The Journal of the

RAC

Second Quarter - 2005

Reliability Analysis Center

Practical Considerations in Calculating Reliability of Fielded Products

By: Bill Lycette, Agilent Technologies

INSIDE

Introduction

A widely used measure of product reliability is Mean Time Between Failure (MTBF). Before making a purchase decision for manufacturing equipment or other items, customers frequently require the supplier to provide an MTBF. However, MTBF is not well understood and false assumptions often lead to poor decisions. Improper MTBF calculations used in head-to-head product comparisons can result in sales lost to competitors, higher procurement and maintenance costs, and customer dissatisfaction with product experience.

This article uses technical discussion, example, and practical application to unveil the mystery behind MTBF. Three of the most commonly used statistical distributions of field failure data (exponential, Weibull, and lognormal) are reviewed. MTBF formulas are presented for each distribution. Monte Carlo simulation is then used to compare and contrast five life data models. The relationship between MTBF and Annualized Failure Rate (AFR) is also discussed and a few of the complexities with performing AFR calculations are reviewed.

Readers will be shown common pitfalls associated with reliability metrics and how they can make more informed purchasing decisions that will lead to an improved customer experience.

The MTBF Riddle

Is it possible for two MTBFs with the same value to tell two completely different reliability stories? To answer this question, an experiment was conducted using Monte Carlo simulation to compare and contrast five different sets of life data that have the same MTBF, namely 50,000 hours. In each of these five cases, 100 data points were generated to fit a specified life data distribution using parameters and a seed selected to result in an MTBF of approximately 50,000 hours. Figures 1 through 5 show the resulting probability density functions (*pdfs*).

Reliability Statistics Fundamentals

This article uses three statistical distributions that are important in the field of reliability engineering to model life data, namely the Weibull, exponential and lognormal distributions. We also need to review reliability terminology and the relationship between three fundamental reliability equations.

Firstly, the *pdf* is given by f(t) and represents the relative frequency of failures over time. Secondly, the reliability function is given by R(t) and represents the probability that the product survives until time t. Thirdly, the failure rate function $\lambda(t)$ is given by the following equation, and is also referred to as the hazard rate h(t) or instantaneous failure rate.

$$\lambda(t) = \frac{f(t)}{R(t)}$$

Weibull Distribution

The Weibull distribution is highly valued by the reliability engineer because of its flexibility to model many different life data scenarios.

For life data that fits a Weibull distribution, the probability density function (*pdf*) is given by the following equation, where α is the scale parameter in units of time (also referred to as the characteristic life), β is the unit-less shape parameter, and γ is the location parameter in units of time.

$$f(t) = \frac{\beta}{\alpha}\left(\frac{t-\gamma}{\alpha}\right)^{\beta-1} e^{-\left(\frac{t-\gamma}{\alpha}\right)^{\beta}}$$

Often γ represents shipment transit time of the product. The Weibull reliability function is given by:

$$R(t) = e^{-\left(\frac{t-\gamma}{\alpha}\right)^{\beta}}$$

Therefore, the Weibull failure rate function is given by:

$$\lambda(t) = \frac{\beta}{\alpha}\left(\frac{t-\gamma}{\alpha}\right)^{\beta-1}$$

For any life data that follows a Weibull distribution, the characteristic life, α, is always the operating time, *t*, at which 63.2% of the population is expected to fail.

A value of β less than one indicates a decreasing failure rate and is typical of infant mortality. When β is equal to one, the failure rate function reduces to that given by the exponential distribution and the failure rate is constant at $1/\alpha$. A value of β greater than one indicates an increasing failure rate and is typical of wear-out mechanisms. When β is equal to two, the *pdf* becomes the Rayleigh distribution and the failure rate function increases linearly with time. When the value of β is between three and four, the *pdf* is "normal" in appearance.

