JOURNAL

OF THE RELIABILITY INFORMATION ANALYSIS CENTER

THIRD QUARTER // 2007

RCM AND RISK MANAGEMENT
(PART 1 OF 3)

Lynnwood Yates, RIAC (Wyle Laboratories)

Management is imminently concerned with minimizing the risks associated with their enterprises, while maximizing their profits or asset availability. Reliability-Centered Maintenance (RCM) is a proactive means of protecting their assets through a reasoned and practical maintenance management strategy; however these efforts may frequently fail to realize their potential. The answers may not readily translate into real management decisions or there may be so many recommendations that prioritizing them is very difficult. The following article is the first of a three-part series that proposes practical solutions to this dilemma.

RCM has been evolving in industry and government for forty years. Improvements in technique and approach has resulted in numerous companies providing excellent services, yet one area in which practitioners and customers alike have struggled is in translating the results into practical actions by management. It is apparent that management does not want this effort to fail, yet frequently the results are disregarded or fall into disuse.

The reasons behind management's resistance to clear and beneficial actions are often difficult to gauge. Some of the more commonly observed explanations include:

› Failure to finance the actions necessary to realize the benefits of the analysis
› Failure to recognize the cost and reliability benefits that may be attained
› No clear path for how the recommendations can be implemented
› Overwhelming lists of actions available with no means to efficiently prioritize these actions for incremental execution within limited budgets
› Inability to adequately communicate the benefits to upper management in terms that assist decision making
› Human nature – resistance to change

Frustration derived from this lack of clarity can be avoided by providing managers with both a tool for quantifying the value-added and information needed to answer upper management's desire to make advantageous decisions regarding those assets and enterprises under their care.

Risk

While risk can never be eliminated, it can be managed to an acceptable level. Understanding and appraising these risks can be complex, resulting in decisions which are made on a broad quantified basis. The Office of Safety and Health Administration (OSHA) and the Federal Aviation Administration (FAA) have published guidelines for managing risk from a safety perspective and management schools teach financial risk management to aid in decision making. The shortfall is the interface between initiatives such as RCM or Root Cause Analysis (RCA), hazard/safety risk management and financial risk management. This disjunction needs to be addressed with complete fidelity in order to enable managers to confidently make decisions and implement change.

The evaluation of the impact of failures (criticality) is often the first step in determining a risk assessment. While risk assessment may be accomplished in a variety of ways, one method commonly employed is Failure Modes, Effects and Criticality Analysis (FMECA). This bottom up analysis, in conjunction with a top-down Fault Tree Analysis (FTA) is frequently completed, ensuing a formal logical analysis that shows, "…the combination of events that results in the occurrence of a specified system level event" [Reference 1]. At a minimum, a team of experienced operators, maintainers, or engineers should make a formal assessment of the likely failure modes and impact of failures that would cause a loss of the system function or process. RCM is the key mechanism that encompasses all of these processes.

The primary factors considered by the RCM team are generally cost and severity of the loss (e.g. loss of an aircraft and two hundred people or loss of three days of production at $40,000 per day). Non-tangible considerations may include the loss of confidence in a system's reliability by operators, maintainers or the public. Risk management is a critical element in every RCM program.
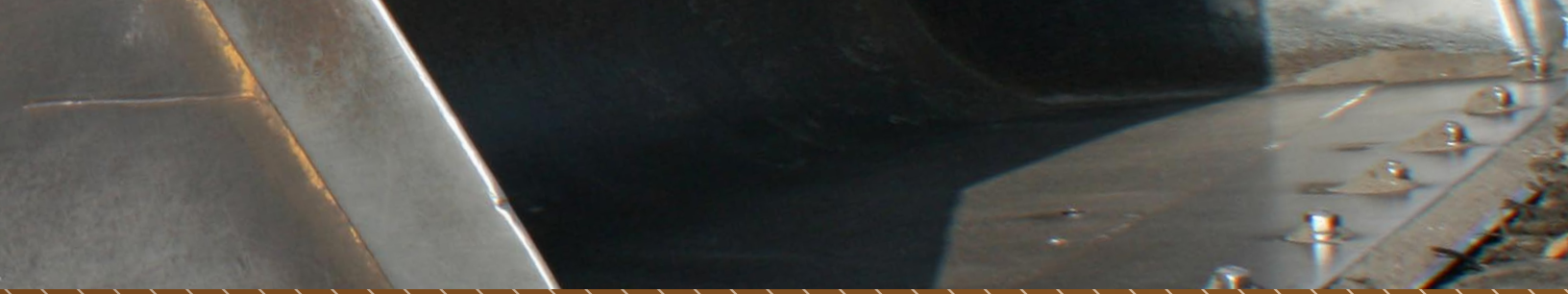
Management of Unacceptable Risks

Inherent in any management position is making decisions that balance resources with risk. Risk can be relatively high when managing a nuclear power plant that could potentially affect many people catastrophically, or an airliner carrying hundreds of people with the possibility of billions of dollars in litigation. Within military aviation, various concerns must also be included, as well as those mentioned in the introduction.

Readiness to protect our country is at the top of military aviation's management concerns. Further considerations must be made in regard to the loss of expensive assets that have a long lead time to replace, if replacement is even possible, loss of life and injury, as well as the loss of abilities from highly trained operators/maintainers. Other factors that affect the determination of acceptable risks may be difficult, if not impossible to gauge, such as using a different aircraft to complete a mission or the cost of a lost mission. Political reaction to a catastrophe, national confidence being shaken, or losses in project funding are just some of the impacts included in risk calculation. Due attention must also be given in consequence to the frequently changing importance placed upon these factors owing to external policy changes.

One of the easier means by which to rank risk is to compare the cost of loss/repair to the cost of redesign or changes in maintenance strategy. However, even these seemingly simple comparisons can in actuality be unfeasible, because the lead time required to purchase an item or the logistics support may not be available.

Many managers place a very high reliability standard on their assets or processes. This increased, and sometimes unrealistic, requirement is expensive and often beyond budget. Quantitative Risk Assessment (QRA) results can provide managers with a number, allowing for an educated ranking of risks with consideration for both importance and limited funds. Because quantitative numbers are more precise than the qualitative ones, there is a tendency to place more significance upon them; however, caution must be taken so as not to rely on these numbers exclusively. For example,

the QRA can yield a very low probability of failure, yet the analyst may not have considered all the failure modes, human error, or the operating environment in which the asset is used. Additionally, if an assessment is based on the fact that a failure has not happened in millions of flight hours, and is not likely to happen, but the component is actually at the end of its useful life after fatiguing for many years, the results could be disastrous. Care must be taken to consider how a failure happens, and its failure characteristic (e.g. wear-out or infant mortality). RCM enables the characterization of failures or potential failures to insure appropriateness of maintenance practices.

RCM analysts must define the risks associated with potential failures in a meaningful way so that clear and adequate information is available to managers. Managers are then armed with the information necessary to make decisions that protect and enhance their systems and processes.

Qualitative Risk Management

Qualitative Risk Assessment is a tool to help managers prioritize risk in broad categories of criticality and probability, as shown in Table 1 from MIL-STD-882D [Reference 2]. Although qualitative assessment is often used in the design phase where no failure data exists [Reference 3], fielded systems can benefit in a greater way due to the availability of failure data.

Categories may be broad such as, failure 'happens occasionally', and is of 'marginal criticality', yet have specific value ranges assigned, e.g. occasional is defined as 3 to 6 times a year per aircraft or has a Mean Time Between Failures (MTBF) of between 20,000 and 40,000 flight hours for a fleet of aircraft. When numeric ranges or probabilities are identified, this analysis becomes what is frequently termed a 'semi-qualitative' risk assessment (see Tables 2, 3 and 4).

Table 1. *Mishap Severity Codes*

Description	Category	Environmental, Safety & Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss > $1M, or irreversible severe environmental damage that violates law or regulation
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss > $200K but < $1M, or reversible environmental damage causing a violation of law or regulation
Marginal	III	Could result in injury or occupational illness resulting in one or mare lost work days, loss > $10K but < $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss > $2K but < $10K, or minimal environmental damage not violating law or regulation

Table 2. *Probability of Occurrence Classification*

Description	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life	Continuously experienced
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life	Will occur frequently
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life	Will occur several times
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life	Unlikely, but can reasonable be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life	Unlikely to occur, but possible

Table 3. *Hazard Risk Matrix*

Probability	Category			
	Catastrophic I	Critical II	Marginal III	Negligible IV
Frequent (A)	1	3	7	13
Probable (B)	2	5	9	16
Occasional (C)	4	6	11	18
Remote (D)	8	10	14	19
Improbable (E)	12	15	17	20

Table 4. *HRI Action Management Guidance*

Hazard Risk Index		Corrective Action
1 to 5	Unacceptable Risk	Mandatory correction, elimination or control. Requires acceptance by Higher Management if not corrected.
6 to 8	Undesirable Risk	Attempt should be made to eliminate or control. Requires program management approval for risk acceptance and concurrence by program management.
9 to 12	Acceptable Risk	Program management awareness recommended
13 to 20	Acceptable Risk	No action required

The Hazard Risk Index (HRI) method is commonly used today in military organizations to manage risk. Although adequate for risk management in general, a major drawback of this method is that it "…could hide critical information pertinent to the prioritization" [Reference 3] within a category. Military engineers conduct a Hazard Risk Assessment (HRA) of risks that are unacceptable, or that have been identified through the HRI. Unfortunately, with few formalized procedures or written guidelines, the effectiveness of the HRA process is dependant on the skills and talents of individual analysts.

Quantitative Risk Analysis

QRA further refines the qualitative process by calculating the probabilities of all relevant events or circumstances associated with the critical events. The main difference from qualitative risk assessment is that "…each variable is represented by a probability distribution function instead of a single value" [Reference 3]. Despite numeric calculation allowing greater fidelity for evaluating risks, heavy reliance on accurate failure data and probability estimates serves as a major disadvantage. Probabilities ought to represent the probability density function (PDF) of each failure mode to accurately characterize the probabilities with respect to time

or number of events. The accuracy of the data analysis is necessitated with the quality of the results being directly proportional to the accuracy. The analysis can be considerably intensive and expensive, and can yield flawed conclusions if the data is inaccurate. Weibull, Reliability Growth Analysis (RGA), or actuarial modeling are commonly used to formalize these PDF distributions.

