JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)

ARTICLE

Vol.29; No.2. May-August | 2021

Using a Fault Tree Technique to a System Safety Analysis

Ali Salman Abdulkadhim[1]

[1] Babylon Education Directorate, alisalmanabudalk77@gmail.com Babel, Iraq

*Corresponding author email: alisalmanabudalk77@gmail.com

Received: 5/6/2021	Accepted: 27/7/2021	Published: 1/8/2021

Abstract:

In this paper a fault tree technique is used as a system safety analysis, it is a top-down deductive analysis structured in terms of events rather than components. For analysis system safety gates and rules of Boolean algebra are applied to determining cut sets which represents quantitative and qualitative analysis with illustrative examples.

Conclusion:

1.The use of FT technique determines the minimal cut sets of systems which in term is very useful in lowering the maintenance cost for the aim of the safety to make empty from hazards.

2. We can find the reliability of any system and identify the risk areas for that system and through them we can determine the integrity of the system.

3. The most important and commonly used tools of evaluating system reliability is the fault tree method, which can be used to find and analyze the integrity of the system as it gives more accurate and reliable results.

Keywords:

fault tree , cat sets, minimal cut set, path set, safety , safety system , reliability, or-gate , and-gate, event, basic event , top event

Citation:

Ali Salman Abdulkadhim[1]. Using a Fault Tree Technique to a System Safety Analysis. Journal of University of Babylon for Pure and applied science (JUBPAS). May-August, 2021. Vol.29; No.2; p: 234-243.

استخدام تقنية شجرة الأخطاء لتحليل سلامة النظام

علي سلمان عبد الكاظم

[1] **مديرية تربية بابل** alisalmanabudalk77@gmail.com: بابل-العراق

*__Corresponding author email:__ alisalmanabudalk77@gmail.com

Received: 5/6/2021	Accepted: 27/7/2021	Published: 1/8/2021

الخلاصة:

في هذا البحث تم استخدام تقنية شجرة الأخطاء كتحليل سلامة النظام ، وهي عبارة عن تحليل استنتاجي تنازلي منظم من حيث الأحداث بدلاً من المكونات. لتحليل نظام بوابات الأمان وباستخدام قواعد الجبر البولي والتي يتم تطبيقها لتحديد مجموعات القطع التي تمثل التحليل الكمي والنوعي مع أمثلة توضيحية .

الاستنتاجات:

١- يحدد استخدام تقنية شجرة الفشل مجموعات الحد الأدنى من مجاميع القطع للأنظمة والتي تكون مفيدة جدًا على المدى في خفض تكلفة الصيانة بهدف تحقيق السلامة لجعلها خالية من المخاطر.

٢. يمكننا ايجاد موثوقية أي نظام وتحديد مجالات المخاطر لذلك النظام ومن خلالها يمكننا تحديد سلامة النظام.

٣. من أهم أدوات تقييم موثوقية النظام طريقة شجرة الفشل ، والتي يمكن استخدامها لإيجاد وتحليل سلامة النظام لأنها تعطي نتائج أكثر دقة وموثوقية.

الكلمات الدالة

شجرة الفشل , مجاميع القطع , الحد الادنى لمجاميع القطع ,مجاميع المسارات ,السلامة, سلامة النظام ,المعولية , بوابة , بوابة – او ,بوابة – و , الحدث , الحدث البسيط , الحدث الاعلى .

Citation:
Ali Salman Abdulkadhim[1]. Using a Fault Tree Technique to a System Safety Analysis. Journal of University of Babylon for Pure and applied science (JUBPAS). May-August, 2021. Vol.29; No.2; p: 234-243.

