ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 10, April 2015

Human Factors Reliability Analysis Using Fuzzy Fault Tree

Hany Sallam, Ehab Shafei, E. A. Eisawy
Operation Safety & Human Factors Department, Egyptian Nuclear & Radiological Regulatory Authority

Abstract*— In order to ensure effective prevention of harmful events, the risk assessment process cannot ignore the role of humans in the dynamics of accidental events and thus the seriousness of the consequences that may derive from them. Human reliability analysis (HRA) involves the use of qualitative and quantitative methods to assess the human contribution to risk. HRA techniques have been developed in order to provide human error probability values associated with operators' tasks to be included within the broader context of system risk assessment, and are aimed at reducing the probability of accidental events. Fault tree analysis (FTA) is a graphical model that displays the various combinations of equipment failures and human errors that can result in the main system failure of interest. FTA is a risk analysis technique to assess likelihood (in a probabilistic context) of an event. The objective data available to estimate the likelihood is often missing, and even if available, is subject to incompleteness and imprecision or vagueness. Without addressing incompleteness and imprecision in the available data, FTA and subsequent risk analysis give a false impression of precision and correctness that undermines the overall credibility of the process. To solve this problem, qualitative justification in the context of failure possibilities can be used as alternative for quantitative justification. In this paper, we introduce the approach of fuzzy reliability as solution for fault tree analysis drawbacks. A new fuzzy fault tree method is proposed for the analysis of human reliability based on fuzzy sets and fuzzy operations t-norms, co-norms, defuuzzification, and fuzzy failure probability.

Index Terms— **Human Reliability, Fault Tree, Fuzzy Logic.**

I. INTRODUCTION

In the 1960s, once the impact of human performance on overall system risk had been appreciated, there was a drive to integrate human factors considerations into reliability assessments. These early attempts treated people like any other component in a reliability assessment (e.g., what is the probability of an operator failing to respond to an alarm?). This led to an increased interest in not just the probability of a failure (e.g. an operator failing to close a valve) but also the reasons for its occurrence. Human factors can be defined as "a discipline concerned with designing machines, operations, and work environments so that they match human capabilities, limitations, and needs" [1]. It also can be considered as an environmental, organizational and job factors and human and individual characteristics which influence behavior at work in a way which can affect health and safety [2]. Human factors play a large part in many failures in the critical systems and are recognized as being a contributor to accidents. The accident of Three Miles Island (TMI), which happened in1979 pointed out both the need to better understanding of human factors and improving training and procedures. Today, in spite of the huge amount of work devoted to human factors, an agreed classification of human errors is still missing, and there is an opinion that plant operational procedures should reflect more insights gained by the study of human factors. In order to improve the nuclear safety, human reliability and risk assessment is integrated to identify three major points [3]:

a) Human error (identifying errors that can occur)
b) Human error quantification (identifying how likely the errors are)
c) Human error reduction (identifying the countermeasures that should be taken to improve human reliability).

HRA could be seen as an in-depth assessment of risk, as a function of human performance, whereby a system's vulnerabilities to human failure can be identified, and defenses improved accordingly [4] [5].

Fault tree is a widely used method to perform reliability analysis of engineering systems in industry, particularly in the area of nuclear power generation. The method was developed in the early 1960s to perform safety analysis of the Minuteman Launch Control System at the Bell Telephone Laboratories [6]. A fault tree may simply be described as a logical representation of the relationship of primary fault events that may cause the occurrence of a specified undesirable event, called the ''Top Event''. It is depicted using a tree structure with logic gates such as AND and OR. Conventional FTA, which is based on probability theory and Boolean algebra, is consistent with conventional reliability theory, which is based on the probability and binary-state assumptions. Just like any other reliability analysis approach, the FTA method too has its advantages and disadvantages. Thus, some of the advantages of the FTA method are as follows [7]:

a) It provides insight into the system behavior and can handle complex systems more easily than any other method.
b) It serves as a graphic aid for system management and provides options for management and others to perform either quantitative or qualitative reliability analysis.
c) It highlights failures deductively.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 10, April 2015

d) It allows concentration on one specific failure at a time and requires the involved analyst to comprehend thoroughly the system under consideration before starting the FTA process.