The MTBF of the Weibull distribution is given by the following equation, where Γ is the gamma function.

$$MTBF = \alpha \bullet \Gamma\left(\frac{1}{\beta}+1\right)+\gamma$$

Since $\Gamma(2) = 1$, then the MTBF when β is equal to one and γ is equal to zero is:

$$MTBF = \alpha$$

In other words, the only time that the MTBF equals the characteristic life α is when β is equal to one.

Exponential Distribution

For life data that fits an exponential distribution, the *pdf* is given by the following equation, where λ is the failure rate expressed in failures per unit time and γ is the location parameter in units of time.

$$f(t) = \lambda e^{-\lambda(t-\gamma)}$$

The exponential reliability function is given by:

$$R(t) = e^{-\lambda(t-\gamma)}$$

Therefore, the exponential failure rate function is given by:

$$\lambda(t) = \frac{\lambda e^{-\lambda(t-\gamma)}}{e^{-\lambda(t-\gamma)}} = \lambda$$

The exponential distribution is widely used (and often misused) because of its simplicity, and the fact that it has a constant failure rate λ. The MTBF for the exponential distribution is given by:

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

Note: When β is 1.0, the Weibull distribution is equivalent to the exponential distribution, i.e., MTBF = $\alpha = 1/\lambda$. It is also the only scenario when the MTBF can be directly calculated using the reciprocal of the failure rate.

Lognormal Distribution

The lognormal distribution often describes failure processes involving degradation over time, such as corrosion, metal migration, or chemical reaction. The failure rate function is complex and beyond the scope of this article. The times to failure are lognormally distributed if the natural logarithm of the times to failure is normally distributed.

The MTBF of the lognormal distribution is given by:

$$MTBF = e^{(\tau + 0.5\sigma^2)}$$

For this equation, τ is the mean of the natural logarithm of the times to failure and σ is the standard deviation of the natural logarithm of the times to failure.

Further details of these reliability distributions can be found in the literature (References 1 and 2). Instantaneous failure rates, reliability, and MTBFs can be easily calculated using commercially available software (Reference 3).

The MTBF Riddle Explained

Returning to the experiment where Monte Carlo simulation is used to create five unique models of life data, recall that they all have the same MTBF of 50,000 hours.

Figure 1 shows the 2-parameter Weibull distribution (γ = 0), where β is 0.5 and α is 25,000. This example illustrates the classic case of infant mortality where the instantaneous failure rate is decreasing. The *pdf* shows a very high percentage of early failures followed by a steep decline in the number of failures.

In Figure 2, the 2-parameter Weibull distribution is shown where β is 1.0 and α is 50,000. This result is the same that one would get with the single-parameter exponential distribution, namely $1/\alpha = \lambda$. A β value of 1.0 yields a failure rate that is constant over time. It is also the only Weibull scenario where α is equal to the MTBF. The *pdf* in this case starts off at a moderately high level and then the frequency of failures drops off steadily over time.

