Theory and Methods for Calculating Probability of Hazardous Events

by Vito Faraci, Jr., Greenlawn, New York

Calculating the probability of "undesirable events" very often involves analyzing the various ways equipment can fail. Today, Fault Tree Analysis (FTA) is by far the most commonly used tool for qualitative and quantitative risk analyses. FTA was introduced in 1962 at Bell Labs, and for about 20 years it was the *de facto* standard of the engineering community.

"Markov techniques give us the ability to more accurately calculate solutions to non-combinatorial problems."

Starting in the early 1980s, a group of NASA mathematicians performed studies that clearly exposed some very subtle FTA limitations. In an effort to overcome these limitations, NASA developed algorithms using Markov Analysis (MA), a sub-topic of Probability, designed not necessarily to replace but to support FTAs. With respect to Reliability and Risk Assessment, the integration of MA with FTA has been a giant step forward. Engineers can now more accurately solve a much larger set of "Risk" problems than they could before.

MA was introduced in 1907 by Russian mathematician A.A. Markov. It is interesting to note that although this knowledge has been around for some time, it is only recently that the engineering community has taken advantage of this science. For example, within the past three years, NASA has been employing Markov methods for Probabilistic Risk Assessments for the Space Shuttle systems, and FTA and reliability software manufacturers have integrated Markov techniques into their risk assessment software programs.

Because of the lack of documentation written in a clear, common language, knowledge of Markov Analysis still remains a little sketchy within the engineering community. This article is not intended as a "how to solve" tutorial, even though it will reveal some such details. Its objective is simply to raise the level of awareness of Markov Analysis, what it is, why it is required, and what it does.

Constant Failure Rate Devices

Failure characteristic of constant failure rate devices

Assume 100 devices, all operating at time t = 0.
Probability of success = $P_s = e^{-\lambda t}$
Probability of failure = $P_f = 1 - e^{-\lambda t}$
where e = 2.71828, λ = constant failure rate, t = time.

Note that the percentage of device failures is the same for each time interval. This is the telltale characteristic of a constant failure rate.

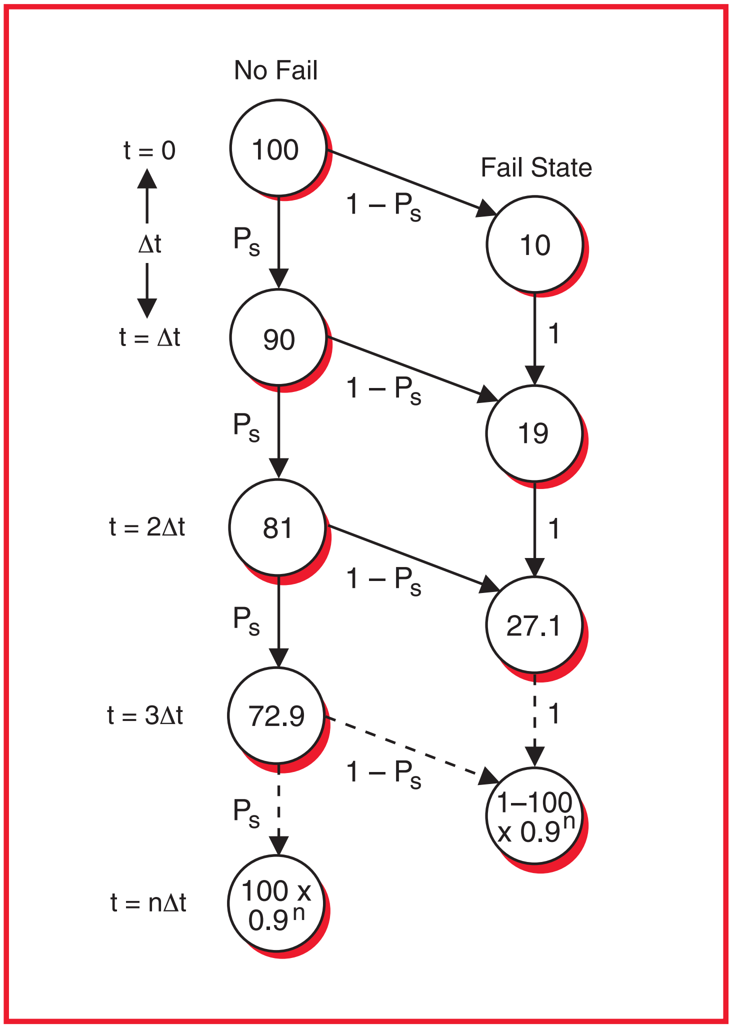


Figure 1 — Failure characteristic of constant failure rate devices.

Non-Constant Compared with Constant Failure Rate Devices

The following is only one example of a probability of failure (P_f) of a non-constant failure rate device. In this case, the device exhibits a "normal" distribution of failure.The P_f of this device is a "non-integrable" function that needs to be treated in a separate discussion involving non-constant failure rate devices.

$$P_f = \frac{1}{s\sqrt{2\pi}} \int_0^t e^{-\left(\frac{(x-u+hl)^2}{2s^2}\right)} dx$$

Here, u = mean time to failure, s = standard deviation, hl = hours previously logged, and t = time.

Unlike constant failure rate devices, the probability of success for these devices will not be constant for equal time intervals. Furthermore, the mathematics required for solving P_f for these devices is more complex, as can be deduced by comparing the above equation with that of a constant failure rate equation $P_f = 1 - e^{-\lambda t}$.

The P_f vs. Time graph in Figure 2 compares a constant failure rate device (Electrical) with a non-constant failure rate device (Mechanical), both having the same Mean Time Between Failure (MBTF).

Combinatorial vs. Non-Combinatorial Logic

Combinatorial Logic

a) Two or more input states define one or more output states. Output states are related by defined rules that are independent of previous states.

b) Logic depends solely on combinations of inputs.

c) Time is neither modeled nor recognized.

d) Outputs change when inputs change, irrespective of time.

e) Output is a function of, and only of, the present input.

Non-Combinatorial Logic (Sequential Logic)

Logic of output(s) depends on combinations of present input states, and combinations of previous input states. In other words, non-combinatorial logic has memory while combinatorial logic does not. Engineers commonly refer to this as sequential logic.

Fault Tree Advantages:

a) Acts as a visual tool that can be used to pinpoint system weaknesses.

b) Exhibits clear representation of logical processes that lead to a system or subsystem failure (clear, qualitative representation of failure propagation).

c) Reveals relatively simple equations for P_f calculations yielding quantitative analyses that do not require high-powered math.

d) Proves to be a very effective tool for the fault isolation process.

