# On Reliability: A Mathematical Fault Tree

M. S. Fahmy, A. I. Ahmed, M. Khalil

•

Faculty of Engineering, October University for Modern Sciences and Arts (MSA), Egypt.
msfahmy@msa.edu.eg; ahmed.ibrahim22@msa.edu.eg; mkibrahim@msa.edu.eg

### Abstract

*Fault tree analysis (FTA) is a top down approach that was initially used and developed in Bell laboratories in the year 1962 by H Watson and A Mearns for the intercontinental ballistic missile (ICBM) system for the US air force called the Minuteman System. Since then, the technique has been adopted and adapted by many companies who are interested in reliability engineering and dangerous technology. Today FTA is widely used in system safety and reliability engineering, aerospace, nuclear power, chemical and process, pharmaceutical, petrochemical and other high-hazard industries; but is also used in fields as diverse as risk factor identification relating to social service system failure and in software engineering for debugging purposes and is closely related to cause-elimination technique used to detect bugs. Now FTA is considered as one of the most important system reliability and safety analysis techniques. Fault tree analysis has proved to be a useful analytical tool to analyze the potential for system or machine failure by graphically and mathematically representing the system itself. It is a top-down approach that reverse-engineers the root causes of a potential failure through the root cause analysis process. Our main contribution is to develop a mathematical theory of fault tree analysis using some statistical concepts relating to probability of series and parallel systems to set up a mathematical model that represent any hierarchical control system to calculate its reliability for both homogeneous and nonhomogeneous structures. A Fault Tree is a hierarchical model used to analyze the probability that an event will occur. Fault Tree provides all the tools needed to build graphic representations of large-scale problems gracefully so we can use it to set up a mathematical model that represent any hierarchical control system and evaluate its reliability using our general mathematical formula that represent the structure in its two cases. The graphical representation (fault tree diagram) for a hierarchical controlled system enabled us to set up a mathematical general formula that help us to evaluate the reliability of the system in general case (nonhomogeneous structure) and another derived formula for the special case (homogeneous structure). This analysis may help to understand how one or more small failure events lead to a catastrophic failure.*

**Keywords:** Reliability, Mathematical Modeling, Analysis of Fault Tree, Serial and Parallel Systems

## 1. Introduction

Reliability as a state can be a factor of of many parameters; such as, Mean Time To Failure, Reliability, Availability and few others. These terms have been developing over the last six decade. Its evident that such a concept will be portrayed in a structure of system or systems, Barlow in 1973 and Fussel in 1974, discussed the fault tree construction and concept respectively [1 and 2]. In some articles it has been observed that many of the quantities computed by fault tree analysis can also be computed using the concepts and techniques of reliability theory. Henceforth, this paper aims to build and construct an intuitive rigor of understanding reliability in the realm of Mathematical Statistics, in form of a fault tree mathematical model, whereas we aim to introduce the concepts in a matter of detail, building the theory upon prior establishments, and presenting a a general model by the end, incorporating the aforementioned usage of the prior sections. It serves, to add, that general assumptions will be accounted for and discussed, also mentioned when done otherwise. The Introduction section will serve as a block of terms, dissected into multi-topics that adds up to the required definition this paper aims to deliver. For in Section 1 we get to understand what reliability as a concept with their basic definitions. In Section 2 we discuss how system connections influence their reliability, and least in Section 3; We present and elaborate the homogeneity of a system of fault tree representation, giving a derived general model by the end.

## 1.1. Basic Definitions and Concepts

In this section we introduce some basic terms as reliability and its components, as well as its rigor definitions.

### 1.1.1 Reliability: What we quantify as reliable

Reliability purposefulness can be interpreted as; it serves as a developmental method for Engineering. In which it helps in: cost, effort, and time efficiency. It is essential to grasp that reliability is not a property, but a characteristic of an item, in which it is expressed by the probability that the said system will function as expected for a stated time interval [3]. It is usually denoted by R. One can view reliability in other terms, namely, a quantitative approach, as from said approach, the one thing we care about the most, is how long a system stays operational with no interruption. However, this does not imply that redundant parts might not fail, as they can fail and be repaired without causing an operational interruption at system level. Thus, one may conclude that, the concept of reliability can be applied to both repairable and non-repairable systems.