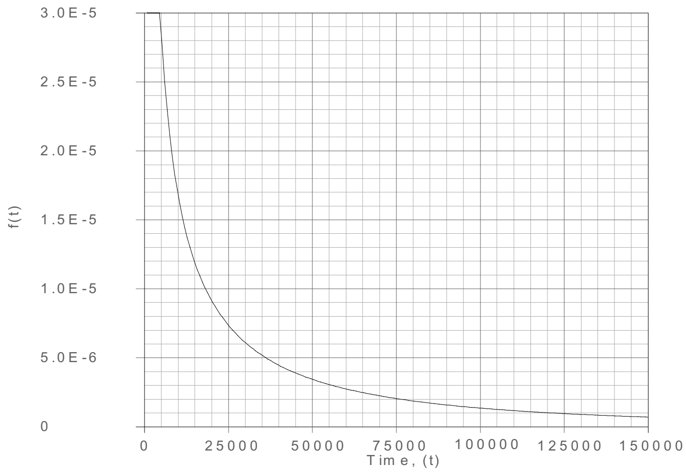


Figure 1. pdf for 2-Parameter Weibull Distribution: α = 25,000 and β = 0.5

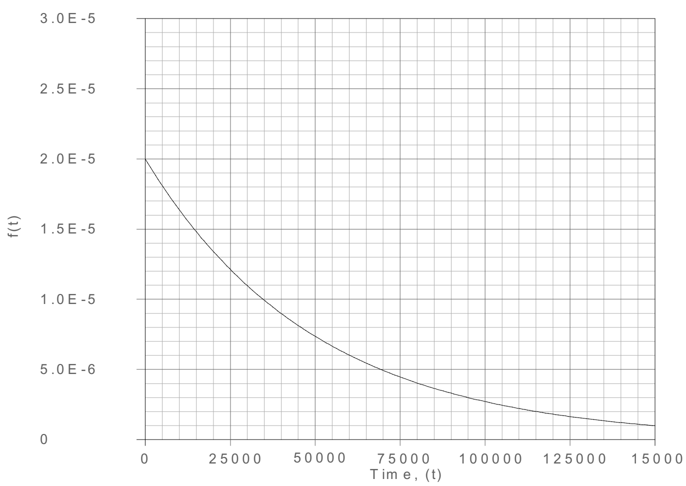


Figure 2. pdf for 2-Parameter Weibull Distribution: α = 50,000 and β = 1.0

Figure 3 shows the 2-parameter Weibull distribution where β is equal to 2.0 and α is 56,419. The *pdf* has a slightly normal appearance and is positively skewed. The frequency of failures starts off low, steadily increases and then gradually tapers off.

A 2-parameter Weibull distribution where β is 3.0 and α is 55,992, is shown in Figure 4. The *pdf* appears to be normally distributed. In this scenario, a strong wear-out mechanism is at work. The frequency of failures starts out at a very low level, then increases rapidly and subsequently decreases rapidly.

