the POR gate we need to know the failure rate of components. However, at present we have the failure possibility of components in the fuzzy form. So, we have to obtain the fuzzy failure rate of components from the fuzzy failure possibility of the components. This can be done in two steps. In the first step, the fuzzy possibility will be converted to failure probability (FP) using equation (22). In the second step, the failure rate can be obtained using the following equation.

$$\lambda = \frac{-\ln(1 - FP)}{t} \quad (25)$$

where $\lambda$ is the failure rate and $t$ is the mission time.

**Fuzzy operator for the PAND gate:**
If the failure rate of an event $i$ is represented by a triangular fuzzy number as $\lambda_i = (l_i, m_i, n_i)$, then using equation (9) the fuzzy probability of the outcome of the PAND gate can be defined as:

$$P_{PANDF} = \left\{\prod_{i=1}^{N} l_i \sum_{k=0}^{N} \left[\frac{e^{(u_k t)}}{\prod_{\substack{j=0 \\ j \neq k}}^{N} (u_k - u_j)}\right], \prod_{i=1}^{N} m_i \sum_{k=0}^{N} \left[\frac{e^{(u_k t)}}{\prod_{\substack{j=0 \\ j \neq k}}^{N} (u_k - u_j)}\right], \prod_{i=1}^{N} n_i \sum_{k=0}^{N} \left[\frac{e^{(u_k t)}}{\prod_{\substack{j=0 \\ j \neq k}}^{N} (u_k - u_j)}\right]\right\} \quad (26)$$

**Fuzzy operator for the POR gate:**
If the failure rate of an event $i$ is represented by a triangular fuzzy number as $\lambda_i = (l_i, m_i, n_i)$, then using equation (10) the fuzzy probability of the outcome of the POR gate can be defined as:

$$P_{PORF} = \left\{\frac{l_1\left(1 - \big(e^{-(\sum_{i=1}^{N} l_i)t}\big)\right)}{\sum_{i=1}^{N} l_i}, \frac{m_1\left(1 - \big(e^{-(\sum_{i=1}^{N} m_i)t}\big)\right)}{\sum_{i=1}^{N} m_i}, \frac{n_1\left(1 - \big(e^{-(\sum_{i=1}^{N} n_i)t}\big)\right)}{\sum_{i=1}^{N} n_i}\right\} \quad (27)$$

13

We can see that the fuzzy operators for the Boolean gates use the failure possibility of events as input and produce the output as fuzzy possibilities. On the other hand, the fuzzy operators for the temporal gates use the fuzzy failure rate as input and produce the output as a fuzzy probability. As the top event is represented as the logical OR of different MCSQs, we need to convert the fuzzy probability values obtained by the temporal gates into fuzzy possibility value. Failure possibility from failure probability can be obtained from equation (22) as follows:

$$FFPS = \begin{cases} \dfrac{1}{1 + \left(\dfrac{K}{2.301}\right)^3}, & \text{if } FP \neq 0. \\ 0, & \text{if } FP = 0. \end{cases} \tag{28}$$

where FFPS is fuzzy failure possibility score, FP is failure probability, and $K = \log_{10}\left(\dfrac{1}{FP}\right)$.

### 3.4. Importance Measures

Importance measures determine the various contributions of basic or intermediate events to the occurrence of the top event or how a change in any of these events can affect the occurrence of the top event. This information can be served as a useful source of data for resource allocation (upgrade, maintenance, etc.) and helps stakeholders in improving system dependability (safety, reliability, availability etc.). In classical FTA, Fussell-Vesely and Birnbaum importance measures [1] are widely used as a part of the quantitative analysis based on the fixed failure rates of the components. In this section, a similar importance measure technique is shown which is suitable to be applied to the systems having components with fuzzy failure data.

The evaluation of the contribution of different basic events to the top event probability is very important in identifying the critical components. The importance measures used in the traditional probabilistic approaches are not applicable in the case of fuzzy set theory based approaches because in this case basic event failure data is represented as fuzzy possibilities rather than crisp probabilities. So we have to define new importance measures that are suitable for the fuzzy set theory based methodology. Different methodologies (e.g., [13, 50, 22]) have already been proposed to quantify fuzzy importance measures.

In this paper, we calculate the fuzzy importance of a basic event by taking the difference between the fuzzy top event possibilities with and without the presence of the basic event. Let $\tilde{P}_{T_i=1}$ be the fuzzy failure possibility of the top event with the basic event $i$ fully unavailable, i.e., fuzzy possibility of the basic event '$i$' is considered as $\{1, 1, 1\}$. On the other hand, $\tilde{P}_{T_i=0}$ is the failure possibility of the top event when the possibility of basic event '$i$' is $\{0, 0, 0\}$, i.e., the basic event '$i$' is fully available. In conventional approaches, the Birnbaum importance is obtained by taking the difference between $\tilde{P}_{T_i=1}$ and $\tilde{P}_{T_i=0}$ where $\tilde{P}_{T_i=1}$ and $\tilde{P}_{T_i=0}$ are crisp values . However, in this case, $\tilde{P}_{T_i=1}$ and $\tilde{P}_{T_i=0}$ are fuzzy numbers, hence, we need to find distance between these numbers to find the fuzzy importance of a basic event. The distance between two fuzzy numbers can be obtained using Euclidean or Hamming distance [51]. In this paper, we use the Euclidean distance to obtain the distance between two fuzzy numbers. As a result, the fuzzy importance measure (FIM) for a basic event '$i$' is defined as:

$$FIM(E_i) = ED[\tilde{P}_{T_i=1}, \tilde{P}_{T_i=0}] \tag{29}$$

where $ED[\tilde{P}_{T_i=1}, \tilde{P}_{T_i=0}]$ is the Euclidean distance between $\tilde{P}_{T_i=1}$ and $\tilde{P}_{T_i=0}$.
If $\tilde{P}_{T_i=1} = \{a_1{}^1, \ b_1{}^1, c_1{}^1\}$ and $\tilde{P}_{T_i=0} = \{a_1{}^0, \ b_1{}^0, c_1{}^0\}$ then

$$FIM(E_i) = ED[\tilde{P}_{T_i=1}, \tilde{P}_{T_i=0}] = \sqrt{(a_1{}^1 - a_1{}^0)^2 + (b_1{}^1 - b_1{}^0)^2 + (c_1{}^1 - c_1{}^0)^2} \tag{30}$$

