ISSN 2277 – 8322

Enhancing Computer System Reliability Using Fault Tree Analysis

Antima Saxena[1], Tanuj Manglani[2]

Department of CSE, YIT, Jaipur, India

Department of Electrical Engineering, YIT, Jaipur, India

Email : saxenayit@gmail.com, idtanuj@gmail.com

***Abstract* - Fault Tree Analysis of different systems is the qualitative and quantitative analysis of their fault occurrence. The fault tree analysis is a deductive failure based approach, where an undesired state of the system is specified and analyzed to find the ways in which the system can reach that state. The availability of a computer-based FTA methodology will greatly benefit the computer system . Ideally, FTA can be standardized through a computer package that reads information contained in process block diagram and provides automatic aids to assists engineers in engineering and analyzing fault trees. In order to enhance the reliability of computer system, the fault symptoms are defined and then its fault tree model has been established. All the common fault causes are figured out qualitatively by Fussel algorithm and are classified as 8 minimal cut sets. At last, the happening probability of top event, important degree of probability and key importance of each basic event are quantitatively calculated.**

***Keywords*- Computer System, Fault Tree, Qualitative Analysis, Quantitative Calculation, Minimal cut set, FTA**

I. INTRODUCTION

Fault tree analysis (FTA) is a diagrammatic and logical method to evaluate the probability of an accident resulting from the sequences and combinations of faults and failure events. A fault tree describes a model and interprets the relations between the malfunctions of the component and observed symptoms. Thus, the fault tree is useful for understanding logically the mode of occurrence of a fault. Furthermore for given failure probabilities of system components, the probability of the top event can be calculated. Fault Tree Analysis (FTA) is a powerful tool for analyzing the reliability and safety of large-scale complicated system. In the early 1960s, scientists in Bell laboratory first bring forward the FTA method. After that, Boeing Company improved the method to make it suitable for computer processing. Now there are many computer software of FTA available. FTA methods have entered into industry such as chemistry, light industry, electron, machinery manufacturing, etc. [1]. This paper focuses on quantitative and qualitative analysis of fault trees. The test system in this paper is taken as computer system.

II. FAULT TREE ANALYSIS METHODS

Fault tree were first developed in the 1960s to facilitate unreliability analysis of the Minuteman missile system [2] .They provide a compact, graphic, intuitive method to analyze system reliability. Traditional fault tree use Boolean gates to represent how component failures combine to produce system failures, and they are analyzed using cut sets (or other Boolean algebraic methods) or Monte Carlo simulation [3]. When FTA is used for analyzing a system, what we are concerned is to find all kinds of possible causes that lead to certain unexpected event (called top event in the following). Top event is usually the system failure or some kind of failure mode. FTA method finds all possible event combination which makes the top event happen with deductive method. It reflects logic relation of computer system and resulted top event. This relationship is represented by figure which is like an upside down tree and hence named fault tree. The fault tree show the relationship between the events and logical symbols such as the AND, OR, XOR etc. are use to depict the relationship between the event. The two basic gate categories used in fault tree are the OR gate and the AND gate. Due to the fact that the gates relate the events in the same way as Boolean expressions, all the Boolean laws can be applied in the fault tree. The most difficult part of creating a fault tree is the determination of the top level event. The selection of the top event is crucial since hazards in the systems will not be comprehensive unless the fault trees are drawn for all significant top level events. Once the top event has been defined, the next step is to determine the events related to the top event and the logical relations between them, using logical symbols to define the relations. The output of an AND gate only exists if all the inputs events exist. The output of an OR gate exists provided at least one on the input events exist. The relationships between the events are standard logical relations and can therefore be expressed using any form of Boolean algebra or truth table.

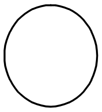
A successful FTA requires the following steps be carried out:
1. Identify the *objective* for the FTA.
2. Define the *top event* of the fault tree.
3. Define the *scope* of the FTA.
4. Define *ground rules* for the FTA.
5. *Construct* the fault tree.
6. *Evaluate* the fault tree.
7. *Interpret* and present the results.

The procedure of FTA analysis is: choose the top event and then construct the fault tree, finally assess the fault tree qualitatively or quantitatively.

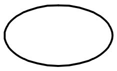
III. SYMBOLOGY

Symbology is the building blocks of the fault tree. There are two types of symbols which appear in the fault tree structure: gates and events.

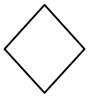
Primary Event: The primary events of a fault tree are those events, which, for one reason or another have not been further developed.



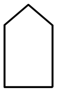
Basic Event: A basic initiating fault requiring no further development. These are found on the bottom tiers of the tree and require no further development or breakdown.