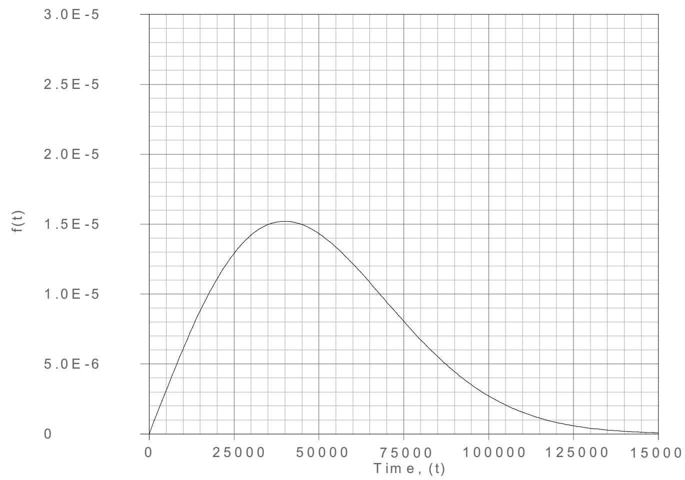


Figure 3. pdf for 2-Parameter Weibull Distribution: α = 56,419 and β = 2.0

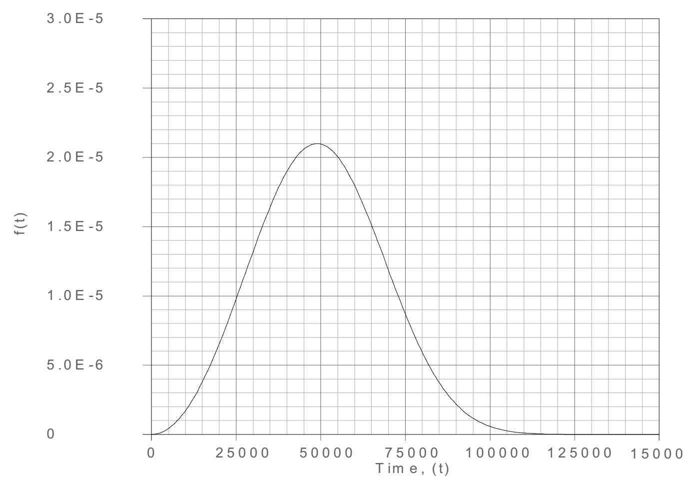


Figure 4. pdf for 2-Parameter Weibull Distribution: α = 55,992 and β = 3.0

Finally, in Figure 5, the lognormal distribution is illustrated where τ is 10.3 and σ is 1.0196. The resulting *pdf* is similar in shape to what is seen in Figures 1 and 2, suggesting modest infant mortality where the failure frequency initially starts out high but then steeply declines.

In comparing the five examples, it is clear that MTBF on its own yields very little insight into: 1) the instantaneous failure rates expected over the service life of the product, or 2) the expected survival percentage (reliability function) at any point in time. In fact, without knowledge of how life data is distributed, mistakes in equipment or material procurement decisions are bound to occur.

Table 1 shows the expected reliability of the five life data examples. Suppose a design engineer is developing a system that uses a power supply assembly from two suppliers, both of whom offer an MTBF specification of 50,000 hours. If the required reliability is 80% at 10,000 hours, then selecting a supplier whose power supply life data behaves as shown in Example 1 (β = 0.5) would yield extremely disappointing results for the customer who purchased the system.

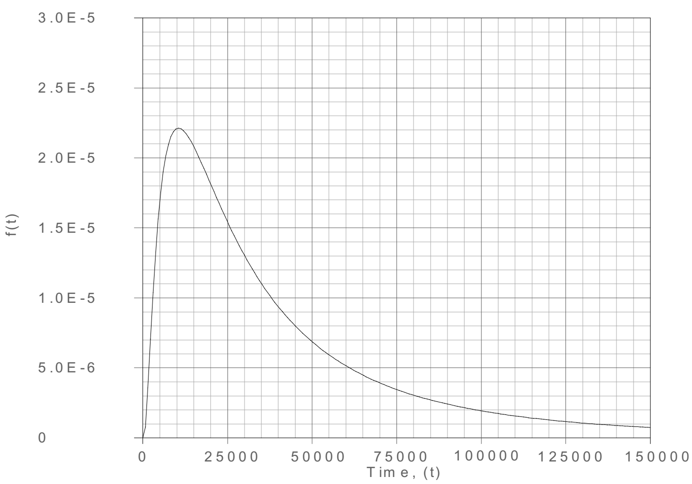


Figure 5. pdf for Lognormal Distribution: τ = 10.3, σ = 1.0196

On the other hand, suppose the customer-use model of the system dictates a service life of less than 1,000 hours at which point the system is discarded. Further assume that a reliability of 95% at 1,000 hours is acceptable. Lastly, assume that the power supply assembly from Supplier A has life data distributed as shown in Example 2 (β = 1.0) and costs one-half of an equivalent power supply assembly from Supplier B that has life data distributed as shown in Example 4 (β = 3.0). Clearly, considerable cost savings could be realized by purchasing from Supplier A.

Uncertainty in Reliability Metrics

Most hardware suppliers cite a single MTBF number, i.e., they provide a point estimate of the MTBF. However, sampling error associated with such a metric can be significant and can lead to costly problems. Understanding the suppliers' confidence bounds on the point estimate can have significant bearing on the buying decision.

Figures 6 and 7 illustrate how two identically-distributed sets of life data can have very different confidence bounds. In both cases, a 2-parameter Weibull distribution represents the underlying life data, with β equal to 1.0 and α equal to 50,000 hours. The only difference between the two examples is the number of failures: 10 failure events are modeled in Figure 6 and 100 failure events in Figure 7. Both examples show the 2-sided confidence bounds. Significant uncertainty exists in the product's reliability function when the number of failures in the reliability model is low. Failure to factor in this uncertainty can lead to unexpected, disappointing, and costly results experienced by the customer.

