International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 03, March-2015

Overview of Fault Tree Analysis

Pallavi Sharma
Student
Department of Mechanical Engineering
Maulana Azad National Institute of Technology
Bhopal, India

Dr. Alok Singh
Assistant Professor
Department of Mechanical Engineering
Maulana Azad National Institute of Technology
Bhopal, India

***Abstract*—To increase the reliability of the system the failure data analysis is required. Fault tree analysis is the basic method which focuses on failure modes of any system and the probabilities of occurrence/ probability risk analysis associated with it. FTA represents major fault or critical failures associated to the system and causes for the faults graphically. Here we get to know the probability of failure of the give basic event with the help of which we get the probability of failure of the top event. This paper gives an overview of fault tree analysis and its methodology with the implementation.**

Keywords – Fault Tree Analysis, Reliability, Probability risk analysis

I. INTRODUCTION

Fault tree analysis is the technique used for reliability analysis for complex systems. The fundamental concept is translation of failure behaviour of model into visual diagram or logic models. Fault tree analysis (FTA) is the most commonly used technique for causal analysis in risk and reliability studies. This analysis method is mainly used in the field of safety engineering to quantitatively determine the probability of a safety hazard [1]. It is a deductive approach so as to get the probability of top event.FTA is failure analysis in which undesired state is analysed using Boolean logic. FTA was developed in 1962 at Bell Laboratories by H.A Watson, under a U.S Air Force Ballistics Systems Division contract to evaluate the Minuteman I Intercontinental Ballistic Missile (ICBM) Launch Control System. The concept of FTA was expanded by the reliability experts. Boeing and AVCO expanded its use to Minuteman II system in 1963-1964[2]. Since then it is used in number of system safety assessment and reliability engineering field such as nuclear reactor, chemical industry, manufacturing industries, circuit board, petrochemical industry etc.

FTA involves the events from hardware wear out, material failures or combinations of deterministic contributions to the event stemming from assigning failure rates to the branches. Failure rates are obtained from MTBF of the component, unit or subsystem.FTA can be used as a design tool which can identify accident and can also be used as diagnostic tool predicting most likely system failure [3].

The fault tree provides a diagrammatic description of the way in which a system can fail in a specific mode. The importance of the fault tree for safety system analysis is that it yields a complete description of the various causes of the system failure. Hence the engineers can identify and rectify any problem areas in the design.

II. REVIEW OF FTA

FTA seen for the first time in the literature for use on safety of nuclear power and missile systems as early as the mid-1960‘s. Griffen (1966)[4], suggested that FTA is useful in analysis of system design focused on avoidance of catastrophic nuclear accidents, whereas Sellers provides an early discussion of FTA as applied to missile systems (1967)[5]. FTA was adopted relatively quickly into other fields, such as reliability analysis of computing and electrical systems (Nieuwhof, 1975; Dugan et al., 1993)[6]. Another early user of FTA methods was the National Aeronautics and Space Administration (NASA). NASA began using risk analysis by doing analyzing the simple observed failures, and then progressing over time to the use of probabilistic models to predict probability of failures within their systems (Pate-Cornell and Dillon 2001)[7]. FTA got coverage at 1965 system safety symposium in Seattle sponsored by Boeing and university of Washington[8]. Boeing began using FTA for civil aircraft design in 1966[9][10].

In 1976 the U.S. Army Material Command incorporated FTA into an Engineering Design Handbook on Design for Reliability [11]. The reliability centre in Rome laboratory with defence technical information centre published documents on FTA in 1960’s [12][13]. In 1975 U.S nuclear regulatory commission began using probabilistic risk assessment method including FTA within nuclear power industry [14]. PRA research was expanded followed by 1979 incident at Three Mile Island which led to the publication of NCR fault tree handbook NUREG-0492[15].

Following process industries hazards such as Bhopal disaster(1984) and piper alpha explosion(1988) OSHA(United States Department of Labor Occupational Safety and Health Administration) PSM(Process Safety Management) Recognized FTA as an acceptable method for process hazard analysis[16]. NASA began using risk analysis by doing analyzing the simple observed failures, and then progressing over time to the use of probabilistic models to predict probability of failures within their systems (Pate-Cornell and Dillon 2001)[17].

