The Journal of the RAC

Third Quarter - 2004

Reliability Analysis Center

INSIDE

Hazardous Events

By: Vito Faraci Jr., BAE Systems

Abstract

Calculating the probability of "undesirable events" 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 twenty years was the "de facto" standard of the engineering community. Starting in the early 80s, 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), designed not necessarily to replace, but to support FTAs.

MA was introduced in 1907 by a Russian mathematician by the name of 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 or so, NASA has been using Markov methods for probabilistic risk assessments for the Shuttle systems. In addition, FTA and Reliability Software manufacturers have integrated Markov techniques into their risk assessment software programs.

With respect to reliability and risk assessment, the integration of MA with FTA has been a giant step forward. Engineers can now solve more accurately a larger set of "risk" problems than they could before. However, due to a lack of documentation written in a clear common language, knowledge of MA still remains a little "sketchy" within the engineering community.

Objective

This article is not intended to be a "how to solve" tutorial even though it will reveal some 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. To this end, several illustrative examples will be presented. The topics to be discussed are:

1. Combinatorial vs. Non-combinatorial Logic
2. Fault Tree Advantages and Limitations
3. Why Markov Analysis?
4. Markov Analysis Compared with FTA
5. Combinatorial & Non-combinatorial Type Problems

Combinatorial vs. Non-combinatorial Logic

Combinatorial Logic. Combinatorial logic is characterized by the following.

1. Two or more input states define one or more output states. Output states are related by defined rules that are independent of previous states.
2. Logic depends solely on combinations of inputs.
3. Time is neither modeled nor recognized.
4. Outputs change when inputs change irrespective of time.
5. 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. That is, non-combinatorial logic has memory; combinatorial logic does not.

Fault Tree Advantages

The chief advantages of a fault tree are that it:

1. Acts as a visual tool which can be used to pinpoint system weaknesses.
2. Exhibits clear representation of logical processes that lead to a system or sub-sys-

tem failure (clear qualitative representation of failure propagation).
3. Reveals relatively simple equations for probability of failure (P_f) calculations yielding quantitative analyses that do not require high powered math.
4. Is 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.

1. [In a fault tree it is] Difficult to allow for transient & intermittent faults or standby systems with spares.
2. If a system has many failure conditions, separate fault trees may need to be constructed for each one.
3. [In a fault tree it is] 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 regarding fault trees and Markov Analysis.

1. MA does not have these limitations.
2. Sequence dependent events are included and handled naturally.
3. Covers a much wider range of system behaviors.

Close examination of the NASA and ARP 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.

Some Pros and Cons

Fault Tree Analysis handles combinatorial type problems both qualitatively and quantitatively extremely well, but has difficulty with non-combinatorial problems in both areas. Markov Analysis handles non-combinatorial as well as combinatorial problems, but 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.

Example Markov State Diagram

Figure 1 illustrates a Markov state diagram. The following principles apply to this and all such diagrams.

- Various system states are represented.
- A transition rate is a function of the failure or repair rate.
- States are mutually exclusive.
- The sum of the probabilities must equal 1.

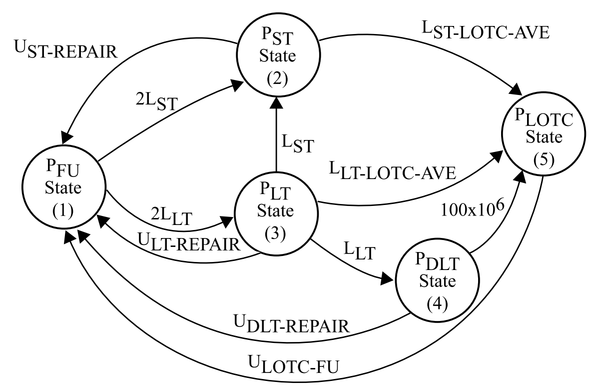


Figure 1. An Example of a Markov State Diagram

Markov Analysis Compared with FTA

Different types of failure rate characteristics are not an issue. FTA and Markov methods can handle both constant and non-constant failure rates. The major factor that sets the two methods apart is in the handling of combinatorial and/or non-combinatorial type problems.

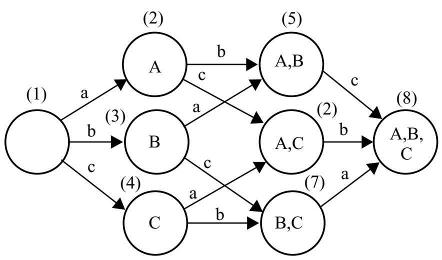
As mentioned before Markov handles combinatorial as well as non-combinatorial problems. Although there is no need of Markov for solving combinatorial type problems, (FTA handles them well enough) the next few examples will be demonstrated for the sake of illustration and comparison.

For purposes of simplification, the examples that follow will be limited to "constant failure rate" type problems. Solutions to "non-constant failure rate" type problems require somewhat different techniques and need to be discussed separately.

Combinatorial Type Problems

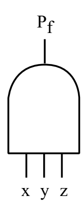
The author published a paper on Markov in the Third Quarter 2001 issue (Volume 9, Number 3) of the RAC Journal. Examples were provided of combinatorial problems. The examples that follow are additional examples of combinatorial problems. Readers may download a pdf of the referenced Journal at <http://rac.alionscience.com/rac/jsp/journal/racjournals.jsp?cat&2032&2001%20Journals>.

Problem 1: 3 Components in Parallel (Combinatorial). Three black boxes start operation at the same time. Box A, B, and C have failure rates a, b, and c respectively. Successful system operation requires that Box A, B <u>or</u> C be functional. Find P_f. Note that the results shown in Figures 1A and 1B from each method, FTA and MA, are identical.



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

Figure 1A. Markov Model for Problem 1



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

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

Figure 1B. FTA Approach for Problem 1

Problem 2: Fault-Tolerant Diode Circuit, Probability of Circuit Short (Combinatorial). The diode circuit shown in Figure 2A 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 λ. Derive the equation for the probability of a "SHORT." Let a, b, c, and d = λ = failure rates of failure mode SHORT for diodes A, B, C, and D respectively. The Markov model for analyzing the diode circuit in Figure 2A is shown in Figure 2B. The FTA model is shown in Figure 2C.

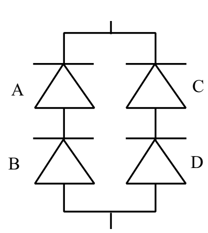


Figure 2A. Diode Circuit Model 1

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

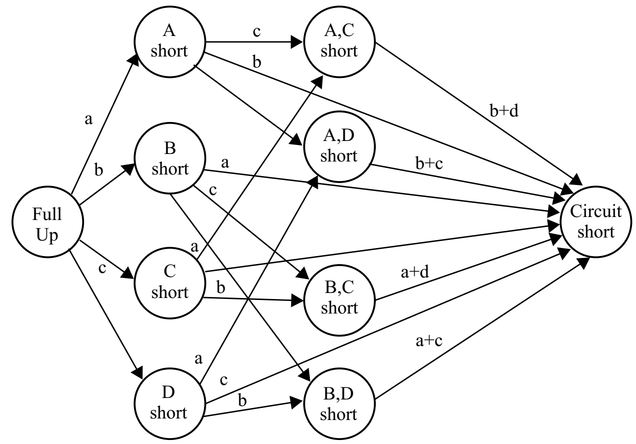
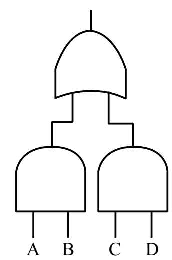


Figure 2B. Markov Model for Problem 2

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



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

Figure 2C. FTA Model for Problem 2

Problem 3: Fault-Tolerant Diode Circuit, Probability of Circuit Open (Combinatorial). The diode circuit in Figure 3A 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 OPEN mode (assuming identical diodes) is λ. Derive the equation for the probability of an OPEN circuit. Let a, b, c, and d = λ = failure rates of failure mode OPEN for diodes A, B, C, and D respectively.

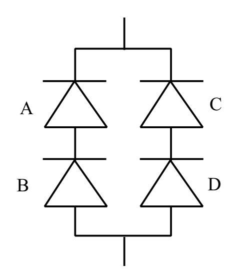


Figure 3A. Diode Circuit Model 2

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

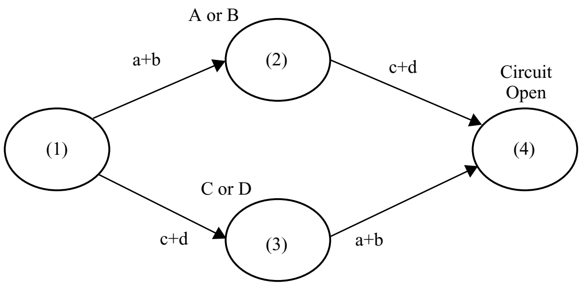
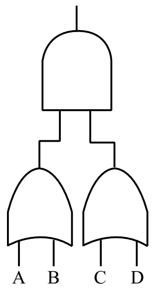


Figure 3B. Markov Model for Problem 3



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

Figure 3C. FTA Approach for Problem 3

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

Each of the solutions in Table 1 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 of the table will all be integers. This is a telltale characteristic of all combinatorial type problems.

