Boolean Algebra Application in Analysis of Flight Accidents

Casandra Venera BALAN (PIETREANU)*

*Corresponding author
"POLITEHNICA"of University Bucharest, Aerospace Engineering Department
Polizu Street 1-7, sector 1, Bucharest 011061, Romania
casandra.pietreanu@yahoo.com

DOI: 10.13111/2066-8201.2015.7.4.4

Received: 06 October 2015 / Accepted: 04 November 2015

The 36th "Caius Iacob" Conference on Fluid Mechanics and its Technical Applications
29 - 30 October, 2015, Bucharest, Romania, (held at INCAS, B-dul Iuliu Maniu 220, sector 6)
Section 4. Mathematical Modeling

Abstract: *Fault tree analysis is a deductive approach for resolving an undesired event into its causes, identifying the causes of a failure and providing a framework for a qualitative and quantitative evaluation of the top event. An alternative approach to fault tree analysis methods calculus goes to logical expressions and it is based on a graphical representation of the data structure for a logic - based binary decision diagram representation. In this analysis, such sites will be reduced to a minimal size and arranged in the sense that the variables appear in the same order in each path. An event can be defined as a statement that can be true or false. Therefore, Boolean algebra rules allow restructuring of a Fault Tree into one equivalent to it, but simpler.*

Key Words: *Boolean algebra, fault tree analysis, accident investigation, probabilistic risk assessment*.

1. INTRODUCTION

Various failure modes can be induced by safety issues and the increasing complexity in technological systems. As accident investigation evolves, due to the fact that the causal factors of accidents are complex, they must be broken down into categories.

The attempt to identify all the risks or failures in a system used to be impossible, and it is still a desideratum for engineers.

The quantitative and qualitative approach to risk assessment contributed to the aviation safety, and risk quantification and modeling could establish the influence of individual errors and their probability.

The different types of measures taken in risk analysis are defined using integrated Probabilistic Risk Assessment (PRA) tools. Probabilistic risk assessment (PRA) techniques and Fault tree analysis (FTA), rely on a cause-effect chain, and were developed to link hazards and failures and determine the top event (a specified undesired event) [6]. They are logical, systematic tools used in safety analysis for uncovering weaknesses.

The characteristics of an accident and the link between causes and effects are defined by accident models.

The main types of analytical accident methods are: inductive and deductive.

a.) The inductive methods answer the "What happens if…?" question.

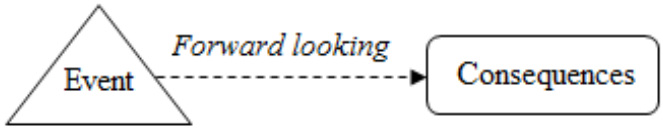

Figure 1. Inductive model

Inductive models assume the existence of a component/condition and analyze the condition's effect. They induce the undesired consequences of an event, define scenarios for an initiating event, and then identify, define and describe the subsequent events linked to the initiating event. Possible failed states and corresponding effect of a condition on the system are determined by this method.

Table 1. Possible failed states and corresponding effect

Component	Failure Probability
A	f_A
B	f_B
.	.
.	.
.	.

Depending on different applications, the probability of failure can be unreliability or failure rate.

The failure probability (F) for the system is: $F = f_A + f_B + \cdots$

b.) The deductive models are able to resolve the causes for an event by deducing them. Reasoning from general to the specific, this method determines in what way the failed state can happen and what are the events that contribute to that. Therefore, an event will be defined by the related causes to be resolved using appropriate logic, until primary causes are identified.

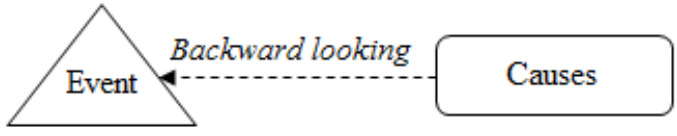

Figure 2. Deductive model

An example of a deductive method is the Fault Tree Analysis, where contributing faults of the accident are built systematically.

2. FAULT TREE ANALYSIS

Causal methods establish the main causes of an accident providing a hierarchical description of the factors and estimating the probability of occurrence of events, and have gone through major stages that especially match the developments in engineering.