Conditioning Event: Specific condition or restrictions that apply to any logic gates.

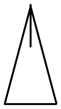


Undeveloped Event: An event which is not further developed either because it is of sufficient consequences or because information is unavailable.

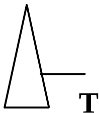


External Event: An event which is normally expected to occur.

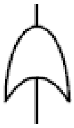
Transfer Symbols:



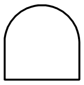
TRANSFER IN: Indicates that the tree is developed further at the occurrence of the corresponding TRANSFER OUT (e.g., on another page).



TRANSFER OUT: Indicates that the portion of the tree must be attached at the corresponding TRANSFER IN.



OR GATE: OR Gate indicates that one or more inputs event are required to produce the output event.



AND GATE: AND Gate indicates that all inputs events are required to cause the output event.

For a given Computer System fault tree, if events corresponding to the basic event set occurring cause top event occurring, then the basic event set is called a cut set. Fault tree analysis begins with listing the minimal cut set. A cut set is a set of basic events whose occurrence causes the top event to occur. A minimal cut set is a cut set that would not remain a cut set if any of its basic events were removed [4]. To get the minimal cut set, a top-down algorithm, Fussell-vesely algorithm will be used [5].

Each minimal cut set consist of a combination of specific component failures, and hence the general n component minimal cut set can be expressed as

$$M = X_1 . X_2 . X_3 \ldots.. X_n$$

Where X_1, X_2 , X_3,,, X_n are component failures on the tree.

IV. FAULT TREE ANALYSIS OF COMPUTER SYSTEM

The fault tree is constructed for the problem under study as shown in fig. 1. The top event for this problem is the computer not functioning. The computer functioning failure can be broadly classified into three parts: no power and no cold air failure and RAM damaged.

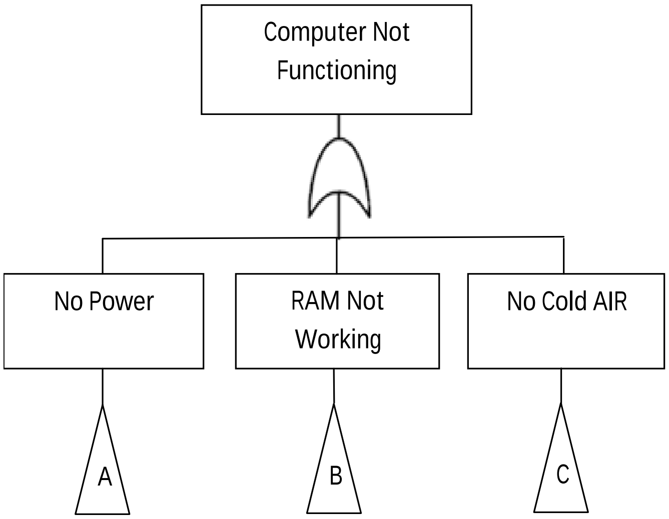


Fig. 1: Fault Tree

The logical relation between these two intermediate events and the top event is represented using or gate. The power failure or RAM damaged or cold air failures are the first level events which cause the system to fail.

The no power can be attributed to two causes: a main out and UPS out. The logical relationship between these two intermediate events and no power event is represented using an AND gate. RAM not working can be attributed to three causes: dust in RAM and RAM damaged or RAM misplaced. The logical relationship between these three intermediate events is represented using an OR gate.

The no cold air can be attributed to three causes: blower not working, no cooling water supply and compressor not functioning. The logical relationship between these three intermediate events and no cold air event is represented using an OR gate. The blower not working can be attributed to two causes: blower defective and no power to blower. The logical relationship between these two intermediate events and blower not working event is represented using an OR gate.

The no power to blower can be attributed to two causes: mains out and genset out. The logical relationship between these two intermediate events and no power to blower event is represented using an AND gate.

The compressor not functioning can be attributed to two causes: compressor out and no power. The logical relationship between these two intermediate events and compressor not functioning event is represented using an OR gate.

No power can be attributed to two causes: mains out and genset out. The logical relationship between these two AND gate.