Using the above equation, we can calculate importance measure for all the basic events and rank them in accordance with their importance index. For two basic events $E_i$ and $E_j$, if $FIM(E_i) > FIM(E_j)$ then the basic event $E_i$ will have greater importance then the basic event $E_j$.

14

## 4. Case Study and Evaluation

To show how the fuzzy temporal fault trees can be used to perform reliability analysis of dynamic systems, we use the case study of a fault tolerant fuel distribution system of a ship, shown in Fig. 5.
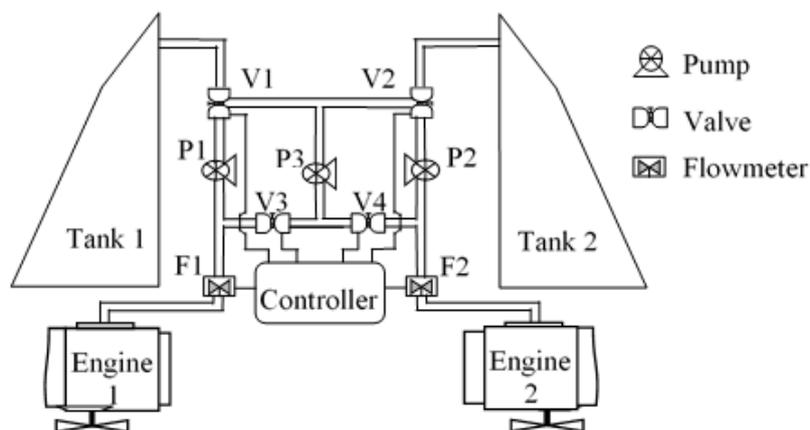


Figure 5: Fault tolerant fuel distribution system of a ship

The system consists of:

1. Two identical fuel tanks to store fuel and they are connected to other system components using polythene piping.
2. Three unidirectional fuel pumps to provide fuel to the engines from the tanks.
3. Four valves that can activate some paths or block some paths according to the requirements of the system in different situations. These valves are software controlled.
4. Two flowmeters to measure the rate of fuel flow through the pipes and these measurements are used in deciding the paths to activate and deactivate to maintain the proper fuel flow to the engines.
5. Two engines to provide thrust for the ship and are responsible for the manoeuvrability of the ship.
6. A central controller that controls different valves to activate and deactivate different paths to maintain the proper fuel flow to the engines.

Under normal operating conditions, there are two primary fuel flows: Engine 1 receives fuel from Tank 1 through Pump 1 (P1), and Engine 2 receives fuel from Tank 2 through Pump 2 (P2). Pump 3 (P3) is a standby pump which can take over the task of P1 or P2 in case one of them fails. Flowmeters F1 and F2 monitor the rate of fuel flow to the Engine 1 and 2 respectively, and provide sensory information to the Controller. In the presence of failure, if insufficient fuel flow to either of the engines is detected, then the Controller introduces dynamic behaviour to this system by activating the standby pump and redirecting the fuel flow accordingly through the valves V1 - V4. For instance, if insufficient fuel flow to Engine 1 is detected, then the Controller can activate P3 and open valves V1 and V3, and thus maintain fuel flow to Engine 1 through P3 instead of P1. On the other hand, if insufficient fuel flow to the Engine 2 is detected, then the Controller will activate P3 and open valve V2 and V4 instead. So, we can see that P3 can take over the task of either P1 or P2, but not both. A failure of both P1 and P2 will result in at least one engine being starved of fuel. For example, if P1 fails and P3 replaces it, then P3 is no longer available to replace P2 if that pump also fails. This results in degraded propulsion functionality for the vessel, as speed and manoeuvrability will be reduced, and may result in grounding or a collision.

### 4.1. Qualitative analysis of the system to generate TFT

To be able to perform the quantitative analysis, the qualitative information about the failure behaviour of the system must be obtained. Pandora temporal gates can be used to model the dynamic behaviour of

15

the above mentioned system and helps to correctly capture the sequences of events that can lead to failure. For simplicity, internal failure of the engines themselves and the failure of the tanks are left out of the scope of this analysis. The Pandora temporal fault tree for the failure behaviour of the fault tolerant fuel distribution system was constructed via model-based synthesis from Pandora descriptions of local failure logic of the components. Failure modes of the different components of the systems are abbreviated and shown in Table 2. At the top level, the causes of omission of fuel to Engine1 and 2 can be expressed using

