Reliability Analysis Using Fault Tree Analysis: A Review

Ahmed Ali Baig, Risza Ruzli, and Azizul B. Buang

***Abstract*—This paper reviews the literature published on the recent modifications made in the field of risk assessment using Fault Tree Analysis (FTA)in the last decade. This method was developed in 1960's for the evaluation and estimation of system reliability and safety. In this paper we have presented the general procedure for FTA, its application in various fields and the modifications that have been made through the time to overcome the inadequacies of the method. In the last section some of the future wok is also discussed with a simplified methodology.**

***Index Terms*—Fault tree analysis (FTA), risk assessment, reliability and safety, hazard analysis, FTA modification.**

I. Introduction

Fault Tree analysis translates the physical system into a logical diagram due to which it is one of the most favored method used these days by the people involved in reliability and safety calculations in industry. It was originated from aerospace industry and then adapted by nuclear power plant industry to qualify and quantify the hazards and risks involve in nuclear power generation. This approach is becoming very famous in chemical process industry as a result of the successful use in the power industry[1]–[7].

FTA is a top down deductive analysis in which the causes of an event are deduced. It gives a visual model of how equipment failure, human error and external factors have contributed towards an accident or event. It uses logical gates and small events to present the path of an accident through different steps and hence a fault tree is constructed for the particular event. The technical failures can be represented as basic event while human errors can be represented as intermediate events that may intensify to become a technical failure[8]. As shown in Table I, the gates used can explain different ways in which the human-machine interaction may have resulted into an accident for e.g. AND gate means that both the initial events are needed to occur in for the intermediate event to occur while OR gate means only one of the initial event may become the cause of intermediate event [8], [9]. The top and intermediate events are represented by a rectangle in a fault tree in which top event is the accident and the intermediate events are the occurrences that have somehow contributed to the top event to happen. Basic events are the lowest level of resolution in the fault tree, represented by a circle while underdeveloped events are those which are not further developed in a fault tree and are represented by a diamond. AND, OR and inhibitor gates are also represented by rectangle where inhibitor gate is a special case of an AND gate in which the output depends whether the input event is present and it qualifies the condition required. Ayyub, B. M describes the procedure for fault-tree is consisted of 8 steps [8]:

- Define the system of interest: the boundaries of interest are defined in this step on which analysis is to be made along with the conditions of the system.
- Define top event of the system: Specify the problem on which the analysis will be made like shutdown, pipe rupture etc.
- Define tree top Structure: Define the events and the conditions that lead to the top event.
- Explore each branch in successive level of details: Determine the events and conditions that lead to the intermediate event and keep repeating this process at different successive levels unless the fault tree is completed.
- Solve the fault tree for the combination of events contributing to the top event: Examine all the event and conditions that are necessary for the top event to occur and develop a minimal cut set.
- Identify important dependent failure potentials and adjust the model appropriately: Study the event and find the dependencies among the event that can cause a single or multiple events and conditions to occur simultaneously.
- Perform quantitative analysis: Use the past statistical data to evaluate or predict the future performance of the system.
- Use the results in decision making: Find the conditions in which the system is at most potential hazard and place appropriate measure and recommendations to counter with such risk.

II. Pros and Cons of Using FTA

FTA is a very effective risk assessment tool but when it comes to a reasonably complex system, that includes a large number of equipment and process variables, the fault tree becomes enormous and takes quite of a time to be completed. A team of engineers works over it and even then it may take years to complete without the surety of weather all the failure possibilities are considered or not.

The concept of partial failure in a fault tree does not exist. If the equipment is partially working it is considered as fully unavailable or in failure mode. This partial failure changes the reliability of a system but the FTA has no effect of such condition in its results.

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.

The probability calculation for a top event requires the

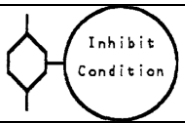
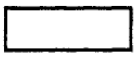
Manuscript received March 9, 2013; revised May 27, 2013.

The authors are with Universiti Teknologi PETRONAS, Malaysia (e-mail: ahmed1dec@gmail.com).

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.