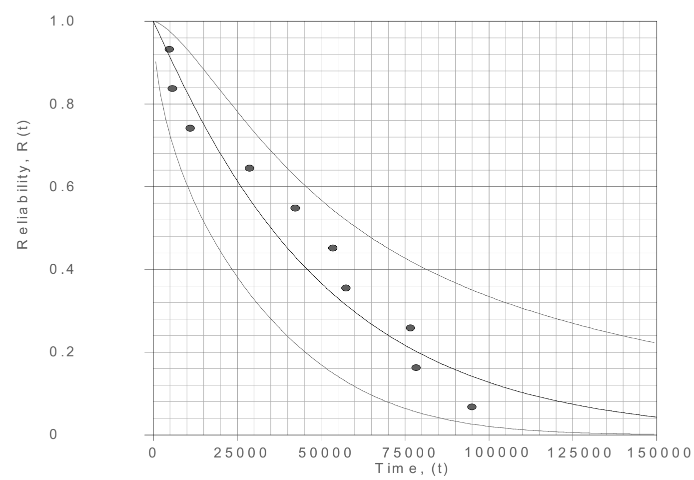


Figure 6. Weibull Distribution: β = 1.0, 10 Failures, 90% CB

Table 1. Reliability of Life Data Distributions that all Have an MTBF of 50,000 Hours

Life Data Distribution⇒	Reliability at Mission End Time				
	Ex. #1	**Ex. #2**	**Ex. #3**	**Ex. #4**	**Ex. #5**
	Weibull	**Weibull ***	**Weibull**	**Weibull**	**Lognormal**
Mission End Time ⇓	**α = 25,000 β = 0.5**	**α = 50,000 β = 1.0**	**α = 56,419 β = 2.0**	**α = 55,992 β = 3.0**	**τ = 10.3 σ = 1.0196**
100	0.936	0.998	1.000	1.000	1.000
200	0.912	0.996	1.000	1.000	1.000
500	0.865	0.990	1.000	1.000	1.000
1,000	0.815	0.981	1.000	1.000	1.000
5,000	0.636	0.906	0.992	0.999	0.924
10,000	0.529	0.820	0.967	0.994	0.777
20,000	0.409	0.671	0.876	0.953	0.536
30,000	0.335	0.548	0.743	0.850	0.382
40,000	0.284	0.447	0.589	0.681	0.282
50,000	0.245	0.365	0.438	0.473	0.214
60,000	0.215	0.300	0.305	0.275	0.166
70,000	0.190	0.243	0.199	0.129	0.132
80,000	0.170	0.198	0.122	0.047	0.106
90,000	0.153	0.161	0.070	0.013	0.087
100,000	0.139	0.131	0.037	0.003	0.072

*The exponential distribution is equivalent to the Weibull distribution when β = 1.0.

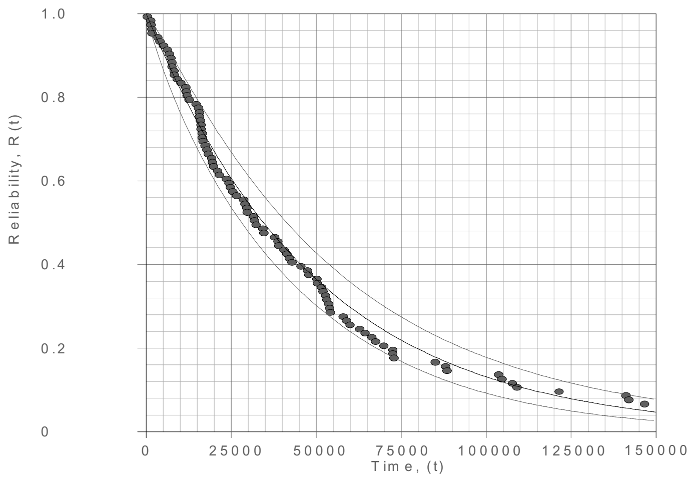


Figure 7. Weibull Distribution: β = 1.0, 100 Failures, 90% CB

Using AFR to Calculate MTBF

In the previous sections we saw how MTBF is calculated using statistical models of field failure data. Often, field failure data is incomplete or the expertise to create such a failure data model is unavailable. In the absence of such information or methods, the all-too-common (and flawed) practice is to use the familiar annualized failure rate (AFR). This method involves taking the reciprocal of the AFR and multiplying it by the hours per year of operation time T, that is