**Definition 1.1** (Reliability)**.** Given $n$ statistical identical systems, which starts into operations at $t = 0$, $\bar{v} < n$ is to accomplish them successfully, where $\bar{v} \in \mathbb{R}^n$.Then, We can write that the ratio $\frac{\bar{v}}{n}$ is a mere random variable which converges to the true value of the reliability as $n$ increases. Namely, $\lim_{n\to\infty} \frac{\bar{v}}{n} = R$: $|\frac{\bar{v}}{n} - R| < \epsilon$

**Definition 1.2** (Reliability)**.** It is the ability of an object (or process or service) to function as expected to fulfil the demanded tasks under given conditions. In other accurate words reliability is the probability a component or system will perform as designed. In which the value would range from [0,1]. reliability is related to failure rate by a simple exponential function: $R = e^{-\lambda t}$ Where $R$ is the reliability, $e$ is the Euler constant, $\lambda$ is the failure rate, and $t$ is the time.

### 1.1.2 Essential Metrics: Basic Definitions

Few Metrics need to be defined in order to be able to calculate the reliability of a system [3, 4, and 5].

**Definition 1.3** (Failure rate ($\lambda$))**.** The frequency of a component failure per unit time, it is an essential metric that is used to calculating either reliability or availability.

$$\lambda = \frac{1}{MTBF} \equiv \frac{1}{MTTF}$$

**Definition 1.4** (Repair rate ($\mu$))**.** The frequency of successful repair operations performed on a failed component per unit time.

$$\mu = \frac{1}{MTTR}$$

**Definition 1.5** (Mean time to failure (MTTF))**.** The average time duration before a non-repairable system component fails.

$$\text{MTTF} = \frac{\sum Hours\ of\ Operation}{\sum Units} \equiv \frac{1}{\lambda}$$

**Definition 1.6** (Mean time between failure (MTBF))**.** The average time duration between inherent failures of a repairable system component.

$$\text{MTBF} = \frac{\sum Hours\ of\ Operation}{\sum Failurs} \equiv \frac{1}{\lambda} \equiv \text{MTTF+ MTTR}$$

## 2. System Types: Analysis

What we are concerned about mathematically, when we are assessing the reliability of a system is its own basic sub-systems. The purpose of this paper, is to detail the explanation to the process, given a system or a network of systems that are adjoined together. The physical layout or rather the connection of the system is of a cruciality to both its functioning, and its reliability.

### 2.1. Series Systems

A network with $N$ systems or blocks in a series link (Figure 1 [3]) where the failure of any one item causes the entire system to fail [3]. As a result, for a series system to perform properly, all of its components must function properly within the time range specified $t$.

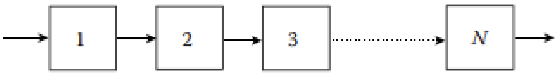

**Figure 1:** *Series System*

**Definition 2.1.** (Reliability of a Series System) The reliability of a system in a series connection is the probability that all $N$ items succeed during its intended interval of time $t$.

$$R_s(t) = R_1(t) \cdot R_2(t) \dots R_N(t) = \prod_{i=1}^{N} R_i(t)$$

A practical conclusion is that the reliability of a series system is always lower than the reliability of any of its components.

We are also concerned with the instantaneous failure rate, one can conclude such an outcome by recalling the definition of $\lambda(t)$:

$$\lambda_s(t) = \frac{-d \ln \prod_{i=1}^{N} R_i(t)}{dt} \equiv \sum_{i=1}^{N} \frac{-d \ln R_i(t)}{dt} \equiv \sum_{i=1}^{N} \lambda_i(t)$$

### 2.2. Parallel Systems

In a parallel arrangement or link, a system failure is caused by the failure of all components, not just one. As a result, the performance of only one unit will be enough to ensure the system's overall success.