1. Introduction

The deficiencies outlined in this paper were alluded to through the system safety study. As we worked in this study to identify and clarify the dangers and undesirable events that are caused by the equipment and machines that are operated in the work environment. We have to draw attention to a very important matter when conducting an analysis. It must determine what are the dangers and risks resulting from friction and interaction of any system with the surrounding environment and what are the dangers that arise at the beginning or during operation and even upon completion or maintenance. A reverse research technique has been chosen to construct the rift trees, which start from small events at the end of the tree that are linked by logic gates, whether (or, and) the use of Boolean algebra when dealing with and calculating them, which we arrange in the form of lower shear groups that link these events according to the logical relationship between them up to the higher event, which is the failure of the system, so that the occurrence of any of these groups, the lower shear, leads to the occurrence of the higher event (system failure). Therefore, work must be done to identify these groups and address them to ensure that they do not occur when the system works. One minimum set of parts has occurred, which in this case is called a single point failure and it also leads to system failure. Safety is defined as the avoidance of conditions that can cause injury, severe damage, loss of life to equipment and possibly the surrounding environment. Thus the main problem here is on washouts which may make integrity hazards. The object is to locate through layout which these washout are possible to occur, to assessment their probability of appearance and to take reformist behavior, some of the failure modes that are difficult to estimate are those related to safety with a low probability of occurrence. A system safety failure is usually caused by a combination of events because of designed safety features with back up or redundancy.

2. Preliminaries

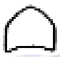
Definition 2.1:[8] Reliability is for the component to perform the tasks and functions required of it for a certain period of time, according to certain controls and conditions.

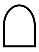
Definition 2.2:[8] A fault tree is a graphical expression of the relationships between vehicles, through which we track the progress of the system steps and lead to the failure of the system.

Definition 2.3:[6] A basic event is a requisite elementary fault event required no more expansion . It is symbol by circle ○

Definition 2.4:[6] Undeveloped event is that event which is not sophisticated This is because it is insufficient in and of itself or that information about it is not available . It is symbol by rhombus ◇

Definition 2.5:[8] An Intermediate is an event that occurs due to a single event or a group of events that are logically related by logical gates, the intermediate event is symbolizes by rectangle ▭

Definition 2.6:[6] The OR – gate It is a device used to indicate whether an outlet event occurs only when one or more input events happen. There are may be more than one of input events to the OR gate which symbolized by 

Definition 2.7:[6] The AND – gate is used to indicate that an output error requires that all input errors occur together. There may be more than two AND gate input errors, which symbolized by 

Definition 2.8:[8] A cut set It is a group of vehicles that, if any of them are removed, there will be no path to the other side

Definition 2.9:[3] A system is a group of vehicles, machines, workers, equipment and programs linked to each other with a specific formation and at any level, whether simple or complex to perform a specific work or an intended production or perform any other task at a specific time.

Definition 2.10:[1] Safety is to stay away and avoid all causes that lead to risks that threaten the safety of the environment, individuals, workers, machines, the work system, facilities and property.

Definition 2.11:[3] System safety is to ensure the application of all safety principles, objectives and techniques and management quality to improve safety within the scope of the operational environment at every stage of that system.

Definition 2.12:[7] Safety analysis is a methodology of procedures that are used for systems analysis, by which all possible risks, safety standards and objectives are identified and evaluated.

Definition 2.12:[7]: It is a measure of the level of decrease in risk given by the safety function. This standard is considered important in industrial facilities, especially nuclear, medical and petroleum.

3. Structure of fault tree and safety

3.1. Structure of fault tree

Since First use of Fault Tree Analysis (FTA) was in 1961 at Bell Telephone Laboratories FT. It is one of the most important techniques, the easiest and the most used in assessing the integrity of the system. In our present time, In the twentieth and twenty-first centuries, Reliability specialists work to create an automatic failt tree in order to provide ready-made fault tree templates in order to assist workers and researchers in order to avoid mistakes in creating a manual breakdown tree and to save time and effort on them. One of the biggest challenges facing reliability researchers in the automation process is not the automation itself. It is the way in which the system is formulated. The way in which events are linked in the fault tree is by logic gates, which are linking those events to the highest event and according to the type of those gates, which have many types according to the type of failure tree, whether dynamic or static

3.2. Structure of safety

To know the safety structure of any system, we must first know the structure of that system, what are its components, the units of that system, how it works, the function required of it, the type of safety that we want to study, and the factors of those safety that are available and which we must provide to it, since determining the type of safety is important to determine the structure of that safety. Directly or indirectly, a large number of accidents are related to the structural specifications of the facilities, laboratories, and workplaces in addition to the availability of safety and security conditions in those facilities, and any breach in these standards or conditions will lead to the occurrence of some injuries and may in some cases lead to death among the personnel of workers or Those in that environment. Thus, one of the most important things that must be provided in work facilities is a good design of the structural aspects of work areas in addition to regular preventive maintenance in those facilities.