Table 2: List of Basic Events for the fuel distribution system

| Basic Events | Description |
| --- | --- |
| P1 | Failure of Pump 1 |
| P2 | Failure of Pump 2 |
| P3 | Failure of Pump 3 |
| V1 | Failure of Valve 1 (e.g. blockage or stuck closed) |
| V2 | Failure of Valve 2 (e.g. blockage or stuck closed) |
| V3 | Failure of Valve 3 (e.g. blockage or stuck closed) |
| V4 | Failure of Valve 4 (e.g. blockage or stuck closed) |
| E1 | Omission of fuel to Engine 1 |
| E2 | Omission of fuel to Engine 2 |
| S1 | Failure of Flowmeter sensor 1 (e.g. sensor readings stuck high) |
| S2 | Failure of Flowmeter sensor 2 (e.g. sensor readings stuck high) |
| CF | Failure of Controller |

temporal gates as follows:

$$E1 = ((\texttt{O-Pump1} \wr \texttt{O-Pump2}) \wedge \texttt{O-Valve3}) \vee (\texttt{O-Pump2} \lhd \texttt{O-Pump1}) \vee (\texttt{O-Pump2} \, \& \, \texttt{O-Pump1})$$

$$E2 = ((\texttt{O-Pump2} \wr \texttt{O-Pump1}) \wedge \texttt{O-Valve4}) \vee (\texttt{O-Pump1} \lhd \texttt{O-Pump2}) \vee (\texttt{O-Pump1} \, \& \, \texttt{O-Pump2})$$

As E1 and E2 are caused by the same events in the opposite sequences, we focus on the failure behaviour of Engine 1. Omission of fuel to Engine1 (E1) has three possible causes, depending on the sequence of events:

1. If there is no fuel from Pump1 (O-Pump1), then Pump3 replaces it, as long as Pump2 has not failed first; this precondition can be represented using the POR gate. Thus in this situation, an omission of fuel can be caused by omission of fuel from both Pump1 and Pump3 (via Valve3).
2. If Pump2 fails first, then Pump3 replaces it and will be unavailable to replace Pump1 if it also fails. Thus sequential failure of Pump2 and then Pump1 will lead to an omission of fuel to Engine1 (represented using the PAND gate).
3. If both Pump2 and Pump1 fail at the same time (represented with the SAND gate), then Pump3 can only replace one of them. Behaviour in this situation is non-deterministic (as Pump3 may replace either Pump1 or Pump2, but not both), and thus as a pessimistic estimation, simultaneous failure of Pump1 and Pump2 is given as a cause of failure for both engines.

Following the process outlined in [52], the expanded fault tree expressions for the failure of Engine 1 can be derived as:

$$E1 = (P1 \vee P1 \wr P2 \wr CF \wr V1) \wr (P2 \vee P2 \wr P1 \wr CF \wr V2) \wedge (V3 \vee P3 \vee (V1 \lhd P1 \wr P2 \wr CF) \vee (V1 \& P1 \wr P2 \wr CF) \vee (S1 \lhd P1 \wr P2)$$

16

$\lor$ (CF◁P1≀P2) $\lor$ (S1&P1≀P2) $\lor$ (CF&P1≀P2) $\lor$ (V2◁P2≀P1≀CF) $\lor$ (V2&P2≀P1≀CF) $\lor$ (S2◁P2≀P1) $\lor$ (CF◁P2≀P1) $\lor$ (S2&P2≀P1) $\lor$ (CF&P2≀P1)) $\lor$ (P2∨P2≀P1≀CF≀V2) ◁ (P1∨P1≀P2≀CF≀V1) $\lor$ (P2∨P2≀P1≀CF≀V2) &(P1∨P1≀P2≀CF≀V1)

After minimising the above expressions using Pandora temporal laws, the resulting minimal cut sequences to cause the failure of Engine 1 are shown in Table 3.

Table 3: Minimal Cut Sequences to cause the failure of Engine 1

| Minimal Cut Sequence | Description |
|---|---|
| $(P1 \wr P2) \wedge P3$ | Failure of Pump 1 before Pump 2 (if Pump 2 fails at all) and Pump 3 |
| $(P1 \wr P2) \wedge V1$ | Failure of Pump 1 before Pump 2 (if Pump 2 fails at all) and Valve 1 |
| $(P1 \wr P2) \wedge V3$ | Failure of Pump 1 before Pump 2 (if Pump 2 fails at all) and Valve 3 |
| $(S1 \triangleleft P1) \wr P2$ | Failure of Flowmeter 1 before Pump 1, as long as Pump 2 has not failed yet |
| $(S1\&P1) \wr P2$ | Simultaneous failure of Flowmeter 1 and Pump 1, as long as Pump 2 has not failed yet |
| $(CF \triangleleft P1) \wr P2$ | Failure of Controller before Pump 1, as long as Pump 2 has not failed yet |
| $(CF\&P1) \wr P2$ | Simultaneous failure of Controller and Pump 1, as long as Pump 2 has not failed yet |
| $P2 \triangleleft P1$ | Failure of Pump 2 before Pump 1 |
| $P1\&P2$ | Simultaneous failure of both Pump 1 and Pump 2 |

As mentioned earlier, it is assumed that all events are independent and the probability of two independent events occurring at the same time is effectively 0, therefore MCSQs consisting of SAND gate will not be considered during the quantitative analysis. Thus for this example system, minimal cut sequences $(S1\&P1) \wr P2$ , $(CF\&P1) \wr P2$ and $P1\&P2$ are not considered further. Without these MCSQs the graphical representation of the temporal fault tree of the failure behaviour of Engine 1 is shown in Figure 6.

*4.2. Quantitative evaluation of the system reliability*

In this paper, to illustrate the idea of using fuzzy temporal fault tree analysis to evaluate system reliability, triangular fuzzy numbers are used to represent the failure possibility of basic events. The mission time of the system is considered to be 10000 hours. That means, at the end of the analysis, we will obtain the fuzzy possibility and overall probability of the system failure after 10000 hours. Due to the vagueness of the failure rate data of the basic events, experts' linguistic judgements are used to quantify the failure possibilities of the basic events. For this study, a group of six experts is constituted to provide their opinion regarding the failure possibility of the basic events and they are provided with different system related information, e.g. mission time and system architecture. The weighting score and weighting factor of the chosen experts are calculated by using Table 1 and shown in Table 4. Note that this scheme is used here for illustration purposes; other schemes are also possible and can be adjusted to account for opinions that carry higher weights because they are based on a stronger, more explicit and objective rationale if available. For example an expert may have consulted published reliability databases of similar components.