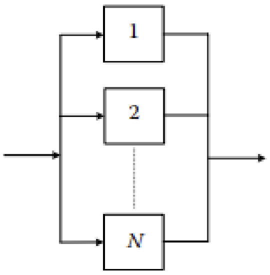

**Figure 2:** *Parallel System*

**Definition 2.2** (Reliability of a Parallel System)**.** For a set of $N$ independent items connected in parallel (Figure 2 [3]), their failure rate is be given by:

$$F_s(t) = F_1(t) \cdot F_2(t) \dots F_N(t) = \prod_{i=1}^{N} F_i(t)$$

Since $R_i(t) = 1 - F_i(t)$

$$R_s(t) = 1 - F_s(t) = 1 - \prod_{i=1}^{N} [1 - R_i(t)]$$

The instantaneous failure rate is still an essential metric, however in parallel configuration, it is not as trivial to come up with one. one can start with the definition that the failure rate is $h(t) = \frac{-d \ln R(t)}{dt}$, yet it will lead to a complicated formula, for instance, let a system of two units with constant failure rate be connected in parallel, their failure rate can be given by;

$$\lambda_s(t) = \frac{\lambda_1 \exp(-\lambda_1 t) + \lambda_2 \exp(-\lambda_2 t) - (\lambda_1 + \lambda_2) \exp(-(\lambda_1 + \lambda_2)t)}{\exp(-\lambda_1 t) + \exp(-\lambda_2 t) - \exp(-(\lambda_1 + \lambda_2)t)}$$

For the same instance, or case; of an $N$ identical units in parallel with a constant failure rate, their reliability can be put to as:

$$R_s(t) = 1 - [1 - \exp(-\lambda t)]^N$$

## 2.3. General Structure

Consider the K-out-of-N system, which is a more general structure of series and parallel systems (Figure 3 [3]). If any combination of K units out of N independent units works in this type of system, the system is guaranteed to succeed. Assume that all units are identical for the sake of simplicity. The likelihood that the system will work is represented by the binomial distribution [7]:

$$R_s(t) = \sum_{r=K}^{N} \binom{N}{r} [R(t)]^r [1 - R(t)]^{N-r} = 1 - \sum_{r=0}^{K-1} \binom{N}{r} [R(t)]^r [1 - R(t)]^{N-r}$$

The majority of practical systems are neither parallel nor series, but rather a blend of the two. Parallel-series systems are a common name for these systems. A complex system that is neither series nor parallel alone, nor parallel-series, is another sort of complex system. Which is referred to as nonparallel-series system (Figure 4 [3]).

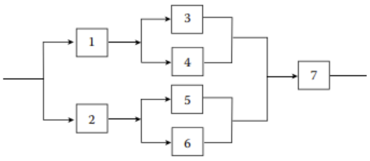

**Figure 3:** *A parallel-series system*

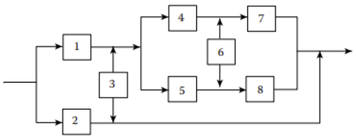

**Figure 4:** *A nonparallel-series system*

## 3. Homogeneity of a System

In this section we discuss the homogeneity of a system in form of a fault tree, where their nodes branching, and rate of distribution affect their reliability. We start by introducing what a fault tree is, then how they are analyzed.

### 3.0.1 Fault Trees and Reliability Block Diagrams

It is important to understand the essential difference between RBDs and fault tree diagrams; RBDs work in success space while, FTDs work in failure space; the FTDs addresses the failure combinations while the RBDs address the success combinations. Also FTDs are traditionally used in analyzing fixed probabilities, while RBDs may include time-varying distributions for the blocks' failure or success, in addition to other properties like restoration or repair distributions [5 and 6].

### 3.0.2 Fault Tree Analysis

Fault Tree Analysis can be explained simply as an analytical technique that describes an undesired state of the system. normally that is in a critical state from a safety standpoint. The system is inspected in the environmental context and operation to extract all credible ways for the undesired event to occur [3,4, and 5]. It is also important to point out that a fault tree is a graphic model of the different sequential and parallel combinations of faults that will happen in the investigated model. In fact, using the model of fault tree is more convenient to deal with, because it is qualitative model that enable us to evaluate it quantitatively and do not change the qualitative nature of the model itself.