On the other hand, the biggest advantage of using FTA is that it starts from a top event that is selected by the user for a specific interest and the tree developed will identify the root cause. The FTA has the ability to be used with computer and generate results using computer applications for improved analysis

TABLE I: SYMBOLS USED IN FTA AND THEIR DESCRIPTION [10]

Symbol	Meaning and Description
	AND gate: It requires the occurrence of all the input events for a resulting output event.
	OR gate: It requires the occurrence of any single input event for the resulting output event.
	Inhibit Event: The output event will occur only if the input event and inhibit event occurs.
	Basic Event: The last finding event with cannot further be defined
	Intermediate Event: It is the resulting event of different interacting events.
	Undeveloped Event: When the required information is unavailable the event cannot further be developed.
	Transfer Symbols: Used to transfer the fault tree to other location on sheet.

III. APPLICATIONS AND MODIFICATIONS

Initially FTA was used immensely by the Nuclear power generation but later on it becomes famous in all aspects of safety assessment in various fields. According to the literature review, FTA was integrated with the power flow model that identifies the importance measure corresponding to the selected load and the importance measure corresponding to the whole power system. The results of this research show the power calculated in the system by power model and it shows that the most important power lines are not always those that have the highest power flow during the normal regime of work [1]. The highest probability of failure was found in two disconnected switched in a substation. Another risk assessment was made that used FTA on a rail yard where hazardous chemicals are received and stored. A plan was proposed for the expansion of the yard and as a response from the community about the safety of the people this assessment was performed. Event tree is populated with empirical data to calculate the probabilities of major spills of 6 chemicals (Vinyl Chloride, Sodium hydroxide, Mono-ethylene glycol, Propylene, Hexene and Hexane). The impact radii is calculated by using US EPA's RMP *Comp software for offsite consequence analysisat 25 ºC, wind speed 1.5m/s and atmospheric stability class F. The largest impact radius was found to be of vinyl Chloride and Propylene as 700m (0.43 mi).According to EPA guidelines, a the vapor cloud will be formed after the release and will involve 10% of the cloud mass in case of explosion [2].

During the literature search a different application of FTA was observed by [6]. In this paper a research was made to find out the suitable measures to prevent suicide in railway systems. FTA and Haddon's ten energy-based injury prevention strategies were discussed and it was theoretically proved that more than 20 strategies can be used to prevent these accidents, out of which most of them were in the hands of the railway owners. Keeping the same concept of application [11], their concept of FTA was put forward. This paper emphasizes on the application of FTA to occupational hazards with top events as injury, staircase slipping hazard etc. A hazard tree is developed that represents the hazard base model. The procedure is implemented in the program GAP (Hazard Analysis Program), which enables one to generate and evaluate occupational hazard trees.

With the passage of time FTA was incorporated with different types of features and add-ons to support, supplement, modify and enhance the performance of this method. As mentioned above, some of the key disadvantages of FTA were studied and new techniques were hybridized with FTA, a brief description of these modifications in the light of its drawbacks is given:

A. A Time Consuming Method

Conventional FTA can be very time consuming and vulnerable to human error, so a potential computer aided methodology to construct FT is developed that works directly from the block diagram, avoiding the heavy and tedious work of creating digraphs, transition tables, decision tables, and knowledge-based rules. The algorithm is designed on small cause-and-effect tree to model the cause-and-effect logic of each component in a computer readable form. This algorithm is presented on the basis of component-by-component instead of loop-by-loop or node-by-node basis. In views of the author, the automatic fault tree synthesis using computer codes can be an initial step, independent check to assist or supplement a manual FTA [12].

Another paper emphasizes on developing a computer automated tool called PROFAT II bases on the analytical simulation algorithm (named as AS II).It is discussed that some of the major difficulties that are faced in developing the FTA of complex systems includes the nature and complexity of the steps involved with the construction of fault tree, the complexity of fault propagation mechanism, difficulty in acquiring and obtaining the failure reliability data, the computation time that is relatively more than other methods, hence increased costs and less reliable results due to large uncertainty involved in the input data. So, new techniques are used to upgrade the software pack of PROFAT (PRObabililistic FAult Tree) to overcome these problems of former tool [13].