Risk may be ranked using any of the available methods; however, the best method is without exception the one that meets management's decision needs. City managers in Los Angeles, California, developed a system by which to rank the disaster impact of events such as earthquake, flooding, tsunami, drought, etc. (Table 5). The tool aids managers in establishing the optimal use of available resources and services to protect the population during disasters [Reference 4].

The criteria were determined and quantified by the managers. As an example, the magnitude of an event was defined as the physical and economic impact by size, threat to life, threat to property (individual, public sector, business and manufacturing, and tourism). Duration, distribution, and other factors were quantified on a 0 to 3 scale (3 being most important) and then summed and ranked.

The qualitative assessment above fits the city managers' needs, but not necessarily those of military managers. The approach differs from military risk assessment, where the ability to protect the country factors highly and the value of each asset varies greatly. This method, however, could be perfectly adequate for military managers if characterized correctly. This form of risk assessment has an advantage over the QRA method as it is easily understood and ranked,

thereby aiding the managers to optimize decision-making. Intangible considerations can also be applied to the rank-sum method, as demonstrated in the following historical event:

"For logistics support in 1907 through 1909, President Roosevelt had a fleet painted white and a required condition of dress for the crew, and sailed the fleet around the world. It had been determined that the appearance and general condition of the vessels would have a psychological impact that would help avoid confrontation. With the deferral of painting or cleaning the hulls of modern vessels, the projection is more of disrepair and fostering a negative projection." [Reference 5].

The importance of risk assessment in RCM is apparent when decisions must be made that satisfy both asset reliability demands and the limitations of declining resources. These issues will be discussed in Parts 2 and 3 to be published in future issues of the RIAC Journal.

Acknowledgments

Table 5. City of Los Angeles Hazard Risk Analysis

Natural Hazard	Magnitude	Duration	Distribution	Area Affected	Frequency	Probability	Vulnerability	Community Priority	Total Value
Earthquake	3	3	3	3	2	3	2	3	22
Brush Fire	2	2	2	2	3	3	2	2	18
Flood	2	2	2	2	3	3	2	2	18
Landslide	1	1	1	1	2	3	1	1	11
Tsunami	3	2	1	2	1	1	2	0	12
Drought	1	2	2	3	2	2	1	1	14
Severe Weather[1]	1	1	2	2	2	2	2	1	13
Health Issues[2]	2	2	2	3	2	2	2	2	17

Note 1: High heat, high winds, coastal erosion, tornados, etc.
Note 2: Small pox, SARS, West Nile, severe influenza

In addition to being a very talented researcher, she is recognized by Who's Who of American Woman and Who's Who in Finance and Industry, a winner of a National Science Foundation fellowship as an undergraduate, and a co-author of published papers on cancer research.

Final thanks to Michele Dunlap, BA, Bath Spa University, Bath England, for her exhaustive editing to convert this author's 'Americanized language' into true English. She is an accomplished editor and historian.

References

1. Dodson, B, & Nolan D. (2001). Reliability Engineering Handbook. Tucson, Arizona: QA Publishing, LLC.
2. Department of Defense. (2000). Standard Practice for System Safety. MIL-STD-882D, Air Force Material Command, Wright-Patterson Air Force Base, Ohio.
3. Vose, D. (2006). Risk Analysis a Quantitative Guide (2nd Ed.). West Sussex, England: John Wiley & Sons Ltd.
4. Los Angeles City Managers' Hazard Risk Plan. (2004). Unidentified internet pdf source. Link lost.
5. Penrose, H. (2007). The Motor Diagnostics and Motor Health Newsletter. February 1, 2007. Retrieved from http://www.motordoc.net/toc.htm, 1 Feb 2007

Bibliography

1. Bowles. J. (2003). An Assessment of RPN Prioritization in a Failure Mode Effects and Criticality Analysis. Proceedings Annual Reliability and Maintainability Symposium.
2. Department of Defense. (1980). Procedures for Conducting a Failure Mode Effects and Criticality Analysis. MIL-STD-1629A, Washington, D.C.
3. SAE JA 1011, Evaluation Criteria for Reliability-Centered Maintenance (RCM) Processes, issued in January 2002
4. Reliability Information Analysis Center, Practical Application of Reliability-Centered Maintenance (RCM) Processes. Issued in 2003.
5. Smith, Anthony M., Reliability Centered Maintenance: Gateway to World Class Maintenance. Elsevier Butterworth-Heinemann, Burlington, MA, 2004.
6. United States Air Force. (1991). Military Handbook; Reliability Predication of Electronic Equipment. MIL-HDBK-217F.
7. United States Air Force. (2000). Air Force System Safety Handbook. Kirtland Air Force Base, New Mexico.

Connect to the university ranked No. 1
for supply chain education...

The Reliability Information Analysis Center -- in partnership with Penn State Executive Programs and the Center for Supply Chain Research -- offers targeted on-site programs to enhance your organization's supply chain performance. Learn from an internationally recognized faculty, as well as leading supply chain practitioners from top companies. Emerge with expertise you and your organization can put into immediate use.

To bring these educational offerings directly to your site, contact the RIAC at http://theRIAC.org or 1-877-363-RIAC

RIAC

PENNSTATE
1855
SMEAL
College of Business

CSCR

DÉJÀ VU - CAN WE STOP IT FROM HAPPENING AGAIN

Ned H. Criscimagna, President, Criscimagna Consulting LLC

Recently, the author was part of a team reviewing a major weapon system program that was experiencing a series of reliability setbacks during system testing. A series of consecutive failures had everyone scurrying to find solutions. One of the challenges was that many failures had no common cause or symptom. Instead, the team found a number of causes, stemming from design issues, manufacturing processes, assembly procedures, and test procedures.

The review team made many constructive recommendations for solving the problems, supplementing those actions the contractor was already taking. Just as importantly, the team identified systemic problems that were not confined to this one program. As one of the team members responsible for reviewing the reliability aspects of the program, the author was disappointed to see many of the same problems, and recommendations, that marked numerous programs he observed over his forty-two years in the aerospace business. For him, it was déjà vu all over again. The questions are why do these problems continue to occur, and why doesn't every program follow some basic reliability practices.

In this article, the author presents his own opinions as to why meeting reliability requirements continues to be an elusive goal for most programs. Some lessons learned over his forty-two years of professional work are also presented.

Why the Problems Continue

There are five basic reasons why the same reliability problems haunt program after program:

1. The Reliability Cycle
2. Unreachable Goals
3. Success Orientation
4. Cost Growth and Budget Uncertainty
5. Failure to Learn

1. The Reliability Cycle. Reliability began as a recognized discipline immediately after World War II. Robert Lusser, a German engineer and aircraft designer, developed the first reliability equation while working with Werner von Braun on the V-1 missile program during the war. Called Lusser's Law, it states that the reliability of a series system is equal to the product of the reliability of its component subsystems, if their failure modes are statistically independent.

US commercial airlines began incorporating many of the electronic systems used by the military during the war. Using electron tubes, these systems tended to fail with alarming regularity. Although repair costs were not a major consideration for the military during the war, they were for commercial airline operators. They called upon ARINC, Inc., the airline-owned communications company, to conduct research into improving the reliability of electron tubes.

In the years that have followed, reliability has gone through cycles of being "in" or "out" in terms of the attention given and resources dedicated to the discipline. In the late 1960s to early 1980s, the military services and the Department of Defense (DoD) had dedicated offices, policies, regulations, and engineers working on reliability. The Air Force Institute of Technology (AFIT) had a master's program focused on reliability. The DoD and the services had regulations specifying what was to be done to achieve reliability. Although, in retrospect, some of these requirements might have been non-value added, the importance of reliability was recognized and there was a concentrated effort to achieve it.

Today, after acquisition reform and many other efforts to streamline and improve acquisition, many in industry and government are again concerned about reliability. Why? Because many of the gains realized in the 70's and early 80's have been lost. If the same intermittent attention had been paid to fatigue strength of airframes, most of us now would hesitate before flying in any aircraft. This reliability cycle frustrates the efforts of those dedicated to its achievement; somehow, we must break this cycle while still making changes as we continue to learn.

2.. Unreachable Goals. Reliability goals frequently are set by optimistic marketers who tell customers what they can provide, or by customers who want reliability close to 100%. Requirements for one system often are copied from the specifications for another or the individuals responsible for determining the requirements have no idea of what constitutes a testable reliability requirement. Perhaps this is why the Army, within the past 5 years, has found

that less than 50% of their weapon system programs are meeting their reliability requirements. Once a requirement is stated in an acquisition document, regardless of its validity, it is difficult to change it.

3. Success Orientation. Program managers do not like to fail. Everyone involved on a program wants it to succeed. All taxpayers want success; after all, it is their sons and daughters who are risking their lives on the success of these systems.

It is one thing to wish, hope, and plan for success. It is another to ignore facts that warn of failure and to take no action. More than 20 years ago, the author participated in a review of another program. The consensus of the review team was that the program office and contractor were ignoring many warning signs and that the program was too success-oriented. Several specific findings and recommendations were made. These were ignored. Within five years, the potential problems identified in the findings came to fruition and could no longer be ignored. The results were schedule delays and cost increases. Some of these delays and increases would still have occurred had the recommendations been implemented, but they would have been less severe. Pursuing success without a willingness to face reality is no virtue.

4. Cost Growth and Budget Uncertainty. Major weapon system programs span many years. During that time, technology continues to change at an accelerating rate. It is natural to want to incorporate the latest technology in the system under development; open system architecture is just one disciplined way to do so. New programs also have many uncertainties associated with them, the very reason development contracts are not fixed price. Both technology growth and uncertainty drive up costs. Nevertheless, cost growth associated with some programs is often the result of requirements growth and unrealistic reporting. In extreme cases, cost growth results in fewer systems being bought and older systems being operated beyond their useful life.