Fault Tree Limitations:

The following is an excerpt from Aerospace Recommended Practices ARP4761 Issue 1996-12:

> *a) Difficult to allow for transient & intermittent faults or standby systems with spares.*
>
> *b) If a system has many failure conditions, separate fault trees may need to be constructed for each one.*
>
> *c) Difficult to represent systems where failure rates or repair rates are state dependent.*

The following is an excerpt from NASA Ref. Publication 1348:

> *Traditionally, the reliability analysis of a complex system has been accomplished with combinatorial mathematics. The standard fault-tree method of reliability analysis is based on such mathematics. Unfortunately, the fault-tree approach is somewhat limited and incapable of analyzing systems in which reconfiguration is possible. Basically, a fault tree can be used to model a system with:*
>
> *1. Only permanent faults (no transient or intermittent faults)*
>
> *2. No reconfiguration*
>
> *3. No time or sequence failure dependencies*
>
> *4. No state-dependent behavior (e.g., state-dependent failure rates)*

Why Markov?

The following is another excerpt from ARP4761 Issue 1996-12:

> *a) MA does not have these limitations.*
>
> *b) Sequence dependent events are included and handled naturally.*
>
> *c) Covers a much wider range of system behaviors.*

Close examination of the above excerpts reveals the practical answer to the "Why Markov" question. It basically has to do with combinatorial vs. non-combinatorial type problems. FTA methods can only approximate and cannot precisely calculate solutions to non-combinatorial type problems. Markov techniques give us the ability to more accurately calculate solutions to non-combinatorial type problems.

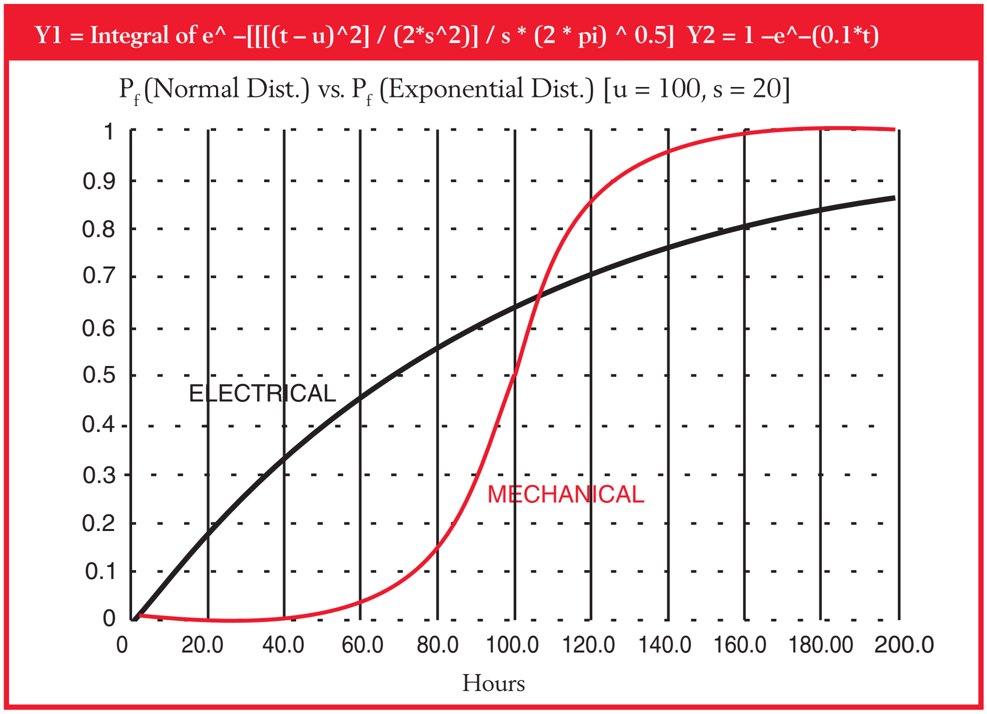


Figure 2 — P_f vs. Time, comparing a constant failure rate device with a non-constant failure rate device.

Some Pros and Cons:
Fault Tree Analysis handles combinatorial type problems extremely well, both qualitatively and quantitatively. However, FTA has difficulty with non-combinatorial problems in both areas.

Markov Analysis handles non-combinatorial as well as combinatorial problems. However, it may not be quite as intuitive as FTA, and usually requires some higher power math for the quantitative analyses.

Introduction to Markov Analysis

If a system or component can be in one of two states (i.e., failed, non-failed), and if we can define the probabilities associated with these states on a discrete or continuous basis, the probability of being in one or the other at a future time can be evaluated using a state-time analysis. In reliability and availability analysis, failure probability and the probability of being returned to an available state are the variables of interest. The best known state-space technique is Markov Analysis.

Markov Analysis Compared with FTA

Although there is no need for Markov in solving combinatorial type problems (FTA handles them well enough), the next few examples will compare Markov Analysis and FTA for the sake of illustration.

Note: For purposes of simplification, the following comparison examples will be limited to “constant failure rate” type problems. Solutions to “non-constant failure rate” type problems require somewhat different techniques and will be discussed separately.

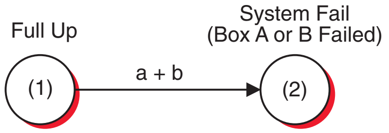
Combinatorial Type Problems

Two Components in Series (Combinatorial):
Two black boxes start operation at the same time. Box A has failure rate a, and Box B has failure rate b. Successful system operation requires that both Box A and Box B be functional. Find P_f = Probability of System Failure.

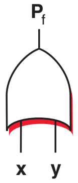
Here, Full Up State = all devices operating, (n) = State Number, and P(n) = Probability of State (n).

Markov Model

FTA Approach



$P_f = P(2) = 1 - e^{-(a+b)t}$



$x = 1 - e^{-at}$ $y = 1 - e^{-bt}$

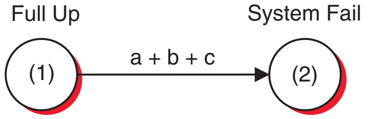
$P_f = x + y - xy = 1 - e^{-(a+b)t}$

Note that the solutions are identical for both methods.

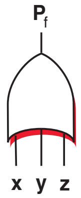
Three Components in Series (Combinatorial):
Three black boxes start operation at the same time. Boxes A, B and C have failure rates a, b and c, respectively. Successful system operation requires that all three boxes be functional. Find P_f = Probability of System Failure.