4. Applying Fault Tree Technique for Safety System:

There are several methods for calculating the reliability of the fault tree for any system, whether it is for any fault tree, and we are not here to enumerate those methods and therefore we will use any method of calculating that reliability of that tree in order to determine the integrity of the system as the system is what determines what If it is a dynamic fault tree or a static fault tree

Example 1. Consider the fault tree taken from [12] for pressure tank fault tree :

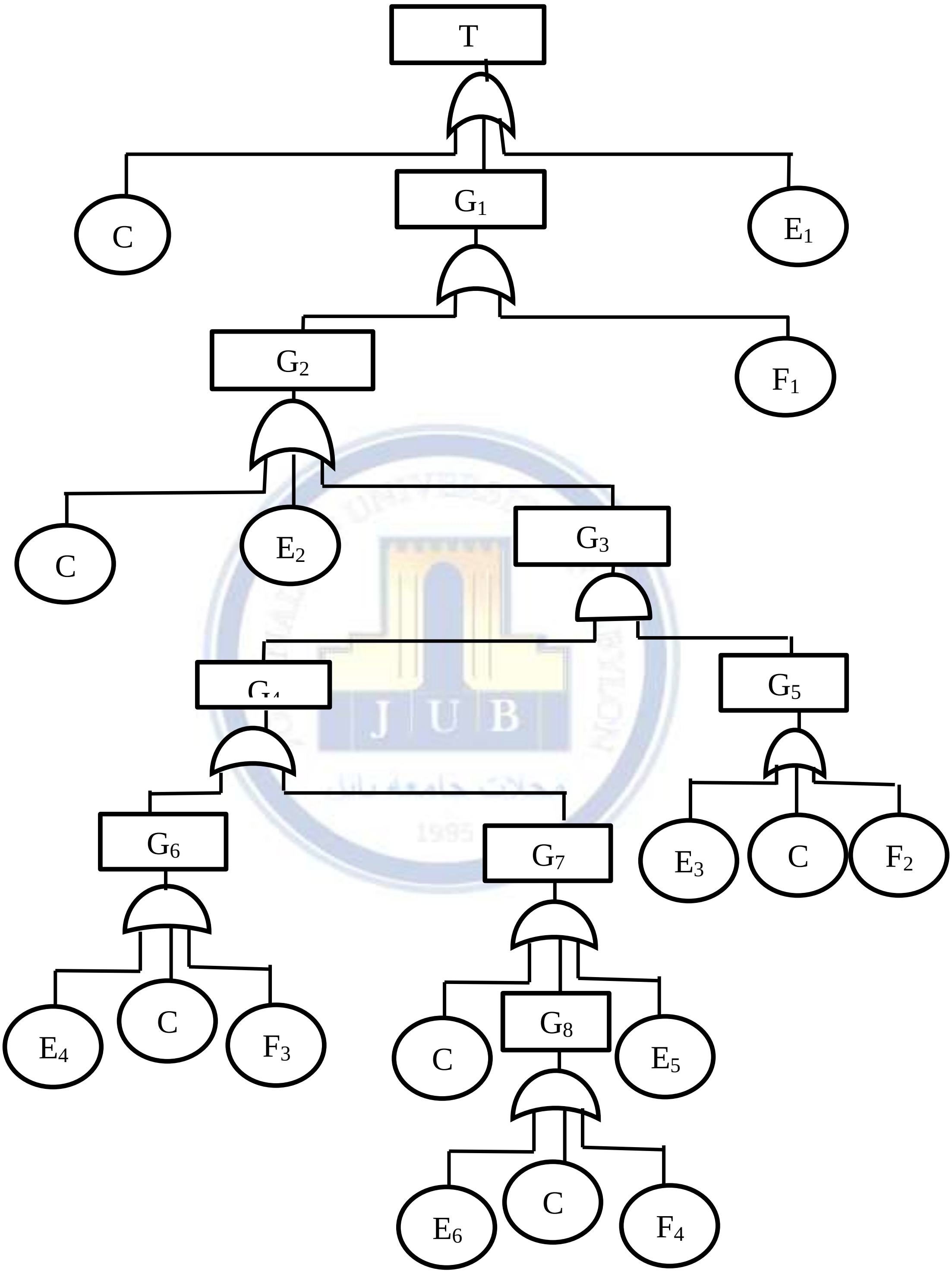


Figure (1) fault tree of pressure tank

So by Boolean algebra rule we find that :

$$T = C_1 + G_1 + E_1,$$

where

$$G_1 = F_1 + G_2$$

$$G_2 = C_2 + E_2 + G_3 \;\Rightarrow\; G_3 = G_4 * G_5$$

$$G_4 = G_6 + G_7 \;\text{ and }\; G_5 = C_3 + E_3 + F_2$$

$$G_6 = E_4 + C_4 + F_3 \;\text{ and }\; G_7 = C_5 + G_8 + E_5$$

$$G_8 = E_6 + C_6 + F_4$$

New by using progressive steps to find every gate neutralization and in sense of distribution law to determine the minimum cut set for each gate

$$G_7 = C_5 + E_6 + C_6 + F_4 + E_5$$

Since $G_4 = G_6 + G_7$, then

$$G_4 = E_4 + C_4 + F_3 + C_5 + E_6 + C_6 + F_4 + E_5.$$