Table 1. Combinatorial Problem Summary Chart

Example Problem	**Pf Solution**	**Equivalent Pf** with $A = e^{-at}$, $B = e^{-bt}$, $C = e^{-ct}$
1	$(1 - e^{-at})(1 - e^{-bt})(1 - e^{-ct})$	$1 - (A+B+C) + (AB+AC+BC) - ABC$
2	$1 - [1 - (1 - e^{-at})^2]^2$	$1 - [1 - (1 - A)^2]^2$
3	$(1 - e^{-2at})^2$	$(1 - A^2)^2$

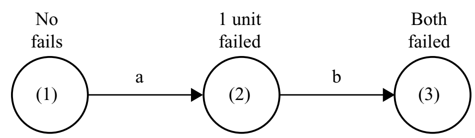
Non-combinatorial Type Problems

Solutions to non-combinatorial problems require different techniques other than traditional combinatorial logic such as that found in FTAs. These methods include solving a set of simultaneous differential equations (DEs), Laplace Transforms, Convolution, and State Sequence Methods. These methods are subjects for another article.

One non-combinatorial type problem in particular 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 require a separate discussion.

Problem 4: 2 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. The solution using Markov analysis and FTA, are shown in Figures 4A and 4B respectively.



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

Figure 4A. Markov Model for Problem 4

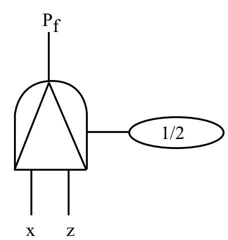


Figure 4B. FTA Approach for Problem 4

$$x = 1 - e^{-at} \qquad y = 1 - e^{-bt}$$
$$P_f = \tfrac{1}{2}xy = \tfrac{1}{2}(1 - e^{-at})(1 - e^{-bt})$$

This problem is another example of sequence failure dependency, and therefore a non-combinatorial type problem. Note again the FTA having difficulty tracking the Markov solution. However, for the first ten hours, the solutions are almost identical as shown in Figure 4C. However, as shown in Figure 4D, 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.

Problem 5: Two components in Parallel with Required Order Factor (ROF) (Non-combinatorial). For this example, what is:

a. The probability that both Boxes fail, <u>and</u> that A fails before B?
b. The probability that both Boxes fail <u>and</u> that B fails before A?

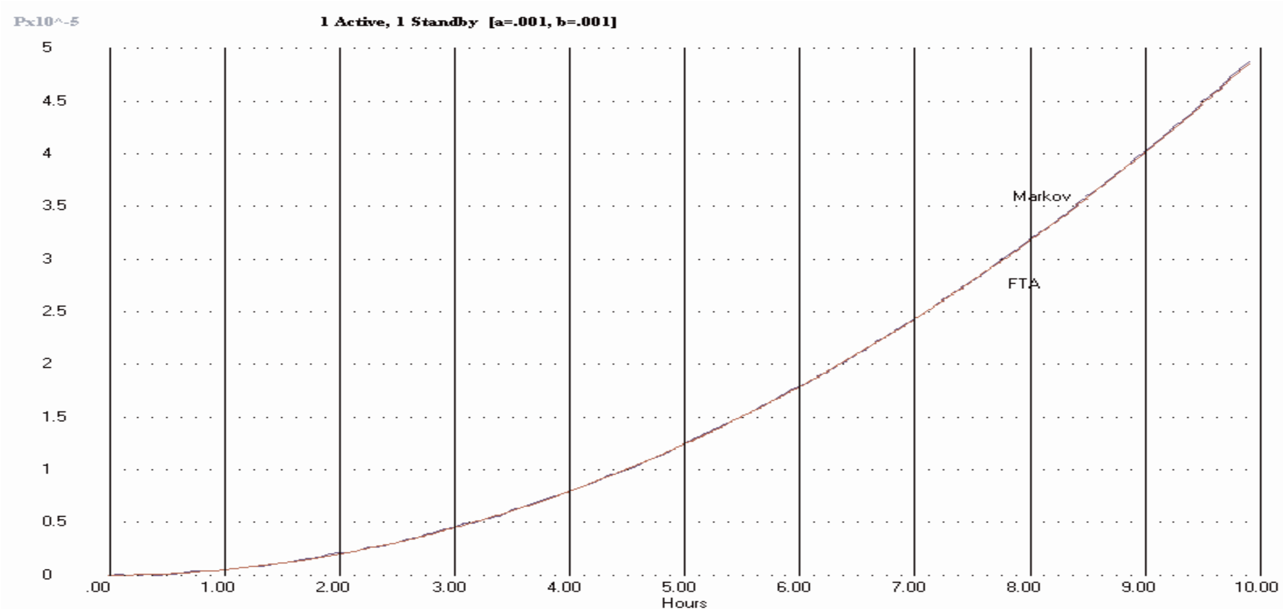


Figure 4C. Graph a Standby Markov, FTA Comparison (0 to 10 hours)

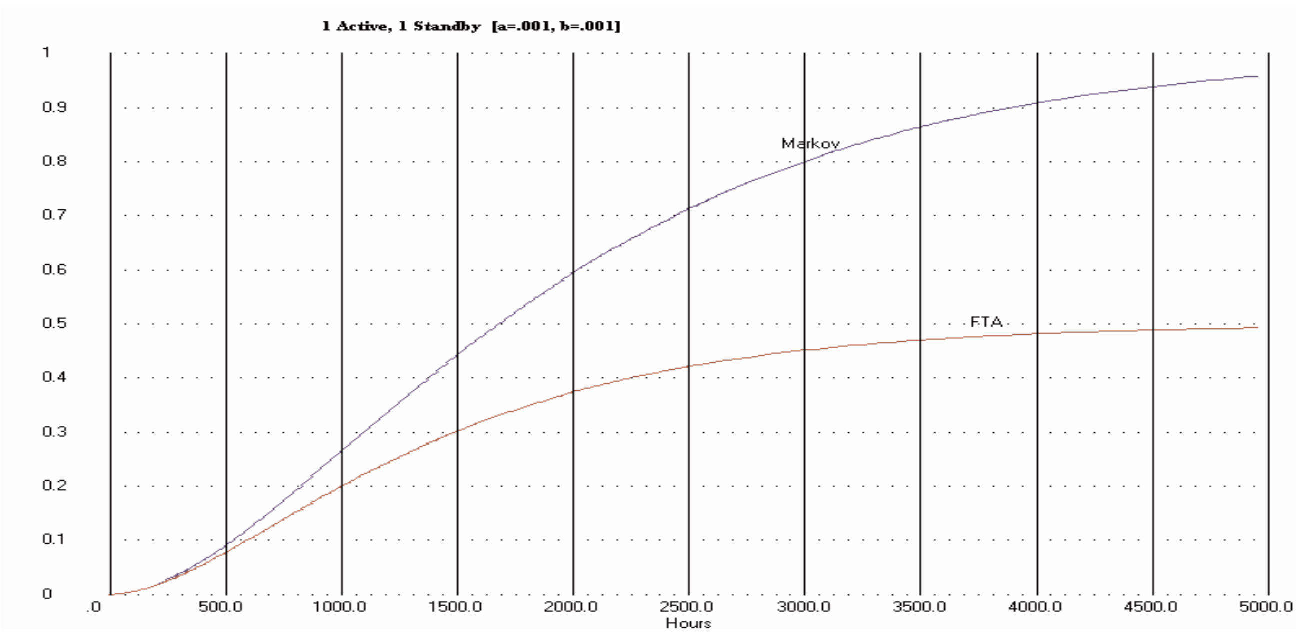


Figure 4D. Graph b Standby Markov, FTA Comparison (0 to 5,000 hours)

The Markov model for this example is shown in Figure 5A.

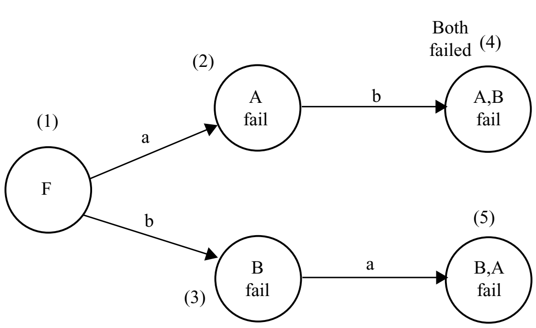


Figure 5A. Markov Model for Problem 5

The Markov solution equations are:

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

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

The fault tree for this example is shown in Figure 5B.