Some cost growth is caused by Congressional changes in budgets from year to year, despite planned budgets in the Future Years Defense Plan and the fact that the program was approved to proceed. These changes are usually reductions that, in turn, require restructuring the program, extending production, and other actions that increase costs.

Frequently, budget reductions disproportionately affect the reliability program. Testing is reduced, unsuitable non-developmental items may be used, or fewer engineering hours are dedicated to analyzing failures and developing corrective actions.

5. Failure to Learn. A government program office may be staffed with military people or government civilians who have not worked on similar programs in the recent past. Many program managers do not manage more than one major program in their career. Without a corporate memory embodied in the staff, it is difficult to apply lessons learned from prior successes and failures. Apparently, the availability of various lessons learned databases, and the resources on the DoD acquisition web site, cannot overcome this problem. If this were not the case, then the same mistakes and oversights would not be found in program after program. From a reliability perspective, these mistakes and oversights are summarized in one idea: basic reliability practices are not followed.

Basic Reliability Practices

Most people who have been involved with acquisition and are familiar with reliability agree that it is a significant aspect of total system performance. The author has found that following some basic practices will help achieve the levels of reliability required in today's weapon systems. The following paragraphs will discuss:

> › The definition of a "reliability practice"
> › Some best practices for reliability

The Definition of a Reliability Practice

A reliability practice is any method, tool, procedure, or process that has been proven successful, is widely used, is practical and can be implemented, and is documented. Let's look at each element of this definition.

a. The practice has been successfully proven over time. When engineers find something that works, they tend to keep doing it. Time also gives those who use the practice an opportunity to

refine and improve the practice based on observed results.

b. The practice is widely used, especially by "best in class" organizations. Popularity is not always a good indicator of a good practice, let alone a best practice. Still, when a large number of organizations use a given practice, it tends to have more credibility. That credibility increases when those organizations are recognized as "best in class."

c. The practice is practical. At many symposia, papers are presented that pose new theories or postulate new approaches. Such theoretical work is essential to the continued progress in engineering disciplines such as reliability. However, these theories and approaches may not be practical to apply. The information to implement them may be elusive, or the tools either undeveloped or too cumbersome to be of practical use. For a practice to be considered "best", engineers must be able to apply it economically and effectively. They must be able to implement it in a timely manner consistent with aggressive schedules and limited budgets (two constraints common in both the private and public sectors).

d. The information needed to apply the practice is documented and readily available. Practices that require information that is impossible or impractical to collect are of little use. Even when the information can be collected, it may be considered proprietary. In these cases, each organization wishing to apply the practice must collect its own information, which for some organizations may be cost-prohibitive.

Some Best Practices.

a. Distinguish "designing for reliability" from "the numbers". Numerical predictions are all-too-often the focus of too many people. Predictions have become the center of many controversies within the reliability community. Advocates of different methods argue for their choice or attack the choices of others.

Predictions, or as the author prefers to call them, assessments, are simply an attempt to quantify the level of reliability using all of the information available at the time the prediction is made. Many methods are available, and each can serve a purpose if used appropriately. Methods that are appropriate in the concept development phase, such as similarity analysis, are inappropriate for assessing component reliability when test data are available. Assessment of system reliability during actual operation in the field requires an entirely different approach.

Few question the need for the "numbers". Engineers need a quantitative way to judge their progress in meeting a reliability requirement. Logisticians need to understand which spares to keep at the operating site, and in what quantities. Maintenance planners need a logical and quantitative way to select preventive maintenance tasks. Reliability assessments help meet all of these needs. Nonetheless, the emphasis during design should be not on the "numbers" but on the failure mechanisms of parts, the integration of those parts into assemblies, and so forth.

Better predictions do not make for better systems. Without sound engineering, a better prediction will probably only tell you that the reliability is too low at the end of development. Consequently, engineers and managers must focus on those practices, such as those that follow, that yield high reliability.

b. Start with parts and materials selection. The process of parts and material selection is arguably the foundation of design. Structural materials are important to reliability because structural integrity is equivalent to structural reliability. Unless materials are chosen that have the needed strength, corrosion-resistance, and other properties commensurate with the environment, the structure will be unreliable.

System reliability is limited by the least reliable safety- or mission-critical part. Although redundancy can compensate when parts with sufficient reliability cannot be found, it is expensive, can add parts (in the case of switched standby redundancy), and increases weight. Most parts should (1) have a minimum reliability requirement, (2) be carefully selected for the environment and application, and (3) be used in a way that capitalizes on their strengths. Reliability of critical parts should be determined through life testing.

c. Pay attention to reliability at each indenture level. Once the parts with the requisite reliability have been selected (or designed) for the application, a comparable level of attention must be given to integrating the parts into subassemblies, subassemblies into assemblies, and, finally, into the system. An appropriate level of effort toward meeting reliability requirements must be expended at each indenture level. Problems not found at lower levels will have a greater affect on cost, schedule, and performance when found at higher levels (See item i).

d. Understand how and why items fail in their application under the conditions of use. Some refer to this element as understanding the physics of failure. Only by understanding the underlying causes of failure at each level of indenture can engineers iterate their design to eliminate, or at least reduce the frequency or effect of, a failure. This process should begin before we have anything to test, and continue through testing and into actual use.

e. Design for all aspects of the application environment. "Environment" is used in its broadest sense. It includes packaging, handling, and transportation of the system, its individual subsys-

tems, assemblies, and parts. It includes storage, servicing, maintenance, and operation. Without knowing the stresses that the system must withstand, engineers cannot properly design for the environment. They can attempt to compensate by using Highly Accelerated Stress Testing and other approaches. However, the author knows of no engineer who wouldn't want a high-fidelity characterization of the actual environment.

f. Use robust design techniques. Robust design is sometimes referred to as the Taguchi Method, which is an approach that begins with selecting the best methods for characterizing the product and environment, evaluating failure mechanisms, and identifying the design changes needed to eliminate design weaknesses. These methods include design of experiments; parameter design; and statistical design techniques such as stress-strength interference.

g. Use redundancy judiciously. Although redundancy generally increases mission reliability, it comes with penalties (See Item b). Depending on whether standby or active redundancy is used, the added complexity of failure detection and function-switching equipment can actually decrease mission reliability.

Even when the number of mission failures decreases because of redundancy, the overall number of mission-critical and non-critical system failures in a given time increases. This overall reliability is termed basic or logistics reliability. In general, redundancy increases mission reliability but decreases basic

reliability. Thus, redundancy is a trade-off between higher levels of mission success probability and logistics costs, weight, and total cost.

h. Conduct development testing at each level of indenture and take action based on the results. Testing is the means by which engineers validate the results of analysis and modeling, uncover unanticipated problems, and investigate the interactions and synergies of integrating individual subassemblies, assemblies, and subsystems. Development testing has four purposes:

1. Identify and analyze design weaknesses
2. Prioritize design weaknesses
3. Develop design changes to eliminate or reduce the severity of the design weakness
4. Verify the effectiveness of the design change

The process of design, test, and redesign, when applied to improving reliability, is sometimes referred to as test-analyze-and-fix. A model is often used to plan the improvement to be achieved and then to track it (reliability growth).

i. The design team should develop a Reliability Case that presents progressive assurance that the reliability requirements are achievable, properly understood by the developing organization, and are being achieved.

The Reliability Case can include different types of evidence:

PRODUCT ON THE HORIZON

RIAC REPERTOIRE with QuART PRO

The purpose of the "RIAC REPERTOIRE with QuART PRO" product is to provide users with DVD-based and on-line asynchronous training that will (1) develop the skills of those who want to learn more about the practical and theoretical aspects of reliability engineering, (2) enhance the reliability engineering skills of seasoned practitioners, and (3) prepare students for the ASQ Certified Reliability Engineer (CRE) exam, if they choose to pursue this professional certification. The RIAC REPERTOIRE training program consists of 5 modules covering Reliability Management, Probability and Statistics for Reliability, Reliability in Design and Development, Reliability Modeling and Predictions, and Reliability Testing.

REPERTOIRE
RELIABILITY TRAINING FOR PROFESSIONALS ON THE GO

Those who purchase the DVD, or the 5-module set of the on-line program, will receive the QuART PRO software free of charge. The QuART PRO suite includes over 25 easy-to-use reliability tools that cover guidance and application of reliability design, analysis, testing and support techniques.

1. Quantitative Evidence from defined methods of analysis to generate metrics that demonstrate the required (or desirable) reliability features in the target product. This type of evidence includes the results of any testing.
2. Qualitative Evidence, which focuses on the processes used for development and support of the system. It seeks to assure satisfaction of reliability requirements by inference, based on the demonstrable quality, maturity, and integrity of the underlying engineering and management processes.
3. Historical or Comparative Evidence, which could be relevant for systems already in use. Comparative evidence could be relevant for a system that is a variant of, or similar to, an existing product. The information provided might include both quantitative and qualitative aspects of the product and the associated support services.

When the best practices just described are discussed with technical people who do not work in reliability, a common reaction is "These don't seem to be much more than good sense and sound engineering". They are, of course, correct in this observation. Why, then, are they not applied consistently on all programs? "Reasons" abound. "There is insufficient time, insufficient money, or both." "The system is made up of NDI so reliability is not an issue." This system is similar to one that has good reliability."

Despite these "reasons," the truth is that it is always less expensive and causes less schedule delays to do it right the first time than to try to fix it later.

Some Closing Thoughts

In this brief article, it is impossible to address all of the complications that make system acquisition one of the most challenging jobs in the world. The discussions are, by necessity, abbreviated and treat the acquisition process in a simplified manner. Political, technical, staffing, and other factors contribute to the challenges. Nonetheless, the basic practices discussed in the article have been proven to work. They help government and contractor staffs manage inherent program risks. They contribute to the development of systems that are effective, and upon which our warfighters can rely. And that is the ultimate goal of any program.

Editor's Note
Ned H. Criscimagna is President of Criscimagna Consulting LLC and has over 41 years experience in reliability and maintainability engineering, aircraft maintenance, DOD and military service policy development, defense acquisition, and acquisition logistics. Ned previously served in many roles for the Reliability Analysis Center (RAC) before it became the Reliability Information Analysis Center (RIAC) in June 2005, and we are pleased that he continues that affiliation in support of the RIAC Training Program.