In order to obtain the experts' opinions about the failure possibilities of the basic events as linguistic terms, seven levels of qualitative linguistic terms, i.e., Very Low (VL), Low (L), Fairly Low (FL), Medium (M), Fairly High (FH), High (H), and Very High (VH) are defined (see Table 5). The conversion scale of the linguistic terms to the fuzzy numbers are obtained using the methodology shown in [24].
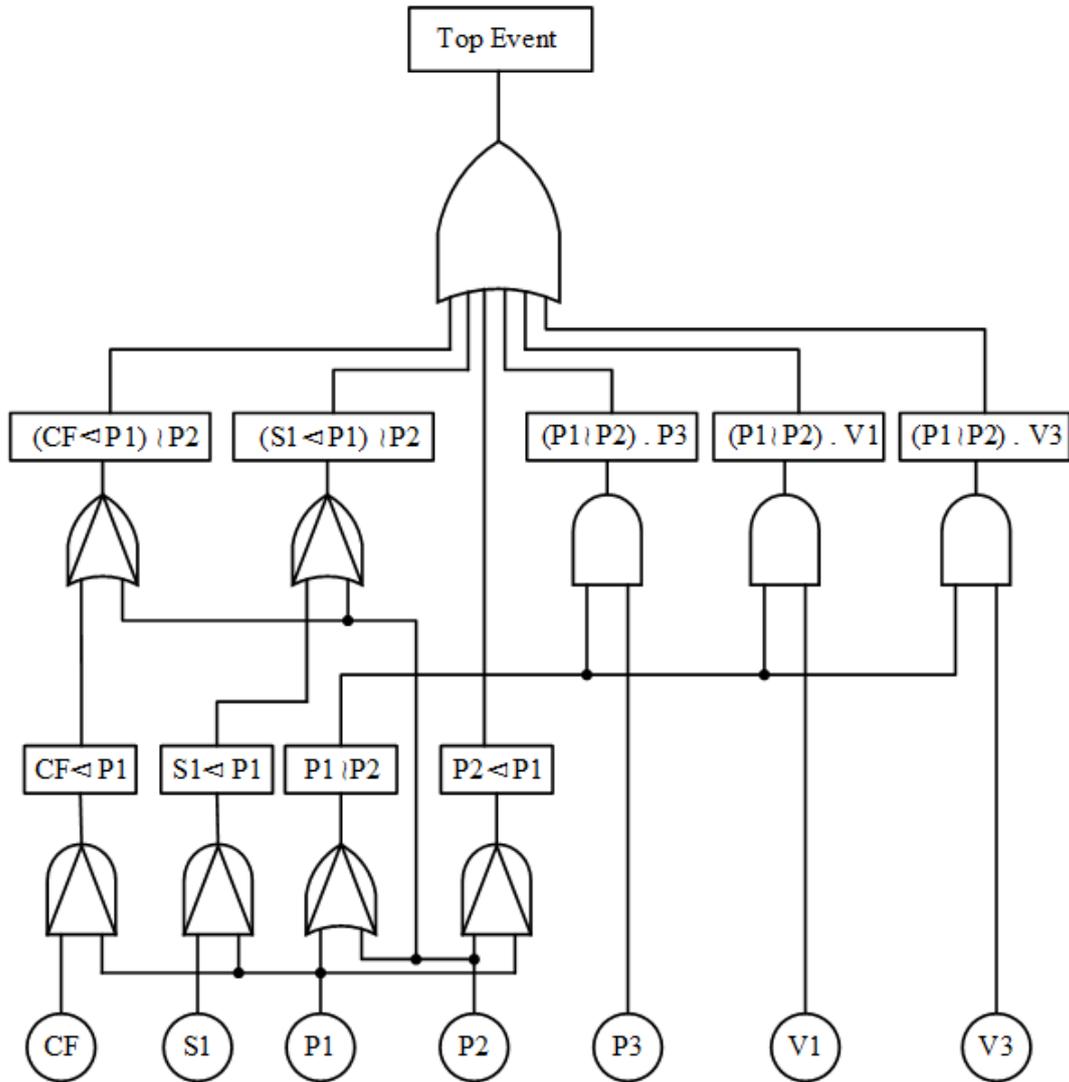
17

Figure 6: Temporal Fault Tree of failure behaviour of Engine 1

The opinions of the different experts regarding the failure possibility of the basic events are shown in Table 6. As the experts are different and have different backgrounds and experiences, their opinions can vary widely from one basic event to another. These variations are accounted for by the weighting process so there is no need to discount particular values. It is therefore necessary to aggregate the results to obtain an agreement among the conflicted views of the experts. Using the methodology shown in section 3.1.2, the experts' opinions are aggregated to obtain a single consensus about the failure possibility of basic events. These aggregated results are shown in Table 7.

Now, from the qualitative analysis, we have the minimal cut sequences that are necessary and sufficient to cause the system failure, i.e., no fuel to Engine 1 in this case. From the expert opinions we have the fuzzy failure possibilities of the basic events in the triangular fuzzy form. Therefore, we can quantify the minimal cut sequences using the values from Table 7 and the fuzzy operators defined in section 3.3. The results of quantification of the minimal cut sequences are shown in Table 8.

Using equation (24) and the fuzzy possibilities of the MCSQs from Table 8, the fuzzy possibility of the top event (no fuel to Engine 1) is obtained, which is also a triangular fuzzy number: (0.877, 0.952, 0.989).