Markov Model

FTA Approach



$P_f = P(2) = 1 - e^{-(a+b+c)t}$



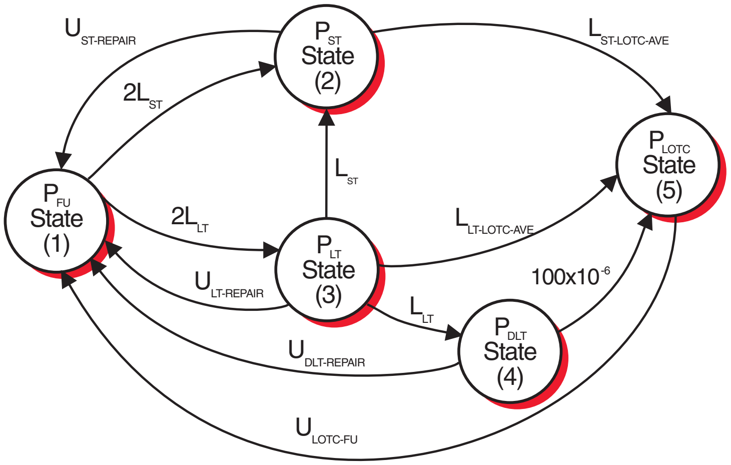
$x = 1 - e^{-at}$ $y = 1 - e^{-bt}$ $z = 1 - e^{-ct}$

$P_f = x + y + z - xy - xz - yz + xyz$

$= 1 - e^{-(a+b+c)t}$

Note again the identical solutions.

Two Components in Parallel (Combinatorial):
Two black boxes start operation at the same time. Box A has failure rate a, and Box B has failure rate b. Successful

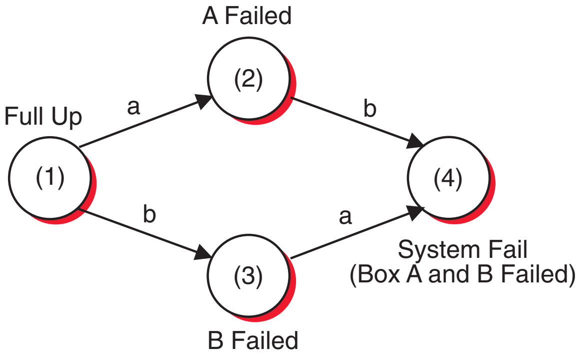


Example Markov State Diagram:
Represents various system states.
Transition rate is function of failure or repair rate.
States are mutually exclusive.
The sum of the probabilities must equal 1.

Figure 3 — Example Markov state diagram.

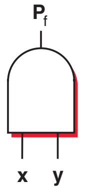
system operation requires that Box A or Box B or both be functional. Find P_f .

Markov Model (2 in Parallel)



$$P_f = P(4) = (1 - e^{-at})(1 - e^{-bt})$$

FTA Approach

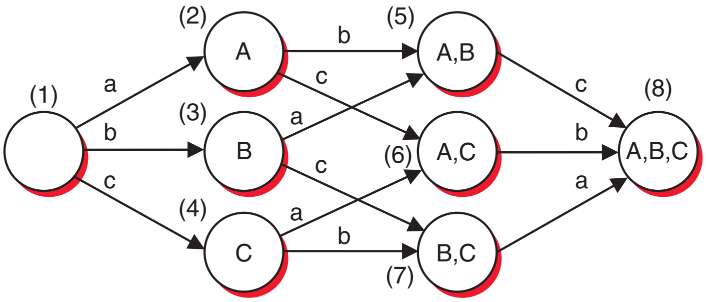


$$x = 1 - e^{-at} \qquad y = 1 - e^{-bt}$$
$$P_f = xy = (1 - e^{-at})(1 - e^{-bt})$$

Three Components in Parallel (Combinatorial)

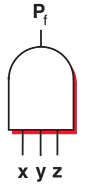
Three black boxes start operation at the same time. Boxes A, B and C have failure rates a, b and c, respectively. Successful system operation requires that Box A, B or C be functional. Find P_f.

Markov Model (3 in Parallel)



$$P_f = P(8) = (1 - e^{-at})(1 - e^{-bt})(1 - e^{-ct})$$

FTA Approach



$$x = 1 - e^{-at} \qquad y = 1 - e^{-bt} \qquad z = 1 - e^{-ct}$$
$$P_f = xyz = (1 - e^{-at})(1 - e^{-bt})(1 - e^{-ct})$$

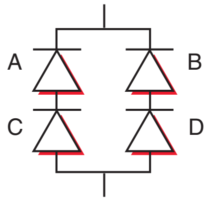
Again, the results are identical for this combinatorial type problem.

Fault-Tolerant Diode Circuit, Probability of Short Circuit (Combinatorial):

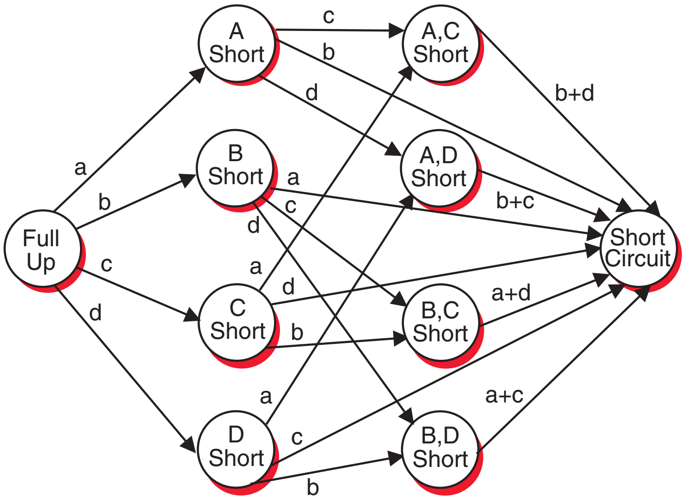
The diode circuit below is a model of a fault-tolerant diode configuration. The two possible failure modes for a diode are a SHORT circuit or an OPEN circuit. The failure rate for the SHORT mode (assuming identical diodes) is l. Derive the equation for the probability of a "Short Circuit."

Let a, b, c and d = failure rates of failure mode SHORT for diodes A, B, C and D, respectively.

Diode Circuit

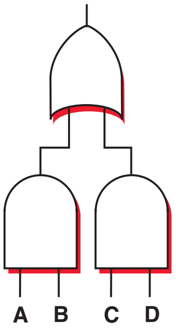


Markov Model



If A = B = C = D = $(1 - e^{-\lambda t})$ then $P_{Short} = 1 - [1 - (1 - e^{-\lambda t})^2]^2$.

FTA Approach



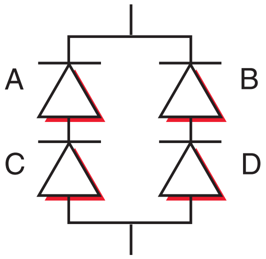
$$P_{Short} = 1 - [1 - (1 - e^{-\lambda t})^2]^2$$

Note that Markov and FTA results are the same, since this is a combinatorial problem.