On the other hand, it does not work well when necessary statistical data is scarce, there is a lack of knowledge (vagueness), or reducible (or epistemic) uncertainty needs to be taken into account. Common reasons for lack of statistical data include the following:

a) The increased complexity of large-scale systems;
b) The collection of statistical data being difficult and/or costly;
c) The rarity of failures in some highly reliable systems; and
d) Data being imprecise or unavailable under various testing conditions.

Moreover, the experience and subjective assessment of experts is often given in natural language, which introduces vagueness and impreciseness. The conventional FTA approach is to some extent unnatural because it relies on conventional reliability theory. Furthermore, in investigation of complex man-made systems and multi-state systems, inaccuracy caused by human errors or poor definitions of failure should also be considered. Also, If a fault tree is developed by different safety professionals, it will be of different nature depending on the developer. This makes the fault tree a non-generic or inexact in nature. For all these defects in fault tree, fuzzy logic is a good candidate solution to complement and enhance fault tree.

II. HUMAN RELIABILITY ANALYSIS

The birth of HRA methods dates from the year 1960, but most techniques for assessment of the human factor, in terms of propensity to fail, have been developed since the mid-'80s. Human reliability is defined as the probability of successful performance of only those human activities necessary to make a system reliable or available [5]. Human error is simply some human output that is outside the tolerances established by the system requirements in which the person operates. Human actions are a source of vulnerability for industrial systems, giving rise to HRA that aims to deepen the examination of the human factor in the workplace. HRA is concerned with identifying, modelling, and quantifying the probability of human errors. Human reliability and error data are the backbone of any human reliability-related prediction. Human reliability methodologists to obtain human reliability-related data frequently use the expert judgment approach [3]. This approach characterized by its low cost and simplicity where a large amount of data can be collected from a small number of expert respondents. The two main drawbacks of this approach are frequent use of less experienced experts than required and less reliable than data collected through other means or approaches. On the other hand, the data collected from experimental studies is normally generated under the laboratory conditions. These conditions may not be the actual representative of the real life conditions. Furthermore, the approach is expensive and time-consuming [4]. Nonetheless, the main advantage of data collected through the experimental studies approach is that the data are probably the least influenced by the subjective elements that may induce some error.

A. Human Error Categorization

Human errors (unsafe acts) are divided into two categories - errors and violations - and these two categories are then divided into subcategories as shown in Fig. 1. Errors are unintentional behaviors, while violations are a willful disregard of the rules and regulations [1].

1- Errors

a) Skill-Based Errors: Errors which occur in the operator's execution of a routine, highly practiced task relating to procedure, training or proficiency and result in an unsafe situation (e.g., fail to prioritize attention, checklist error, negative habit).
b) Decision Errors: Errors, which occur when the behaviors or actions of the operators proceed as intended yet the chosen plan proves inadequate to achieve the desired end-state and results in an unsafe situation (e.g., exceeded ability, rule-based error, and inappropriate procedure).
c) Perceptual Errors: Errors which occur when an operator's sensory input is degraded and a decision is made based upon faulty information.

2- Violations

a) Routine Violations: Violations which are a habitual action on the part of the operator and are tolerated by the governing authority.
b) Exceptional Violations: Violations which are an isolated departure from authority, neither typical of the individual nor condoned by management.

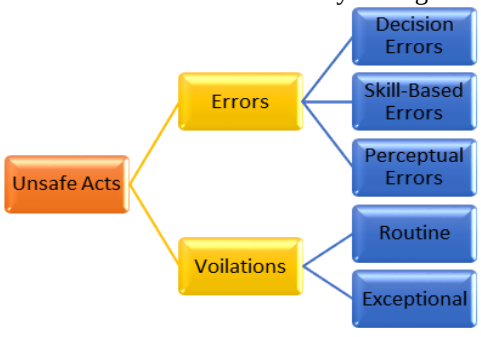

Fig. 1, Human Error Categorization

There are many major factors for the occurrence of human errors/accidents in the industrial sector including power generation. Eleven of these major factors along with their corresponding preventive measures with respect to an individual (in parentheses) are as follows [5]:

1. Performing tasks too fast (Avoid operating equipment when you are tense, tired, or do not feel well).

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 10, April 2015

2. Taking chances and high risks (Avoid ‘‘showing off’’ or thinking that an accident cannot occur).
3. Faulty equipment (Check equipment on regular basis).
4. Sleeplessness and fatigue (Take breaks as considered appropriate to prevent fatigue).
5. Extreme cold or heat (Perform inside tasks/jobs or minimize exposure to extreme temperatures as much as possible).
6. Poor skill (Read instruction manuals with care and get some skilled individual in the area to help you).
7. Medication, drugs, and alcohol (Avoid operating equipment/machines or performing dangerous tasks if you are on some form of drugs, taking medication, or have been drinking).
8. Panic in an emergency situation (Learn first aid so you know exactly what action to take).
9. Let-down from low blood sugar and hunger (Take fructose tablets or eat appropriate snacks to fight let-down).
10. Emotional upsets and anger (Take time to calm down to normal level).
11. Daydreaming and not concentrating (Vary routine to fight monotony as appropriate).

III. FAULT TREE

FTA is a failure analysis technique used for modeling and analyzing failure paths in a system. It's a deductive approach for PSA to assess how likely undesirable events to occur or what their probabilities are [9, 10,11]. It is based on top level events that can occur in the system, and attempting to trace them to root causes as shown in Fig 2. FTA expresses which combination of failures contribute to certain hazard or accident. FTA presented by symbols in a tree structure. The symbols are represented by three major blocks: events, Boolean logic gates, and transfer symbols. Boolean algebra mathematically calculates the probability of the undesired event to occur.

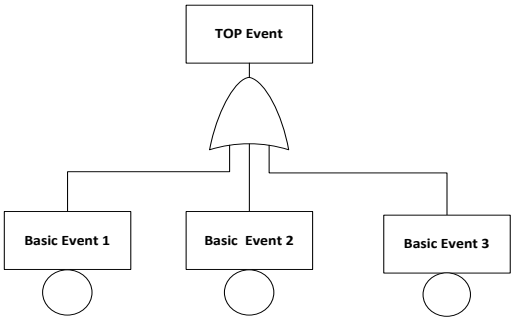

Fig. 2 Simple Fault Tree

Fault tree Mathematical model

FTA is the most commonly used technique used for causal analysis in risk reliability studies. A fault tree can be modelled by a set of AND gates and OR gates connecting between basic events and intermediate events , as shown in Fig. 3 and 4 respectively where [9]:

AND gate with m basic event is given by:

$$Q_0(t) = \prod_{j=1}^{m} q_j(t) \quad (1)$$

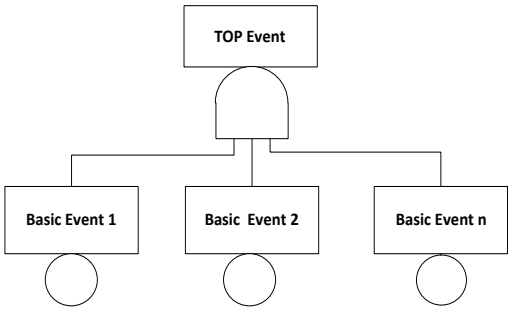

Fig. 3, AND gate connecting *m* basic events

And OR gate with m basic events is given by [9]:

$$Q_0(t) = 1 - \prod_{j=1}^{m} \left(1 - q_j(t)\right) \quad (2)$$

$$\overset{\vee}{Q}(t) = \prod_{j=1}^{r} q_{j,i}(t) \quad (3)$$

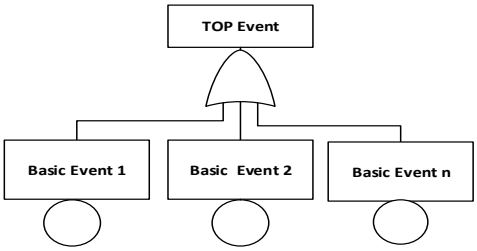

Fig. 4, OR gate connecting *m* basic events

IV. FUZZY FAULT TREE

By considering, the disadvantages of fault tree especially the need for failure data of all the events in the fault tree that are usually not known or not accurately known that decreases the credibility of the analysis. This point represents the main obstacle in risk assessment using FTA where the unavailability of reliability data that makes the procedure time consuming and error-prone. Fuzzy logic and fuzzy sets emerging as the best solution for such situation [8]. Fuzzy logic might be the most effective way when a very little quantitative information is available regarding the probabilities. It deals with imprecise scenarios like ‘less/more’, ‘high/low’, ‘hot/cold’ etc. rather than crisp or quantified values. Fuzzy set, in this paper, will be used to convert this imprecise estimation of experts to a quantified number [9]. The biggest advantage gained from fuzzy logic is that it works on possibilistic terms and converts them into probabilistic values. In contrast to other approaches, fuzzy logic is a simplified platform that is successful when less information is present and reduced developmental time is required to generate the output.

The combination of FTA with fuzzy logic will help in artificially generating the unavailable data. Our proposed

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 10, April 2015

method for integrating FTA and fuzzy logic is shown in Fig 5, it proceeds in the following steps:

1- Covert imprecise estimation of experts into fuzzy numbers represented in the form of linguistic values such as (low, medium, high) instead of probabilities values of basic events, (basic event fuzzification).
2- Replacing logical AND, OR operations by fuzzy operator *t-norms*, and *t-conorms* respectively.
3- Aggregate fuzzy values of the basic events up to the top event.
4- Use a defuzzification method to the top event fuzzy value to get crisp value of the top event. Which represent fuzzy possibility score FPS of the top event.
5- Convert fuzzy possibility score intro fuzzy failure probability of the top event.

Therefore, this proposed methodology uses expert's elicitation and converts it into crisp failure data using Fuzzy Logic approach.

By doing that, the conventional fault tree becomes a fuzzy fault tree. The calculation of the top event probability could be proceeded by applying fuzzy operation on fuzzy sets at every node. More details on the fuzzy operations are given in the following subsection.

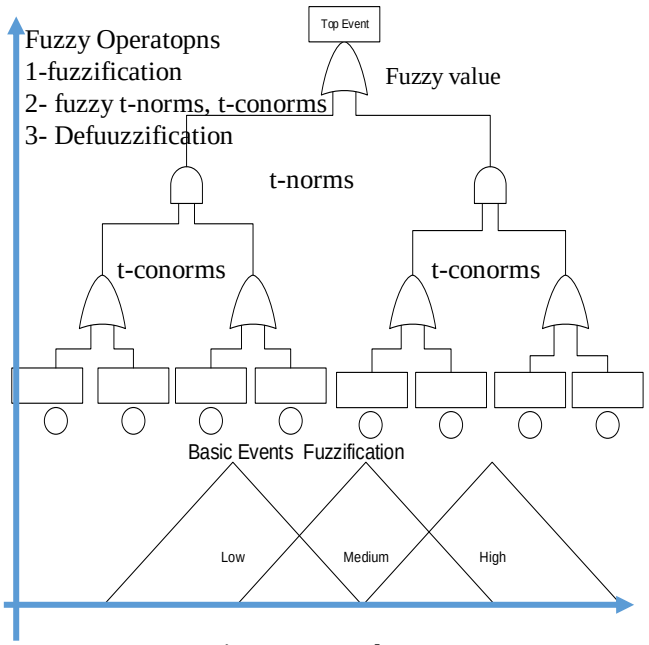

Fig.5 Fuzzy Fault Tree

A. Fuzzy Sets Operations

The fuzzification is the process of transforming crisp values into grades of membership for linguistic terms of fuzzy sets. The membership function is used to associate a grade to each linguistic term. For each input and output variable, two or more membership functions (MF) are defined, normally three but can be more. A qualitative category for each one of them is defined, for example: low, normal or high. The shape of these functions can be diverse but we will usually work with triangles as shown in Fig.5.