B. No Function Representing Time Domain

J. Magott and P. Skrobanek explore a new dimension in

risk assessment that deals with the risk analysis in the time domain. A timing analysis of the safety properties using FTA with time dependencies and time state chart is presented. Derivation for FTA with time is presented along with the calculation of minimal and maximal values of these times from timed-state chart. Parameters such as sequential, alternative, loop (iteration) and parallel have been removed to reduce the complexity of computation[14]. The case study on railroad with controllers is presented and found that this method enables the calculation of the time requirement imposed on safety components. This paper represents an extension to the existing fault tree analysis that does not cover the time requirement in the probabilistic safety assessment. The conventional FTA does not monitor its top event probability as a function of time to follow the changes of the system. So a dynamic Fault tree is developed that enables the evaluation of actual time dependent risk profile that increases the applicability of the FTA [15], [16]. Equations and relations are developed to upgrade the existing models and the knowledge of time dependency of risk can further reduce the plant risk.

C. Low Accuracy of Results

To increase the accuracy of the method, FTA and task analysis are combined to develop a risk analysis technique that can focus on the component/machine failure as well as human error. To overcome this separation line, this methodology is presented in which an FTA is performed on an accident/incident to find the root cause of an undesired event [17]. Later task analysis is applied that identifies the sequence of the tasks that were performed and lead to the undesired event. When the task performed with error is identified, it is recommended by the author to use HEIST (Human Error Identification in System Tool) to determine the psychological errors involved in the human based events and then the performance shaping factor is identified that contributes to the unreliable human actions. The procedure is presented in this paper with an application on a Bulgarian industry.

The concept of condition based maintenance (CM) is not new to industry and the reliability of a system changes due this CM. However, its effect cannot be seen in the reliability analysis. FTA is performed in the design phase and the failure data is collected from available sources or handbooks etc. Condition based FTA is applied on a pre-established FTA with condition monitors (like vibration analysis, oil analysis, power consumption etc.) that updates the failure rate of the sensitive components. The CBFTA (Condition Based Fault Tree Analysis) uses this updated value of failure and recalculates the probability of the top event. This method makes FTA useful and a powerful tool in operational stage until the remaining life of the system [18].

Y. Dutuit and A. Rauzy focuses on estimating the reliability of a system that is made up of both repairable and non-repairable components. Four algorithms are considered: the Murchland lower bound, the Barlow-Proschan lower bound, the Vesely full approximation and the Vesely asymptotic approximation, and the results are compared [19]. The fault tree is constructed by means of binary decision diagram (BDD) and it is presented on different examples. It is concluded that exact value of reliability of a system cannot be obtained but approximations can be made. The Vesely full approximations gave the most accurate results however the Vesely asymptotic approximation was less accurate but faster. Further this method is improved using truncation technique to reduce complexity of BDD [20].

Calculating the importance measure of the initiating and enabling events in a fault tree is an important task. Since the reliability of the system with repairable components cannot be exactly calculated so it is important to classify the events as initiators and enablers, as their role is different in the system and must be treated accordingly. Based on system failure frequency new equations are also developed for calculating the exact importance measure of the initiators and enablers [21].

D. Un-Availability of Reliability or Failure Rate Data

The main obstacle in risk assessment using FTA is the un-availability of reliability data that makes the procedure time consuming and error-prone. For this reason, in this paper generic ranges for probability data are used. These ranges are accounted in different classes and in different functions (e.g. Temperature, pressure, velocity etc.) under different operating and maintenance conditions, thus the data exhibits different failure rates [22]. This procedure contributes towards better and improved FTA with less time consumption and resolves the scarcity of adequate data.