AGENT AUTONOMY APPROACH TO RELIABILITY ASSESSMENT OF COMPLEX DYNAMIC SYSTEMS

Mohammadreza Azakhail, RIAC (University of Maryland)
Mohammad Modarres, RIAC (University of Maryland)

Conventional reliability assessment methods such as fault tree, event tree and reliability block diagrams [1], [2] proved to be cumbersome to capture the dynamics and loss of redundancy of a time dependent system [3], [4]. This is mainly because, in a dynamic system, not only the properties and configuration of components, but also the failure logic may vary by time. This makes it difficult (if possible at all) to list all potential scenarios prior to the modeling stage, as an essential step in conventional methods.

The other constraint is modeling the CCF (common cause failure) within and between independent dynamic assemblies and system blocks. Without a convenient model for the system failure, modeling of the CCF is not practical [5]. In this article, a direct and efficient intelligent agent-oriented simulation is proposed to model the reliability of a long-term complex dynamic system. The failures are simulated using Monte Carlo type methods applied to a system of intelligent computer agents. These software agents act autonomously to mimic their counterparts in a real system. In the first part of this article the intelligent agent-oriented approach is introduced. The approach will be then be further discussed through a case study addressing the reliability of a propulsion system used in NASA's outer planetary phased missions.

Motivations

For redundant systems, fault tree analysis becomes very complex to show the transition behavior of standby assemblies, particularly when the reserve units are not identical or when they are actuated in order. Fault tree generally shows a snap-shot reliability which is not dynamically sensitive to the variation of operational conditions. This calls for separate fault trees for every possible configuration of the system. The number of possible system configurations grows exponentially with the number of components and their states, and this makes the conventional approach quite inconvenient.

In a simple parallel assembly for a reliability block diagram, those failure modes that directly act at the system level may be separated to be considered in a series configuration with the whole parallel assembly. This, however, becomes a hassle for standby units since the presence of these units in the failure logic of the system is time dependent.

Despite the complexity and number of possible scenarios, the final state of each situation has been accurately planned in the design stage. This knowledge is usually documented in the form of a failure modes and effects analysis (FMEA) for the complex system of interest. In such documents, simplicity is achieved by the classification of events and failure modes and effects. This approach allows the modeler to set the conditions and rules for the group of events. Using this state of mind, one can reduce the number of scenario branches that need to be modeled in the simulator. The best example of this situation is the application of cellular automata in the modeling of physical systems [6] in which incredibly complex results may be created by repeating unbelievably simple rules. In the cellular automata approach, every cell has finite states and evolves in a discrete time space by only a few rules to forecast the state of the cell, depending on the state of its neighboring cells. These simple rules amazingly lead the system of cells to very complex situations, apparently impossible to predict from the beginning.

The modeling would be dramatically simplified if one could model a stereotype failure mode within a stereotype component exactly the way they are defined in a typical FMEA document. This makes modeling more or less like posturing the design conditions in general terms, yet including all possible cases. Therefore, the modeler can answer all of the "what if" questions at lower levels of detail and will be able to set the rules and conditions for each group of events.

In this research, a computer-based direct simulation is made to account for the dynamic failure logic, design and control characteristics of the system. In this system simulation, every part of the system is replaced by an intelligent piece of software that represents the properties and behaviors of its real counterpart from the system. These software agents are meant to support the main logic core of the system to evaluate the final state of the complex system, given the final state of the parts. In the following sections, the important aspect of the agent-oriented modeling approach is explained and some benefits and challenges are discussed further.

Agent-Oriented Modeling

Agent-Oriented Modeling is a growing field of study in computer science and artificial intelligence [7]. There is no unique definition for the term 'intelligent agent' in computer science and artificial intelligence. There are a number of on-going debates about the definition of computer agents, their classifications, and even whether an agent is anything but a computer program or not [8]. In our research, the term agent means a collection of properties and methods encapsulated in an entity, which has autonomy in action and the ability to communicate with its environment, and with other agents.

The agent-based approach shares many common characteristics with its ancestor, object-oriented programming, yet each has their own particular place in software development [9]. The importance of agents relies on their autonomy in action and their capability to be mobile. The autonomy and mobility become extremely important when the model needs to be executed in a distributed system environment ranging from a VLSI (very large-scale integration) chip to a coupled shared memory multiprocessor, or from a local cluster of worksta-tions to the Internet [10]. The fact is that the advanced prog-ress of networked technology took modeling beyond the boundary of a single computer power. Web-based distrib-uted problem solving in engineering applications is now an absolute viable goal [11]. Using pure Monte Carlo sampling in this research, the computational time may become an is-sue, since many trials are needed to perceive very small fail-ure rates and probabilities of simple events. Weighted and importance sampling [12] are among possible methods to improve the situation for analyzing complex systems, nev-ertheless the agent-oriented approach provides a means to distribute the load of computation among multiprocessor machines, or even different hosts through the Internet, and opens the door to endless possibilities for the future.

Distributed Intelligence Standpoint

In real engineering applications, the components of the sys-tem are physically distributed. They are also heterogeneous in functional terms, meaning that components and subsystems

have their own properties and behaviors. From the modeling point of view, the objective is to make the system manage-able by reducing the complexity of the system call to a local viewpoint, leading to a hierarchical representation of the sys-tem that ultimately compels a distributed view of the system. Each component has its own persistent thread to influence the final state of the system, which one may consider as a sort of intelligence within the component that makes appropriate decisions on its own destiny (e.g. success or failure). Compo-nents respond to changes, and do it autonomously, using their intelligence by managing their properties and behaviors.

In conventional reliability assessment tools such as fault tree/ event tree and reliability block diagrams, the modeler should think of all possible scenarios and build a model a priori. In the agent-oriented approach, we distribute the failure knowl-edge of the system among the agents and make the problem way more manageable. Therefore, the modeling procedure is basically a distribution of intelligence (i.e. failure knowledge) among the agents of the system, so that groups of scenarios can be modeled at a convenient level of detail.

Treatment of Common Cause Failures

A CCF is the failure of more than one component due to a shared root cause. CCFs are classified as dependent failures. Implicit and explicit methods are two possible approaches to incorporate common cause in the system analysis [13]. Since all available methods for CCF assessment need to be applied to the reliability model of the system [14], one of the constraints in modeling CCFs in the reliability of dynamic complex systems is the lack of a solid model for the system failure. In an agent-based simulation, however, the CCF is modeled using the communication ability of agents, mean-ing that the failed agent communicates the reason for failure to other similar agents and lets them know if it failed due to a common cause. Again, Monte Carlo based sampling can combine the available knowledge on CCFs with the direct simulation of the system. Using this approach, the chance of a CCF is always sampled based on conditional probabilities driven by the data provided on CCF probabilities [15], yet consistent with the dynamic configuration of the system.

Over 20 years in the making.
Relex Reliability Studio

Relex Reliability S

The newest release of the ground-breaking Relex

Studio platform, Relex Reliability Studio 2007,

brings all new power and efficiency to reliability

analyses. With a broad range of additional capabilities

and streamlined features, Relex Reliability Studio 2007

once again demonstrates why Relex is the tool of

choice for reliability professionals worldwide.

See it. Experience it. View the trailer at
www.relexthemovie.com

Relex Reliability Studio

Fault Tree/Event Tree

FMEA/FMECA

FRACAS Corrective Action

Human Factors Risk Analysis

Life Cycle Cost

Maintainability Prediction

Markov Analysis

Optimization and Simulation

Reliability Block Diagram

Reliability Prediction

Weibull Analysis

Impressive new capabilities. Right away, you'll notice the stunning new graphical engine introduced in the Relex Reliability Studio 2007 Architect and *i*Architect platforms. Providing the ability to create a wide array of visually exciting new graphical outputs, Relex Reliability Studio 2007's graphical features are unmatched. Additionally, the newly streamlined Project Navigator insures smooth and efficient Project management, and the new Module Toolbar offers one-click workspace configuration.

Keeping up with today's technology. Relex Reliability Studio 2007 is jam-packed with a remarkable list of technology-based updates. Studio 2007 fully integrates the new 217Plus™ prediction methodology from RIAC. Relex *i*Architect, Relex's Studio's zero-client, web-based interface, introduces a rich new user interface with a true Windows-like look and feel. And, Relex Reliability Studio 2007 supports Microsoft SQL Server 2005®, Oracle® 10g, and Microsoft Vista®.

Ready to learn more? For more details on the new Relex Reliability Studio 2007 features, go to www.relex.com/products/whatsnew2007.asp. Or, put Relex Studio to the test and download a free evaluation copy to check out all the features and capabilities yourself. Go to www.relex.com and click the Download Demo button. Or just pick up the phone and talk to one of our Application Consultants today at 724.836.8800!

Relex
excellence in reliability

Case Study: Ion Propulsion System

Ion propulsion systems are designed to provide thrust for space vehicles for future missions to the outer solar system in NASA's scientific agenda. These missions typically have several phases in which the propulsion system will be required to either move the vehicle through the orbits or maintain it in a particular orbit. A typical ion propulsion system consists of different thruster assemblies (Figure 1) and a propellant supply. The mission profile, design description and failure modes and effects of the propulsion system of interest will be shortly introduced in the following sections. For more details about the propulsion system including design characteristics and reliability related concerns, the interested reader is referred to the conference paper published earlier on this topic [15].
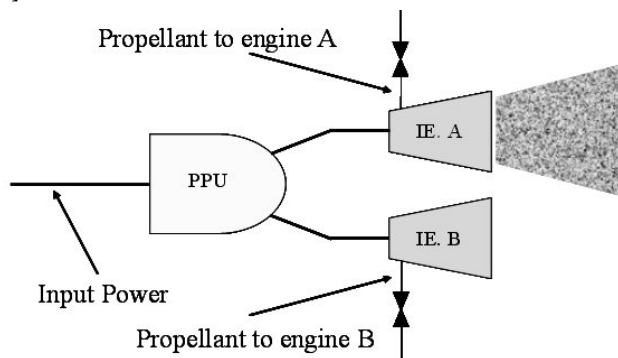

Figure 1. Thruster Assembly

Mission Time Profile

Figure 2 shows the mission phases, as well as the hours of operation, of the propulsion system during the mission. As shown in this figure, the propulsion system only operates partially (i.e., shaded area in Figure 2) in some phases. During
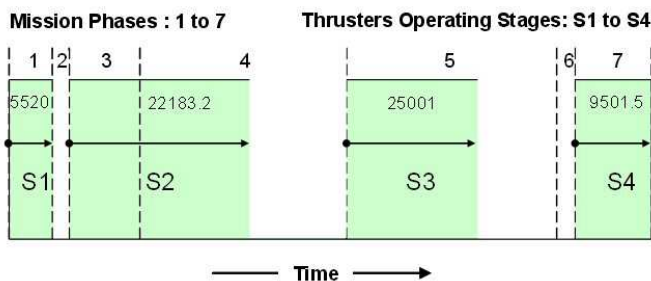

Figure 2. Propulsion System Mission Time Profile

the operation, however, the thrust should be continuously provided from the beginning until the specified operating time expires. As illustrated in Figure 2, it is evident that the whole mission can be summarized into four distinct periods of time (i.e., stages 1 to 4) in which the propulsion system should start at the beginning, continuously operate and, finally, stop at the end of the specified time interval.