Since $G_3 = G_4.G_5$, then

$$G_3 = (E_4 + C_4 + F_3 + C_5 + E_6 + C_6 + F_4 + E_5)(C_3 + E_3 + F_2).$$

Thus

$$\begin{aligned} G_3 = {} & (C_3E_4) + (C_3C_4) + (C_3F_3) + (C_3C_5) + (C_3E_6) + (C_3C_6) + (C_3F_4) + (C_3E_5) + (E_3E_4) \\ & + (E_3C_4) + (E_3F_3) + (E_3C_5) + (E_3E_6) + (E_3C_6) + (E_3F_4) + (E_3E_5) \\ & + (F_2E_4) + (F_2C_4) + (F_2F_3) + (F_2C_5) + (F_2E_6) + (F_2C_6) + (F_2F_4) + (F_2E_5) \end{aligned}$$

Since $G_2 = C_2 + E_2 + G_3$ then

$$\begin{aligned} G_2 = {} & C_2 + E_2 + (C_3E_4) + (C_3C_4) + (C_3F_3) + (C_3C_5) + (C_3E_6) + (C_3C_6) + (C_3F_4) + (C_3E_5) \\ & + (E_3E_4) + (E_3C_4) + (E_3F_3) + (E_3C_5) + (E_3E_6) + (E_3C_6) + (E_3F_4) \\ & + (E_3E_5) + (F_2E_4) + (F_2C_4) + (F_2F_3) + (F_2C_5) + (F_2E_6) + (F_2C_6) + (F_2F_4) \\ & + (F_2E_5). \end{aligned}$$

Since $G_1 = F_1 + G_2$, then

$$\begin{aligned} G_1 = {} & F_1 + C_2 + E_2 + (C_3E_4) + (C_3C_4) + (C_3F_3) + (C_3C_5) + (C_3E_6) + (C_3C_6) + (C_3F_4) \\ & + (C_3E_5) + (E_3E_4) + (E_3C_4) + (E_3F_3) + (E_3C_5) + (E_3E_6) + (E_3C_6) \\ & + (E_3F_4) + (E_3E_5) + (F_2E_4) + (F_2C_4) + (F_2F_3) + (F_2C_5) + (F_2E_6) \\ & + (F_2C_6) + (F_2F_4) + (F_2E_5). \end{aligned}$$