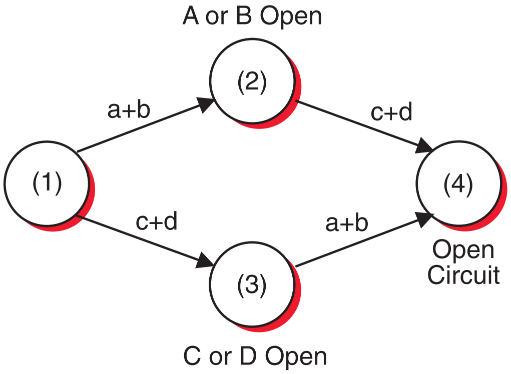
Fault-Tolerant Diode Circuit, Probability of Open Circuit (Combinatorial):
The diode circuit below is a model of a fault-tolerant diode configuration. The two possible failure modes for a diode are a SHORT circuit or an OPEN circuit. The failure rate for the SHORT mode (assuming identical diodes) is l. Derive the equation for the probability of a "Short Circuit."

Let a, b, c and d = failure rates of failure mode OPEN for diodes A, B, C and D, respectively.

Diode Circuit

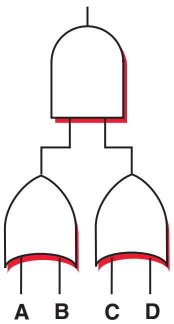


Markov Model (Diode Open)



If A = B = C = D = (1 – e$^{-\lambda t}$) then $P_{\text{Open}} = (1 - e^{-2\lambda t})^2$.

FTA Approach



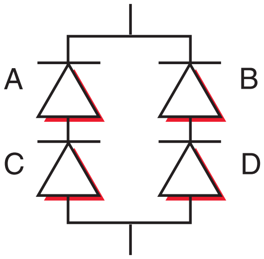
$P_{\text{Open}} = (1 - e^{-2\lambda t})^2$

Note that Markov and FTA results are the same, since this is a combinatorial problem.

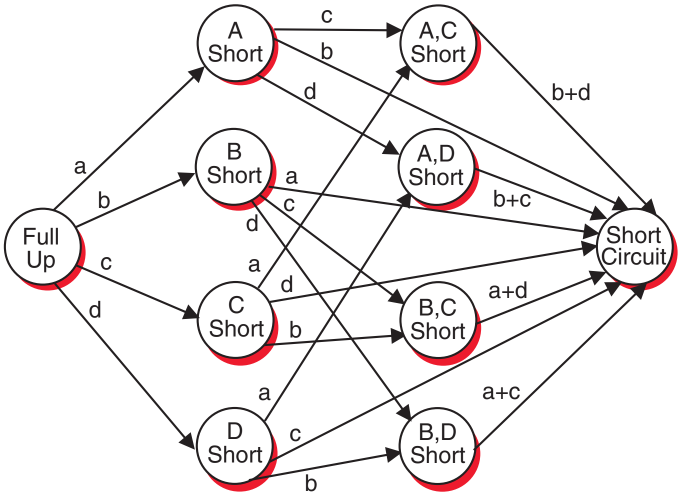
Fault-Tolerant Diode Circuit, Probability of Short Circuit (Combinatorial):
The diode circuit below is a model of a fault-tolerant diode configuration. The two possible failure modes for a diode are a SHORT circuit or an OPEN circuit. The failure rate for the SHORT mode (assuming identical diodes) is l. Derive the equation for the probability of a "Short Circuit."

Let a, b, c and d = failure rates of failure mode SHORT for diodes A, B, C and D, respectively.

Diode Circuit

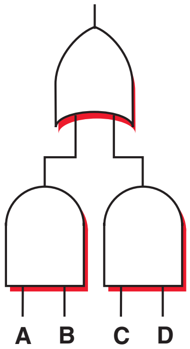


Markov Model (Diode Short)



If A = B = C = D = (1 – e$^{-\lambda t}$) then $P_{\text{Short}} = 1 - [1 - (1 - e^{-\lambda t})^2]^2$.

FTA Approach



$P_{\text{Short}} = 1 - [1 - (1 - e^{-\lambda t})^2]^2$

Note that Markov and FTA results are the same, since this is a combinatorial problem.

Non-Combinatorial Type Problems

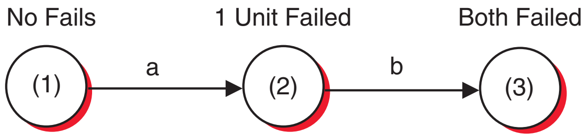
Solutions to non-combinatorial problems require techniques other than traditional combinatorial logic such as that found in FTAs. One non-combinatorial type problem that has intrigued mathematicians for quite some time is the classic “Standby Problem.”

Note: For purposes of simplification, the following comparison examples will be limited to “constant failure rate” type problems. Solutions to “non-constant failure rate” type problems require somewhat different techniques, and thus require a separate discussion.

Two Components Standby Redundant (Non-Combinatorial):

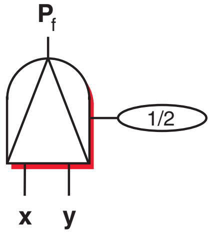
Box A has failure rate a, and Box B has failure rate b. Box A is powered on while Box B remains off. Immediately upon detection of Box A failure, Box B is powered on. Calculate the probability that both boxes fail.

Markov Model (Standby)



$$P(3) = \frac{b}{a-b}(e^{-at}) - \frac{a}{a-b}(e^{-bt}) + 1$$

FTA Approach



$$x = 1 - e^{-at} \qquad y = 1 - e^{-bt}$$

$$P_f = \lambda xy = \lambda(1 - e^{-at})(1 - e^{-bt})$$

This problem is another example of sequence failure dependency, and therefore a non-combinatorial type problem. Note again that the FTA results are having difficulty tracking the Markov solution. For the first 10 hours, the solutions are almost identical, as shown in Figure 4. However, as shown in Figure 5, the FTA error becomes quite apparent as t gets large.

In this example, the MA results are larger than FTA. However, it is important to note that this is not always the case. In other problems, FTA results will exceed MA. In other words, the results can go either way.

Two Components in Parallel with Required Order Factor (ROF) (Non-Combinatorial):

a. What is the probability that both boxes fail *and* that A fails before B?

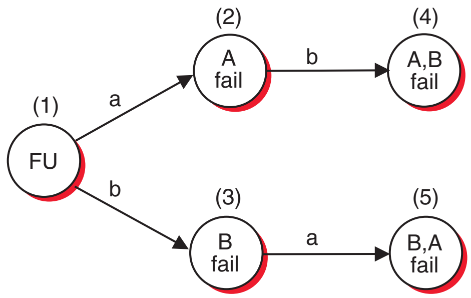
b. What is the probability that both boxes fail *and* that B fails before A?