Having the reliability in the four different stages of the mission provides the information needed for design optimization purposes. This classification also provides a means to deal with the system failure modes that only matter at the start/stop conditions (e.g., failure to close or open a propellant valve).

Design Description

This particular design employs five thruster assemblies with a single propellant supply which is shared for assemblies. Each assembly has one propulsion power unit (PPU) and two ion engines in a redundant configuration. The engine ionizes and accelerates the propellant to produce thrust. Figure 1 shows a sketch of such thruster assemblies. The PPU is providing power to only one of these ion engines and the other engine remains in standby mode unless failed. When ion engine A fails, the unit shuts down the PPU, closes the propellant valve A, switches the PPU to engine B, then opens the propellant valve B and reenergizes the PPU to operate with ion engine B. There are no intermediate switches between a PPU and the ion engines, and all switches are included as part of the PPU.

In Phase One, the success criteria are two out of four assemblies, and in the subsequent phases, three out of five assemblies. Note that in Phase One, only two standby assemblies are available because the mission is considered failed if more than two assemblies fail during this phase. This is obviously dictated by the thrust requirement in the subsequent phases. The general policy is to use the thruster assemblies in order. Failure of one assembly replaces it with the lowest numbered standby unit. Basically, standby assemblies remain standby until they are needed to replace a failed assembly, and always the lowest numbered assembly is triggered first.

Failure Modes and Effects

Table 1 summarizes the failure modes and effect analysis of the propulsion system. The system, as listed in this table, has some modes of failure (such as failure to open/shut down on

demand) that only matter when the system is in the start/stop transitional state. These failure modes can not be easily modeled like a simple event series with the subsystem of interest. For example, 'failure to close' for a propellant valve is treated as an external leakage and results in a lack of propellant for the rest of mission. The contribution of this failure mode in the failure of the propulsion system is time dependent, meaning that it only plays a role when a valve is ordered to be closed. The failure rate or probability of this event can not be considered as a solid block either in the reliability block diagram of an ion engine or the system because this simple event (which is in a series configuration with the whole system when the valve is in closing transitional mode) has no contribution to the reliability of the system when the corresponding engine is in active or standby mode.

Table 1. Failure Modes and Effects Analysis

Component	Failure Mode	Effect
PPU	Fails to start on demand	Assembly failure
	Fails to operate	
	Fails to shut down on demand	
Ion Engine A	Fails to start on demand	Loss of redundancy
	Fails to operate	
Ion Engine B	Fails to start on demand	Assembly failure
	Fails to operate	
Propellant Valve A	Fails to open on demand	Loss of Ion Engine A
	Fails to close on demand	System failure
Propellant Valve B	Fails to open on demand	Loss of Ion Engine B
	Fails to close on demand	System failure

For the exact value of the failure rates and probability of simple events used in this case study, the interested reader is referred to our previously published paper [15].

Hierarchy of Agents

Figure 3 shows the class of agents and their communication scheme as implemented in this particular application. Dashed line boxes demonstrate the possible expansion of the problem. For example, human or software agents which are not considered at this level can be added later, or the
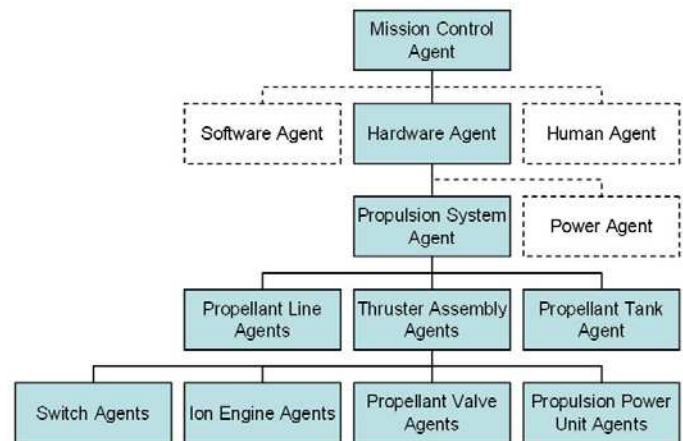

Figure 3. Hierarchy of Agents and Their Communication Scheme

failure of the external power source, which is neglected here, may be considerable in the reliability assessment of other missions.

Later, during the system simulation, clones of these agents will be created automatically. For example, by definition, any assembly has one propulsion power unit, two ion engines and two propellant valves. This requirement is embedded into the assembly agent, so that when the computer creates a new member from the thruster assembly class it will automatically create one propulsion power unit, two ion engines and two propellant valves from the appropriate classes. The new agent, which is cloned from an agent class, automatically inherits all the properties and methods of the parent. This will dramatically reduce the coding requirements, since every module (methods) or variable (properties) will only be introduced one time in the program. Later, in the simulation stage, when an agent is questioned regarding its reliability for a specific mission time, it will automatically contact the appropriate agents to collect enough information prior to making a decision about its destiny.

There are four stages in which reliability needs to be estimated, as explained in the mission time profile section. Based on the requirement of each stage, assemblies and their related components are called for duty. Agents report the status of involved elements and make the mission control agent able to decide whether the propulsion system fails in this stage. If the propulsion system fails, a whole new trial will be started and, if not, the status of all elements is saved and the procedure would proceed to the subsequent stages.
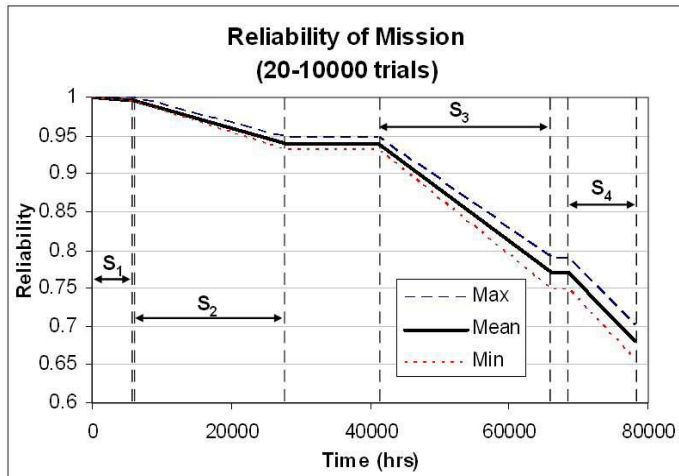
Figure 4. Reliability at Different Stages of Mission

Results

Figure 4 shows the estimated time-dependent reliability of the mission. In this simulation, the estimated reliability for each stage remains constant until the beginning of the next stage. This is basically because, at this period, there is no action with a major reliability concern. This, however, will change if the probabilities of external leakages are being considered in the reliability model of the system [15]. The maximum and minimum bounds presented in Figure 4 are due to the random nature of simulation. The provided results were computed using ten thousand trials. This calculation was then repeated twenty times to show the random nature of Monte Carlo based simulations.

Agent-oriented modeling, as introduced in this work, provides many features to deal with the complexity in dynamic reliability assessment applications. Extremely small probabilities of simple events and component failure rates may force larger numbers of trials to allow the simulation to capture the essence of the component failures. The computational time increases almost proportionally to the number of trials, and may become an issue when probabilities and failure rates are extremely small. The agent-oriented approach in modeling opens the door to parallel and distributed computing to overcome this disadvantage. Nevertheless, the Monte Carlo nature of simulation allows the ability to run the program on many computers simultaneously and reduce the computational time by dividing the required number of trials among them.

References

1. Vesely, W. E., et al., 2002, "NASA Fault Tree Handbook with Aerospace Applications", National Aeronautics and Space Administration (NASA), Washington DC.
2. Office of Safety and Mission Assurance, 2002, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners", NASA Headquarters, Washington DC.
3. Modarres. M., 2006, *Risk Analysis in Engineering, Techniques, Tools, and Trends*, CRC Press, Florida
4. O'Conner, P., 2002, *Practical Reliability Engineering*, John Wiley and Sons, Chichester, England.
5. Mosleh, A., 1991, "Common Cause Failures: An Analysis Methodology and Examples", Reliability Engineering and System Safety, Vol. 34, pp. 249-292.
6. Chopard, B. and Droz, M., 1998, *Cellular Automata Modeling of Physical Systems*, Cambridge University Press, Cambridge UK.
7. Bradshaw, J. (ed.), 1997, *Software Agents*, AAAI Press.
8. Franklin, S., et al., 1996, "Is it an Agent, or Just a Program?: A taxonomy for Autonomous Agents", Proceedings of the Third International Workshop on Agents Theories, Architectures, and Languages, Springer-Verlag.
9. Odell, J., 2002, "Objects and Agents Compared", Journal of Object technology, Vol. 1, No. 1, pp. 41-53.
10. Attiya H., Welch J., 2004, *Distributed Computing, Fundamentals, Simulations and Advanced Topics*, John Wiley and Sons, N J.
11. Cheng, H. C., Fen C. S., 2006, "A Web-Based Distributed Problem- Solving Environment for Engineering Applications", Advances in Engineering Software, Vol. 37, pp. 112-128.
12. Liu, J. S., 2001, *Monte Carlo Strategies in Scientific Computing*, Springer Series in Statistics, Springer-Verlag, New York.
13. Fleming, K. N., Mosleh, A., 1985, "Common-Cause Data Analysis and Implications in System Modeling", Proc. Int'l Topical Meeting on Probabilistic Safety Methods and Applications, Vol. 1, pp. 3/1-3/12, EPRI NP-3912-SR.
14. Mosleh, A., et al., 1989, "Procedures for Treating Common Cause Failures in Safety and Reliability Studies", Procedural Framework and Examples, NUREG/CR-4780, EPRI NP-5613, Vol. 1, Electric power Research Institute.
15. M. Azarkhail, M. Modarres, "An Intelligent Agent Oriented Approach to Risk Analysis of Complex Dynamic Systems with Applications in Planetary Missions", PSAM8 Conference, May 15-19, 2006, New Orleans, Louisiana, USA.