18

Table 4: Weighting factors of six experts

| Expert | Professional position | Experience (years) | Educational qualification | Weighting score | Weighting factor |
|--------|----------------------|--------------------|--------------------------|-----------------|------------------|
| E1 | Professor | $\geq 20$ | PhD | 15 | 0.241935 |
| E2 | Asst. Professor | $10\ to\ 14$ | PhD | 12 | 0.193548 |
| E3 | Engineer | $5\ to\ 9$ | M.Tech | 10 | 0.161290 |
| E4 | Manager | $15\ to\ 19$ | MSc | 12 | 0.193548 |
| E5 | Operator | $< 5$ | Diploma | 5 | 0.080645 |
| E6 | Technician | $5\ to\ 9$ | B.Tech | 8 | 0.129032 |

Table 5: Linguistic variables with conversion scales

| Linguistic Variables | Triangular fuzzy numbers | | |
|----------------------|------|------|------|
| | A | B | C |
| Very Low (VL) | 0 | 0.04 | 0.08 |
| Low (L) | 0.07 | 0.13 | 0.19 |
| Fairly Low (FL) | 0.17 | 0.27 | 0.37 |
| Medium (M) | 0.35 | 0.50 | 0.65 |
| Fairly High (FH) | 0.62 | 0.73 | 0.82 |
| High (H) | 0.81 | 0.87 | 0.93 |
| Very High(VH) | 0.92 | 0.96 | 1.0 |

Table 6: Expert Opinions on the Basic events

| Basic Events | Experts Opinion | | | | | |
|--------------|------|------|------|------|------|------|
| | E1 | E2 | E3 | E4 | E5 | E6 |
| P1 | H | FH | H | M | H | M |
| P2 | H | FH | H | M | H | M |
| P3 | H | H | VH | H | VH | H |
| V1 | FH | M | FH | H | VH | M |
| V3 | M | FH | H | FL | H | M |
| S1 | FH | M | H | H | M | FH |
| CF | FL | FH | FL | FH | M | L |

This fuzzy possibility of the top event can be mapped to a crisp value using the equation (21), and the value calculated by equation (21) is 0.939. So, 0.939 represents the most likely possibility of the system failure after 10000 hours. This value belongs to the set Very High (VH) with 47.5% membership, which

19

Table 7: Aggregation of expert opinion in triangular fuzzy form for the basic events

| Basic Events | Triangular Fuzzy Number | | |
|---|---|---|---|
| | A | B | C |
| P1 | 0.660 | 0.750 | 0.839 |
| P2 | 0.660 | 0.750 | 0.839 |
| P3 | 0.831 | 0.887 | 0.943 |
| V1 | 0.540 | 0.659 | 0.768 |
| V3 | 0.529 | 0.637 | 0.743 |
| S1 | 0.603 | 0.708 | 0.806 |
| CF | 0.369 | 0.473 | 0.568 |

Table 8: Fuzzy possibilities of the MCSQs for omission of fuel to engine 1

| Set | Minimal Cut Sequences (MCSQs) | | | | | |
|---|---|---|---|---|---|---|
| | $(P1 \wr P2) \wedge P3$ | $(P1 \wr P2) \wedge V1$ | $(P1 \wr P2) \wedge V3$ | $(S1 \lhd P1) \wr P2$ | $(CF \lhd P1) \wr P2$ | $P2 \lhd P1$ |
| A | 0.548 | 0.356 | 0.349 | 0.146 | 0.094 | 0.161 |
| B | 0.663 | 0.493 | 0.476 | 0.205 | 0.134 | 0.222 |
| C | 0.788 | 0.642 | 0.621 | 0.296 | 0.189 | 0.321 |

provides a good insight about the reliability of the system. To be able to compare this value with the values produced by other probability based TFT quantification approaches, we need to convert this value into a probability value. The value is converted to a probability value using the equation (22), and the value obtained is 0.119. So the probability of the system failure after 10000 hours is estimated to be 0.119.

For comparison purposes, these results can be contrasted against the results from various established approaches that make use of statistical failure data. The TFT of the same case study is evaluated based on fixed failure rates of components using an analytical approach [7], a Bayesian Network (BN) based method [8] and a Petri Net (PN) based method [53], all considering mission time as 10000 hours. The crisp failure rate values used by the above mentioned approaches are shown in Table 9 [7] and the system unreliability values estimated by the approaches are shown in Table 10. As the analytical and the Petri Net approaches both model time as continuous, these approaches produced a single value. On the other hand, the Bayesian Network based approach divides the time into $n$ equal intervals and therefore the table shows system unreliability values for different numbers of intervals. The value of $n$ must be at least equal to the maximum order of the minimal cut sequences. The order of a minimal cut sequence (MCSQ) is the number of basic events contribute to that MCSQ. The Difference column of Table 10 shows with what percentage the value estimated by the proposed fuzzy approach deviates from the values estimated by the other approaches.

Although there are some small differences between the value estimated by the proposed fuzzy method and the values estimated by other probability based methods, the important thing to note that the fuzzy temporal fault tree analysis enables the analysts to perform reliability analysis of dynamic systems in the presence of uncertain failure rate data of system components while still yielding a reasonably useful result.