In conventional FTA the ambiguous and imprecise events such as human errors are not handled effectively therefore to overcome this problem a hybrid approach is developed using FTA with Fuzzy logic to evaluate the probabilities of such events. Instead of directly using the failure rates, fuzzy failure rates are used for the characterization of imprecise events such as human errors [5], [23], [24]. The failure rates are defined in linguistic ranges as defined by the fuzzy set theory. It is an effective method where both linguistic and probabilistic evaluation is necessary. The method is applied on a human-robot system to illustrate the hybrid technique. This hybrid method is one of the most widely applied methods to overcome the un-adequacy of data and its applications can be observed in different areas of researches. Another example of FTA used with fuzzy logic is the undesired event caused in a spread mooring system used to hold ships and boats during (un)loading conditions [25]. Sensitivity analysis is also made by fuzzy weighted index (FWI) to estimate the impact of basic events on the top events. This method is also observed to be applied in oil and gas sector where fuzzy fault tree is applied where the probability of fire and explosion is determined qualitatively and quantitatively with minimum path set using Boolean algebra [4].

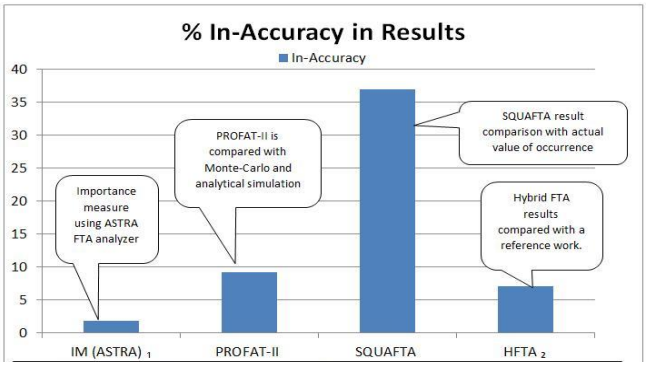


Fig. 1. Comparison of results from different modified versions of FTA

A comparative study of results, over the major changes in FTA, was observed. From literature (see Fig. 1) that Semi-quantitative technique used show quiet deviated results and even after such additions and enhancements the results in case of inadequate failure data, are not satisfactory. The difference in expert's opinion is the key factor involved in the deviation of the results.

IV. Methodology

As computer programming and simulation has become very useful tool in risk assessment it should be used together with the modified techniques. A simple example can be considered from a chemical process plant. In chemical industry corrosion is one of the most common issue hindered in day to day operation. Risk assessments have been made and failure data is presented for established systems. In the presence of this data, a set of correlations or equations can be developed that can be used along with the simulations to predict the failure rate of equipment for newly designed or under developed systems. A simple methodology for valve failure is given in Fig. 2. If valve failure is assumed to be the top event then the probable causes may include the stresses on the valve, pressure, temperature, flow velocity, contaminations, pH etc. the failure rates for these parameters can be found and the remaining may be acquired by the help of computer simulations. Now once the raw information is gathered co-relation can be developed for e.g. In certain operating conditions, due to the collision of solid particles through the valve, the probability of failure can be calculated through the following approach, as shown in Fig. 2.

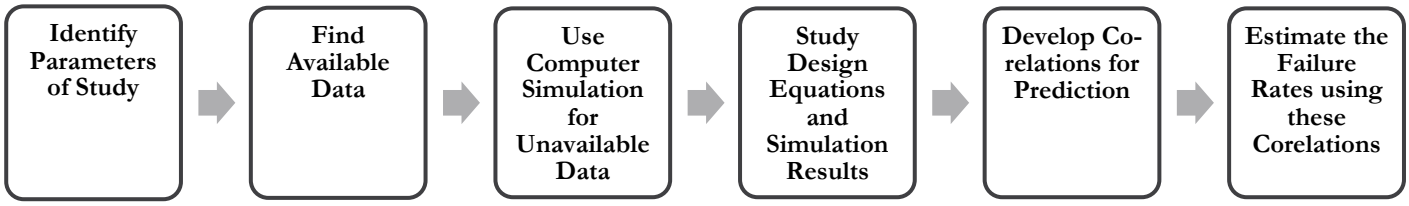


Fig. 2. Methodology of proposed future work

These co-relations will help even when the appropriate or adequate data of reliability is not available. Different kinds of simulation software for chemical process industry are now available and hence the hybridization of such software with this idea can yield reasonably improved results.