The fault tree equations are:

a. $P_f = ½xy = ½\,(1 - e^{-at})(1 - e^{-bt})$

b. $P_f = ½xy = ½\,(1 - e^{-at})(1 - e^{-bt})$

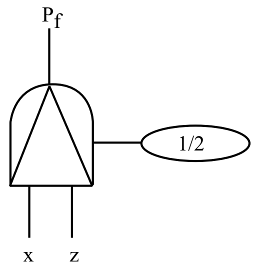


Figure 5B. Fault Tree Approach for Problem 5

Recall Item 3. of the NASA Excerpt. This ROF problem has a sequence failure dependency, and consequently a non-combinatorial type problem. As one can observe, the results for the FTA and Markov model are not the same. The difference is due to the fact that FTA has difficulty handling such problems. Figures 5C and 5D show the FTA error.

Problem 6: 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

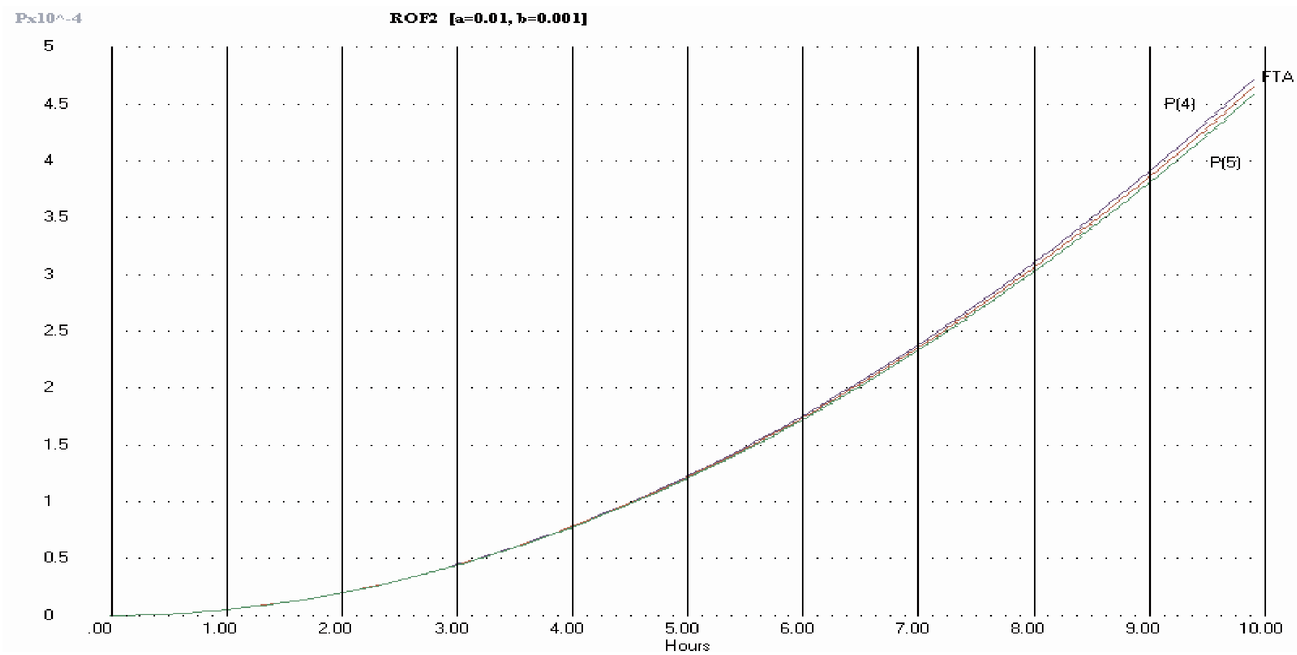


Figure 5C. Graph a ROF Markov, FTA Comparison (0 to 10 hours)

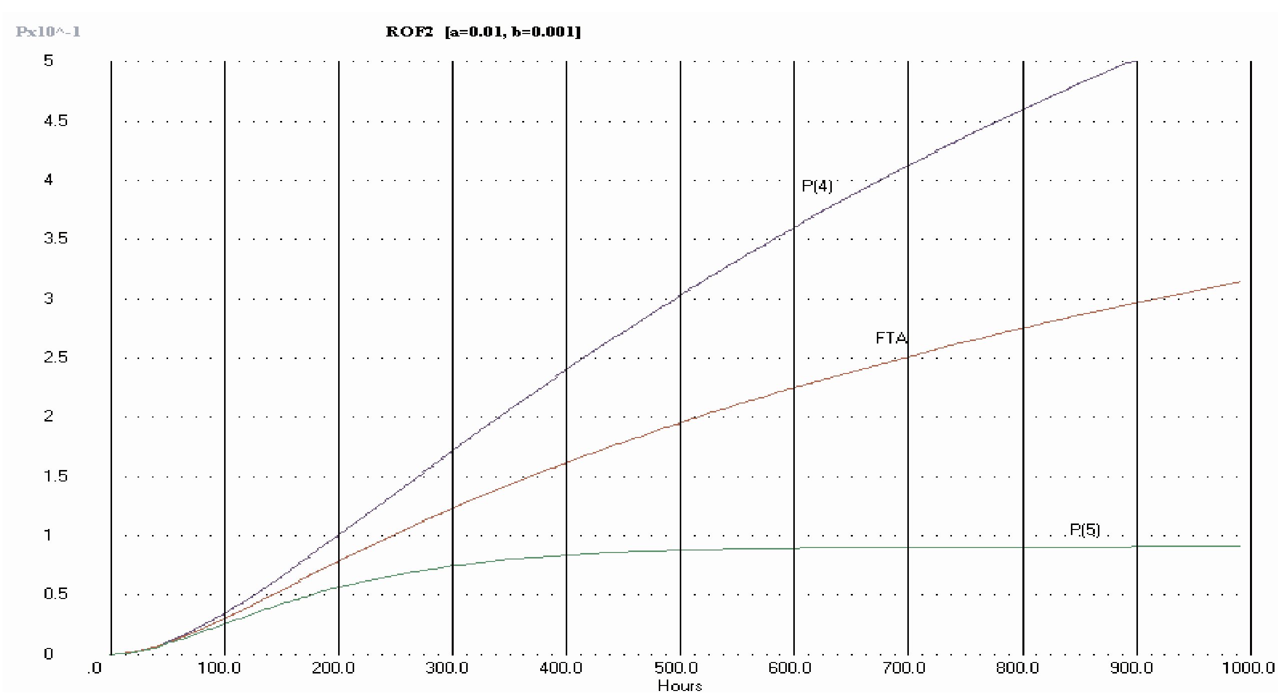


Figure 5D. Graph a ROF Markov, FTA Comparison (0 to 1,000 hours) repair process and is put back on line. Calculate the probabilities of States 1 (Full Up) and 2 (Fail). For this example,

1. "Repair" can be categorized as an intermittent type problem. The device works, then it doesn't, then it works again. Recall Item 1. of the NASA Excerpt. Hence another example of a non-combinatorial problem.
2. Markov has the capability of solving this problem on a continuous basis as shown in Figure 6.

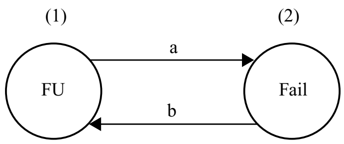


Figure 6. Markov Model for Problem 6

The solution equations are:

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

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

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

Problem 7: 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." Figure 7A shows the Markov Model for this example.

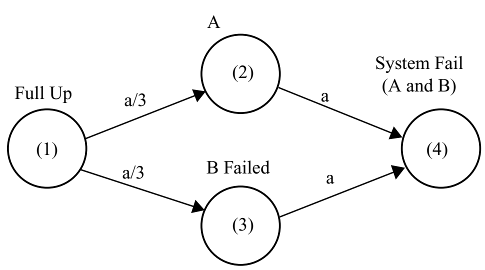


Figure 7A. Markov Model for Problem 7

This is a very interesting problem. At first glance this problem appears to be combinatorial since its Markov Model looks very much like the Markov Model of Problem 3. Construction of an equivalent model, Figure 7B, reveals that it is non-combinatorial.

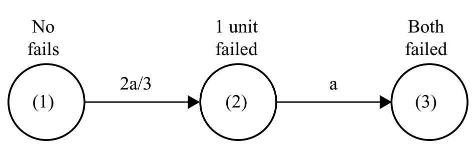


Figure 7B. Equivalent Markov Model for Problem 7

Problem 7: General Solution for n > 1 and n ≠ 2. If the previous problem 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:

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

Problem 7: **General Solution for n = 2**

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

Problem 8: Reconfiguration (Non-combinatorial): A system is made up of three computers with each computer having failure rate "a." Upon detection of failure of any one of the three, the remaining two reconfigure themselves at rate "b," and continue operating. Upon detection of a second failure, the remaining one reconfigures itself at rate "b," and continues operating until it fails. Note that if a computer should fail before a reconfiguration is completed, the system fails. Find P_f. The Markov model for this problem is shown in Figure 8.