In particular, one important aspect of quantitative reliability analysis of system designs is to identify the critical components so that the designers can decide where to focus their efforts on those parts of the system that require most improvement to satisfy the requirements, e.g., by applying fault tolerance strategies. The

20

Table 9: Fixed failure rate values used in Analytical, BN based and PN based approaches

| Basic Events | Failure rate/hour($\lambda$) |
|---|---|
| P1 | 3.2 E-5 |
| P2 | 3.2 E-5 |
| P3 | 3.2 E-5 |
| V1 | 1.0 E-5 |
| V3 | 6.0 E-6 |
| S1 | 2.5 E-6 |
| CF | 5.0 E-7 |

Table 10: Comparison of system unreliability estimated by other approaches with the unreliability estimated by the proposed approach

| Approaches | Unreliability | | Unreliability estimated by the proposed approach | Difference |
|---|---|---|---|---|
| Analytical | 0.135 | | | 11.85% lower |
| Petri Net Based | 0.117 | | | 1.71% higher |
| Bayesian Network Based | with 3 intervals | 0.111 | | 7.21% higher |
| | with 4 intervals | 0.116 | | 2.59% higher |
| | with 5 intervals | 0.119 | 0.119 | same |
| | with 6 intervals | 0.121 | | 1.65% lower |
| | with 7 intervals | 0.122 | | 2.46% lower |
| | with 8 intervals | 0.123 | | 3.25% lower |
| | with 9 intervals | 0.124 | | 4.03% lower |
| | with 10 intervals | 0.124 | | 4.03% lower |

fuzzy importance measures of the fuel system components are calculated according to the method shown in section 3.4.

The components are ranked according to their contribution to the occurrence of the top event (system failure) and the results are shown in Table 11. As seen in the table, for the condition no fuel to Engine 1, the most critical component is Pump 1 (P1) and the least critical component is the Pump 2 (P2). Next most important are the Pump 3 (P3) and Valve 1 (V1).

## 5. Conclusion

Although FTA is a highly successful and widely-used technique for dependability analysis, it does have a number of shortcomings, such as an inability to capture sequential failure behaviour. Extensions have been proposed to address some of these issues, such as DFTs and Pandora, and thereby allowing qualitative and/or quantitative analysis of sequential failure logic in fault trees.

21

Table 11: Fuzzy importance ranking for the basic events

| Basic Events (E) | FIM (E) | Rank |
|:---:|:---:|:---:|
| P1 | 1.722 | 1 |
| P3 | 0.213 | 2 |
| V1 | 0.147 | 3 |
| V3 | 0.145 | 4 |
| S1 | 0.103 | 5 |
| CF | 0.097 | 6 |
| P2 | 0.018 | 7 |

In this paper, we presented a method to combine expert elicitation and fuzzy set theory with temporal fault tree analysis using Pandora to enable reliability evaluation of dynamic systems with uncertain failure probability data. Use of fuzzy set theory and elicitation of expert judgement, which is often provided in natural language, can more explicitly highlight areas of uncertainty in the data. The effectiveness of the proposed method has been evaluated by applying it to a case study and by comparing the results with the results estimated by other existing temporal fault tree quantification methods. The results show that the proposed fuzzy temporal fault tree analysis offers a useful way of evaluating the reliability of dynamic systems when statistical quantitative failure data are unavailable or insufficient.

It is important to emphasise that the results can only be as reliable as the input data, and the inclusion of fuzzy data cannot create accuracy where none previously existed. However our approach of channelling expert judgement and capturing it into a formal approach that uses fuzzy sets will yield at least some estimate of reliability in situations where when failure distribution data are unavailable and therefore any estimation using classical techniques is impossible. Techniques such as importance measures also allow analysts to see the relative contribution of different system elements to the overall failure without relying on an accurate estimation of the system failure probability. In this way, the fuzzy approach enables us to draw helpful conclusions about the failure behaviour of the system even in the absence of concrete failure data, supporting an iterative design process by guiding the focus of future development on the most critical areas of the system architecture.

As a further development to Pandora, the work described in this paper contributes to one of a few techniques that define the state-of-the-art in the area of dynamic fault tree analysis. Furthermore Pandora is part of an innovative and mature body of work on model-based safety analysis which has resulted to commercial tools for analysis and optimisations of systems including the HiP-HOPS [54] and Safety Designer [55] tools. In that sense, the work has the potential to contribute to the industrial state-of-practice in this area.

Although the proposed approach can address the problem of unavailability of failure data, its application presently contains an assumption of exponentially distributed failure probability for components. Therefore, in future, it is worth trying to explore alternative options to allow assumption of other failure distributions in the quantification process. One potential option is to extend this work by defining the fuzzy operators for non-exponentially distributed data by modifying the operators defined in this paper. Another option would be to incorporate uncertainty aspect of failure data in the Bayesian Network based approach which is capable of performing system analysis with both exponentially and non-exponentially distributed data. In future, we hope to extend this work by looking at how the system unreliability estimated by the proposed approach be affected by the different choices of membership functions, weighting scores, expert opinions, etc.

22

# References

[1] W. Vesely, J. Dugan, J. Fragola, J. Minarick, J. Railsback, Fault Tree Handbook with Aerospace Applications, Tech. rep., NASA office of safety and mission assurance, Washington, DC (2002).

[2] J. B. Dugan, S. J. Bavuso, M. A. Boyd, Fault Trees and Sequence Dependencies, in: Proceedings of Annual Reliability and Maintainability Symposium, 1990, pp. 286–293. doi:10.1109/ARMS.1990.67971.

[3] M. Walker, Y. Papadopoulos, Qualitative temporal analysis: Towards a full implementation of the Fault Tree Handbook, Control Engineering Practice 17 (10) (2009) 1115–1125.

[4] J. B. Dugan, S. J. Bavuso, M. A. Boyd, Dynamic fault-tree models for fault-tolerant computer systems, IEEE Transactions on Reliability 41 (3) (1992) 363–377. doi:10.1109/24.159800.

[5] M. Walker, Pandora: A Logic for the Qualitative Analysis of Temporal Fault Trees, Ph.D. thesis, University of Hull (2009).

[6] D. Chen, N. Mahmud, M. Walker, L. Feng, H. Lönn, Y. Papadopoulos, Systems modeling with EAST-ADL for fault tree analysis through HiP-HOPS, IFAC Proceedings Volumes 46 (22) (2013) 91 – 96. doi:10.3182/20130904-3-UK-4041.00043.