The scenarios of failures of events in a complex system/equipment are modeled with logical and probabilistic tools. Reliability and safety analysis are used to define, quantify and describe failures. The failure state of a component/equipment/system can be defined as a

failure mode, which is different from the included process of occurrence (failure mechanism).

The Unreliability (Q) is defined as the probability of failure of a component and equals 1-R (R is the reliability of a component) [6].

$$Q = 1 - e^{-\lambda T}$$

where λ is the component failure rate and T is the component exposure time.

The length of time a component is exposed to failure, called ET (exposure time), can be controlled by testing, monitoring, repair, etc. and has a large effect on the probability calculations used in Fault Tree [6].

$$P = 1.0 - e^{-\lambda T}$$

The basic probability of failure is known and can be directly used for quantification. The combinations of human errors, component failures, environmental factors, etc. can result in an accident that can be broken down into root causes using a Fault Tree [1].

The Fault Tree is a linear method mainly used in failure laws for reliability studies, particularly applied for probability quantification and analysis of risk and maintenance tests. For resolving an undesired event and identify the basic causes, the Fault Tree Analysis uses a deductive process that shows the relationships between events.

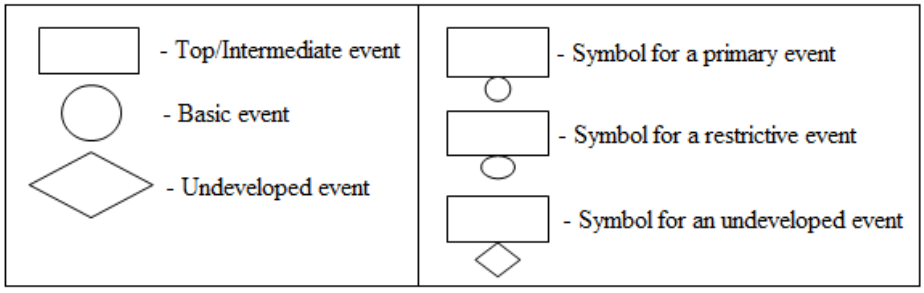

Figure 3. Example of events/ Symbols for primary events

FT provides a method for the cause-effect relationships and is composed of interlinked symbols. A graphic model that displays the combinations of events and the causes of an accident is defined by a fault tree [3]. It can break down an accident into root causes. For example, the crash of an aircraft with loss of lives can be a top event suitable for a fault tree analysis.

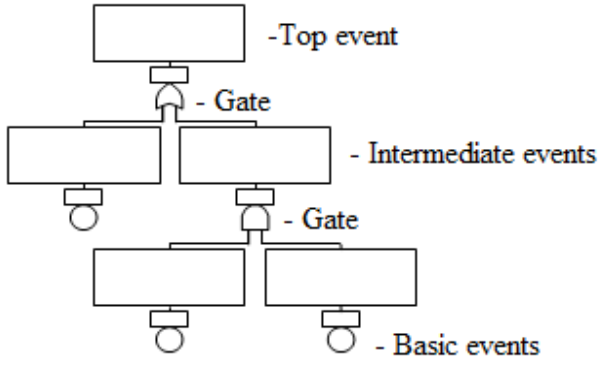

Figure 4. Example of a Fault Tree

Logical event relationships, symbols and diagrams are used in the FTA process to identify the causes of a failure by systematic process. Depending on the relationship between the input events, fault trees can be static or dynamic, meaning they can be insensitive or sensitive to the order of occurrence of events. The combinations of direct and intermediate causes are described with logical operators ("and" and "or") using FT.

The mathematical tools incorporated in FTA are used for critical area focus and the graphical symbols to facilitate analyzing the system from the top down.