## 3.1. Homogeneous and Non-homogeneous systems: Analysis

The homogeneity of a system influences the reliability of the whole system [3] and that can be seen evident in a fault tree, where some demonstrate a homogeneous structure, and some do not. We represent in Figure 5 the model of general fault tree, and define how said figure can be interpreted to be homogeneous or non-homogeneous.

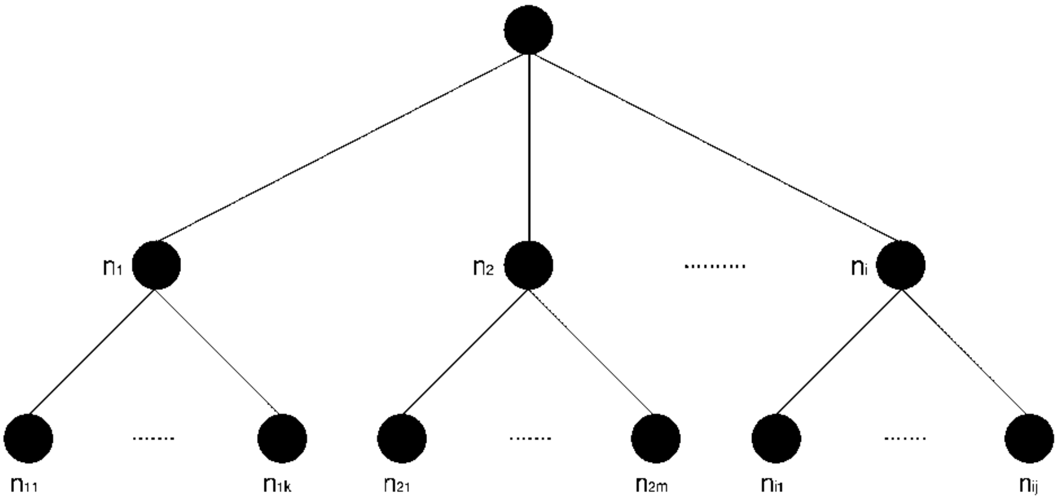

**Figure 5:** *Generic Tree*

**Definition 3.1** (Homogeneity of a tree)**.** A tree is said to be homogeneous if and only if, the number of its sub nodes is equal to the number of every other sub node on any level from the root. Mainly, $n_{1k} = n_{2m} = n_{ij}$

**Definition 3.2** (Non-Homogeneity of a tree)**.** A tree is said to be non-homogeneous if and only if, the number of its sub nodes is not equal to at least one other sub node on any level from the root. Mainly, $n_{1k} \neq n_{2m} \neq n_{ij}$