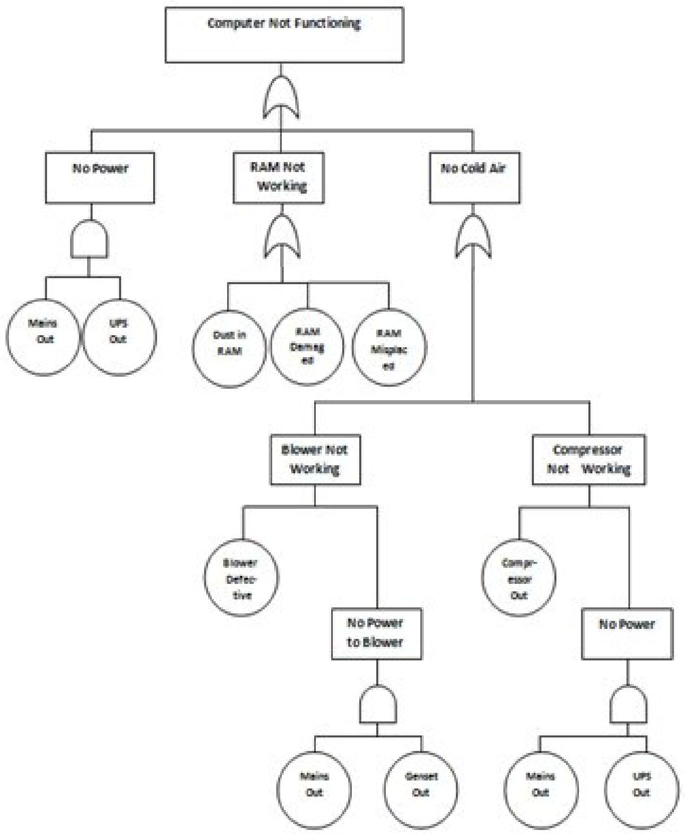


Fig. 2: Fault Tree Model of Computer System

V. QUALITATIVE EVALUATION OF A FAULT TREE

The goal of qualitative analysis is to find out all the fault reasons i.e. all the minimal cut sets which is helpful in fault diagnosis or maintaining the computer system.

For the qualitative analysis of computer system, the different 8 minimal cut set, due to which computer system may fail, are represented by E_1,---- E_8 which are as follows:

E_1 : The mains out.
E_2 : UPS out.
E_3 : Dust in RAM.
E_4: RAM Damaged.
E_5: RAM Misplaced.
E_6: Blower Defective.
E_7: Genset out of order.
E_8: Compressor out of order.

Following events used in this analysis is as follows:

F_1: represents the event that there is no power supply to the computer system.
F_2: represents the event that there is no power supply to the blower.
F_3: represents the event that blower is not working.
F_4: represents the event that there is no power supply to the compressor.
F_5: represents the event that compressor is not working.
F_6: represents the event that there is no cold air.
F_7: represents the events that RAM is not working.

The above events take place only one or several minimal cut set occurs. Hence, the relation between events and minimal cut set can be given by

$F_1= E_1E_2$
$F_2= E_1E_7$
$F_3= E_6+(E_1E_7)$
$F_4= E_1E_2$
$F_5= E_8+ (E_1E_4)$
$F_6= (E_6+(E_1E_7))+ E_8+ (E_1E_4))$
$F_7= E_3+E_4+E_5$

Let, main event computer not functioning is represented by F.
Hence,

$$F= (E_1E_2)+(E_3+E_4+E_5)+ ((E_6+(E_1E_7))+ (E_8+ (E_1E_4)))$$

Hence, the above relation shows that top event takes place only when one or several of them occur.

VI. QUANTITATIVE CALCULATION OF PROBABILITY OF TOP EVENT

The first step in the quantitative evaluation of a fault tree is to find the structural representation of the top event in the terms of the terms of the basic events as done in qualitatively analysis. If the rate of occurrence and fault duration for all basic events are known, and the statistical dependency [6] of each basic event is known (or assumed), then the statistical expectation or probability of the top event can be determined.

For the quantitative evaluation of fault tree of computer system the probability of failures of different components are taken as below:

TABLE I

Sr. No.	Code	Fault	Probability of Failure
1	E_1	Mains Out	0.120
2	E_2	UPS Out	0.095
3	E_3	Dust in RAM	0.080
4	E_4	RAM Damaged	0.040
5	E_5	RAM Misplaced	0.090
6	E_6	Blower Defective	0.070
7	E_7	Genset Out	0.050
8	E_8	Compressor Out	0.860

Using minimal cut set and Boolean algebra [7], the expressions for evaluating the probability of top event of failure P(F) of computer system can be obtained as;

$$P(F) = 1- \prod_{i=1}^{k}[1 - p(k_i)]$$

Where k is the number of minimal cut sets k_i corresponds to the minimal cut set in and $p(k_i)$ is the probability of minimal cut set.

Hence,

P(F)= 1- (1-E_1E_2)(1-E_3)(1-E_4)(1-E_5)(1-E_6)(1-E_1E_7)
(1-E_8)(1-E_1E_4)
= 1-.10154
= .89766

Hence, the fault tree analysis express the inter relation between probability of occurring of fault and minimal cut sets and provides a way to study the root cause of the faults which can be used to improve the reliability [8-11] of computer system.