Thus

$$\begin{aligned} T = {} & C_1 + F_1 + C_2 + E_2 + (C_3E_4) + (C_3C_4) + (C_3F_3) + (C_3C_5) + (C_3E_6) + (C_3C_6) + (C_3F_4) \\ & + (C_3E_5) + (E_3E_4) + (E_3C_4) + (E_3F_3) + (E_3C_5) + (E_3E_6) + (E_3C_6) \\ & + (E_3F_4) + (E_3E_5) + (F_2E_4) + (F_2C_4) + (F_2F_3) + (F_2C_5) + (F_2E_6) + (F_2C_6) \\ & + (F_2F_4) + (F_2E_5) + E_1. \end{aligned}$$

Thus we have five singular vehicle lesser cut sets and twenty four dual lesser cut sets. This is very important for technologists for safety maintenance

Example.2. consider we have FT which was taken from [4]

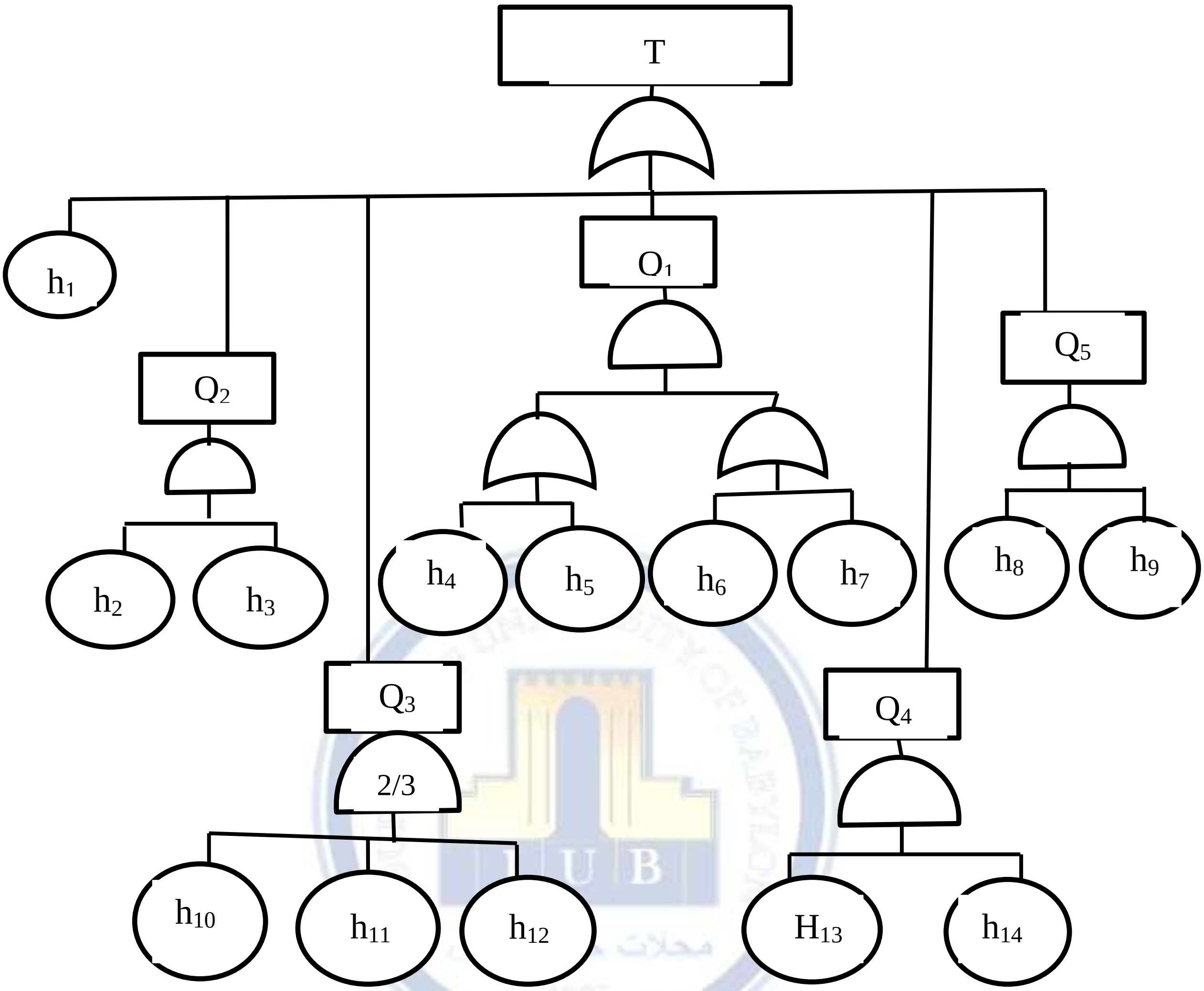


Figure (3) Fault Tree of example (2)