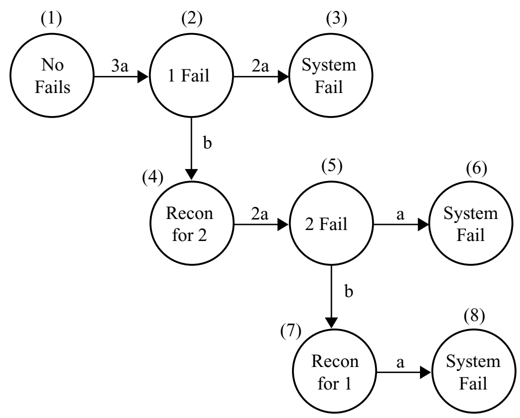


Figure 8. Markov Model for Problem 8

The probability of a system failure is the probability that the system enters state 3 or 6 or 8, and therefore $P_f = P(3) + P(6) + P(8)$. Note: As per Item 2. of the NASA Excerpt "Reconfiguration" is another example of a non-combinatorial problem.

$$P(3) = \frac{2a}{a-b}\left[e^{-3at} - \frac{3a \cdot e^{-(2a+b)t}}{2a+b}\right] + \frac{2a}{2a+b}$$

$$P(6) = \frac{6a^2}{a-b}A + \frac{ab}{(a+b)(2a+b)}$$

(Continued on page 10)

Hazardous Events . . . (Continued from page 7)

where A =

$$\left[\frac{b\cdot e^{-(a+b)t}}{(a+b)(b-2a)} - \frac{b\cdot e^{-3at}}{3a(b-2a)} - \frac{e^{-(2a+b)t}}{2a+b} + \frac{e^{-2at}}{2a}\right]$$

$$P(8) = \frac{6a^2b}{a-b}A - \frac{3b}{a+b}e^{-at} + \frac{b^2}{(a+b)(2a+b)}$$

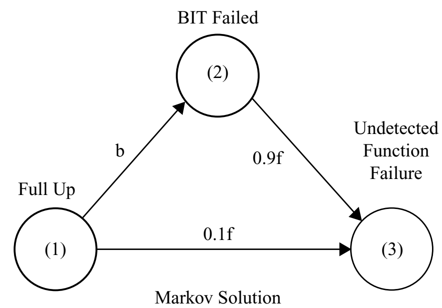
where A =

$$\left[\frac{e^{-(a+b)t}}{(a+b)(2a-b)} + \frac{be^{-3at}}{6a^2(b-2a)} + \frac{e^{-(2a+b)t}}{(a+b)(2a+b)} + \frac{e^{-2at}}{2a^2}\right]$$

Problem 9: 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? Figure 9A shows the Markov model and solution; Figure 9B the FTA model and solution.

FTA Solution:

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



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

Figure 9A. Markov Model and Solution for Problem 9

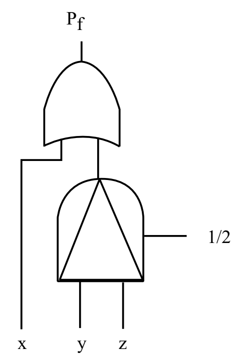


Figure 9B. FTA Model and Solution for Problem 12

Figures 9C and 9D, show graphs for the Undetected Failure problem, in which the Markov and FTA solutions are compared (0 to 100 hours and 0 to 10,000 hours).

Non-combinatorial Problem Summary Chart: Selected examples of non-combinatorial problems are summarized in Table 2.

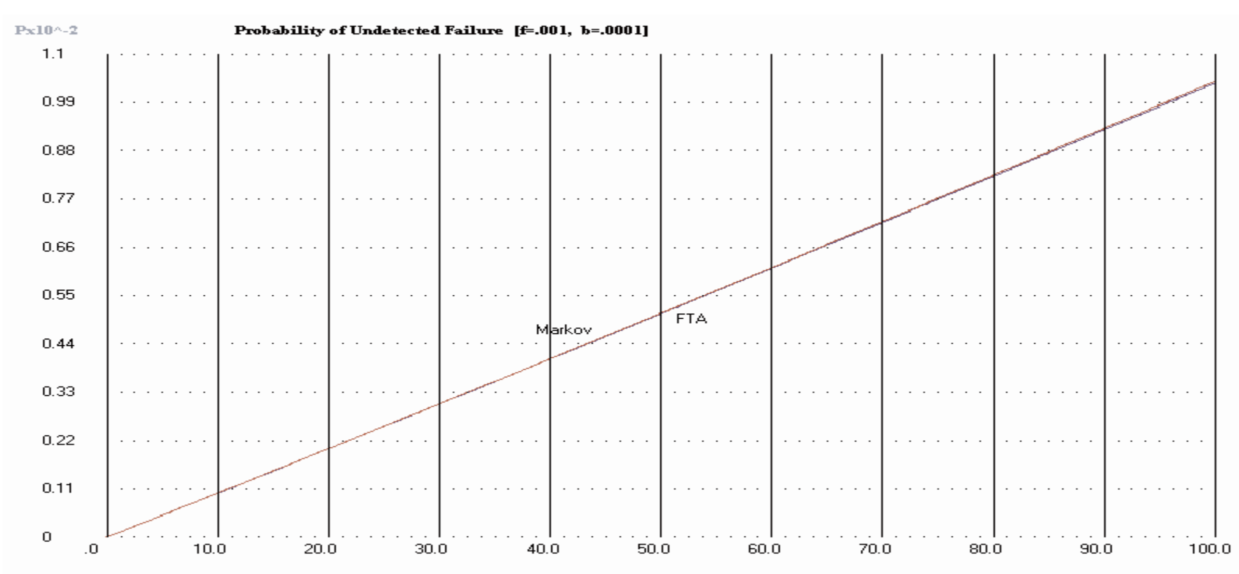


Figure 9C. Graph for the Undetected Failure Problem, Markov vs. FTA (0 to 100 hours)

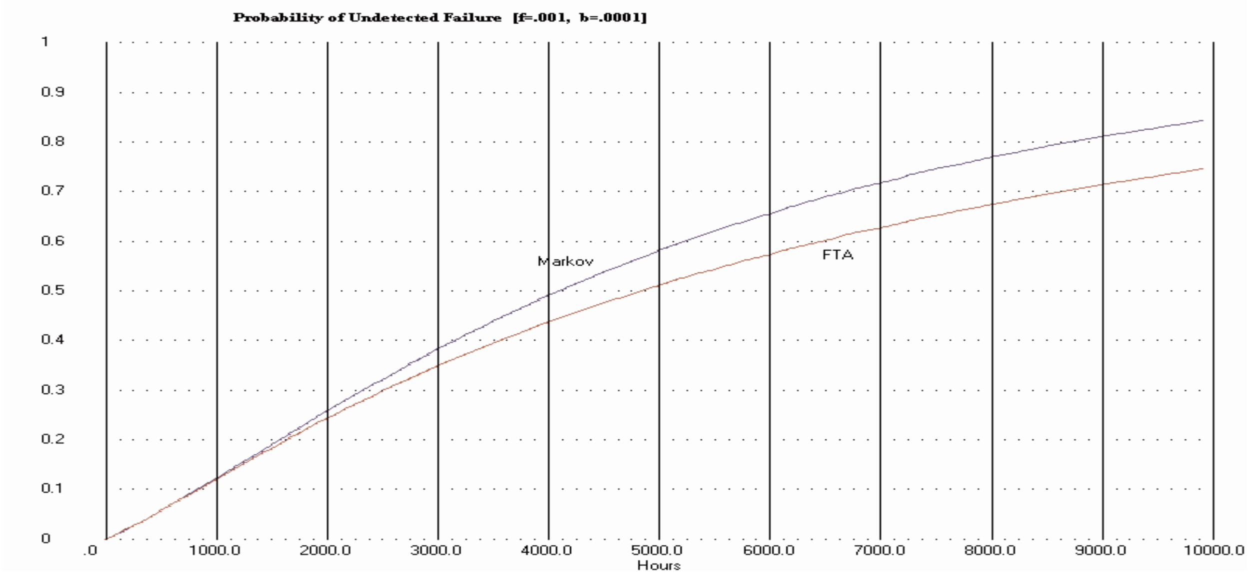


Figure 9D. Graph for the Undetected Failure Problem, Markov vs. FTA (0 to 10,000 hours)

Table 2. Summary of Selected Examples of Non-combinatorial Problems

Example	P_f solution	Equivalent P_f (with $A = e^{-at}$, $B = e^{-bt}$)
Standby	$1+\frac{b}{a-b}e^{-at}-\frac{a}{a-b}e^{-bt}$	$1+\frac{b}{a-b}A-\frac{a}{a-b}B$
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 in column 3, the coefficients and exponents of terms are not all integers. This is the telltale characteristic of non-combinatorial type problems.