V. Conclusion

In this paper a brief review is made over the applications and enhancements made on FTA to make this method more sensitive and effective. An analysis on the disadvantages of FTA was made and the changes that were made to counter these problems. It is observed that for FTA, the presence of reliability data is very important but its unavailability is a major problem for risk assessment. Different techniques are combined like ranking method and fuzzy logic to overcome this problem but satisfactory results cannot be produced due to lack of appropriate methods and unavailability of data. A concept of developing correlations between reliability and different parameters is one of the routs that might achieve desired results.

Acknowledgment

I would like to thank University Technology Petronas (UTP) for their support and funding (GA), my supervisor Dr.Risza Rusli for her understanding, kindness and humble guidance towards my research. All faculty members of Chemical Engineering Department and especially the most, my family for their forever support and Almighty Allah for making this possible.

Reference

[1] B. Mavko, A. V. Ã, and C. Marko, "Application of the fault tree analysis for assessment of power system reliability," *Reliability Engineering & System Safety*, vol. 94, issue 4, pp. 1116–1127, 2009.

[2] T. S. Glickman, "Assessment of hazardous material risks for rail yard safety," *Safety Science*, vol. 45, issue 7, pp. 813–822, 2007.

[3] S. Ju, C. Chen, and C. Chang, "Fault-tree structures of override control systems," *Reliability Engineering and System Safety*, vol. 81, no. 2, pp. 163–181, 2003.

[4] X. Zhao-mei, "Research on FTA of Fire and Explosion in the Crude Oil Gatheringtransport Combination Station," *Procedia Engineering*, vol. 11, pp. 575–582, Jan. 2011.

[5] F. Batzias, A. Bountri, and C. Siontorou, "Solving River Pollution Problems by Means of Fuzzy Fault Tree Analysis," *Advances in Biology, Bioengineering and Environment*, no. 3, pp. 228–233.

[6] I. Svedung, R. Andersson, and H. Ra, "Suicide prevention in railway systems: Application of a barrier approach," *Safety Science*, vol. 46, issue 5, pp. 729–737, 2008.

[7] B. J. M. Ale, "Towards a causal model for air transport safety — an ongoing research project," *Safety Science*, vol. 44, pp. 657–673, 2006.

[8] B. . Ayyub, *Risk analysis in engineering and economics*, 2003.

[9] Y. Y. Haimes, *Risk assessment, modeling and management*, 3rd ed., A John Wiley & Sons Inc. publication, 2009.

[10] W. S. Lee, "Fault Tree Analysis, Methods, and Applications - A Review," *IEEE Transactions on Reliability*, vol. R-34, no. 3, pp. 121–123, 1985.

[11] U. Hauptmanns, M. Marx, and T. Knetsch, "GAP — a fault-tree based methodology for analyzing occupational hazards," *Journal of Loss Prevention in the Process Industries*, vol. 18, issue 2, pp. 107–113, 2005.

[12] Y. Wang, T. Teague, H. West, and S. Mannan, "A new algorithm for computer-aided fault tree synthesis," *Journal of Loss Prevention in the Process Industries*, vol. 15, issue 4, pp. 265–277, 2002.

[13] F. I. Khan and S. A. Abbasi, "Analytical simulation and PROFAT II: a new methodology and a computer automated tool for fault tree analysis in chemical process industries," *Journal of Hazardous Materials*, vol. 75, issue 1, pp. 1-27, 2000.

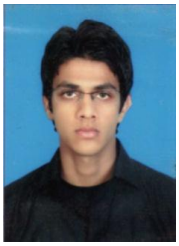
[14] J. Magott and P. Skrobanek, "Timing analysis of safety properties using fault trees with time dependencies and timed state-charts," *Reliability Engineering and System Safety*, vol. 97, no. 1, pp. 14–26, 2012.

[15] B. Mavko, "A dynamic fault tree," *Reliability Engineering & System Safety*, vol. 75, issue 1, pp. 83-91, 2002.

[16] M. Lukowicz, J. Magott, and P. Skrobanek, "Selection of minimal tripping times for distance protection using fault trees with time dependencies," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1556–1571, Jul. 2011.