$$\text{MTBF} = \frac{\text{T}}{\text{AFR}}$$

Such a method has a number of problems associated with it. To begin with, there is the inherent assumption that the failure rate is constant over time, i.e., the life data follows an exponential distribution or Weibull distribution when β is equal to 1.0. Another difficulty is determining what value of T to use. Depending upon assumed customer use models, such as 24 hours per day, 7 days per week (24x7) or 8x5, the resulting MTBF can vary by as much as a factor of four.

The selection of AFR method can also introduce significant variability in MTBF results. Seemingly countless different methods can be used to calculate field failure rates. For instance, Agilent Technologies calculates AFR by taking the number of warranty failures in the reporting month, dividing by the number of units under warranty in that month, and then multiplying by 12 to annualize the result. Jon G. Elerath's paper on the subject does an excellent job in summarizing, comparing and contrasting a number of different techniques (Reference 4). While the reciprocal of AFR may be useful for making a reasonable estimate of MTBF in some cases, the reliability practitioner should at least be aware of the built-in assumptions and potential error that this method introduces.

Other AFR Considerations

In addition to the selection of AFR method, the reliability engineer must pay careful attention to several other variables that influence AFR. For instance, it is critical that failure mode classifications be treated consistently when making head-to-head AFR comparisons. Often, No Trouble Found (NTF) and overstress modes are included in one model but not another. Another important factor is the selection of an appropriate shipment window. Should it be based on the past one-month, six-month or 12-month shipment history? Or should the lowest AFR achieved over the past 12 months of shipment history be used? Consistency of method, sustainability of reliability, and availability of sufficient life data to assure reasonable confidence bounds are important elements to consider.

Another important factor in calculating an accurate AFR is the use of complete and accurate life data. It is best to use warranty data for this calculation because it represents the most complete data set typically available. Customers have financial incentives to return warranty failures to the manufacturer for repair. This affords the greatest opportunity for the manufacturer to collect a complete set of failure data from a range of shipment dates. Out-of-warranty failures may be returned to the manufacturer for repair only in one-third or fewer instances, thus making this data set useless for calculating AFR. Any AFR calculated from the data set will yield an erroneous point estimate of MTBF.

Conclusions

MTBF is often cited by equipment manufacturers as the "go to" reliability metric. However, MTBF on its own provides very little insight into how the failure rate behaves over time or what the expected reliability will be at any given moment. It is also important to understand the uncertainty associated with an MTBF estimate.

In the absence of life data modeling, MTBF is often calculated by taking the reciprocal of AFR and multiplying it by an estimated number of hours per year of operation. This method assumes that the product's failure rate is constant over time; however, such an assumption is frequently far from true.

Without a solid understanding of a product's life data, substantial errors can occur when calculating MTBF and AFR. Decisions based on flawed methods such as these can result in lost sales to competitors, higher costs to procure equipment and material, and disappointed customers.

Acknowledgments

The author wishes to thank John Herniman, Scott Voelker, and Greg Larsen for their inspiration and insights that helped make this article possible.

References

1. Applied Reliability, Second Edition, Paul A. Tobias and David C. Trindade, CRC Press, 1995.
2. Practical Reliability Engineering, Fourth Edition, Patrick D.T. O'Connor, John Wiley & Sons, Inc., 2002.