Methods for Solving Markov (Non-Combinatorial) Problems

Methods for solving non-combinatorial type problems include solving a set of simultaneous differential equations (DEs), Laplace Transforms, Convolution, and State Sequence Method.

Conclusions

- In the world of Risk Analyses (calculating probability of failure), there exists problems which by nature are non-combinatorial as well as combinatorial.
- Analysts need to recognize, and be able to distinguish between both combinatorial and non-combinatorial type problems.
- Analysts should have the tools to solve both types qualitatively and quantitatively.
- Since FTA is easy to understand, very well known, and handles combinatorial problems very well, it is suggested that the analyst 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.

References

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

About the Author

Vito Faraci is a mathematician by education and an electrical engineer by trade. He has 15 years of experience with qualitative and quantitative analyses of reliability, built-in-test, and safety-related events. He has also served as a probability, reliability, and Markov Analysis consultant for the Federal Aviation Administration and commercial airlines. In addition, Mr. Faraci has also served as an adjunct math professor at New York Institute of Technology. He now works for BAE Systems.

An Introduction to Task Analysis

By: Kenneth P. LaSala, Ph.D., KPL Systems

Introduction

Task Analysis is a tool frequently used by human factors experts in analyzing human-machine systems and processes. It examines various aspects of tasks or functions for the following purposes:

- Check that human-machine interfaces are compatible with operator abilities.
- Aid in the development of training plans and manuals.
- Assist in the manpower planning process.

A thorough task analysis provides a substantial amount of insight into the task or function that the designer intends the human to perform. As one matures the task analysis, design trades become more apparent. The information obtained in the task analysis can be useful to reliability engineers as well as human factors specialists because the task analysis identifies factors that might affect the reliability of the human elements of a system as well as the reliability of the non-human system elements.

This article discusses the applications of task analysis and provides a description of the process of performing a task analysis. To assist both the human factors specialist and the reliability engineer in merging task analysis into other system design activities, the article provides a brief checklist that includes reliability topics as well as human factors topics.

Task Analysis Applications

One should conduct a task analysis as part of the design and development of any system or process that includes humans as operators, maintainers, or support personnel. Not only is a task analysis useful in the design of systems that are used in the field, such as radars and automobiles and their maintenance, but also it is extremely useful in the formation of manufacturing and assembly processes and even business processes such as financial processing. Medical instrumentation and procedures could benefit from task analyses. One could even apply a task analysis to commercial operations such as sales clerk positions and inventory control. The use of the checklist at the end of this article, regardless of the level of detail explored for each topic, could lead to revelations about factors that might cause both human errors and the attendant safety and economic consequences of those errors.

One might ask about when to conduct a task analysis. Like many design analyses, a task analysis evolves as the design evolves. The reader might construe the use of the word "design" to apply only to operational systems, but this would be incorrect. To be both reliable and efficient, manufacturing and business processes should be designed in an organized manner. Thus, this article applies the word "design" not only to operational systems but also to processes.

A task analysis actually is an extension of the "functional analysis" that is performed in system engineering. A functional analysis is the activity that identifies the specific actions that are required to meet the specific system or process requirements. Functional analyses usually are hierarchical decompositions of system requirements and the actions that are required to meet the requirements. When a suitable level of detail is reached, then one can start the task analysis. Performing an initial task analysis early in the design process can aid in the proper allocation of functions to humans, hardware or software. Based on the initial task analysis, one could use Fitt's Law (see Reference, page 34) to perform the functional allocation. As the design evolves and the functions progressively become more "locked in," the task analysis becomes more detailed. The various aspects of each function can be "fine-tuned" to enhance performance and reliability. Figure 1 illustrates how task analysis evolves with system or process design.

Basics of Task Analysis

A task analysis identifies the skills and information required to complete the task, the equipment requirements, the task setting, time and accuracy requirements, and the probable human errors and consequences. The results of a task analysis may be used to adjust the performance parameters, change the operating procedures, add or modify job aids and personnel, modify the operating environment, and adjust the maintenance and support processes that are associated with the subject of the analysis.

The task analysis categorizes and analyzes tasks by means of the following taxonomy:

- Mission
- Scenario and conditions
- Function
- Job
- Duty
- Task
- Subtask
- Task element

For each task, one collects and analyzes the following:

- Equipment acted upon
- Consequence of the action
- Feedback information resulting from the action
- Criterion of task accomplishment
- Environments, safety, and health factors
- Estimate of probability of error
- Estimate of the time to perform the task successfully
- Relation of the time and error rate associated with each critical task to the performance time and error rate for the overall system.

The checklist provided at the end of this article expands considerably on the preceding list.

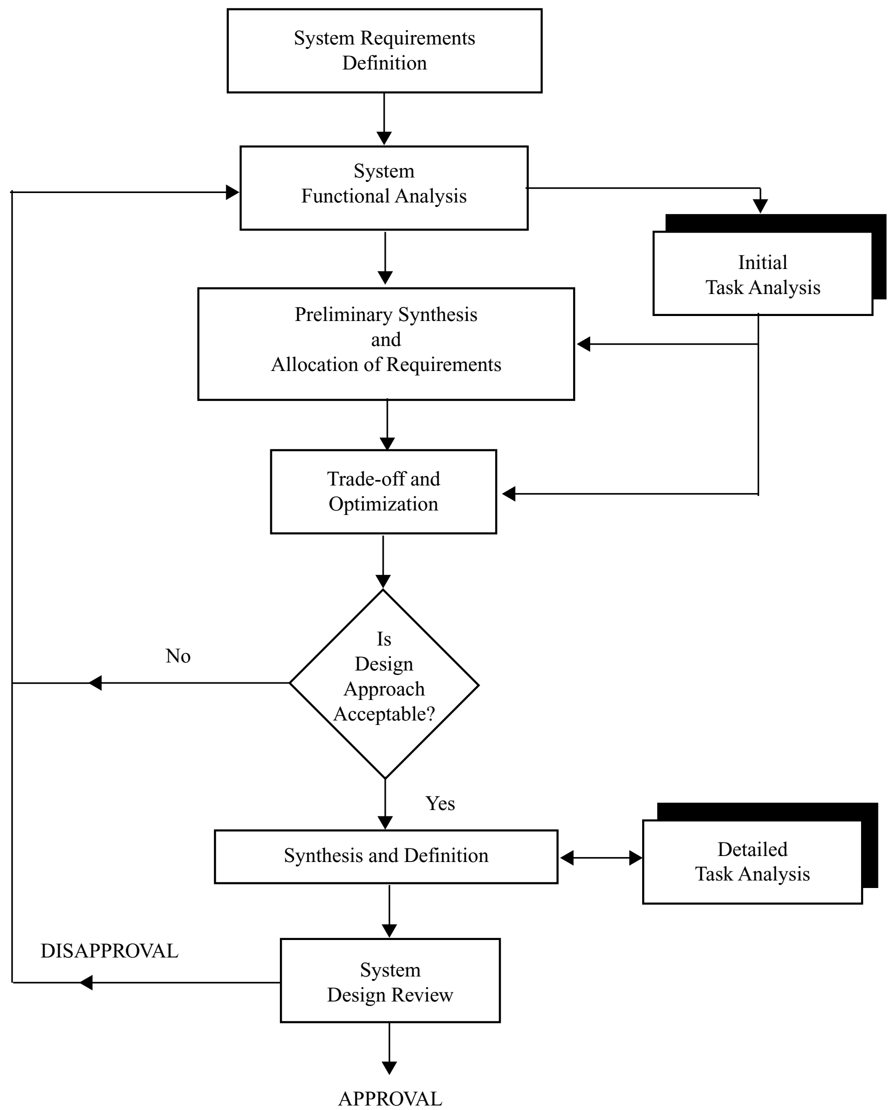


Figure 1. Task Analysis and System Development
(Expanded from B.S. Blanchard and W.J. Fabricky, System Engineering and Analysis 2nd Ed., Prentice Hall, 1990, page 58)

The exact mechanics of conducting the task analysis are actually quite flexible provided they result in the collection of the required data. The most logical mechanism for conducting the task analysis is a multidisciplinary team that includes human factors personnel, reliability engineers, and other hardware and software engineers. This team can perform the task analysis at discrete points in the system development process, as implied by Figure 1, or it can operate on a more or less continuous basis continually updating the initial task analysis with the design details that become available as the system or process evolves.

As mentioned previously, one member of the task analysis team should be a reliability engineer. The need for this person should become apparent when one observes that error probability (or unreliability) is an important part of the task analysis. Error probability alone certainly is informative, but an analysis of error context adds greatly to the value of the error assessment. Reliability engineering tools such as fault tree analyses, failure modes, effects, and criticality analyses, and even reliability prediction establish that needed context and help identify the tradeoffs that are available. Note that the recommended reliability tools include reliability prediction even though reliability prediction methods for human elements are still evolving. Figure 2 shows, in a very simple way, how neglecting the reliability of the human can lead to serious overestimates of system or process reliability.