AN/ALQ-184 (V) Electronic Attack Pod Reprogrammable Low Band Processor Printed Wire Assembly Failure Analysis Study

Warner Robins Air Logistics Center (542 CBSSS/GBEAA) is tasked with sustainment of the AN/ALQ-184 (V) Electronic Attack (EA) Pod. The mission effectiveness of the AN/ALQ-184 (V) EA Pod is degraded because of the frequent failures of the Reprogrammable Low Band Standard Processor Printed Wire Assembly (RLB PWA). The purpose of the work is to provide the 542 CBSSS/GBEAA with a detailed analysis of the underlying causes of the failures associated with the RLB PWA. There are two phases to the analysis: (1) Causal and (2) Failure Elimination and Control.

During the Causal Analysis Phase, the Reliability Information Analysis Center (RIAC) Team evaluated six RLB PWAs and one card cage. The analysis included visual inspections, modeling, environmental, vibration, maintenance, and electrical testing. Although environmental conditions may affect long-term life of different components, they are not root cause failure mechanisms. Visual inspections of the sample PWAs determined that board composition or production flaws are not functional failures. Maintenance practices performed in the field and at the depot are not directly responsible for PWA failure. Better shipping and handling procedures, new tools for easier removal and insertion of the RLB PWA, and a thorough review of technical orders and troubleshooting manuals to eliminate known discrepancies will reduce maintenance time and effort, thus saving money and increasing reliability.

The results of the electrical analysis, however, represent an unusual root cause failure mechanism. Very high voltage pulses (spikes) cause time domain reflections that generate unwanted over-range voltage spikes resulting in U1 IC chip bond wire failure. This failure causes either Vcc node failure (spike on the supply path) or I/O ESD protection circuit coupled failure (current path will still be through each of the Vcc wire bonds and ground). The U1 IC chip bond wires act as high-power fuse protectors, actually protecting the chip from catastrophic burnout. The multiple spikes that cause the bond wires to melt are random and can not be filtered at the source. It is also cost prohibitive to filter out all random pulses.

The RIAC team's Failure Elimination and Control Phase recommendations provided three options for government engineers to consider for root failure mitigation and long-term sustainment of the system: implement an LC network to carry the noise pulses to ground, add diffused or thin film resistors to bond pad wire to ensure noise spike pulses dissipate rapidly to ground, or a combination of both in the form of an LCR network on a separate chip. Follow-on work is planned to either redesign the U1 chip or redesign the PWA to eliminate the failure. This will ensure that the U.S. Air Force can continue to fly the approximately 1,000 AN/ALQ-184 Jammer Pods well into the next decade.
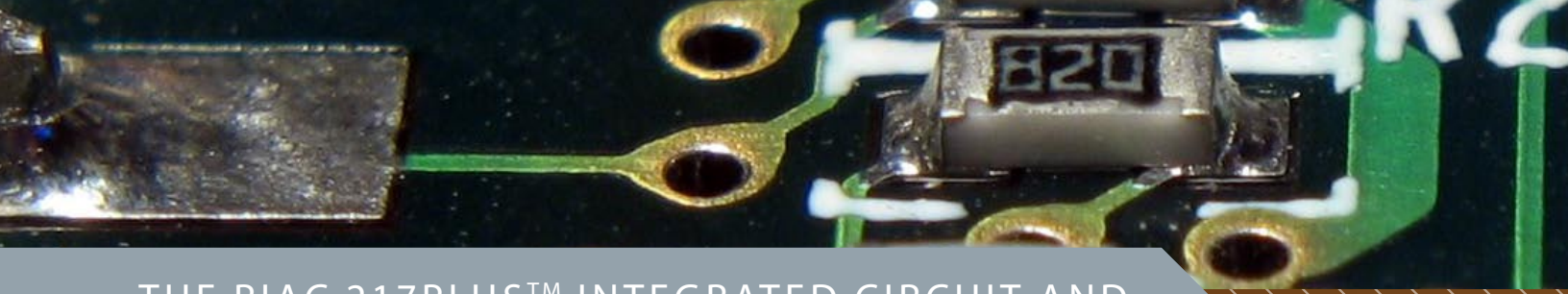
THE RIAC 217PLUS™ INTEGRATED CIRCUIT AND INDUCTOR FAILURE RATE MODELS

David Nicholls, RIAC (Quanterion Solutions Incorporated)

In a previous issue of the RIAC Journal [Reference 1], we provided a high-level introduction to the 217Plus™ component failure rate prediction models, and in the last edition [Reference 2] we presented the 217Plus™ capacitor and diode failure rate models.

In this issue, we present the Integrated Circuit and Inductor component models in their entirety. A brief example will be provided at the end of the article.

217Plus™ Integrated Circuit Failure Rate Models

This section contains models for both nonhermetic and hermetically sealed integrated circuits. The form of the two models is basically the same (differences will be highlighted), but the table look-up parameter values differ.

The failure rate equation for nonhermetic integrated circuits [Reference 3] is:

$$\lambda_P = \pi_G \left(\lambda_{OB} \pi_{DCO} \pi_{TO} + \lambda_{EB} \pi_{DCN} \pi_{RHT} + \lambda_{TCB} \pi_{CR} \pi_{DT} \right) + \lambda_{SJB} \pi_{SJDT} + \lambda_{IND}$$

where,

λ_P = Predicted failure rate, failures per million calendar hours

π_G = Reliability growth failure rate multiplier:

$$\pi_G = e^{\left(-\beta (Y - 1993) \right)}$$

β = *Growth constant. Function of integrated circuit type (see Table 1)*

λ_{OB} = Base failure rate, operating. Function of integrated circuit type (see Table 1)

π_{DCO} = Failure rate multiplier for duty cycle, operating:

$$\pi_{DCO} = \frac{DC}{DC_{1op}}$$

DC_{1op} = *Constant. Function of integrated circuit type (see Table 1)*

π_{TO} = Failure rate multiplier for temperature, operating:

$$\pi_{TO} = e^{\left(\frac{-Ea_{op}}{0.00008617} \left(\frac{1}{T_{AO} + T_R + 273} - \frac{1}{298} \right) \right)}$$

Ea_{op} = *Activation energy, operating. Function of integrated circuit type (see Table 1).*

T_R = *The junction temperature rise above the ambient operating temperature (T_{AO}). The junction temperature is therefore $T_{AO} + T_R$. The T_R can be determined in several ways:*

$T_{Rdefault}$ = Default temperature rise (see Table 1)

T_R = Actual (measured) temperature rise, if known

$T_R = \Theta_{JA} * P$
where Θ_{JA} is the junction-to-ambient thermal impedance and P is the power dissipated by the integrated circuit

$T_R = \Theta_{JC} * P$

where Θ_{JC} is the junction-to-case thermal impedance and P is the power dissipated by the integrated circuit

If this option is used, then T_{AO} should be replaced by T_C, the component case temperature, in the equation for π_{TO}

λ_{EB} = Base failure rate, environmental (see Table 1)
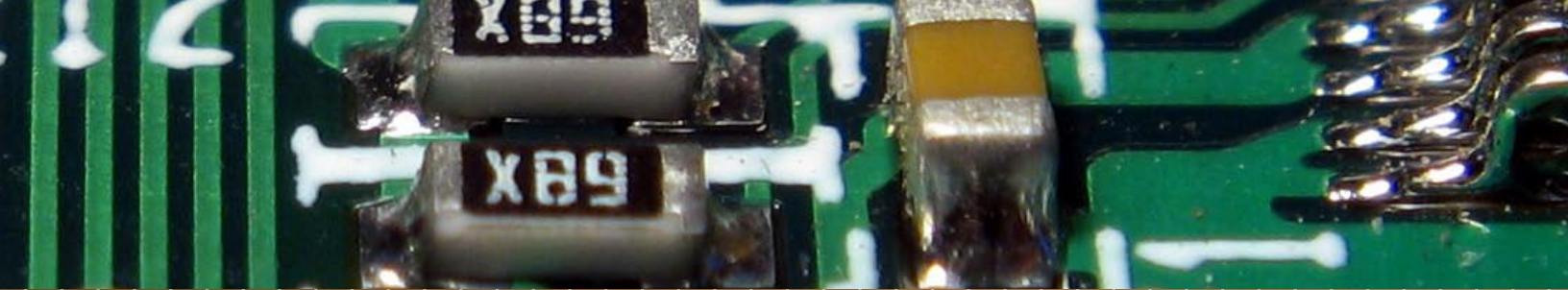
λ_{DCN} = Failure rate multiplier, duty cycle – nonoperating:

$$\pi_{DCN} = \frac{1 - DC}{DC_{1nonop}}$$

DC_{1nonop} = *Constant. Function of integrated circuit type (see Table 1)*

λ_{RHT} = Failure rate multiplier, temperature – humidity:

$$\pi_{RHT} = e^{\left(\frac{-Ea_{nonop}}{0.00008617}\left(\frac{1}{T_A + 273} - \frac{1}{298}\right)\right)} \left(\frac{RH}{0.5}\right)^3$$

Ea_{nonop} = *Activation energy, nonoperating. Function of integrated circuit type (see Table 1)*

λ_{TCB} = Base failure rate, temperature cycling (see Table 1)

π_{CR} = Failure rate multiplier, cycling rate:

$$\pi_{CR} = \frac{CR}{CR_1}$$

CR_1 = *Constant. Function of integrated circuit type (see Table 1)*

π_{DT} = Failure rate multiplier, delta temperature:

$$\pi_{DT} = \left(\frac{T_{AO} + T_R - T_{AE}}{DT_1}\right)^4$$

DT_1 = *Constant. Function of integrated circuit type (see Table 1)*

λ_{SJB} = Base failure rate, solder joint (see Table 1)

π_{SJDT} = Failure rate multiplier, solder joint delta temperature:

$$\pi_{SJDT} = \left(\frac{T_{AO} + T_R - T_{AE}}{44}\right)^{2.26}$$

λ_{IND} = Failure rate, electrical overstress (see Table 1)

NOTE: Environment-type and equipment-dependent default values for DC, T_{AO}, T_{AE} and CR were previously presented in Reference 1, where,

DC = Duty cycle (the percent of calendar time that the system in which the component is operating is in an operational state)

T_{AO} = Ambient temperature, operating (in degrees C)

T_{AE} = Ambient temperature, nonoperating (in degrees C)

CR = Cycling rate (the number of power cycles per-year to which the system is exposed). In this case, it is assumed that the system transitions from a nonoperating environment to an operating environment at the same time that the power is applied.