Fuzzy numbers aggregation techniques are used to aggregate the basic events justification into one justification to calculate component failure probabilities. The min-max reasoning method is used [12, 13]. This method is based on t-norms and co-conorms (see Fig. 6), which are defined as follows:

a) **t-norms, fuzzy intersection (fuzzy AND)**

Let A and B be two fuzzy sets defined in fuzzy space X, the intersection of A and B is the fuzzy set $D = A \cap B$ with membership function [14]:

$$\mu_D(x) = \min[\mu_A(x), \mu_B(x)] \quad \forall x \in X \tag{4}$$

b) **Co-norms, fuzzy union (fuzzy OR)**

Let A and B be two fuzzy sets defined in fuzzy space X, the union of A and B is the fuzzy set $D = A \cup B$ with membership function [1, 15]:

$$\mu_D(x) = \max[\mu_A(x), \mu_B(x)] \quad \forall x \in X \tag{5}$$

c) **Defuzzification**

Defuzzification is the process of representing a fuzzy set with crisp number [14]. The most commonly used defuzzification method is the center of area method also this method is known as the centroid method [2]. The center of the fuzzy set D is determined by:

$$coa(D) = \frac{\sum_{x\min}^{x\max} x.\mu_D(x)}{\sum_{x\min}^{x\max} \mu_D(x)} \tag{6}$$

Defuzzification is used to convert membership functions into fuzzy possibility score FPS [15, 16], where a crisp score that represents the degree of experts belief of the most likely score to indicate that an event may occur. To ensure compatibility between real number and fuzzy FPS, fuzzy possibility score or defuzzified fuzzy number is transformed into fuzzy failure probability FFP [7]:

$$FFP = \begin{cases} \frac{1}{10^k} & FPS \neq 0 \\ 0 & FPS = 0 \end{cases} \tag{7}$$

Where $K = \left[\frac{1-FPS}{FPS}\right]^{1/3} * 2.301$

V.CASE STUDY

In this case study, the operators must isolate the Reactor Coolant System "RCS" from the Decay Heat Removal "DHR" system according to a given sequence. The basic sequence steps required of the operator are listed in Table 1. Essentially, these steps show the operator should restore the signal power, restore the control power to the valves, and then closing the two valves or one of them since valve 1and,

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 10, April 2015

2 are in series and closing one of them will result in successful isolation.

Fig.6 shows the logic structure reflecting the relationship of the task and sequence in a fault tree format [3]. The tasks of restoring signal power, restoring power to control circuits, and failing to close the valves are all under an OR gate, this because failure of any one of these tasks will result in failure to isolate the RCS. In addition, the physical action of closing the valves is represented under an AND gate, showing that for failure to occur, the operator must fail to close both of the valves.

The basic events of the fault tree shown in Fig.7 are fuzzified to fuzzy numbers "*High*", "*Medium*", and "*low*" according to human failure impact on the realization of Major Accident Hazard "MAH" as detailed in Table 2. Then fuzzy operations t-norms and co-norms defined by equations (4) and (5) respectively are used to aggregate the fuzzy numbers which represent the basic events. The fuzzy numbers obtained for intermediate events "operators fail to restore signal power", "operators fail to restore power to control circuit", and "operators fail to take appropriate control action related to valve 1 and 2" are shown in Fig.8.

Table 1 Abbreviated Task List of Operator Actions Required to Isolate RCS from DHR System [3]

1	Operators restore signal power
2	Operators restore power to control circuits
3	Operators close valve 1 (and/or)
4	Operators close valve 2