The task analysis should be kept current with the design effort during each phase of system or process development. The use of a database may help maintain currency. In all cases, the current version of the task analysis should be traceable to earlier versions.

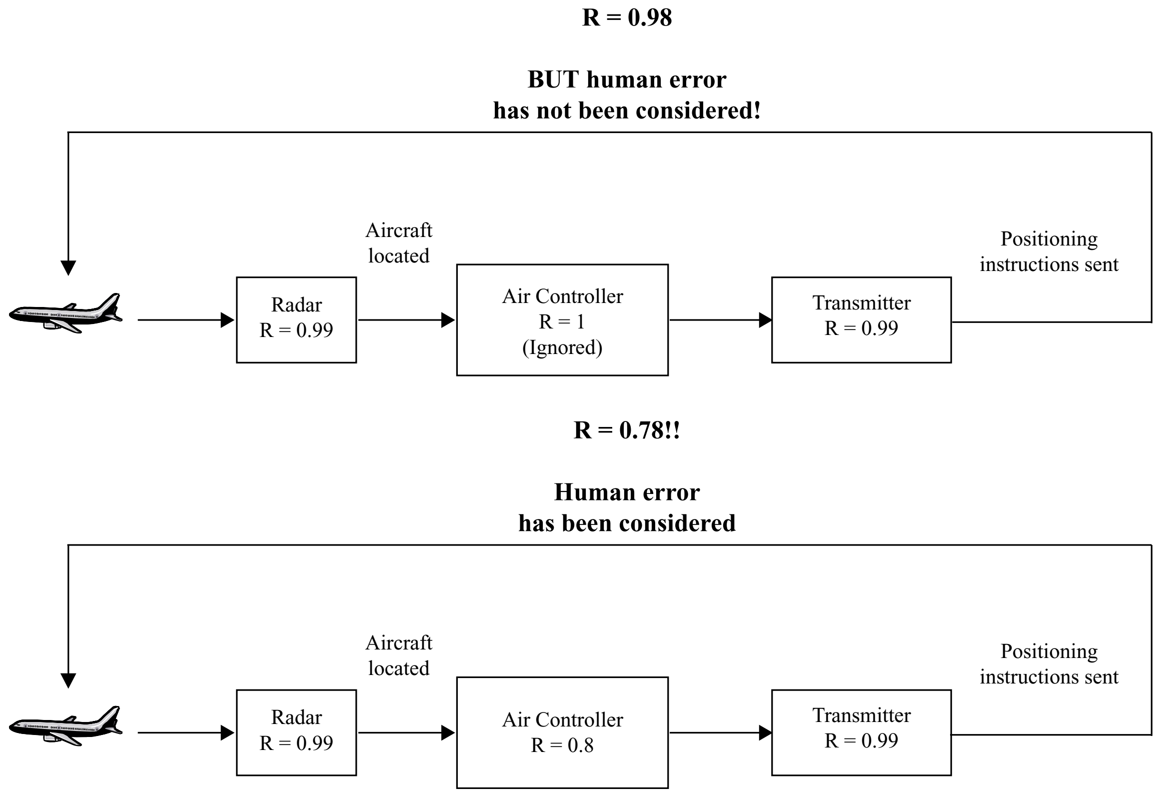


Figure 2. Impact of Human Reliability

Task Analysis Design Checklist

Table 1 is a checklist that may be used for conducting a task analysis that also explicitly considers reliability. This checklist may be used in any stage in the development of a system or process that consists of hardware, software, and humans. Naturally, the collected data will become more specific as the system or process evolves.

For each task or human function in a system or process, collect and analyze the data as shown in Table 1. Note that a “Yes” or “No” answer is only the first step in evaluating the design of a task or function. For items to which a “Yes” response has been given, “how acceptable?” must be asked. The reader is referred to the Reference for more information about specific task analysis tools and design acceptability criteria. For those seeking a more interactive environment, there is the short course entitled ***Human Reliability*** (<http://rac.alionscience.com/pdf/RAC-1ST/Human_Factors_Training.pdf>**)**, available from the Reliability Analysis Center (RAC) at <http://rac.alionscience.com/>. For exploring the quantitative impact of various parameters on task/function and system/process reliability via the Reliable Human-Machine System Developer (REHMS-D) decision support software, please visit <http://pages.prodigy.net/kplsys/rehms.htm>.

Reference

K. LaSala, **A Practical Guide to Developing Reliable Human-Machine Systems and Processes**, Reliability Analysis Center, RAC-HDBK-1190, August 2002.

About the Author

Kenneth LaSala currently is the Director of KPL Systems, an engineering consulting firm that focuses on reliability, maintainability, systems engineering, human factors, information technology, and process improvement. Dr. LaSala has over 33 years of technical and management experience in engineering. He has managed engineering groups and served as a senior technical staff member in systems engineering, reliability and maintainability (R&M), and product assurance for the Air Force, the Navy, the Army, the Defense Mapping Agency, and NOAA. He was the President of the IEEE Reliability Society during 1999-2000 and is the chairman of the IEEE Reliability Society Human Interface Technology Committee. He also currently participates in the DoD Human Factors Engineering Technical Advisory Group and the DoD Advisory Group on Electron Devices. His publications include several papers on R&M, systems requirements analysis, and other engineering topics. He also is the author of a chapter on human machine reliability in the McGraw-Hill *Handbook of Reliability Engineering and Management*, a co-author of the IEEE video tutorial on human reliability, and the author of a MIL-HDBK-338 section on the same topic. His research interests include techniques for designing human-machine systems and progressive system engineering approaches. He received the B.S. degree in Physics from Rensselaer Polytechnic Institute, the M.S. in Physics from Brown University, and the Ph.D. in Reliability Engineering from the University of Maryland.

Table 1. Task Analysis Design Checklist

Required Information	Yes	No	Date & Reviewers
1. Is there a top-level system reliability requirement that has been allocated to the specific task or function?			
2. Has the task or function been properly assigned to a human rather than hardware/software?			
3. Has an Operational Sequence Diagram been developed for the task or function?			
4. Has the equipment acted upon been identified?			
5. Has the consequence of the action been identified?			
6. Has the feedback information resulting from the action been identified?			
7. Have the criteria of task accomplishment been identified?			
8. Has an estimate of the time to perform the task successfully been identified?			
9. Have the following input parameters been identified?			
a. Information required			
b. Information available			
c. Initiating cues			
d. Data display format			
10. Have the following central processing parameters been identified?			
a. Decision or evaluation processes			
b. Decisions reached after evaluation			
c. Job knowledge required			
d. System knowledge required			
e. Academic knowledge required			
f. Significant memorization required			
11. Have the following response parameters been identified?			
a. Actions taken			
b. Body movements required by action taken			
c. Workspace envelope required by actions taken			
d. Workspace envelope available for actions taken			
e. Physical skills required			
f. Frequency or interval of actions			
g. Tolerances of actions			
h. Tools and job aids used			
i. Support and test equipment			
j. Power required			
k. Spares or parts required			
l. Adequacy of space support			
m. Controls used			
n. Controls locations			
o. Instrumentation, displays, and signals used			
p. Instrumentation, display, and signal locations			
12. Have the following feedback parameters been identified?			
a. Feedback required			
b. Feedback available			
c. Cues indicating task completion			
d. Rate of feedback update			
e. Format of feedback			
13. Have the following environmental parameters been identified?			
a. Workspace available			
b. Workspace envelope required			
c. Workplace arrangement			
d. Environment contamination level			
e. Climate (temperature, humidity, oxygen)			
f. Noise			
g. Shock, vibration, motion			
h. Lighting			
i. Workspace accessibility			
j. Workplace accessibility			

(Continued on page 17)

An Introduction to ... (Continued from page 15)

Table 1. Task Analysis Design Checklist (Cont'd)

Required Information	Yes	No	Date & Reviewers
k. Life support and protective gear			
14. Have the following safety parameters been identified?			
a. Types and locations of safety hazards			
b. Cause of safety hazard			
c. Frequency of safety hazard			
d. Consequences of safety hazard			
e. Safety procedures			
f. Recommendation to eliminate or minimize safety hazard			
15. Have factors that affect health been fully identified and evaluated? For example, chemicals, flame and fire, heat, vapors. (See RAC Reference this article, Section 4.3.3)			
16. Have performance standards and workload parameters (e.g., accuracy assessments, workload time line) been identified and evaluated? (See RAC Reference this article, Section 4.3.3)			
17. Have social and organizational parameters, such as personnel interdependence, been identified and evaluated?			
18. Has the impact on system or process reliability been determined qualitatively or quantitatively?			
a. Has the task or function reliability block been modeled as a combination of human, hardware, and software blocks?			
b. Has a fault tree been constructed for the task or function?			
c. Has a failure modes analysis been conducted for the task or function?			
d. Has a quantitative reliability estimated been developed for the task or function?			
e. Has the relation of the time and reliability associated with each critical task to the performance time and reliability for the overall system or process been identified?			