The approach helped them or allowed them to create software that: performs Probability Risk Analysis, permits updating, and allows for real-time support of decisions involving the space shuttle, space station, and some unmanned space missions.

FTA is useful not only in giving a visual representation of the system; it also provides a foundation for identifying and combining probabilities of different events impacting system failure through Boolean logic statements (Bedford and Cooke 2001)[18].

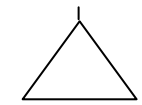
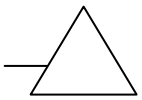
III. THEORETICAL CONSIDERATIONS &SYMBOLS

Fault tree analysis is a deductive method used to identify the casual relationship leading to specific system failure mode. Analytical tree is the graphical representation or picture of the event and it is called tree because their structure resembles a tree having top event as output event and having branches (basic event) as input event [19]. The initial step is to identify the system failure mode of concern which becomes the top event of the analysis. The top event is developed by several branches leading to various sub events which represents the possible cause of the event.

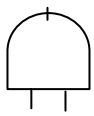
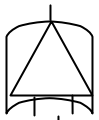
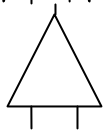
Each fault tree is built up from gates and basic events, the gates link the events together depending upon their casual relationship.

The basic symbols used in FTA are grouped as events, gates and transfer symbols.

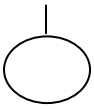
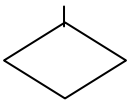
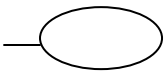
A. *Transfer symbols*

Symbol	Meaning
	Transfer-In
	Transfer-out

B. *Gate symbols*

Symbol	Meaning	Casual relationship
	AND Gate	Output event if all input event occur simultaneouslv
	OR Gate	Output event occur if atleast one input event occur simultaneouslv
	Exclusive OR Gate	Output event occurs if only one input fault occur simultaneouslv
	EXCLUSIVE AND Gate	Output event if all input occurs in specific sequence

C. *Event symbols*

Symbol	Meaning	Casual relationship
	Basic event	Basic initiating fault
	Incomplete event	Event not developed further due to insufficient information
	Conditional event	Conditions applied on gates
	Intermediate event	Fault occur due to one or more antecedent causes through Logic gates

IV. FTA METHODOLOGY

Event in a fault tree are associated with statistical probabilities. As component failure with constant failure rate λ failure probability at the exposure time t will be:

$$P = 1-\exp(-\lambda t)$$

$$P = \lambda t,\ \lambda t<.1$$

Event probabilities depend on the relationship of event hazard function to the interval. The probability of the gate output event depends on the input event probability.
Probability of the AND Gate is given by:

$$P(A \text{ and } B) = P(A \cap B) = P(A)P(B)$$

Probability of the OR Gate is given by:

$$P(A \text{ or } B) = P(A \cup B) = P(A)+P(B)-P(A)P(B)$$

Since failure probabilities on fault trees tend to be small (less than .01), P(A M B) usually becomes a very small error term, and the output of an OR gate may be conservatively approximated by using an assumption that the inputs are mutually exclusive events:

$$P(A \text{ or } B) \approx 0$$

Six basic steps used to develop a fault tree analysis [20]:

I. System configuration understanding
II. Logic model generation
III. Qualitative evaluation of the logic model
IV. Equipment failure analysis and obtain basic data
V. Quantitative evaluation of the logic model
VI. Recommended appropriate corrective actions

SYSTEM CONFIGURATION UNDERSTANDING

In this step, the considered system is understood thoroughly for further analysis. The system failure mode need to be analysed is understood through experience and previous data stored by the user for future reference. System normal working is also considered during this stage of analysis. An important source of information here would be some type of functional layout diagram. This diagram should show all functional interconnection and identify all the components. For some systems that are hardware oriented, functional diagram may not exist.

LOGIC MODEL GENERATION

This is the second step in which logic model is generated with the help of first step gained information. Use of gates and sub events is supported to attain the top event in the diagram. Mostly used gates are AND and OR Gates.