Example	P_f Solution	Equivalent P_f with $A = e^{-at}$, $B = e^{-bt}$, $C = e^{-ct}$
2 in Series	$1 - e^{-(a+b)t}$	$1 - AB$
3 in Series	$1 - e^{-(a+b+c)t}$	$1 - ABC$
2 in Parallel	$(1 - e^{-at})(1 - e^{-bt})$	$1 - A - B + AB$
3 in Parallel	$(1 - e^{-at})(1 - e^{-bt})(1 - e^{-ct})$	$1 - (A+B+C) + (AB+AC+BC) - ABC$
Diode Short	$1 - [1 - (1 - e^{-at})^2]^2$	$1 - [1 - (1 - A)^2]^2$
Diode Open	$(1 - e^{-2at})^2$	$(1 - A^2)^2$

Table 1 — Combinatorial Problem Summary Chart

Note: Each of these solutions can be expressed in terms of integral sums and products of their respective probabilities of successes or failures. In other words, coefficients and exponents of terms in column 3 will all be integers. This is a telltale characteristic of all combinatorial type problems.

Markov Model (ROF)



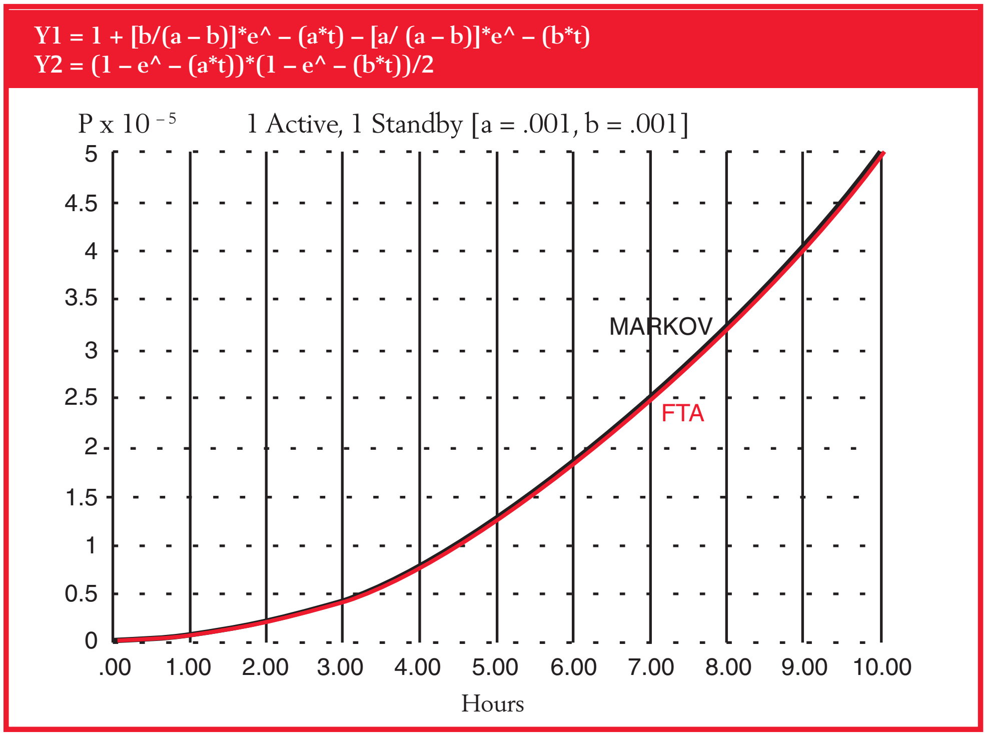


Figure 4 — Standby Markov, FTA Comparison (0 to 10 hours).

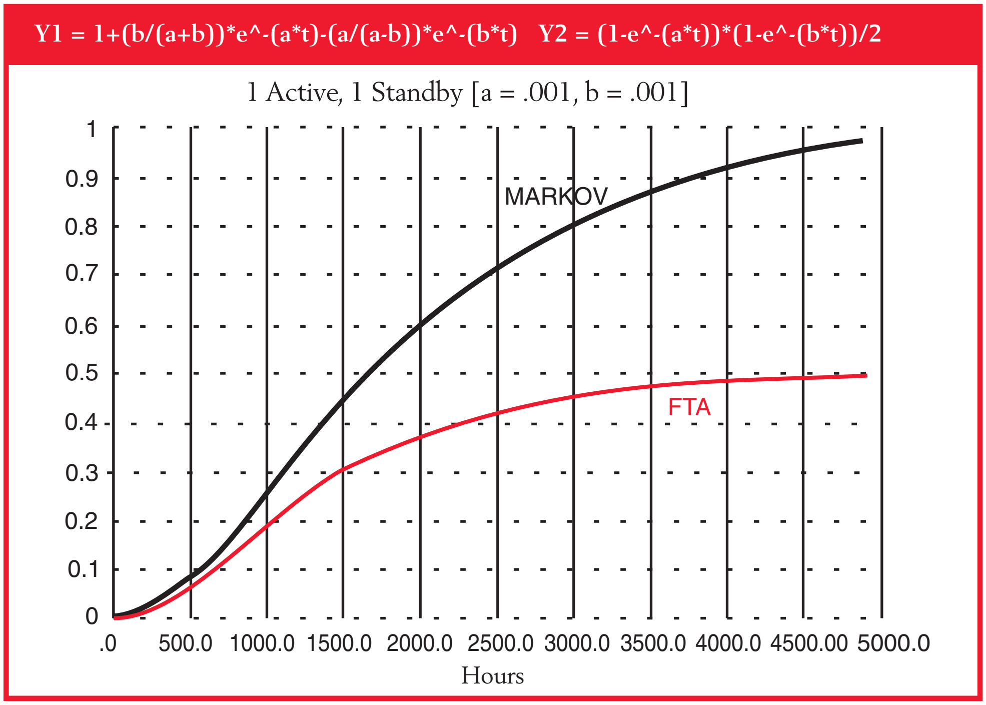
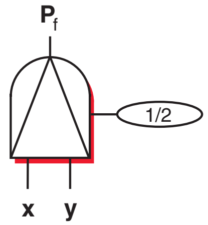


Figure 5 — Standby Markov, FTA Comparison (0 to 5000 hours).

a. $P(4) = a/(a + b) + [b/(a + b)]\, e^{-(a+b)t} - e^{-bt}$

b. $P(5) = b/(a + b) + [a/(a + b)]\, e^{-(a+b)t} - e^{-at}$

FTA Approach



$x = 1 - e^{-at} \qquad y = 1 - e^{-bt}$

a. $P_f = \lambda xy = \lambda\,(1 - e^{-at})(1 - e^{-bt})$

b. $P_f = \lambda xy = \lambda\,(1 - e^{-at})(1 - e^{-bt})$

Recall Item 3 of the NASA excerpt. This ROF problem has a sequence failure dependency, and is consequently a non-combinatorial type problem. As one can observe, the above results are not the same. This is because FTA has difficulty handling such problems.