### 3.2. General Case

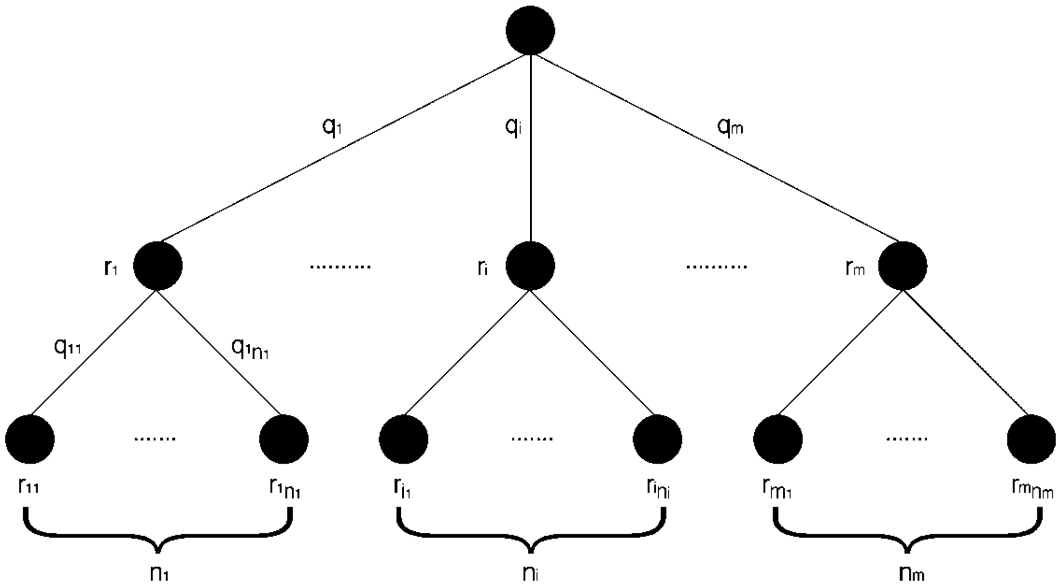

**Figure 6:** $\varphi$ *— Tree*

In Figure 6, let $P_0$ be the reliability of the root; $q_1, \ldots, q_m$ are to be the reliability of the edges, and $r_1, \ldots, r_m$ be the reliability of the nodes of the first level, where $m$ is the number of nodes of the first level; $q_{i_1}, \ldots, q_{in_i}$ be the reliability of edges of second level in the $i$-th subtree; $r_{i_1}, \ldots, r_{in_i}$ be the reliability of nodes of the second level in the i-th subtree, where $n_i$ is the number of edges (nodes) in the $i$-th subtree. It goes evident to see that the number of leaves is equal to $N$, where; $N = n_1 + n_2 + \ldots + n_m$ such that $n_1 \leq n_2 \leq \ldots \leq n_m$ . For the purpose of generality, consider that an arbitrary path from the root to the end is unfailing (successful), if all nodes and edges on said path is unfailing (successful). Now we find the reliability of the tree ($\varphi$) through $V$ paths, throughout the derivation such reliability is detonated $\wp(\varphi; V)$; where; $V = 1, 2, \ldots, N$. $N \in \mathbb{N}$-$\{0\}$.

**Theorem 1.**

$$\wp(\varphi; V) = P_0 \times \sum_{k=0}^{m} \sum_{\substack{A, A \subset \{1,\ldots,m\} \\ |A|=k}} \left[ \prod_{i \in A} \left( 1 - P_i \left( 1 - \prod_{j=1}^{n_i} (1 - P_{ij}) \right) \right) \right] \times$$

$$\left[ \sum_{\substack{a_1+\ldots+a_m=V \\ i \in A \implies a_i=0}} \Bigg( \prod_{i \notin A} (P_i \times \Bigg( \sum_{\substack{B, B \subset \{1,\ldots,n_i\} \\ |B|=a_i}} \Bigg( \prod_{j \in B} P_{ij} \times \Bigg( \prod_{\substack{j \notin B \\ 1 \leq j \leq n_i}} (1 - P_{ij}) \Bigg) \Bigg) \Bigg) \Bigg) \right]$$

Where:

$$P_i = r_i q_i, P_{ij} = r_{ij} q_{ij}, i = 1, \ldots, m \quad i \leq j \leq n_j$$

$$\prod_{\phi} = 1, \quad \sum_{\phi} = 0$$

**Proof.**
We proof the theorem by showing that the probability of failure throughout all paths from the

root to the $i$-th subtree with $n_i$ nodes is equal to

$$1 - P_i \left( 1 - \prod_{j=1}^{n_j} \left(1 - P_{ij}\right) \right)$$

The reliability of the fault tree through exactly a paths (1$\leq a \leq$n$_i$) from the root to the $i$-th subtree is equal to

$$P_i \times \left( \sum_{\substack{B, B \subset \{1,\ldots,n_i\} \\ |B| = a_i}} \left( \prod_{j \in B} P_{ij} \times \left( \prod_{\substack{j \notin B \\ 1 \leq j \leq n_i}} \left(1 - P_{ij}\right) \right) \right) \right)$$