QUALITATIVE EVALUATION OF THE LOGIC MODEL

In qualitative assessment minimal cut sets are performed. Minimal cut sets are obtained by taking Boolean expressions for the top event and then transforming into disjunctive normal form as the dot product is used to represent AND gate and sum is used to represent the OR gate. Laws of Boolean algebra are also used to remove redundancies in expression.

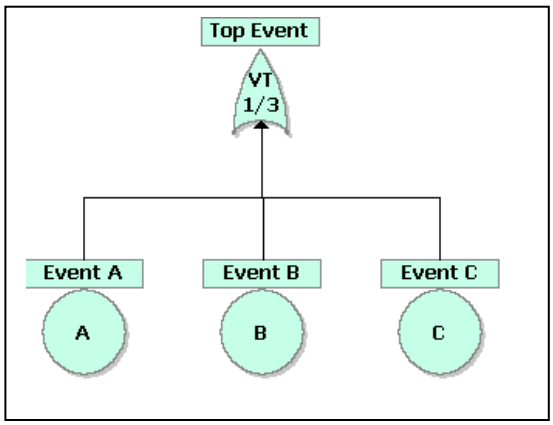
QUANTITATIVE EVALUATION OF THE LOGIC MODEL

Probability of occurrence of the logic gates, In order to estimate the probability of occurrence of the top event, it is essential to estimate the probability of occurrence of the logic gates' output fault events. Equations of probability of occurrence of 'OR' and 'AND' logic gates are given by[21]:

OR GATE

$$P=1-\sum_{i=1}^{n}(1-p_i)$$

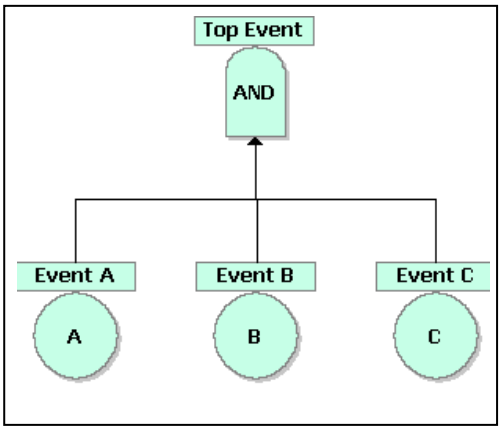
where, P is the probability of top event and
p_i is the probability of basic event
n is number of basic event gates associated



AND gate

$$P=\sum_{i=1}^{n}p_i \qquad (1)$$

where , P is the probability of top event and
p_i is the probability of basic event
n is number of basic event gates associated



V. IMPLEMENTATION OF FAULT TREE ANALYSIS

While implementing some of the steps followed are:

1) Identify the failure effect to be analyzed. This will be critical effect need to be eliminated and may be caused due to combinations of other failures. This may be found by the tools such as FMEA, FMECA etc.
2) Write the failure effect at the top centre in the diagram area and make a clear phrase which may describe the effects precisely.
3) List the failures that may directly contribute to the failure in step 2.
4) Divide the list of failures obtained in step 3 into separate groups.
   a) In group one place all the failure which may result from 2 or 3 failures together. Connect those failures with AND gate.
   b) In group two place all the failures which result from either one or the other failure. Connect those failures with OR gate.
   c) In other groups there can be complex grouping in which one or more than one gate can be connected to get the result.
5) For each failure which has no connections below it. Decide whether or not to develop this further by finding other failures which may contribute to it. If the failure is not to be developed on this diagram, draw it in an appropriate box. Thus, if the failure cannot reasonably be developed further, put it in a circle; if it could be developed, but is not appropriate to do this here, and then use a diamond-shaped box. If the failure is to be developed, repeat step 3 to find contributory failures and appropriate gates.
6) When the diagram is complete, examine it to draw conclusions and plan for appropriate plans.