Figures 6 and 7 show the FTA error.

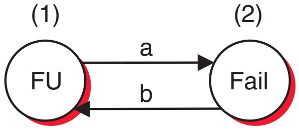
One Component with Repair (Non-Combinatorial):

A black box has failure rate a and an average repair rate b. Immediately upon detection of a failure, the box goes into a repair process and is put back on line. Calculate the probabilities of States 1 and 2.

Notes:

1. "Repair" can be categorized as an intermittent type problem. The device works, then it doesn't, then it works again. Recall Item 3 of the NASA excerpt. Hence, this is another example of a non-combinatorial problem.
2. Markov has the capability of solving this problem on a continuous basis, as shown in Figure 8.

Markov Model (Repair)



$$P(1) = \frac{b}{a+b} + \frac{a}{a+b}\left(e^{-(a+b)t}\right)$$

$$P(2) = \frac{a}{a+b} - \frac{a}{a+b}\left(e^{-(a+b)t}\right)$$

Note from the above equation that when t gets large, P(1) approaches the value b/(a+b) which is commonly known as "Availability."

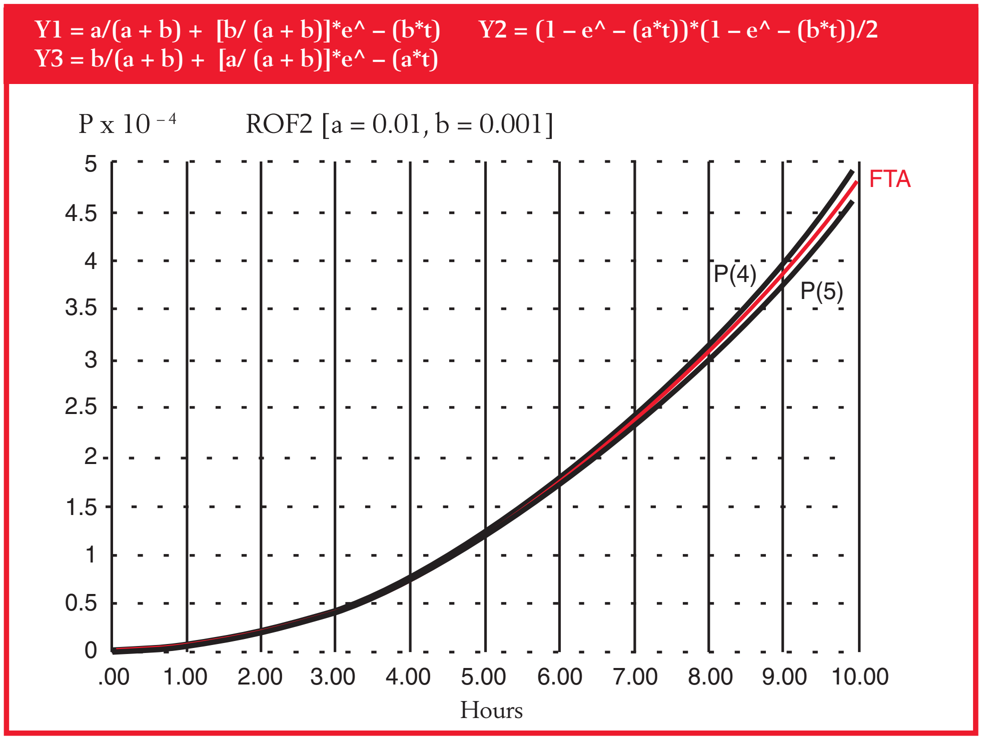


Figure 6 — ROF Markov, FTA Comparison (0 to 10 hours).

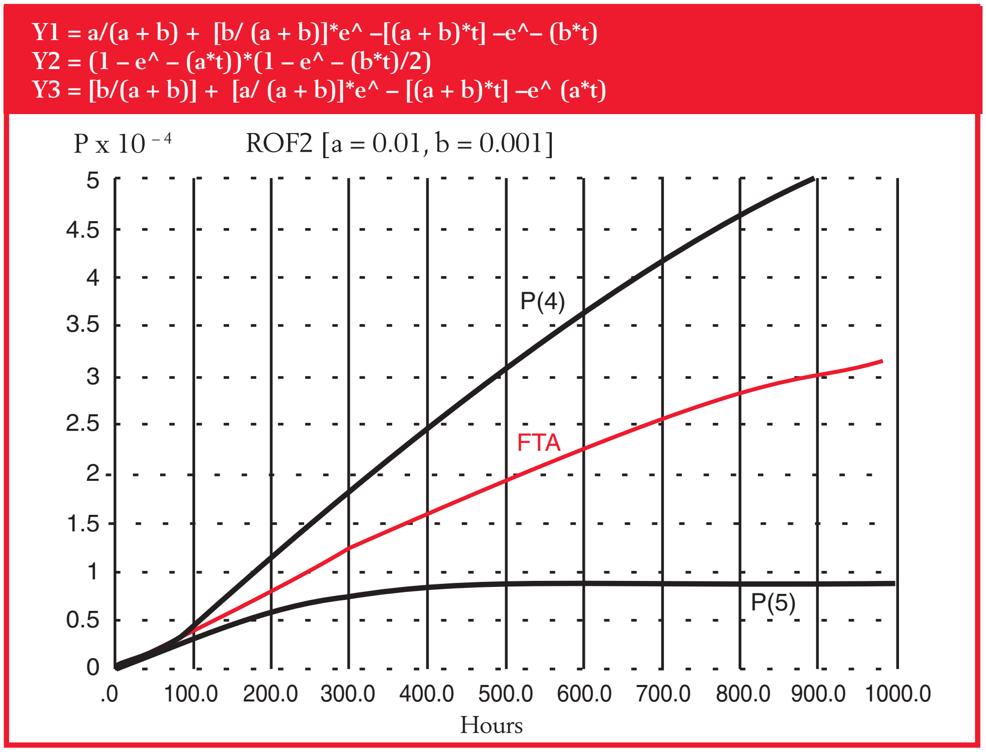
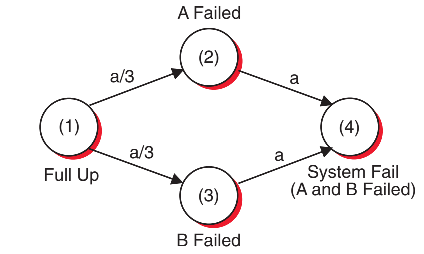


Figure 7 — ROF Markov, FTA Comparison (0 to 1000 hours).