Further we remark that the event of having exactly V paths to operate successfully is considered the sum of all mutually exclusive events of the types; there are exactly $a_1$ paths operate simultaneously successfully ending in the first subtree, $a_2$ paths operate simultaneously successfully ending in the second subtree, and $a_m$ paths operate simultaneously successfully ending in the $m$-th subtree; where $a_1 + a_2 + \ldots + a_m = V$. From here it follows

$$\wp(\varphi; V) = P_0 \times \left( \sum_{\substack{a_1 + \ldots + a_m = V \\ 0 \leq a_j \leq n_j}} \prod_{i=1}^{m} \Omega(i, a_i) \right)$$

where

$$\Omega(i, a_i) = \begin{cases} 1 - P_i \left( 1 - \prod_{j=1}^{n_j} \left(1 - P_{ij}\right) \right) & a_i = 0 \\ P_i \times \left( \sum_{\substack{B, B \subset \{1,\ldots,n_i\} \\ |B| = a_i}} \left( \prod_{j \in B} P_{ij} \times \left( \prod_{\substack{j \notin B \\ 1 \leq j \leq n_i}} \left(1 - P_{ij}\right) \right) \right) \right) & a_i \neq 0 \end{cases} \qquad \blacksquare$$

### 3.3. Special Case

For the special case that the system behaves in a homogeneous matter as per Definition 3.1. Namely, this implies that: $q_1 = q_2 = \ldots = q_m = q_0$, and for the second level operating on the same type and identical conditions: $q_{11} = \ldots = q_{1n_1} = q_{21} = \ldots = q_{2n_2} = \ldots = q_{m1} = \ldots = q_{mn_m} = q_1$. It trivially follows that $r_{11} = \ldots = r_{1n_1} = r_{21} = \ldots = r_{2n_2} = \ldots = r_{m1} = \ldots = r_{mnm} = r_1$, and $n_1 = n_2 = \ldots = n_m = n$.
By transforming the formula of Theorem 1, by change of assertions; namely: $P_1 = P_2 = P_m = q_0 r = p_1; P_{11} = P_{12} = \ldots = P_{m_1} = \ldots = P_{mn_m} = q_1 r = p_2$.
Let $\wp(\ \varphi_1\ ;\ V)$ denote the reliability of such case, from Section 2.3 it follows:

**Corollary 1.**

$$\wp(\ \varphi_1\ ;\ V) = p_0 \times \sum_{k=\left\lceil \frac{V}{n} \right\rceil}^{m} \left\{ \binom{m}{k} \times p_1^k \times \left[1 - p_1 \times \left(1 - (1 - p_2)^n\right)\right]^{m-k} \times \binom{k \times n}{V} \times p_2^V \times (1 - p_2)^{(k \times n) - V} \right\}$$

Where; $\binom{m}{k} = \frac{m!}{k!(m-k)!}$ And $\left\lceil \frac{V}{n} \right\rceil$ is the smallest integer greater than $\frac{V}{n}$

## 4. Conclusion

A theoretical study is introduced for a mathematical model that can describe a hierarchical control system (homogeneous and non-homogeneous) in order to evaluate its reliability. This investigation of the reliability is highly suitable for study of many Engineering applications ranging from industrial process control, through production management to Economic and other systems.

## References

[1] Barlow, E. (1973). Introduction to Fault Tree Analysis. Research Air Force Systems Command.

[2] Fussell, J. B. (1974). Fault Tree Analysis - Concepts and Techniques. Nato Advanced Study Institute On Generic Techniques Of System Reliability Assessment, Nordhoff Publishing Company.

[3] Rausand, M., Hyland, A. (2004). System Reliability Theory: Models, Statistical Methods, and Applications (2nd ed.). Wiley.

[4] Epstein, Weissman. (2009). Mathematical Models for Systems Reliability. CRC Press.

[5] Mavko, B., V., A., Marko, C. (2009). Application of the fault tree analysis for assessment of power system reliability (Vol. 94). Reliability Engineering System Safety.

[6] Curcuru, G., Galante, G. M., La Fata, C. M. (2013). An imprecise Fault Tree Analysis for the estimation of the Rate of Occurrence Of Failure. J Loss Prev Process Ind.

[7] Carpitella, S., Certa, A., Izquierdo Sebastin, J., La Fata, C. M. (2018). k-out-of-n systems: an exact formula for the stationary availability and multi-objective configuration design based on mathematical programming and TOPSIS. Journal of Computational and Applied Mathematics.