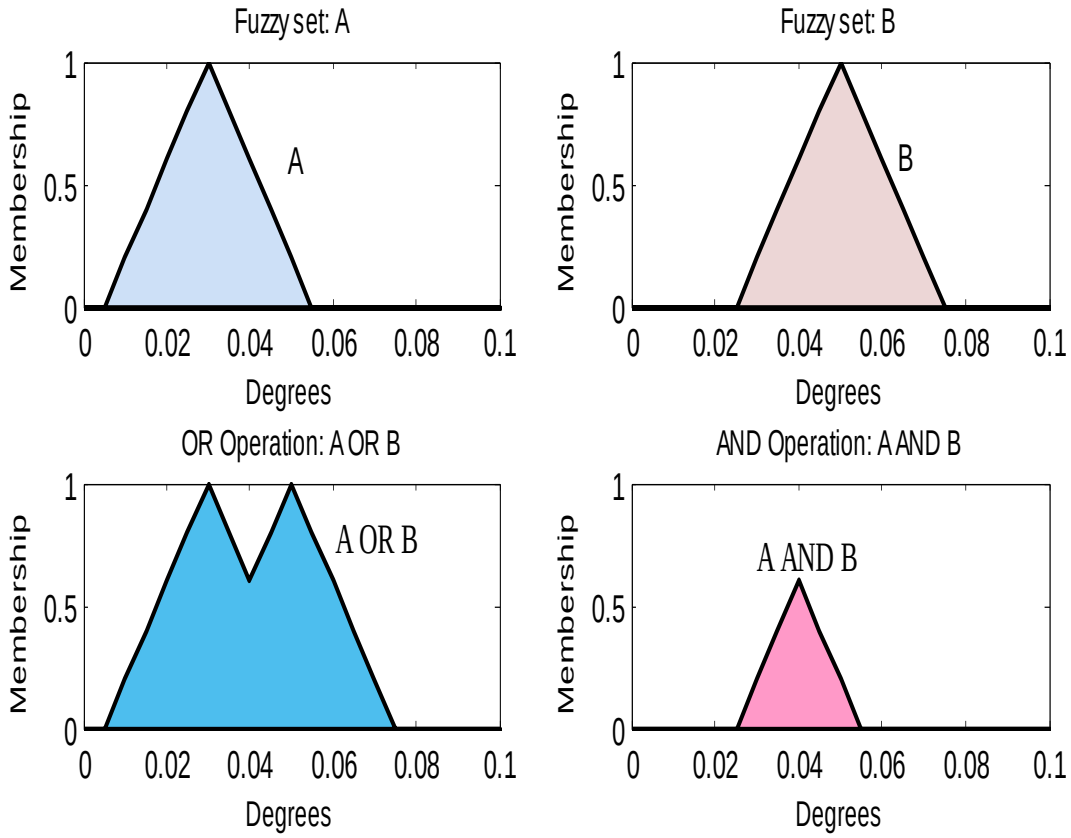

Table 2 Human Failure Fuzzification

Human Failure	Meaning
High (H)	A human failure could result directly in realization of a MAH
Medium (M)	A human failure could escalate to a MAH if various other barriers fail
Low (L)	A human failure should not lead directly or indirectly to a MAH

The centroid defuzzification method is used to get a crisp value, which represents fuzzy possibility score. According to equation (6), the fuzz possibility score is 0.499.
To get the failure probability of the top event, equation (7) is used which results a failure probability equal to 0.005.

Fig.6, Fuzzy Operations (t-norms and co-norms)