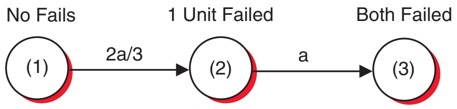
Load Sharing (Non-Combinatorial):
Consider a parallel load-sharing system consisting of two components A and B. Under the load-sharing conditions, each component carries one-half of the load. If under half-load conditions, the failure rate for each component is one-third of the full load failure rate. The full-load component failure rate is a.

Markov Model (Load Sharing)



$$P(3) = 2e^{-at} - 3e^{-(2a/3)t} + 1$$

Equivalent Markov Model



This is a very interesting problem. At first glance, this problem appears to be combinatorial since its Markov Model above looks very much like the model of two components in parallel. Construction of an equivalent model reveals that it is non-combinatorial since this model now looks like that of two components in standby redundant. This equivalent model reveals that this system has a state-dependent failure rate, and as a result, is actually a non-combinatorial type problem.

General Solution for n > 1 and n ≠ 2:
If the above problem had read,"If under half-load conditions, the failure rate for each device is 1/n times the full load failure rate," the solution would be:

$$P(3) = \left(\frac{2}{n-2}\right)e^{-at} - \left(\frac{2}{n-2}\right)e^{-(2a/n)t} + 1$$

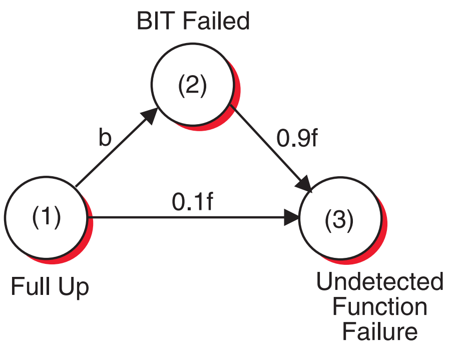
General Solution for n = 2

$$P(3) = \frac{a^2t^2e^{-at}}{2}$$

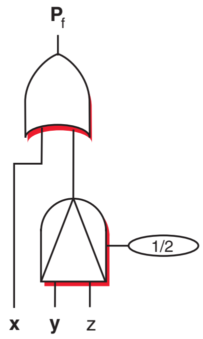
Function Failure Undetected (Non-Combinatorial):

A certain system incorporates Built-In-Test (BIT), which detects 90% of function failures of an electrical device. The function has failure rate f, and BIT has failure rate b. Assuming the function and BIT are checked during preflight, what is the probability of the function failing undetected?

Markov Model (Undetected)



FTA Approach



Markov Solution:
$P_f = 1 - (.8f/(.8f–b))e^{-(.1f+b)t} + (b/(.8f - b))e^{-.9ft}$

FTA Solution:
x = Prob (Function fails undetected) = 0.1 x f x t
y = Prob (Function fails detected) = 0.9 x f x t
z = Prob (BIT fails) = b x t where t is the elapsed time measured with preflight being start of count.
$P_f = x + yz/2 - xyz/2 \;=\; x + yz(1-x)/2$
$\Rightarrow P_f = 1 - [e^{-.1ft} + e^{-ft} + e^{-(.1f+b)t} - e^{-(f+b)t}]/2$

Additional Notes

1. There is absolutely no relationship between logic (combinatorial or non-combinatorial) of the interconnections of components within a system and the failures rates (constant or non-constant) of the components. When calculating probability of system failure, the analyst must account for both the failure characteristics of each component, and the interconnect logic.

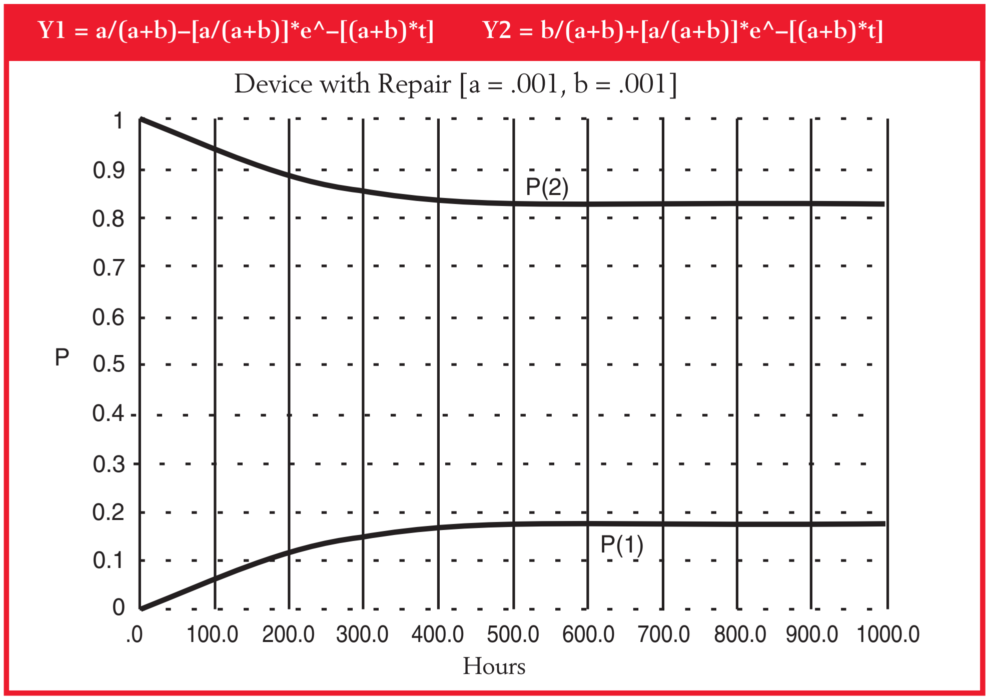


Figure 8 — Theory and Methods for Calculating Probability of Hazardous Events.