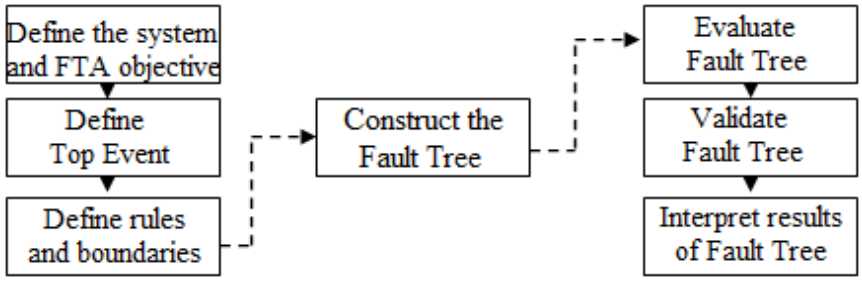

Figure 5. Steps in the construction of a Fault Tree

A FT consists of rectangles or circles blocks that contain binary logic gates and graphical descriptions of failure [7].

This logic and deductive model links the consequence with all the errors, components or subsystems. Basic failures are linked to the top event through intermediate failures.

Starting from the top event, the fault tree determines previous faults by creating an arborescent structure on different levels. FT is backward developed from the end of the system to the top (source), the construction begins at the top, and this iterative process goes through the tree branches. So, in FTA the starting point of the analysis is the end result, linked to immediate causes through logical symbols by a systematic process. When FT only consists of basic events faults that cannot be further developed, we can consider that the limit of the resolution has been reached.

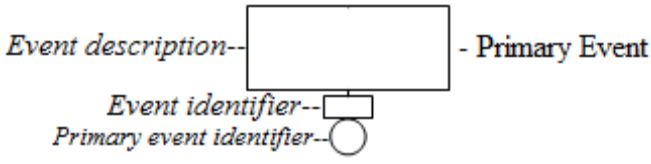

Figure 6. Description of a Primary Event

Establishing the limit and the level of details on a fault tree is given by the failure data existence or the results required, knowing that at the bottom of the FT are the basic events.

The top event has to be properly defined in order to establish a good result and conclusion. By discovering its basic causes, the top event can be resolved. It is usually a system failure and it answers the questions "What?" and "When?", describing the event and the time when it happened. One can understand the gates used in FT by comparing them to electrical switches. They can permit (or inhibit) the passage of the fault logic into the levels of the tree structure. The symbols of the gates show the relationship of the input for the output events, which can be considered as higher and lower events.

Just as the gates represent the outcome of the analysis, events can be seen as inputs for the gates.

The basic types of gates (except the special ones that are particular cases of the two) used in a FT are "AND" and "OR".

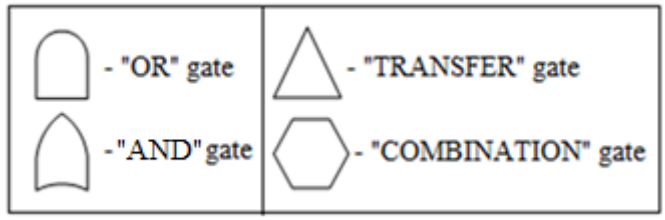

Figure 7. Main gates in a Fault Tree

An event can be resolved into specific causes by using the "OR" gate. This gate creates the union of the inputs; this way, the output occurs if one or more of the inputs occur. So, the input faults for this gate are never all the causes of the output fault. On the other hand, the intersection of the inputs is represented by the "AND" gate. This gate shows that output fault occurs only if all the inputs occur.