CONCLUSION

This paper gave an overview of conventional fault tree analysis in reliability assessment of the system. This technique can be effectively used in calculating reliability of the complex systems thus making the analysis easier. This technique helps the personnel to redesign the critical parts and get to know the reason behind the failure of the required top event or the critical parts leading to the failure and improve the reliability and safety of the system. Here an assessment can be made by changing the parameters used to define top event and the interdependencies of the events that are to take place may further change the structure of the logic diagram.

REFERENCES

[1] Sarfraz Ali Quadri, Swapneel R. Zende, Dhananjay R. ,Reliability Estimation using Fault Tree Analysis Method.

[2] Mohammad Sadegh Javadi, Azim Nobakht, Ali Meskarbashee, Fault Tree Analysis Approach in Reliability Assessment of Power System, International Journal of Multidisciplinary Sciences and Engineering, sept 2011.

[3] M.H.J Bollen, Effects of adverse weather and aging on power system reliability, IEEE Trans. Ind. Appl (2001).

[4] Griffin, C. W. "Introducing Fault Tree as a Tool for Nuclear Safety Analysis." Transactions of the American Nuclear Society (1966)

[5] Sellers, R. F. "Fault Tree Analysis as Applied to Missile Systems." Journal of Spacecraft and Rockets (1967)

[6] Nieuwhof, G. W. E. "Introduction to Fault Tree Analysis with Emphasis on Failure Rate Evaluation." Microelectronics and Reliability (1975)

[7] Pate-Cornell, Elisabeth and Robin Dillon. "Probabilistic Risk Analysis for the NASA space shuttle: A Brief History and Current Work." Reliability Engineering and System Safety (2001)

[8] DeLong, Thomas. "A Fault Tree Manual" (pdf). Master's Thesis (Texas A&M University). 1970

[9] Eckberg, C. R. WS-133B Fault Tree Analysis Program Plan (Rev B). Seattle, WA: The Boeing Company, 1964

[10] Hixenbaugh, A. F. Fault Tree for Safety. Seattle, WA: The Boeing Company, 1968

[11] Evans, Ralph A. Engineering Design Handbook Design for Reliability. US Army Material Command, 1976.

[12] Begley, T. F.; Cummings Fault Tree for Safety. RAC. 1968

[13] Anderson, R. T.Reliability Design Handbook. Reliability Analysis Center, 1976

[14] Acharya, Sarbes; et al. Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (pdf). Washington, DC: U.S. Nuclear Regulatory Commission. NUREG–1150, 1990

[15] Vesely, W. E.; et al. Fault Tree Handbook (pdf). Nuclear Regulatory Commission. NUREG–0492, 1981

[16] Elke, Holly C., Global Application of the Process Safety Management Standard.

[17] M.H.J Bollen, Effects of adverse weather and aging on power system reliability, IEEE Trans. Ind. Appl. (2001).

[18] T. Solver, Reliability in performance-based regulation,Licentiate Thesis, Royal Institute of Technology, Sch. Elec. Eng., Stockholm, Sweden, 2005.

[19] Masdi Muhammad, M. Amin Abd Majid, A Case Study of Reliability Assessment for Centrifugal Pumps in a Petrochemical Plant, Fourth world congress on engineering asset management Athens, Greece, September 2009.

[20] Li DQ, Jiang SH, Chen YF, Zhou CB. System reliability analysis of rock slope stability involving correlated failure modes. KSCE Journal of Civil Engineering 2011.

[21] Dhillon BS. Power system reliability, safety and management. Univ. of Ottawa; 1983.

[22] T. Solver, Reliability in performance-based regulation, Licentiate Thesis, Royal Institute of Technology, Sch. Elec. Eng., Stockholm, Sweden, 2005.

[23] Masdi Muhammad, M. Amin Abd Majid, A Case Study of Reliability Assessment for Centrifugal Pumps in a Petrochemical Plant, Fourth world congress on engineering asset management Athens, Greece,September 2009.

[24] Li DQ, Jiang SH, Chen YF, Zhou CB. System reliability analysis of rock slope stability involving correlated failure modes. KSCE Journal of Civil Engineering 2011.

[25] Bedford, Tim and Roger Cooke. Probabilistic Risk Analysis: Foundation and Methods. New York: Cambridge University Press, 2001.