[7] E. Edifor, M. Walker, N. Gordon, Quantification of Priority-OR Gates in Temporal Fault Trees, in: F. Ortmeier, P. Daniel (Eds.), Computer Safety, Reliability, and Security SE - 9, Vol. 7612 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2012, pp. 99–110.

[8] S. Kabir, M. Walker, Y. Papadopoulos, Reliability Analysis of Dynamic Systems by Translating Temporal Fault Trees into Bayesian Networks, in: F. Ortmeier, A. Rauzy (Eds.), Model-Based Safety and Assessment, Vol. 8822 of Lecture Notes in Computer Science, Springer International Publishing, Cham, 2014, pp. 96–109. doi:10.1007/978-3-319-12214-4.

[9] Y. A. Mahmood, A. Ahmadi, A. K. Verma, A. Srividya, U. Kumar, Fuzzy fault tree analysis : a review of concept and application, International Journal of System Assurance Engineering and Management 4 (1) (2013) 19–32. doi:10.1007/s13198-013-0145-x.

[10] H. Tanaka, L. T. Fan, F. S. Lai, K. Toguchi, Fault-Tree Analysis by Fuzzy Probability, IEEE Transactions on Reliability R-32 (5) (1983) 453–457.

[11] L. Zadeh, Fuzzy Sets, Information and Control 8 (3) (1965) 338–353.

[12] K. B. Misra, G. G. Weber, Use of fuzzy set theory for level-I studies in probabilistic risk assessment, Fuzzy Sets and Systems 37 (2) (1990) 139–160. doi:10.1016/0165-0114(90)90038-8.

[13] P. Suresh, A. Babar, V. Raj, Uncertainty in fault tree analysis : A fuzzy approach, Fuzzy Sets and Systems 83 (2) (1996) 135–141.

[14] G.-S. Liang, M.-J. J. Wang, Fuzzy fault-tree analysis using failure possibility, Microelectronics Reliability 33 (4) (1993) 583–597.

[15] P. Gmytrasiewicz, J. A. Hassberger, J. C. Lee, Fault tree based diagnostics using fuzzy logic, IEEE Transactions on Pattern Analysis and Machine Intelligence 12 (11) (1990) 1115–1119.

[16] D. Singer, A fuzzy set approach to fault tree and reliability analysis, Fuzzy Sets and Systems 34 (2) (1990) 145–155.

[17] C.-T. Lin, M.-J. J. Wang, Hybrid fault tree analysis using fuzzy sets, Reliability Engineering and System Safety 58 (1997) (1997) 205–213.

[18] P. W. H. Chung, M. Jefferson, A Fuzzy Approach to Accessing Accident Databases, Applied Intelligence 9 (2) (1998) 129–137. doi:10.1023/A:1008263918762.

[19] D. Yuhua, Y. Datao, Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis, Journal of Loss Prevention in the Process Industries 18 (2) (2005) 83–88.

[20] M.-H. Shu, C.-H. Cheng, J.-R. Chang, Using intuitionistic fuzzy sets for fault-tree analysis on printed circuit board assembly, Microelectronics Reliability 46 (12) (2006) 2139–2148. doi:10.1016/j.microrel.2006.01.007.

[21] R. Ferdous, F. Khan, B. Veitch, P. R. Amyotte, Methodology for computer aided fuzzy fault tree analysis, Process Safety and Environmental Protection 87 (4) (2009) 217–226.

[22] S. K. Tyagi, D. Pandey, V. Kumar, Fuzzy Fault Tree Analysis for Fault Diagnosis of Cannula Fault in Power Transformer, Applied Mathematics 2 (11) (2011) 1346–1355.

[23] D. Wang, P. Zhang, L. Chen, Fuzzy fault tree analysis for fire and explosion of crude oil tanks, Journal of Loss Prevention in the Process Industries 26 (6) (2013) 1390 – 1398. doi:http://dx.doi.org/10.1016/j.jlp.2013.08.022.

[24] S. Rajakarunakaran, A. M. Kumar, V. A. Prabhu, Applications of fuzzy faulty tree analysis and expert elicitation for evaluation of risks in LPG refuelling station, Journal of Loss Prevention in the Process Industries 33 (2015) 109–123. doi:10.1016/j.jlp.2014.11.016.

[25] A. Verma, A. Srividya, S. Prabhudeva, G. Vinod, Reliability analysis of Dynamic fault tree models using fuzzy sets, Communications in Dependability and Quality Management 9 (4) (2006) 68–78.

[26] L. Yang, Analysis on Dynamic Fault Tree Based on Fuzzy Set, Applied Mechanics and Materials 110-116 (2011) 2416–2420.

[27] Y. F. Li, H. Z. Huang, Y. Liu, N. Xiao, H. Li, A new fault tree analysis method : fuzzy dynamic fault tree analysis, Eksploatacja i Niezawodnosc-Maintenance and Reliability 14 (3) (2012) 208–214.

[28] Y. F. Li, J. Mi, Y. Liu, Y. J. Yang, H. Z. Huang, Dynamic fault tree analysis based on continuous-time Bayesian networks under fuzzy numbers, Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability (2015) 1–12doi:10.1177/1748006X15588446.

[29] S. Kabir, E. Edifor, M. Walker, N. Gordon, Quantification of Temporal Fault Trees Based on Fuzzy Set Theory, in: Proceedings of the Ninth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, Springer International Publishing, Brunów, 2014, pp. 255–264. doi:10.1007/978-3-319-07013-1_24.