Table 1: Integrated Circuit, Nonhermetic Parameters

Part Type	λ_{OB}	λ_{EB}	λ_{TCB}	λ_{IND}	λ_{SJB}	β	DC_{1op}	Ea_{op}	$T_{Rdefault}$	DC_{1nonop}	Ea_{nonop}	CR_1	DT_1
Digital, Nonhermetic	0.000007	0.000385	0.000249	0.000263	0.00485	0.473	0.28	0.8	13	0.72	0.3	482.46	26.5
Linear, Nonhermetic	0.000013	0.001997	0.000089	0.001562	0.00485	0.293	0.28	0.8	25	0.72	0.3	482.46	26.5
Memory/Microprocessor, Nonhermetic	0.000008	0.000634	0.000025	0.000552	0.00485	0.479	0.28	0.8	20	0.72	0.3	482.46	26.5

The failure rate equation for hermetic integrated circuits [Reference 3] is:

$$\lambda_P = \pi_G\left(\lambda_{OB}\pi_{DCO}\pi_{TO} + \lambda_{EB}\pi_{DCN}\pi_{TE} + \lambda_{TCB}\pi_{CR}\pi_{DT}\right) + \lambda_{SJB}\pi_{SJDT} + \lambda_{IND}$$

Where all variables are as defined for the nonhermetic integrated circuit model, except:

- π_{TE} replaces π_{RHT} in the nonoperating failure rate calculation, and π_{TE} is calculated as:

$$\pi_{TE} = e^{\left(\frac{-Ea_{nonop}}{0.00008617}\left(\frac{1}{T_{AE}+273} - \frac{1}{298}\right)\right)}$$

  where

  Ea_{nonop} = *As defined above*

- The equation for π_{DT} is:

$$\pi_{DT} = \left(\frac{T_{AO} + T_R - T_{AE}}{DT_1}\right)^{4.8}$$

- All look-up table values are from Table 2:

217Plus™ Inductor Failure Rate Model

The failure rate equation for inductors [Reference 3] is:

$$\lambda_P = \pi_G\left(\lambda_{OB}\pi_{DCO}\pi_{TO} + \lambda_{EB}\pi_{DCN}\pi_{TE} + \lambda_{TCB}\pi_{CR}\pi_{DT}\right) + \lambda_{IND}$$

λ_P = Predicted failure rate, failures per million calendar hours

π_G = Reliability growth failure rate multiplier:

$$\pi_G = e^{\left(-\beta(Y - 1993)\right)}$$

β = *Growth constant. Function of inductor type (see Table 3).*

λ_{OB} = Base failure rate, operating (see Table 3)

π_{DCO} = Failure rate multiplier for duty cycle, operating:

$$\pi_{DCO} = \frac{DC}{DC_{1op}}$$

DC_{1op} = *Constant. Function of inductor type (see Table 3)*

π_{TO} = Failure rate multiplier for temperature, operating:

$$\pi_{TO} = e^{\left(\frac{-Ea_{op}}{0.00008617}\left(\frac{1}{T_{AO}+T_R+273} - \frac{1}{298}\right)\right)}$$

Ea_{op} = *Activation energy, operating. Function of inductor type (see Table 3)*

T_R = *The junction temperature rise above the ambient operating temperature (T_{AO}). The junction temperature is, therefore, $T_{AO}+T_R$. The T_R can be calculated in several ways:*

$T_{Rdefault}$ = Default temperature rise (see Table 3)

T_R = Actual temperature rise, if known

λ_{EB} = Base failure rate, environmental (see Table 3)

π_{DCN} = Failure rate multiplier, duty cycle - nonoperating:

$$\pi_{DCN} = \frac{1 - DC}{DC_{1nonop}}$$

DC_{1nonop} = *Constant. Function of inductor type (see Table 3)*

Table 2: Integrated Circuit, Hermetic Parameters

Part Type	λ_{OB}	λ_{EB}	λ_{TCB}	λ_{IND}	λ_{SJB}	β	DC_{1op}	Ea_{op}	$T_{Rdefault}$	DC_{1nonop}	Ea_{nonop}	CR_1	DT_1
Digital, Hermetic	0.00027	0.00026	0.00021	0.00072	0.00485	0.33	0.33	0.8	13	0.67	0.3	349.12	30
Linear, Hermetic	0.000084	0.00053	0.000048	0.00045	0.00485	0.33	0.33	0.8	25	0.67	0.3	349.12	30
Memory/Microprocessor, Hermetic	0.0002	0.0012	0.00071	0.00078	0.00485	0.33	0.33	0.8	20	0.67	0.3	349.12	30

Table 3: Inductor Parameters

Part Type	λ_{OB}	λ_{EB}	λ_{TCB}	λ_{IND}	β	DC_{1op}	Ea_{op}	$T_{Rdefault}$	DC_{1nonop}	Ea_{nonop}	CR_1	DT_1
Choke	0.0000766	0.0000819	0.0000328	0.0000148	0	0.40	0.47	0	0.60	0.080	413	13.23
General	0.0000008	0.0000018	0.0000003	0.0000002	0	0.40	0.47	0	0.60	0.080	413	13.23

π_{TE} = Failure rate multiplier, temperature – environment:

$$\pi_{TE} = e^{\left(\frac{-Ea_{nonop}}{0.00008617}\left(\frac{1}{T_{AE}+273} - \frac{1}{298}\right)\right)}$$

   Ea_{nonop} = *Activation energy, nonoperating Function of inductor type (see Table 3)*

λ_{TCB} = Base failure rate, temperature cycling (see Table 3)

π_{CR} = Failure rate multiplier, cycling rate:

$$\pi_{CR} = \frac{CR}{CR_1}$$

   CR_1 = *Constant. Function of inductor type (see Table 3)*

π_{DT} = Failure rate multiplier, delta temperature:

$$\pi_{DT} = \left(\frac{T_{AO} + T_R - T_{AE}}{DT_1}\right)^2$$

   DT_1 = *Constant. Function of inductor type (see Table 3)*

λ_{IND} = Failure rate, induced (see Table 3)

As with the Integrated Circuit models, the environment-type and equipment-dependent default values for DC, T_{AO}, T_{AE} and CR were previously presented in Reference 1.

Example Calculation

What is the predicted failure rate of a digital, nonhermetic integrated circuit manufactured in 2006. The IC operates in a "Ground, Mobile, Heavy-wheeled" vehicle with an assumed operating temperature of 55°C, a dormant temperature of 14°C and a relative humidity of 40%. The actual temperature rise of the device is not known. The operating profile of the equipment is typical of military ground equipment, with a duty cycle of 45% and a cycling rate of 263 cycles per year.

The failure rate equation for a nonhermetic integrated circuit [Reference 3] is:

$$\lambda_P = \pi_G \left(\lambda_{OB}\pi_{DCO}\pi_{TO} + \lambda_{EB}\pi_{DCN}\pi_{RHT} + \lambda_{TCB}\pi_{CR}\pi_{DT}\right) + \lambda_{SJB}\pi_{SJDT} + \lambda_{IND}$$

where,

   $\pi_G = e^{(-\beta(Y-1993))} = 0.002136$

      β = 0.473 (from Table 1) and
      Y = 2006 (given)

   λ_{OB} = 0.000007 (from Table 1)

$$\pi_{DCO} = \frac{DC}{DC_{1op}} = 1.607$$

      DC = 0.45 (given as 45%)
      DC_{1op} = 0.28 (from Table 1)

$$\pi_{TO} = e^{\left(\frac{-Ea_{op}}{0.00008617}\left(\frac{1}{T_{AO} + T_R + 273} - \frac{1}{298}\right)\right)} = 50.83$$

      Ea_{op} = 0.80 (from Table 1)
      T_{AO} = 55 (given)
      $T_{Rdefault}$ = 13 (from Table 1)

   λ_{EB} = 0.000385 (from Table 1)

$$\pi_{DCN} = \frac{1 - DC}{DC_{1nonop}} = 0.7639$$

      DC = 0.45 (given as 45%)
      DC_{1nonop} = 0.72 (from Table 1)

$$\pi_{RHT} = e^{\left(\frac{-Ea_{nonop}}{0.00008617}\left(\frac{1}{T_{AE} + 273} - \frac{1}{298}\right)\right)}\left(\frac{RH}{0.5}\right)^3 = 0.3272$$

      Ea_{nonop} = 0.30 (from Table 1)
      T_{AE} = 14 (given)
      RH = 40% (given)

   λ_{TCB} = 0.000249 (from Table 1)

$$\pi_{CR} = \frac{CR}{CR_1} = 0.5451$$

      CR = 263 (given)
      CR_1 = 482.46 (from Table 1)

$$\pi_{DT} = \left(\frac{T_{AO} + T_R - T_{AE}}{DT_1}\right)^4 = 17.24$$

T_{AO} = 55 (given)
$T_{Rdefault}$ = 13 (from Table 1)
T_{AE} = 14 (given)
DT_1 = 26.5 (from Table 1)

λ_{SJB} = 0.00485 (from Table 1)

$$\pi_{SJDT} = \left(\frac{T_{AO} + T_R - T_{AE}}{44}\right)^{2.26} = 1.589$$

T_{AO} = 55 (given)
$T_{Rdefault}$ = 13 (from Table 1)
T_{AE} = 14 (given)

λ_{IND} = 0.000263 (from Table 1)

$$\lambda_P = 0.002136\left[(0.000007)(1.607)(50.83) + (0.000385)(0.7639)(0.3272) + (0.000249)(0.5451)(17.24)\right]$$
$$+ (0.00485)(1.589) + (0.000263)$$

λ_P = 0.007976 f/10^6 calendar hours

Next Issue

The next issue of the RIAC Journal (4th Quarter 2007) will present the 217Plus™ transformer and optoelectronic devices failure rate models in more detail.