RMSQ Headlines

Root Cause Analysis for Beginners, Quality progress, published by American Society for Quality, July 2004, page 45. This article provides a good introduction to root cause analysis, defines what it is, describes its purpose, and describes a four-step process for determining the root cause of an event. A useful Root Cause Map is provided to help explain the process.

Using Software metrics and Program Slicing for Refactoring, CrossTalk, published by Software Technology Support Center (USAF/AMFC), July 2004, page 20. This article explains how using specific software metrics, and a technique called program slicing, designers can develop software systems that have higher quality and are more maintainable than would be otherwise possible.

Pentagon Setting Guidelines for Aircraft Interoperability, National Defense, published by NDIA, July 2004, page 47. With the increasing number and variety of unmanned aerial vehicles (UAVs), the Pentagon is considering establishing interoperability standards for UAVs. Although not advocating standard or common operating systems, the Pentagon is looking at requiring standard interfaces to allow UAVs to interact with each other.

Six Sigma and Supply Chain Excellence, Quality Digest, published by QCI International, August 2004, page 34. The article presents a 12-step approach for integrating six sigma and lean and applying the result to the supply chain.

The Challenge of Producing Quality Material in an Environment of Reform, Defense AT&L, published by the Defense Acquisition University, September-October 2004, page 30. In this article, the author presents his views of how acquisition reform has negatively affected the role of the quality discipline in military hardware production programs. Solutions for strengthening quality are presented that stress a back-to-basics approach.

Bridging the Military-Commercial Reliability Gap, Defense Standardization Program Journal, published by the Defense Standardization Program Office, April-June 2004, page 58. The authors describe a gap between the approaches to reliability used by the military and commercial industry. They propose that the military modify its approach to bridge the gap.

Evaporative Spray Cooling for Electronic Assemblies and Systems, Defense Standardization program journal, published by the Defense Standardization Program Office, April-June 2004, page 68. The authors examine the advantages and limitations of using evaporative spray cooling for electronics. They compare evaporative cooling with traditional air-based cooling on the basis of cost, reliability, maintenance, and performance.

PRISM Column

Software Reliability

Modern electronic systems typically contain significant amounts of software. Therefore, for a reliability assessment tool to be complete, it must include provisions for the estimation of software reliability. Many of the existing software reliability models are estimation models that require empirical test data. In many cases, data is simply not available at a point in time when a reliability estimate of a system is needed. Therefore, it was necessary to develop a predictive software reliability model that does not require empirical data. Like the PRISM hardware models, the technique must be based on readily accessible data and information.

Like the hardware model, the premise of the software model is that the inherent fault density of software can be estimated as a function of the development processes. However, in the software model, a separate process grading criteria is not included. Rather, due to its acceptance within the industry, the SEI (Software Engineering Institute) Capability Maturity Model (CMM) is used for this purpose. Once the inherent fault density is estimated as a function of the achieved CMM level, it is converted to a failure rate based on the defined operational profile of the software.

Reliability growth characteristics are modeled in a manner similar to that of hardware. For example, the potential for reliability growth is assessed and the likely failure rate impact, as a function of time, is estimated. Both the growth rate and the time to stabilization are estimated for this purpose. The default time for products to plateau and their residual fault content to stabilize is typically 48 months following its initial release. Subsequent product releases, such as a new software version, typically take 24 months to stabilize. In the case of software, this reliability growth is a function of the organization that will perform the field maintenance, which may be different than the development organization.

The user must assess the SEI Capability Maturity Model Level of the process developing the code. This assessment should be based upon the actual SEI assessment, if that exists. Lacking an SEI assessment of the development facility, one can use the Safety Level of the Software Level that the software is being developed to meet, or the ISO 9000 facility rating. If none of the cited process ratings exist, then review the SEI CMM Level requirements to determine and apply the CMM Level that most reasonably fits this product.

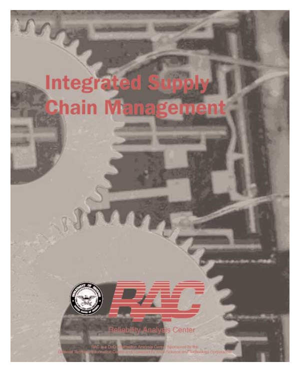
For more information on PRISM feel free to contact the PRISM team by phone (315-337-0900) or by E-mail (<rac_software@alionscience.com>). To obtain additional information including a demo version of the software go to (<http://rac.alionscience.com/prism>).

RAC Product News

In July, the RAC released the following new products.

Operational Availability Handbook: RAC-HDBK-3180. This handbook presents a practical overview of the concept of operational availability and several supportability measures and their use in different phases of a system's life cycle. It is intended to be a practical guide. Although several useful equations are provided, it is not intended to be an exhaustive mathematical or engineering treatise. This handbook is based on one initially developed by the Department of the Navy in the mid 1980s to address the combined consideration of Operation Availability and cost in all levels of systems acquisition and design related decision-making. This handbook generalizes and broadens the application of the concepts and incorporates the tenets of acquisition reform, organizational re-alignment, and provides additional clarity to the interaction between Operation Availability and cost of ownership. Although many of the terms and initiatives discussed herein are specific to the military, the basic concepts are also applicable to industrial and commercial products. Order Code: OPAH Price: $50 US, $60 Non-US (Web Downloadable). <http://rac.alionscience.com/rac/jsp/webproducts/products.jsp?detail=OPAH>

Integrated Supply Chain Management: RAC-HDBK-3190. A supply chain is a group of activities organized to deliver a product or service to customers. From that standpoint, supply chains have existed in one form or another ever since the dawn of commerce. However, in recent years, the attention of business and industry has become focused more strongly on the concept of supply chain management as a force for competitive advantage. This business strategy is based upon the concept of the total value chain. This handbook focuses on implementing a customer-focused supply chain management system. It describes the set of activities associated with planning and executing processes for delivering products and services to end customers, provides a brief summary of some supply chain models that have been published over the past 5-10 years, and presents the concepts and definitions of total cost of ownership and life cycle cost. It presents supply considerations for designing a supply chain, guidelines for optimizing the chain, and methods for managing supply chain management. Order Code: ISCM Price: $75 US, $85 Non-US (Web Downloadable). <http://rac.alionscience.com/rac/jsp/webproducts/products.jsp?detail=ISCM>



Future Events in Reliability, Maintainability, Supportability & Quality

Workshop on Accelerated Stress Testing & Reliability
October 6-8, 2004
Chicago, IL
Contact: John Proulx
General Motors
Tel: (310) 257-3714
E-mail: <john.proulx@gm.com>
On the Web: <http://www.ewh.ieee.org/soc/cpmt/tc7/ast2004/>

Special Symposia on Contact Phenomena in MEMs
October 24-27, 2004
Long Beach, CA
Contact: Dr. Lior Kogut
University of California at Berkeley
Department of Mechanical Engineering
5119 Etcheverry Hall
Berkeley, CA 94720-1740
Tel: (510) 642-3270
Fax: (510) 643-5599
E-mail: <kogut@newton.berkeley.edu>
On the Web: <http://www.asmeconferences.org/IJTC04/> (click on Special Symposia on Contact Mechanics)

7th Annual Systems Engineering Conference
October 25-28, 2004
Dallas, TX
Contact: Dania Khan
NDIA
2111 Wilson Blvd., Suite 400
Arlington, VA 22201
Tel: (703) 247-2587
Fax: (703) 522-1885
E-mail: <dkhan@ndia.org>
On the Web: <http://register.ndia.org/interview/register.ndia?PID=Brochure&SID=_1430NWW>

DoD Maintenance Symposium & Exhibition
October 25-28, 2004
Houston, TX
Contact: Customer Service
SAE World Headquarters
400 Commonwealth Drive
Warrendale, PA 15096-0001
Tel: (877) 606-7323
Fax: (724) 776-0790
E-mail: <CustomerService@sae.org>
On the Web: <http://www.sae.org/calendar/dod/>

World Aviation Congress
November 2-4, 2004
Reno, NV
Contact: Chris Durante
SAE
SAE World Headquarters
400 Commonwealth Drive
Warrendale, PA 15096-0001
Tel: (520) 621-6120
Fax: (520) 621-8191
E-mail: <cdurante@sae.org>
On the Web: <http://www.sae.org/events/wac/>

30th International Symposium for Testing & Failure Analysis
November 14-18, 2004
Worchester, MA
Contact: Matthew Thayer
Advanced Micro Devices
Austin, TX
Tel: (512) 602-5603
E-mail: <matthew.thayer@amd.com>
On the Web: <http://www.edfas.org/istfa>