[30] H. Boudali, P. Crouzen, M. Stoelinga, Dynamic Fault Tree analysis using Input / Output Interactive Markov Chains,

in: Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, IEEE Computer Society, Washington DC, 2007, pp. 708–717.

[31] H. Boudali, P. Crouzen, M. Stoelinga, A Rigorous, Compositional, and Extensible Framework for Dynamic Fault Tree Analysis, IEEE Transactions on Dependable and Secure Computing 7 (2) (2010) 128–143.

[32] G. Merle, J.-M. Roussel, J.-J. Lesage, Algebraic determination of the structure function of Dynamic Fault Trees, Reliability Engineering & System Safety 96 (2) (2011) 267–277.

[33] G. Merle, J.-M. Roussel, J.-J. Lesage, A. Bobbio, Probabilistic Algebraic Analysis of Fault Trees With Priority Dynamic Gates and Repeated Events, IEEE Transactions on Reliability 59 (1) (2010) 250–261.

[34] G. Merle, J.-M. Roussel, J.-J. Lesage, Quantitative Analysis of Dynamic Fault Trees Based on the Structure Function, Quality and Reliability Engineering International 30 (1) (2014) 143–156.

[35] D. Codetta-Raiteri, The Conversion of Dynamic Fault Trees to Stochastic Petri Nets, as a case of Graph Transformation, Electronic Notes in Theoretical Computer Science 127 (2) (2005) 45–60.

[36] X. Zhang, Q. Miao, X. Fan, D. Wang, Dynamic fault tree analysis based on Petri nets, in: 8th International Conference on Reliability, Maintainability and Safety(ICRMS), IEEE, Chengdu, 2009, pp. 138–142.

[37] H. Boudali, J. B. Dugan, A Continuous-Time Bayesian Network Reliability Modeling, and Analysis Framework, IEEE Transaction on Reliability 55 (1) (2006) 86–97.

[38] D. Marquez, M. Neil, N. Fenton, Solving Dynamic Fault Trees using a New Hybrid Bayesian Network Inference Algorithm, in: 16th Mediterranean Conference on Control and Automation, IEEE, 2008, pp. 609–614.

[39] S. Montani, L. Portinale, A. Bobbio, D. Codetta-Raiteri, Radyban: A tool for reliability analysis of dynamic fault trees through conversion into dynamic Bayesian networks, Reliability Engineering & System Safety 93 (7) (2008) 922–932.

[40] J. Fussell, E. Aber, R. Rahl, On the Quantitative Analysis of Priority-AND Failure Logic, IEEE Transactions on Reliability R-25 (5) (1976) 324–326.

[41] A. Bobbio, L. Portinale, M. Minichino, E. Ciancamerla, Improving the analysis of dependable systems by mapping fault trees into Bayesian networks, Reliability Engineering & System Safety 71 (3) (2001) 249–260. doi:10.1016/S0951-8320(00)00077-6.

[42] E. J. Henley, H. Kumamoto, Reliability engineering and risk assessment, Vol. 193, Prentice-Hall Englewood Cliffs (NJ), 1981.

[43] J. D. Esary, F. Proschan, Coherent Structures of Non-Identical Components, Technometrics 5 (2) (1963) 191–209.

[44] T. J. Ross, Properties of membership functions, fuzzification, and defuzzification, in: Fuzzy Logic with Engineering Applications, John Wiley & Sons, Ltd, 2004, pp. 89–116. doi:10.1002/9781119994374.ch4.

[45] T. J. Ross, Development of membership functions, in: Fuzzy Logic with Engineering Applications, John Wiley & Sons, Ltd, 2004, pp. 174–210. doi:10.1002/9781119994374.ch6.

[46] H.-M. Hsu, C.-T. Chen, Aggregation of fuzzy opinions under group decision making, Fuzzy Sets and Systems 79 (3) (1996) 279 – 285. doi:http://dx.doi.org/10.1016/0165-0114(95)00185-9.

[47] R. Zwick, E. Carlstein, D. V. Budescu, Measures of similarity among fuzzy concepts: A comparative analysis, International Journal of Approximate Reasoning 1 (2) (1987) 221 – 242. doi:http://dx.doi.org/10.1016/0888-613X(87)90015-6.

[48] L. X. Wang, A course in fuzzy system and control, Prentice-Hall PTR, 1997.

[49] T. Onisawa, An approach to human reliability in man-machine systems using error possibility, Fuzzy Sets and Systems 27 (2) (1988) 87–103.

[50] A. C. F. Guimarees, N. F. F. Ebecken, FuzzyFTA : a fuzzy fault tree system for uncertainty analysis, Annals of Nuclear Energy 26 (1999) 523–532.

[51] M. M. Deza, E. Deza, Encyclopedia of distances, Springer, 2009.

[52] M. Walker, L. Bottaci, Y. Papadopoulos, Compositional Temporal Fault Tree Analysis, in: Proceedings of the 26th International Conference on Computer Safety, Reliability and Security (SAFECOMP'07), 2007, pp. 106–119.

[53] S. Kabir, M. Walker, Y. Papadopoulos, Quantitative evaluation of pandora temporal fault trees via petri nets, IFAC-PapersOnLine 48 (21) (2015) 458–463. doi:10.1016/j.ifacol.2015.09.569.

[54] Y. Papadopoulos, M. Walker, D. Parker, S. Sharvia, L. Bottaci, S. Kabir, L. Azevedo, I. Sorokos, A synthesis of logic and bio-inspired techniques in the design of dependable systems, Annual Reviews in Control (2016) 1–13doi:10.1016/j.arcontrol.2016.04.008.
URL http://linkinghub.elsevier.com/retrieve/pii/S1367578816300116

[55] I. GmbH, SimulationX SafetyDesigner (2012).
URL https://www.simulationx.com/simulation-software/beginners/safety-designer.html