VII IMPORTANT DEGREE OF PROBABILITY

The change ratio between the probability of top event's and the probability q_i of basic event Xi's (i=1~8) is called the basic event's important degree of probability [12].

$$I_F(i) = \frac{\partial F_S}{\partial q_i}$$

VIII KEY IMPORTANCE

Key importance is change ratio of q_i divided by that of F_S. It balances the importance degree of every basic event with sensitivity and their fault probability. The larger value of key importance is, the top event is more likely to happen [10], thus it is easy to remove some certain faults quickly and take measurements in case of further malfunction or latent danger if key importance is ordered from largest to smallest. Key importance is calculated with formula:

$$I_C\text{(i)}= \frac{q_i}{F_s} I_F(i)$$

TABLE II

Basic Event	Important degree of probability	Key importance
E1	.01827	.00244
E2	.01243	.00132
E3	.11123	.00991
E4	.10711	.00477
E5	.11246	.01128
E6	.11004	.00858
E7	.01235	.00069
E8	.73097	.70031

From table we can conclude:

I_F(8) > I_F (5)> I_F (3) > I_F (6)> I_F (4)> I_F (1)> I_F (2)= I_F (7)
I_C(8) > I_C (5)> I_C (3) > I_C (6)> I_C (4)> I_C (1)> I_C (2)> I_C (7)

The larger I_F (i) is, the more likely top event is to take place , to reduce the probability of top event ,the happening probability of basic event 8,5,3,6,4,1,2,7 should be cut down as much as possible. Considering the significance of key importance , first of all , we should suspect and check the emergence of basic event 8,5,3,6,4,1,2,7 and then carry out the fault diagnosis or adjust control strategy on the basis of the value of $\boldsymbol{I_C}$ (i).

IX. CONCLUSION

Fault tree analysis has been applied to predict the failure probability or failure frequency of computer system in terms of the failure and repair parameters of the system components. A qualitative analysis has been proposed regarding the safety of the system and the identification of critical system elements if the system to be upgraded. Qualitative analysis has been carried out to find all the fault reasons which has been represented by minimal cut sets which is helpful in fault diagnosis or maintaining the computer system. In the work, key importance the statistical expectation or probability of the top event has been determined using quantitative analysis. This express the inter relation between probability of occurring of fault and minimal cut sets and provides a way to study the root cause of the faults which can be used to improve the reliability of the test systems. In the computer system, it is found using quantitative analysis that maximum value of key importance is of compressor. So, to improve the reliability of the computer system the basic event E8 i.e. compressor must be diagnosis firstly to reduce the probability of the fault.

X. REFERENCES

[1] Cao Jinhua, cheng Kan, Introduction of Reliability Mathematics, higher education press, 2006.

[2] H.A. Watson and Bell Telephone Laboratories, “Launch Control Safety Study,” Bell Telephone Laboratories, Murray Hill, NJ USA, 1961.

[3] Dugan J B, Coppit D. developing a low- cost high-quality software tool for dynamic fault tree analysis,IEEE Transaction on Reliability, 2000, 49(1): 49-59.

[4] Chen Kai, Lu Shulan, Li Fengling, reliability mathematics ,JiLin education press, 1989

[5] Xu Renzuo, Reliability allocation for modular software system designed for multiple customers, vol. 20,no.1, pp.5-10. Jan. 1999

[6] Zhang Li., Deng Zhi-liang, “Human errors in complex man-machine systems,” China safety science journal, Transaction on Reliability, vol, 6, Jun1996, pp 35-37.

[7] Hennings, W. and. Kuznetsov, N. Yu, FAMOCUTN and CUTQN “Computer codes for fast analytical evaluation of large fault trees with replicated and negated gates,” IEEE Trans. Reliability, 1995, pp. 368–376.

[8] 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, 28-30 September 2009.

[9] ZHENG Yanyan XU Renzuo State Key Laboratory of Software Engineering of Wuhan University, Wuhan, China “A Human Factors Fault Tree Analysis Method for Software Engineering,” IEEE,2008

[10] Guoyin Liu, Shaofen Lin , Xiaoxia Jiang, Qinglin Chen, Shaohui Liu, “Stimulation Analysis to Marine Crane Hydraulic System reliability Based on Fault Tree,” Ship & Ocean Engineering, 2008,37,(2):71-72.

[11] Schneeweiss W. G., “The Fault Tree Method (in the Fields of Reliability and Safety Technology),” Lilole-Verlag, Berlin 2000.

[12] Rui Quan, Baohua Tan, Shuhai Quan, “Study on Fault Tree Analysis of Fuel Cell Stack Malfunction”, International Conference on Measuring Technology and Mechatronics Automation 2010.