References

1. "An Introduction to the RIAC 217Plus™ Component Failure Rate Models", Journal of the Reliability Information Analysis Center, First Quarter 2007, available for PDF download from the RIAC at http://theRIAC.org
2. "The 217Plus™ Capacitor and Diode Failure Rate Models", Journal of the Reliability Information Analysis Center, Second Quarter 2007, available for PDF download from the RIAC at http://theRIAC.org
3. Denson, W.K., "Handbook of 217PlusTM Reliability Prediction Models", Reliability Information Analysis Center (RIAC), 26 May 2006, ISBN 1-933904-02-X
4. "An Overview of the 217Plus™ System Reliability Assessment Methodology", Journal of the Reliability Information Analysis Center, Fourth Quarter 2006, available for PDF download from the RIAC at http://theRIAC.org

RIAC JOURNAL SURVEY
THIRD QUARTER – 2007

Journal Format ☐ Hard Copy ☑ Web Download

How satisfied as you with the **content** (article technical quality) in *this issue* of the Journal?

☐ Very Satisfied ☐ Satisfied ☐ Neutral ☐ Dissatisfied ☐ Very Dissatisfied

How satisfied as you with the **appearance** (layout, readability) of *this issue* of the Journal?

☐ Very Satisfied ☐ Satisfied ☐ Neutral ☐ Dissatisfied ☐ Very Dissatisfied

How satisfied as you with the **overall quality** of *this issue* of the Journal (compared to similar magazines, newsletters, etc.)?

☐ Very Satisfied ☐ Satisfied ☐ Neutral ☐ Dissatisfied ☐ Very Dissatisfied

How did you become **aware** of *this issue* of the Journal?

☐ Subscribe ☐ Colleague ☐ Library ☐ RIAC Website ☐ RIAC Email ☐ Conference/Trade Show

Would you **recommend** the RIAC Journal to a colleague?

☐ Definitely ☐ Probably ☐ Not Sure ☐ Probably Not ☐ Definitely Not

Please suggest general **changes / improvements** to the RIAC Journal that would improve your level of satisfaction:

_____

_____

_____

_____

Please suggest further **topics** for the RIAC Journal that might help it to better meet your needs:

_____

_____

Overall satisfaction

☐ Very Satisfied (5) ☐ Satisfied (4) ☐ Neutral (3) ☐ Dissatisfied (2) ☐ Very Dissatisfied (1)

CONTACT INFORMATION (OPTIONAL)

Name _____ Position/Title _____

Organization _____ Office Symbol _____

Address _____ City _____ State _____ Zip _____

Country _____ Email _____

Phone _____ Fax _____

My Organization Is ☐ Army ☐ Navy ☐ Air Force ☐ Other DoD/Government ☐ Industry ☐ Academic ☐ Other

I need help with a reliability, maintainability, quality, supportability, or interoperability problem. ☐ Please contact me

OCTOBER

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

10th Annual Systems Engineering Conference // San Diego, CA USA

Oct 22, 2007 thru Oct 25, 2007
Contact: Britt Bommelje, Associate Director // P 703.247.2587 // bbommelje@ndia.org

2nd System Safety 2007 International Conference // London, UK

Oct 22, 2007 thru Oct 24, 2007
Contact: Institution of Eng & Technology // P +44 (0) 1438 765650 // F +44 (0) 1438 765659
// jacquie.lee@theiet.org

2007 Combatant Commanders Workshop // Suffolk, VA USA

Oct 29, 2007 thru Oct 30, 2007
Contact: Defense Technical Information Center // P 703.767.8236 // F 703.767.8273
// DTICCoComWorkshop@dtic.mil

Unmanned Systems Interoperability Conference // San Diego, CA USA

Oct 29, 2007 thru Oct 31, 2007
Contact: http://consult-tlw.com/USIC1.htm

NOVEMBER

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Zero Downtime 2007 // Scottsdale, AZ USA

Nov 06, 2007 thru Nov 07, 2007
Contact: Nick Depperschmidt, Equipment Protection Magazine
P 800.803.9488 x111 // nickd@infowebcom.com

IMAPS 2007 - The 40th International Symposium on Microelectronics // San Jose, CA USA

Nov 13, 2007 thru Nov 15, 2007
Contact: IMAPS // P 202.548.4001 // F 202.548.6115 // imaps@imaps.org

DoD Maintenance Symposium & Exhibition // Orlando, FL USA

Nov 13, 2007 thru Nov 16, 2007
Contact: Nancy Eiben, SAE International // P 724.772.8525 // naneiben@sae.org

DECEMBER

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

RIAC Open Training Program // Orlando, FL USA

Dec 04, 2007 thru Dec 06, 2007
Contact: Pat Smalley, Reliability Information Analysis Center // P 877.363.7422 or
315.351.4200 // F 315.351.4209 // psmalley@theRIAC.org

IPC/JEDEC Global Conference on Lead Free Reliability and Reliability Testing for RoHS Lead Free Electronics // Austin, TX USA

Dec 03, 2007 thru Dec 05, 2007
Contact: IPC - Association Connecting Electronics Industry // F 847.615.7105 //
FConf@ipc.org

JANUARY 2008

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

54th Annual Reliability and Maintainability Symposium (RAMS 2008) // Las Vegas, NV USA

Jan 28, 2008 thru Jan 31, 2008
Contact: www.rams.org

Total Life Cycle Cost Benefits Calculator for Root Cause Failure Analysis Decision-Making

by David Nicholls

The purpose of this Microsoft Excel® Workbook is to estimate the net total life cycle cost (TLCC) impact of performing root cause failure analysis and corrective action (CA) identification, implementation and verification to improve system, product, assembly, component, part or process reliability. It is intended to be an aid to the decision-making process that can be used to justify (or not) the upfront financial investment needed to perform root cause failure analysis and CA for specific failure incidents and compare them to the savings that may be achieved over the long term by virtue of the improved reliability of the system, product, assembly, component, part or process. It should be noted that net TLCC impact may be only one factor in determining whether root cause failure analysis and CA should be pursued. Other factors that should be considered may include, but not be limited to, (1) the criticality of the item function, (2) safety/liability impacts associated with a failure (regardless of net TLCC), (3) contractual requirements, (4) schedule constraints and/or (5) resource constraints. Where cost is the sole determining factor, however, the results generated by this tool can be used to convince the user, his/her management, a Program Manager and Senior Management of the long-term financial benefits to the company of determining the root cause of a failure, and implementing the corrective action necessary to improve reliability.

The contents of this Workbook cover three separate areas for which root cause failure analysis and CA activities can be implemented. These areas are (1) Hardware, (2) Process and (3) Software. When doing the net TLCC calculations, the user fills in the relevant information in each of these three areas, as necessary, to adequately describe all of the actions needed to implement the full root cause analysis and CA process. For example, a hardware failure may result in a root cause analysis and corrective action process that is traced back to a defective process, or a need to change software. Therefore, the net TLCC analysis should include the various cost elements associated with each of these areas. The Hardware, Process and Software areas are subdivided into the following tabs: (1) the costs associated with performing root cause analysis (RCA Yes), (2) the costs associated with not performing RCA (RCA No), and (3) the net TLCC impact associated with that area (RCA Net TLCC). There is a summary tab (NET TLCC - SUMMARY) that combines the results to present the composite net TLCC impact that should be used to support the decision to proceed with root cause failure analysis and CA (or not) for that specific failure incident.

Reducing Program Risk Through Independent Testing for 57 Years

Wyle Laboratories, Inc. has provided trusted agent test and evaluation services for more than 57 years. Throughout that period, Wyle has provided quality data that has been key to reducing program risk, resulting in increased system effectiveness for the warfighter. From component testing in the early development phases to independent test engineering services s u p p o rting the operational test phase, through ongoing life cycle evaluation and support, Wyle's exceptional services have been unparalleled across the test continuum.

→ T E S T   C O N T I N U U M →

Advanced Concept Technology Demonstration	Advanced Technology Demonstration	Operational Assessment	Contractor Test and Evaluation	Developmental Test and Evaluation	Initial Operational Test and Evaluation	Live Fire Test and Evaluation	Operational Assessment	Initial Operational Test and Evaluation	Follow-on Operation Test and Evaluation	Joint Test and Evaluation

Through its dedication to provide high level engineering expertise at all stages of the testing process, Wyle today significantly improves the operational performance, effectiveness, and suitability of sea, air, land and space systems and platforms. With capability, capacity and commitment, Wyle reduces program risk, getting the very best systems fielded for the warfighter.

wyle laboratories

www.wylelabs.com   e-mail: service@wylelabs.com

http://theRIAC.org

Save time and money at the RIAC's online store where you can browse, order, and immediately download electronic versions of most of the RIAC's products.

> Online Product Store

> RMQSI Library

> Technical Answers

> The RIAC Journal

> Upcoming Training Courses

> What's New at RIAC

Reliability Information Analysis Center
6000 Flanagan Road │ Suite 3 │ Utica, NY 13502-1348