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 10, April 2015

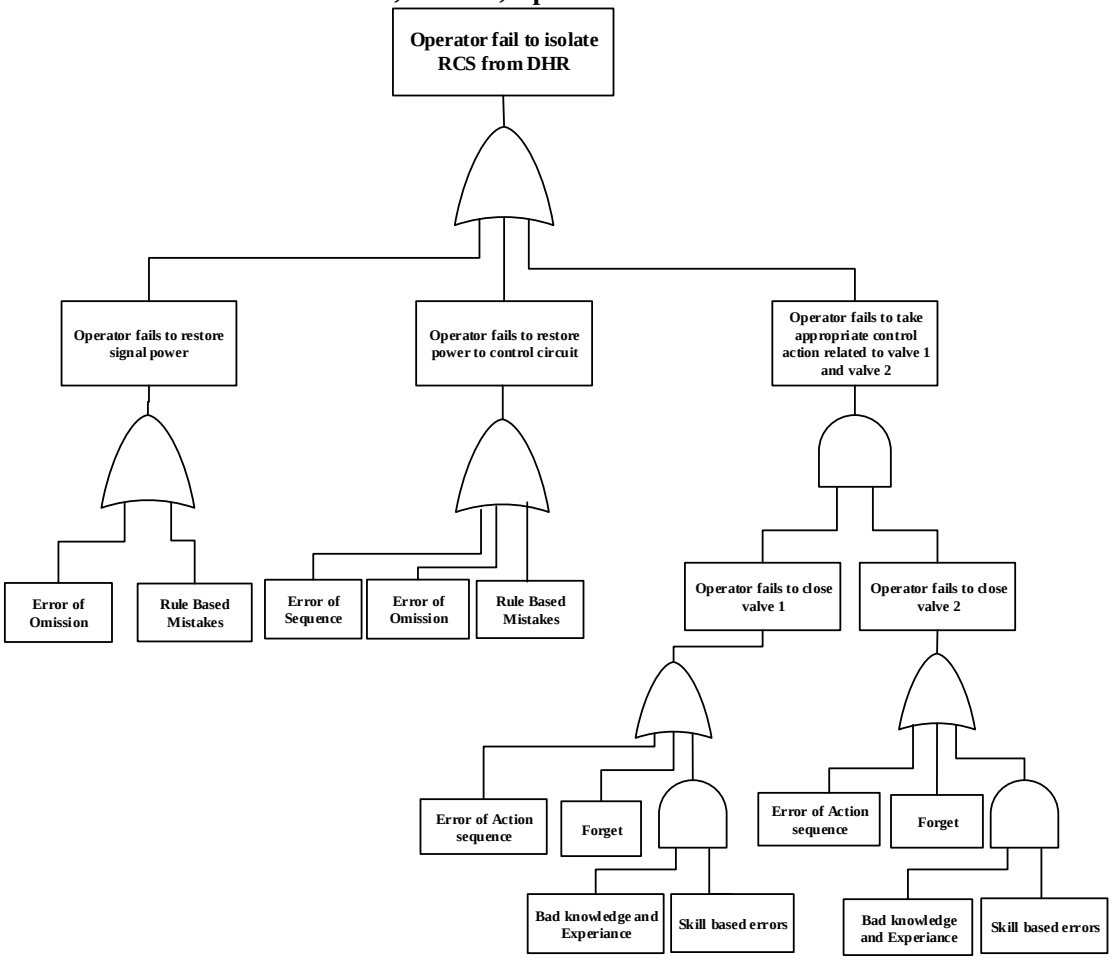

Fig. 7 Human Factors Fault tree

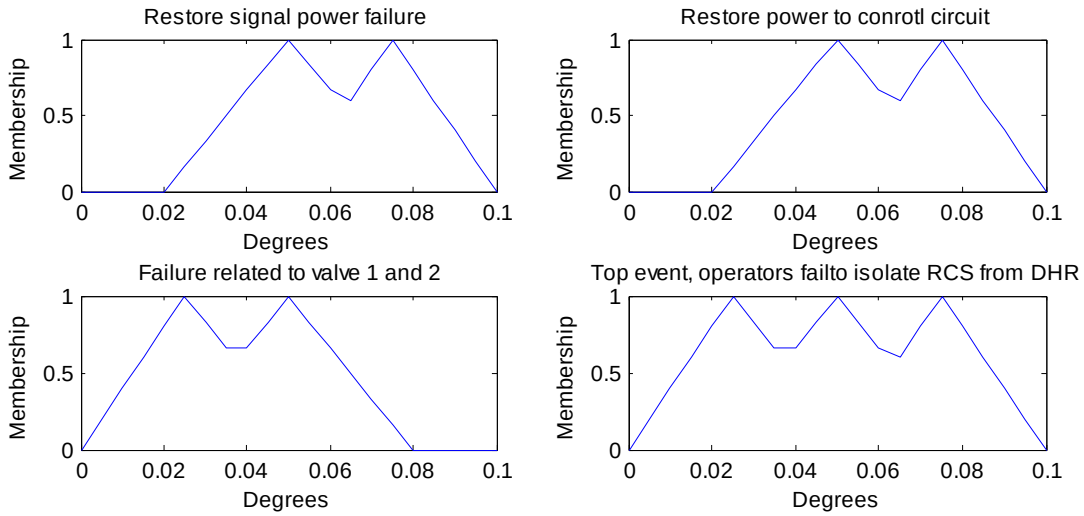

Fig. 8, Result of Aggregation of Intermediate Events and Top Event

IV. CONCLUSION

Correct human reliability analysis by fault tree requires complete and precise data about human faults. In most of cases, the objective data of the basic events are incompleteness and imprecision or vagueness. So, fault tree risk assessment gives a false impression of precision and correctness that undermines the overall credibility of the process. In this paper, a new fuzzy fault tree method is proposed for the analysis of human reliability based on fuzzy sets and fuzzy operations t-norms, co-norms, defuuzzification, and fuzzy failure probability. This method overcomes the incomplete and imprecise difficulties of HRA using FTA. The basic idea of the proposed method is based

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 10, April 2015

on fuzzificating fault tree by representing basic events probabilities crisp values by fuzzy values in the form of linguistic values such as low, medium, and high to express the degree in which experts believe in basic events happening. Instead of fault tree AND, OR operations, fuzzy operators t-norms, co-norms, and defuzzification are used to give conclusion about the top event in the form of fuzzy possibility score. This fuzzy possibility score value is converted into fuzzy failure probability.