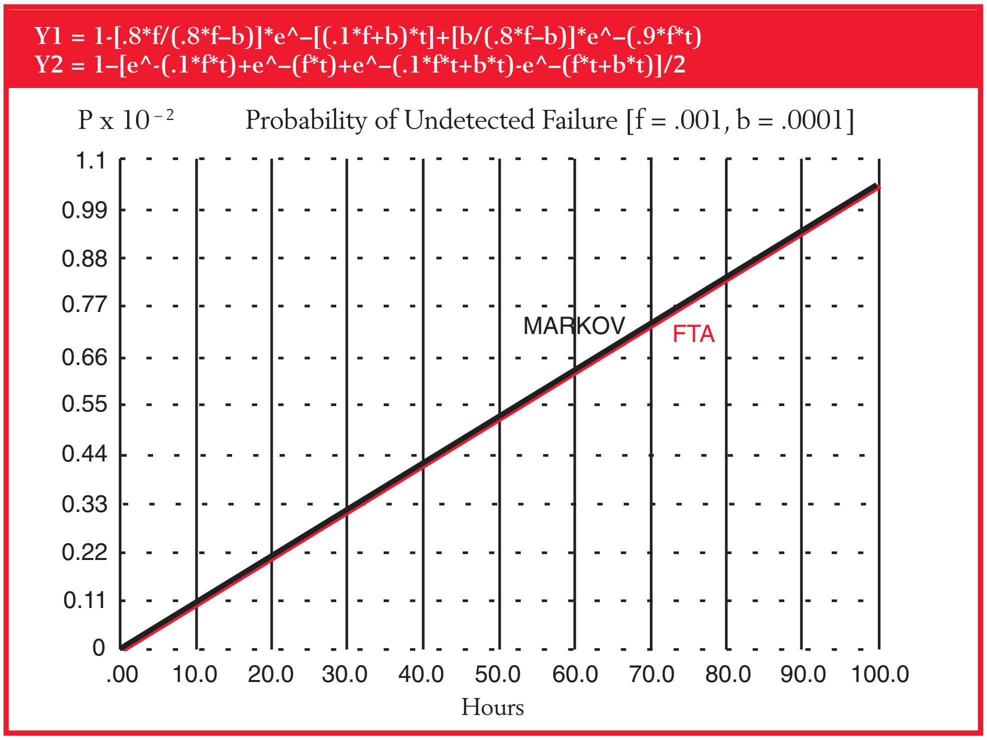


Figure 9 — Undetected Markov vs. FTA (0 to 100 hours).

2. FTA methods can handle both constant and non-constant failure rate components. Its limitation lies in the handling of non-combinatorial logic.
3. Markov handles both constant and non-constant failure rate components, as well as both types of logic.
4. It is interesting to note that Markov has many other applications. For example, Markov is used in statistics, speech analysis and recognition, data compression techniques, population analysis, biology, telecommunications, chemical reaction analysis, and financial mathematics, just to name a few.

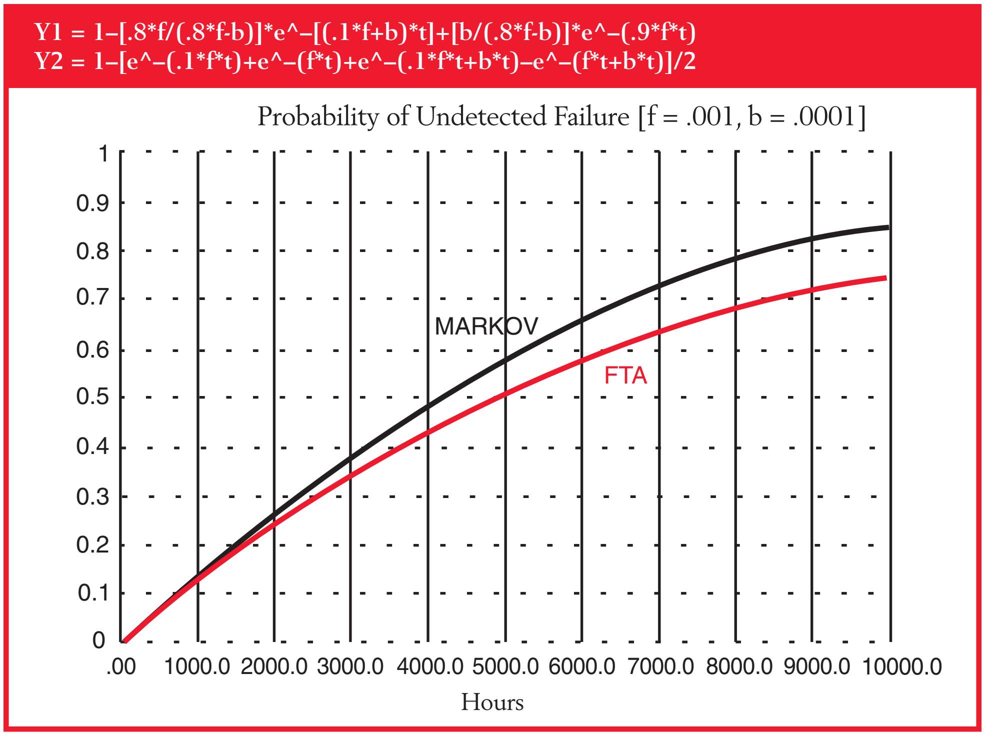


Figure 10 — Undetected Markov vs. FTA (0 to 1000 hours).

Table 2 — Non-Combinatorial Problem Summary Chart (Selected Examples).

Example	P_f Solution	Equivalent P_f with $A = e^{-at}$, $B = e^{-bt}$
Standby	$1 + \frac{b}{a-b} e^{-at} - \frac{b}{a-b} e^{-bt}$	$1 + \frac{b}{a-b} A - \frac{a}{a-b} \mathbf{B}$
ROF	$\frac{a}{a+b} + \frac{b}{a+b} e^{-(a+b)t} - e^{-bt}$	$\frac{a}{a+b} + \frac{b}{a+b} AB - B$
Repair	$\frac{b}{a+b} + \frac{a}{a+b} e^{-(a+b)t}$	$\frac{b}{a+b} + \frac{a}{a+b} AB$
Load Sharing	$2e^{-at} - 3e^{-(2a/3)t} + 1$	$2A - 3A^{2/3} + 1$

Note: Solutions to non-combinatorial problems cannot be expressed in terms of integral sums, products and exponents of their respective probabilities of successes or failures. Notice that in column 3, the coefficients and exponents of terms are not all integers. This is the telltale characteristic of non-combinatorial type problems.

Conclusions

In the world of Risk Analyses (calculating probability of failure), there are problems that, by nature, are non-combinatorial as well as combinatorial. Although in the early days of FTA, the existence (or differentiation) of these types of problems was a little obscure, engineers today are taking a closer look.

Markov methods may or may not be required for a failure analysis. What is important is that the analyst have the capability to make intelligent decisions as to whether the analysis requires Markov or not. Analysts should have the tools to solve both combinatorial and non-combinatorial type problems both qualitatively and quantitatively.

Since FTA is easy to understand, very well known, and handles combinatorial problems very well, the analyst should continue to use FTA whenever dealing with combinatorial types. It is suggested that MA *not* be used as a substitute for FTA, but rather as a supplement whenever non-combinatorial type problems are encountered.

About the Author

Vito Faraci is an electrical engineer at BAE Systems in Greenlawn, New York. He has 15 years of experience in qualitative and quantitative analyses of reliability and safety-related events as well as Built-In-Test design, and has served as a Markov/FTA/Reliability consultant for the Federal Aviation Administration and commercial airplane manufacturers. In addition, he has served as adjunct professor of mathematics at New York Institute of Technology.

References

1. Aerospace Recommended Practices ARP4761 Issue 1996-12.
2. NASA Ref. Publication 1348.