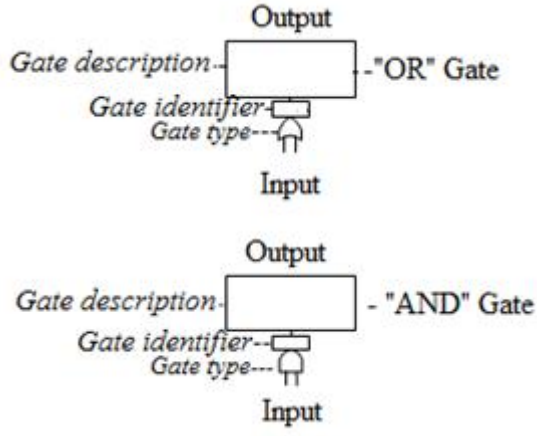

Figure 8. Description of "OR" and "AND" gates in a Fault Tree

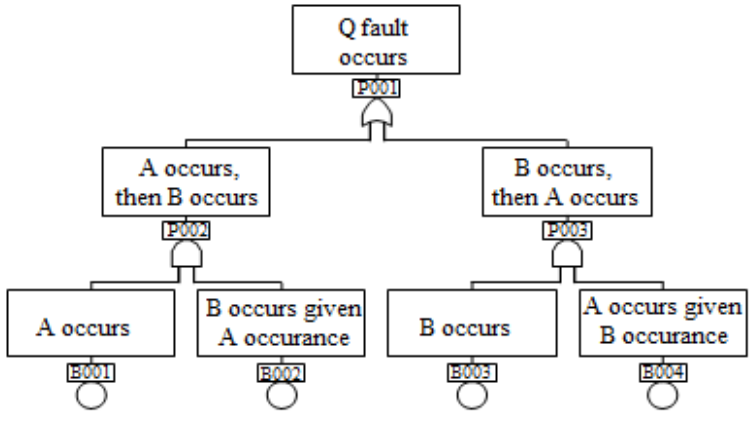

Figure 9. Example of a Fault Tree using "OR" and "AND" gates

Therefore, the gate events presented can be seen and expressed as a logic equation of an input and expressed in terms of basic events through a substitution approach. The basic

(lowest level cause) and the undeveloped events are considered terminating events and define where the analysis stops. A fault tree also contains transfer "IN" and "OUT" gates, presented below.

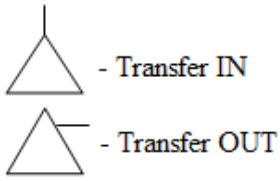

Figure 10. Transfer symbols in a Fault Tree

Transfer IN-the FT continues to develop at the occurrence of "Transfer OUT". Transfer OUT- the level of FT has to be attached to the "Transfer IN".

3. BOOLEAN ALGEBRA APLICATION

A FT consists of: the top event and the intermediate events (causing the pivotal event), linked to basic events through logic gates [1].

As discussed, fault trees make a representation of the causes that must take place for other events to occur, by using logical diagrams. The presented events can be basic ones, called "failures", or can be initiated by other events, in which case they are called "faults". Through gates (inputs and outputs) and specific symbols, this analysis sets links between faults and also between faults and failures [5].The higher event considered is the Output gate, and the so-called lower or basic faults are the Input gates. This way, when defining a fault tree structure, one must go from high to low.

As known, Boolean algebra is defined by union, intersection, and complementation operations, which are represented by different symbols.

The link between Boolean representation and FT analysis can also be defined through this Output and Input gate example, because the links between events (made by the gates) are the same as the Boolean operations. So, in relation to fault trees, algebra rules found in Boolean techniques have a practical importance, because FT is a representation of the links between the faults that caused the event (accident). By translating a FT to equivalent Boolean equations (that defines events in terms of other basic events), one can express the failure of a system through its basic components. Using Boolean rules, the fault Tree can be simplified and reduced. The simplification of the already constructed FT means that algebraic techniques for reduction must be applied in a useful way. This can be achieved only by a good understanding of Boolean rules. Let's take for example a two-input events "OR" gate.

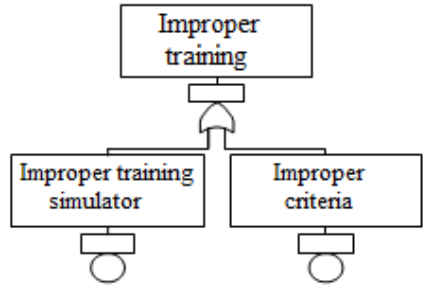

Figure 11. Example of a "OR" gate

The example refers to improper training for pilots, a fault that combined with others, could have led to an event (incident or accident).

This means that in order for the top event ("Improper training") to occur, at least one of the faults ("Improper training simulator" and "Improper criteria") must occur.

So, the Boolean union operation "+" is equivalent to the "OR" gate, therefore, the simplified expression Q=A+B can be successfully used.