By Boolean algebra rules we find that

$$T = h_1 + Q_1 + Q_2 + Q_3 + Q_4 + Q_5$$

$$Q_1 = (h_4 + h_5)(h_6 + h_7)$$

$$Q_2 = h_2 h_3$$

$$Q_3 = (h_{10} h_{11}) + (h_{10} h_{12}) + (h_{11} h_{12})$$

$$Q_4 = h_{13} h_{14}$$

$$Q_5 = h_8 h_9$$

$$T = h_1 + (h_4 + h_5)(h_6 + h_7) + h_2 h_3 + (h_{10} h_{11}) + (h_{10} h_{12}) + (h_{11} h_{12}) + h_{13} h_{14} + h_8 h_9$$

$$T = h_1 + h_4h_6 + h_4h_7 + h_5h_6 + h_5h_7 + h_2h_3 + h_{10}h_{11} + h_{10}h_{12} + h_{11}h_{12} + h_{13}h_{14} + h_8h_9$$

Therefore the minimal cut sets are

$$h_1\ ,h_4h_6\ ,h_4h_7\ ,h_5h_6\ ,h_5h_7\ ,h_2h_3\ ,h_{10}h_{11}\ ,h_{10}h_{12}\ ,h_{11}h_{12}\ ,h_{13}h_{14}\ and\ h_8h_9$$

Conflict of interests.

There are non-conflicts of interest.

References.

[1] NASA System Safety Handbook "Volume.2: System Safety Concepts, Guidelines, and Implementation Examples" NASA/SP-2014-612 ,Version 1.0 November 2014.

[2] Marvin Rausand "Reliability Of Safety-Critical Systems Theory and Applications" Published by John Wiley & Sons, Inc., Hoboken, New Jersey, 2014.

[3] NASA System Safety Handbook "Volume.1: System Safety Framework and Concepts for Implementation" V.1, NASA/SP-2010-580, Version 1.0, 2011.

[4] M. Sallak , C. Simon and J. Aubry "A Fuzzy Probabilistic Approach for Determining Safety Integrity Level"IEEE Transactions on Fuzzy Systems, Vol.16, No.1, February 2008.

[5] B.S. Dhillon "Applied Reliability and Quality" Springer Series in Reliability Engineering, Springer-Verlag London Limited 2007.

[6] Nikolaos Limnios ,***"Fault Trees"*** ISTEL *td* , 6 Fitzroy Square London WIT5DX .UK , 2007 .

[7] Lars Harms – Ringdahl "Safety Analysis" Taylor and Francis 11. New Fetter Lane, London EC4P4EE,2005.

[8] Srinath L.S. ,"Reliability Engineering ", 4thedtion Affiliated East , (2005),Wast Press Private Limited -New –Delhi.

[9] Hoang Pham "Handbook of Reliability Engineering" Springer-Verlag London Limited 2003.

[10] Air Force System Safety Handbook" designing the safest possible systems consistent with mission requirements and cost effectiveness" Air Force Safety Agency Kirtland AFB NM 87117-5670 Revised July 2000.

[11] Joanne Beachta Dugan , Kevin J. Sullivan, and David Coppit "Developing a Low-Cost High-Software Tool for Dynamic Fault-Tree Analysis" IEEE Transaction on Reliability, vol. 49,no.1, march 2000.

[12] W.E. Vesely , F.F. Goldberg , N.H. Roberts and D.F. Haasl " Fault Tree Handbook" U.S. Nuclear Regulatory Commission.1981.

[13] Felix Redmill " Understanding the Use, Misuse and Abuse of Safety Integrity Levels1" Internet Archive Way back Machine 2017.