CMMI Technology Conference
November 15-18, 2004
Denver, CO
Contact: Dania Khan
NDIA
2111 Wilson Blvd., Suite 400
Arlington, VA 22201-3061
Tel: (703) 247-2587
Fax: (703) 522-1885
E-mail: <dkhan@ndia.org>
On the Web: <http://www.sei.cmu.edu/cmmi/events/commi-techconf.html>

Aircraft Survivability 2004
November 30 - December 2, 2004
Monterey, CA
Contact: Ann Saliski
NDIA
Arlington, VA 22201
Tel: (703) 247-2577
Fax: (703) 522-1885
E-mail: <asaliski@ndia.org>
On the Web: <http://register.ndia.org/interview/register.ndia?PID=Brochure&SID=_18H0GAMD9&MID=5940>

19th International Maintenance Conference
December 5-8, 2004
Naples Coast, FL
Contact: Reliabilityweb.com
P.O. Box 07070
Fort Myers, FL 33919
Tel: (239) 985-0317
Fax: (309) 423-7234
E-mail: <info@reliabilityweb.com>
On the Web: <http://www.maintenanceconference.com/>

Aging Aircraft 2005
January 31 - February 3, 2005
Palm Springs, CA
Contact: Ric Loeslein
NAVAIR, Aging Aircraft Program
Patuxent River, MD 20670-1161
Tel: (301) 342-2179
Fax: (301) 342-2248
E-mail: <loesleinGF@navair.navy.mil>
On the Web: <http://www.agingaircraft.utcdayton.com/>

Commercialization of Military and Space Electronics Conference & Exhibition
February 7-10, 2005
Los Angeles, CA
Contact: Dale Stamp
CTI, Inc.
Huntsville, AL 35801
Tel: (256) 536-1304
Fax: (256) 539-8477
E-mail: <dstamps2173@cti-us.com>
On the Web: <http://www.cti-us.com>

21st Annual National Logistics Conference & Exhibition
February 28 - March 3, 2005
Miami, FL
Contact: Dania Khan
NDIA
2111 Wilson Blvd., Suite 400
Arlington, VA 22201
Tel: (703) 247-2587
Fax: (703) 522-1885
E-mail: <dkhan@ndia.org>
On the Web: <http://register.ndia.org/interview/register.ndia?PID=Brochure&SID=_dkhan@ndia.org>

Also visit our Calendar web page at <http://rac.alionscience.com/calendar>

From the Editor

The branches of science, such as physics, chemistry, and astronomy, focus on theory. Scientists postulate theories as they strive to find and understand the basic principles and phenomena of our physical universe. Engineers, on the other hand, apply theory in designing and building the systems and processes on which we have come to rely. These systems and processes include bridges, consumer electronics, commercial aircraft, petroleum refining, and the myriad of products that we in our daily life now take for granted.

It is easy for engineers to focus on the tools, models, and mathematics of their profession or on the results themselves, the products that roll off the assembly lines. Too often, we lose touch with or feel remote from those who must use the results of our analyses, tests, and designs. It is important for every engineer to keep the customer in mind. The customer may be a family who relies on the safety and reliability of their car as they travel on vacation. It may be several hundred passengers who trust that the aircraft on which they fly will arrive safely at their destination. Or it could be the operator of a manufacturing machine who is concerned with both safety of operation and quality of output.

For those of us who work with military systems, our customers are the men and women who stand guard at home and abroad defending our way of life. These sailors, soldiers, marines, and airmen are our fathers and mothers, brothers and sisters, spouses, and children. They are our friends, our fellow Americans. They are America's warfighters.

Those of us who once served in the military recall the pain of loss whenever a comrade in arms failed to return from a mission. Those of us who worked to maintain combat systems still feel the frustration when we had to cope with ambiguous diagnostics, poor maintainability, or inadequate reliability. These problems were offset by the dedicated efforts of young men and women, but only by working incredibly long hours under harsh conditions.

I am and have been for many years a member of the community of reliability and maintainability engineers. My professional life is filled with statistical distributions, Weibull analysis, failure analysis, FMEAs, and the many methods and tools of the reliability engineering discipline. Whenever I find myself thinking of my job only in terms of weapon systems, I remember my days in uniform. Then I see the faces of those with whom I served.

Ned H. Criscimagna

Whenever any of us are lulled into focusing only on the discipline and the product, an event occurs that jolts us back to reality. Events such as the Gulf War, 9/11, and the continued fighting in Afghanistan and Iraq help us realize that our jobs are not just to help make reliable systems. Instead, we have a mission to help assure that our service men and women have the weapons they need to defend freedom, achieve victory on the battlefield, and return safely to their families and loved ones.

Alion employees who directly operate the RAC, and the entire Alion Science and Technology Corporation, are conscious of the debt we owe to those in uniform who stand watch around the globe. We are committed to serving them by carrying out the RAC mission to the best of our ability. Our contributions pale when compared with the sacrifices made by those in uniform. Nonetheless, we will continue doing whatever we can to assure that our service men and women have the most reliable weapons systems possible. We continue to dedicate ourselves to helping gain victory on the battlefield, to ensuring the safety of our men and women in uniform, and to the continued safeguarding of freedom.

Our Real Customers!

Army Makes Reliability a Key Performance Parameter

Vice Chief of Staff of the Army George W. Casey, Jr. has directed that reliability be assessed as a potential Key Performance Parameter (KPP) during the Joint Capabilities Integration and Development System (JCIDS) process. He promulgated the requirement in a March 27, 2004 memorandum sent to key Army leaders, commanders, directors, program executive officers, and direct reporting program offices.

In paragraph 2 of his memorandum, General Casey stated:

> "The intent of this policy is to improve reliability of Army systems and materiel, enhance combat power, improve survivability for the Soldier and reduce logistics demand. Published studies and audits have documented that reliability has a significant impact on mission effectiveness, logistics effectiveness, and life-cycle costs. Improved reliability of Army systems and material will enable logistics efficiency and effectiveness, while enhancing readiness and warfighting capability."

The point of contact for Reliability as a KPP is Donald C. Crissup, SAAL-LP. He can be contacted at (703) 604-7421, DSN 664-7421, or by E-mail at <donald.crisup@us.army.mil>.

New DoD Supportability Guidebook

A new supportability guidebook has been released by the Office of the Secretary of Defense. Titled "Designing and Assessing Supportability in DoD Weapon Systems: A Guide to Increased Reliability and Reduced Logistics Footprint," the guide can be found at the Defense Acquisition university's AT&L Knowledge Sharing System Web Site at:

<http://acc.dau.mil/simplify/ev.php?ID=15943_201&ID2=DO_TOPIC>

Upcoming November Training

Electronic Design Reliability

This intensive course is structured for all key participants in the reliability engineering process. Included are systems and circuit design engineers, quality engineers and members of related disciplines having little or no previous reliability training. The course deals with both theoretical and practical applications of reliability; all considerations related to the design process including parts selection and control, circuit analysis, reliability analysis, reliability test and evaluation, equipment production and usage, reliability-oriented trade-offs, and reliability improvement techniques.

Reliability Engineering Statistics

The Reliability Statistics Training Course is a three-day, applications-oriented course on statistical methods. Designed for the practitioner, this course covers the main statistical methods used in reliability and life data analysis. The course starts with an overview of the main results of probability and reliability theory. Then, the main discrete and continuous distributions used in reliability data analysis are overviewed. This review of reliability principles prepares the participants to address the main problems of estimating, testing and modeling system reliability data. Course materials include the course manual and RAC's publication "Practical Statistical Tools for the Reliability Engineer."

Weibull Analysis

This three-day hands-on workshop starts with an overview of best practice Weibull analysis techniques plus a quick illustrative video of three case studies. The entire New Weibull Handbook© by Dr. Abernethy, the workbook provided for the class, is covered beginning with how to make a Weibull plot, plus interpretation guidelines for "good" Weibulls and "bad" Weibulls. Included are failure prediction with or without renewals, test planning, regression plus maximum likelihood solutions such as WeiBayes, and confidence calculations. All students will receive WinSMITH™ and VisualSMITH™ Weibull software and will get experience using the software on case study problems from industry. Computers are provided for the class. Related techniques Duane/AMSAA Reliability Growth, Log-Normal, Kaplan-Meier and others will be covered. This class will prepare the novice or update the veteran analyst to perform the latest probability plotting methods such as warranty data analysis. It is produced and presented by the world-recognized leaders in Weibull research.

For more information <http://rac.alionscience.com/training>.

Date: November 2-4, 2004
Location: Orlando, FL

Reliability Analysis Center
201 Mill Street
Rome, NY 13440-6916

The Journal of the

RAC

Reliability Analysis Center

PRSRT STD
US Postage Paid
Utica, NY
Permit #566

(315) 337-0900 General Information
(888) RAC-USER General Information
(315) 337-9932 Facsimile
(315) 337-9933 Technical Inquiries

rac@alionscience.com via E-mail

http://rac.alionscience.com Visit RAC on the Web