Where Q="Improper training", A="Improper training simulator" and B="Improper criteria". Now, considering the probabilities,

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

or using Boolean algebra:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

Furthermore, if the gate has "n" inputs (for example, going on with the case of improper training, another event can be the "Improper interface man-machine", or "Bad abilities of the pilot", or "Insufficient training", etc.), the Boolean expression will be:

$$Q = A1 + A2 + A3 + \ldots + An.$$

So, in this case:

"Improper training"= "Improper training simulator" + "Improper criteria" + "Improper interface man-machine" + "Bad abilities of the pilot"+"Insufficient training" +⋯(and so on). Considering environmental factors, here is an example of an output with 3 inputs referring to: "Turbulence", "The incidence of sunlight" and "Frost".

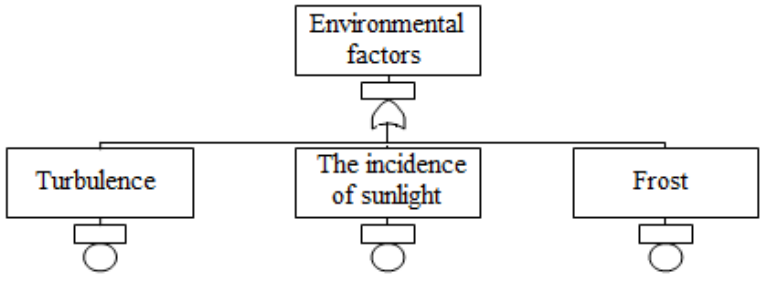

Figure 12. Example of a "OR" gate with 3 inputs

And the examples could go further with 4 outputs, and so on. Below is one that takes in account the risk of inadequate management as a sum of other factors such as "Inadequate evaluation of the risk" + "Wrong evaluation of risk" + "Unpermitted evaluation of risk" + "Subjective evaluation of risk".

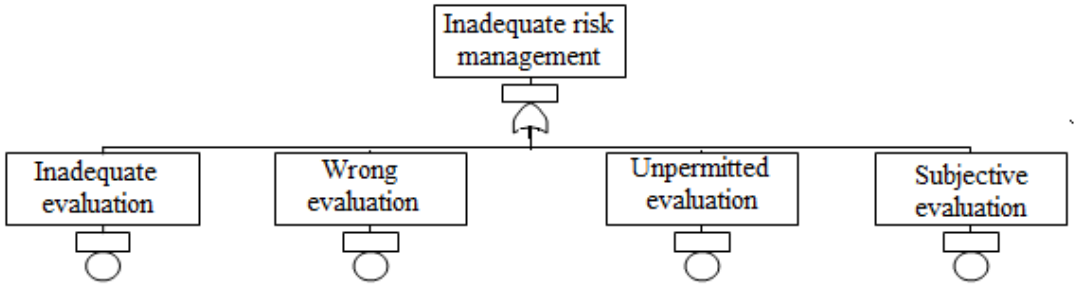

Figure 13. Example of a "OR" gate with 4 inputs

A possible OR gate probability expansion is defined as:

$$P=(\sum 1st\ terms)-(\sum 2nd\ terms)+(\sum 3rd\ terms)-(\sum 4th\ terms)+(\sum 5th\ terms)-\ldots$$

Applied for 3 inputs:

$$P = (P_1 + P_2 + P_3) - (P_{12} + P_{13} + P_{23}) + (P_{123})$$

In order for the fault above the gate to occur, all the input events must be produced when considering a "AND" gate.

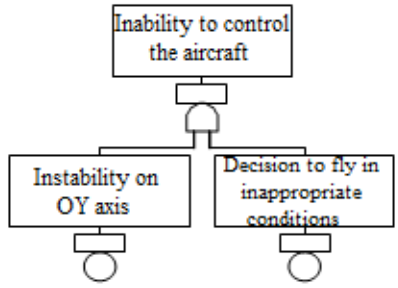

Figure 14. Example of a "AND" gate

This is equivalent to the intersection in Boolean algebra, which has this "·" symbol. So, the top event, Q ("Inability to control the aircraft") will occur if and only if all the basic events ("Instability on OY axis" and "decision to fly in inappropriate conditions") occur, and will have the expression:

$$Q=A\cdot B.$$

And the attached probabilities:

$$P(A\ and\ B) = P(A|B)\ P(B) = P(B|A)\ P(A)$$

that becomes:

$$P(A\cap B) = P(A|B)\ P(B) = P(B|A)\ P(A).$$

Also, if we consider a bigger number of inputs, for example "n", the Boolean expression will have the next form:

$$Q=A_1\cdot A_2\cdot A_3\cdot\cdots\cdot A_n$$

Considering n=3, $Q=A_1\cdot A_2\cdot A_3$. In this case, another input might be "The pilot's inability to stabilize the aircraft". So, the fault tree will be:

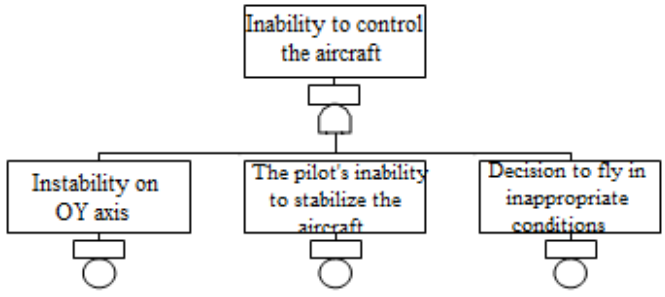

Figure 15. Example of a "AND" gate with 3 inputs

It is also important to take into account that we must consider the rules of a "minimal cut set", which is the sufficient simplest combination of primary events that will cause the

TE (top event) to produce. But, it only one of the elements in the "minimal cut set" will not occur, than the accident (top event) will be avoided. Therefore, different fault trees have different numbers of "minimal cut sets".

4. CONCLUSIONS

In order to obtain combinations that may cause the failure of the system, the probability of failure must be calculated using the probabilities of those causes (components).

FTA is used to investigate and model (potential) faults and to quantify the contribution of these causes to the unreliability of a system.

A fault tree is not a model that describes all the possible causes for system failure; it includes the errors that contribute to reaching the top event that shows a particular failure mode.

The qualitative nature of the FTA and also the quantifying aspect make the model one of the most important and applied linear sequential methods.

So, the logic of a system failure can be understood by developing a FT, which is a descriptive tool that can be evaluated by transforming it to equivalent logic equations in order to obtain different types of information.

For the reduction of a fault tree to its minimum cut sets, Boolean laws and rules can be successfully applied, thus developing an optimized process which is simpler and easier.

Logical expression and representation use graphical methods to define decision diagrams. Managing to reduce sites to minimal while keeping the variables in the same order and path, and obtaining an equivalent and simpler Fault Tree is allowed by using Boolean algebra rules.

Although the importance of linear and sequential methods used in probabilistic risk assessment and safety analysis are well known and defined, moreover, when the process is optimized by using Boolean algebra, the new generation of systemic, nonlinear models create a wider perspective over the accident investigation.

REFERENCES

[1] M. Stamatelatos, *Fault Tree Handbook with Aerospace Applications*, Prepared for NASA Office of Safety and Mission Assurance, NASA Headquarters, Washington, DC 20546, August, 2002.

[2] M. Rausand, *System Analysis, Event Tree Analysis*, Chapter 3, Department of Production and Quality Engineering Norwegian University of Science and Technology, System Reliability Theory (2nded), Wiley, 2004.

[3] J. Marshall, *An Introduction to Fault Tree Analysis (FTA)*, The University of Warwick, Peuss 2011/2012.

[4] W. E. Vesely, F. F. Goldberg, N. H. Roberts and D. F. Haasl, *Fault Tree Handbook*, U.S. Nuclear regulatory Commission, Systems and Reliability Research, Office of Nuclear Regulatory Research, NUREG-0492, Washington, D.C. 20555, 1981.

[5] C. A. Ericson, *Fault Tree Analysis*, September 2000.

[6] E. J. Henley and H. Kumamoto, *Probabilistic Risk Assessment and Management for Engineers and Scientists*, IEEE Press (2nd edition), 1996.

[7] J. Andrews, *Fault Tree Analysis*, Department of Mathematical Sciences Laughborough University, LE11 3TU, UK, 1998.