REFERENCES

[1] Julie Bell & Justin Holroyd, "Review of human reliability assessment methods", Health and Safety Laboratory 2009.

[2] Marianna Madonna, Giancarlo Martella, Luigi Monica, Elisa Pichini Maini, Laura Tomassin,"The Human Factor in Risk Assessment: Methodological Comparison between Human Reliability Analysis Techniques", Prevention Today, 2009, Vol. 5, no. 1/2, 67-83.

[3] David I. Gertman, Harold S. Blackman, Human Reliability and Safety Analysis Data Handbook, by John Wiley & Sons Inc. 1994.

[4] Blackman, H.S., Gertman, D.I., Boring, R.L.: Human error quantification using performance shaping factors in the SPAR-H method. In: 52nd Annual Meeting of the Human Factors and Ergonomics Society (2008).

[5] Shappell, S.A., and Wiegmann, D.A "The Human Factors Analysis and Classification System, HFACS", Office of Aviation Medicine Federal Aviation Administration, Feb. 2000.

[6] J.H. Purba, J. Lu, D. Ruan, G. Zhang, "A Failure Possibility-Based Reliability Algorithm for Nuclear Safety Assessment by Fault Tree Analysis", In proceeding of: The 1st International Workshop on Safety & Security Risk Assessment and Organizational Cultures (SSRAOC2012).

[7] Purba, Julwan Hendry, et al. "Probabilistic safety assessment in nuclear power plants by fuzzy numbers." 9th Int. FLINS Conf., Chengdu. Vol. 4. 2010.

[8] J. B. Dugan, "Fault-Tree Analysis of Computer-Based Systems," Annual Reliability and Maintainability Symposium, January 2001.

[9] Renjith, VR and Madhu, G and Nayagam, Lakshmana Gomathi V and Bhasi, AB (2010) Two-dimensional fuzzy fault tree analysis for chlorine release from a chlor-alkali industry using expert elicitation. *In: Journal of Hazardous Materials, 183 (1-3). pp. 103-110.*

[10] Dokas, I.M., D.A. Karras, and D.C. Panagiotakopoulos, Fault tree analysis and fuzzy expert systems: Early warning and emergency response of landfill operations. Environmental Modeling and Software, 2009. 24(1): p. 8-25.

[11] Tyagi S.K, Pandey D., Tyagi R., "Fuzzy set theoretic approach to fault tree analysis", International Journal of Engineering, Science and Technology, Vol. 2, No. 5, 2010, pp. 276-283.

[12] Julwan Hendry Purba, Jie Lu, Guangquan Zhang, "Fuzzy Failure Rate for Nuclear Power Plant Probabilistic Safety Assessment by Fault Tree Analysis," Computational Intelligence Systems in Industrial Engineering Atlantis Computational Intelligence Systems Volume 6, 2012, pp. 131-154.

[13] B.S. Mahapatra and G.S. Mahapatra, "Intuitionistic fuzzy fault tree analysis using intuitionistic fuzzy numbers", International Mathematical Forum, 5, 21(2010), 1015 – 1024.

[14] Ferdous, Refaul, et al. "Methodology for computer aided fuzzy fault tree analysis." Process safety and environmental protection 87.4 (2009): 217-226.

[15] Cheong C. W., Hui Lan A. L., Web Access Failure Analysis – Fuzzy Reliability Approach, International Journal of the Computer, the Internet and Management Vol. 12, no.1, (January – April, 2004), pp. 65 – 73.

[16] Abdelgawad, M. and Fayek, A. (2011). "Fuzzy Reliability Analyzer: Quantitative Assessment of Risk Events in the Construction Industry Using Fuzzy Fault-Tree Analysis." J. Constr. Eng. Manage., 137(4), 294–302.