[17] D. E. Doytchev and G. Szwillus, "Combining task analysis and fault tree analysis for accident and incident analysis: A case study from

Bulgaria," *Accident Analysis & Prevention*, vol. 41, issue 6, pp. 1172–1179, 2009.
[18] D. M. Shalev and J. Tiran, "Condition-based fault tree analysis (CBFTA): A new method for improved fault tree analysis (FTA), reliability and safety calculations," *Reliability Engineering & System Safety*, vol. 92, issue 9, pp. 1231–1241, 2007.
[19] Y. Dutuit and A. Rauzy, "Approximate estimation of system reliability via fault trees," *Reliability Engineering & System Safety EI SCI*, vol. 87, no. 2, pp. 163–172, 2005.
[20] S. Contini and V. Matuzas, "Analysis of large fault trees based on functional decomposition," *Reliability Engineering & System Safety*, vol. 96, no. 3, pp. 383–390, Mar. 2011.
[21] S. Contini and V. Matuzas, "New methods to determine the importance measures of initiating and enabling events in fault tree analysis," *Reliability Engineering and System Safety*, vol. 96, no. 7, pp. 775–784, 2011.
[22] U. Hauptmanns, "Semi-quantitative fault tree analysis for process plant safety using frequency and probability ranges," *Journal of Loss Prevention in the Process Industries*, vol. 17, issue 5, pp. 339–345, 2004.
[23] M. Kumar and S. P. Yadav, "The weakest t-norm based intuitionistic fuzzy fault-tree analysis to evaluate system reliability," *ISA transactions*, vol. 51, no. 4, pp. 531–8, Jul. 2012.
[24] S. K. Tyagi, D. Pandey, and R. Tyagi, "Fuzzy set theoretic approach to fault tree analysis," *International Journal of Engineering, Science and Technology*, vol. 2, no. 5, pp. 276–283, 2010.
[25] A. Mentes and I. H. Helvacioglu, "An application of fuzzy fault tree analysis for spread mooring systems," *Ocean Engineering*, vol. 38, no. 2–3, pp. 285–294, 2011.



Ahmed Ali Baig was born in Kuwait on December 1, 1988. From the very beginning, Mr. Baig has been inspired by intellectuals and their accomplishments with respect to the welfare of the society and his dream to become of such intellectual, in order to do so, he completed his schooling from one of the highly reputable schools. His interest in engineering made him to select the pre-engineering course for his college and this decision directed his potential to become a Chemical & Process Engineer. In January 2012, with majors in Polymers and Petrochemical studies from NED University of Engineering and Technology Karachi, Pakistan, he was awarded the degree of Bachelors of Engineering.

Soon after his graduation and within no time his potential was recognized by one of the leading tyre industry named as "General Tyre and Rubber Co." Karachi, Pakistan. On April 22, 2012 he served his first day as Trainee Production Engineer (MTO, Management Trainee Officer). His thirst for knowledge made him accept the opportunity to work as a Research Scholar and pursue his Masters Degree in Chemical Engineering at Universiti Teknologi PETRONAS, Malaysia, where he is currently conducting his research in the field of Industrial safety.

Mr. Baig was an active member and one of the founders of the Society of Polymers and Petrochemical Engineers (SPPE). He was dealing with the local industries in resolving their engineering problems and finding funds for the development and progress of the society.

Risza Binti Rusli was born in Malaysia and acquired her primary education from Malaysia. Soon after her schooling her bright ways in learning directed her towards her Degree in Chemical Engineering from University of Newcastle Upon Tyne, Tyne and Wear, United Kingdom. She followed her pursuit for education and completed her Masters from University of Aberdeen, United Kingdom. She also completed her PhD in chemical engineering with her specialization in Risk management and Reliability.

Dr. Risza is now a senior lecturer in Universiti Teknologi PETRONAS, serving for brightening the future of hundreds of young researchers.

Azizul B. Buang was born in Malaysia with his primary educated form his home town. Soon after his schooling, Mr. Buang joined University of Leeds, Leeds, West Yorkshire, England where he completed his engineering in the field of chemical engineering which than happens to be leading him towards his Master's Degree from University of Wales, England with his majors in Process Engineering.

Mr. Buang is now working as an occupational & process safety expert and lecturer in Universiti Tekinologi PETRONAS, Malaysia.