3. Life Data Analysis Reference, ReliaSoft Publishing, ReliaSoft Corporation, Tucson, Arizona, 1997.
4. "AFR: Problems of Definition, Calculation and Measurement in a Commercial Environment", J.G. Elerath, Reliability and Maintainability Symposium Annual Proceedings, January 24-27, 2000, pp. 71-76.

About the Author

Bill Lycette is a Senior Reliability Engineer with Agilent Technologies. He has 24 years of engineering experience with Hewlett-Packard and Agilent Technologies, including positions in reliability and quality engineering, process engineering, and manufacturing engineering of microelectronics, printed circuit assemblies and system-level products. Mr. Lycette is a Certified Reliability Engineer.

Risk Management and Reliability

By: Ned H. Criscimagna, Alion Science and Technology

Introduction

Risk management is one of the critical responsibilities of any manager. The term "risk management" is used by managers and analysts in a number of diverse disciplines. These include the fields of statistics, economics, psychology, social sciences, biology, engineering, toxicology, systems analysis, operations research, and decision theory.

Risk management means something slightly different in each of the disciplines just mentioned. For social analysts, politicians, and academics it is managing technology-generated macro-risks that appear to threaten our existence. To bankers and financial officers, it is usually the application of techniques such as currency hedging and interest rate swaps. To insurance buyers and sellers, it is insurable risks and the reduction of insurance costs. To hospital administrators it may mean "quality assurance." To safety professionals, it is reducing accidents and injuries. For military acquisition managers, it means identifying, prioritizing, and managing the technical, cost, and schedule risks inherent in developing a new weapon system.

This article discusses how an effective reliability program can be a valuable part of an overall risk management effort for military system acquisition programs.

What is Risk?

The American Heritage® and Webster dictionaries define the term similarly. These definitions can be summarized as:

1. Possibility of suffering harm or loss: Danger.
2. A factor, course, or element involving uncertain danger: Hazard.
3. The danger or probability of loss to an insurer.
4. The amount that an insurance company stands to lose.
5. One considered with respect to the possibility of loss to an insurer (a good risk, e.g.)

A more general definition of risk, perhaps more appropriate for acquisition, is:

> *Risk is the chance that an undesirable event might occur in the future that will result in some negative consequences.*

This latter definition of risk is often expressed as an equation (Reference 1):

Risk Severity = Probability of Occurrence x Potential Negative Impact

In the sense of the definition just given, risk is a part of everyday life. We all are faced with uncertainties in our lives, our careers, and our decisions. Since we cannot avoid such uncertainties, we must find ways to deal with them.

Similarly, the acquisition manager faces uncertainty concerning the technical challenges in designing a new system, and the cost and schedule estimates. Much effort is expended in trying to assess the technical challenges of a new program, in estimating the costs associated with that program, and in scheduling the program. In addition to the many constraints placed upon the manager, such as budgets, timeframes, and technical state-of-the-art, the uncertainties, or the risks, make the job of managing the program to a successful conclusion a difficult one.

Technical risk affects cost and schedule. As stated in an article in the Journal of Defense Acquisition University (Reference 2):

> There is no dispute that there is a strong relationship between technical risk and cost and schedule overruns, nor is there any dispute that DoD Project Offices must assess and mitigate technical risk if they are to be successful. However, what must be kept in mind is that technical risk in-and-of-itself does not directly result in cost and schedule overruns. The moderating variable is the manner in which a project's contract is crafted and how deftly the contract is administered, given the nature of a project's technical risk.

As an aside, in his 1999 thesis (Reference 3) written for the Naval Postgraduate School, James Ross identified poorly defined requirements as one of the highest risks during pre-solicitation. Without very clearly defined, justifiable, and realistic requirements, the already difficult task of risk management during program execution is even more difficult.

What is Risk Management?

One can compare the job of program management to that of a ship captain directing the safe passage of the vessel through waters filled with reefs and icebergs, sometimes fighting currents and foul weather. The captain may have navigation charts but they may be inaccurate or incomplete. Electronic navigation and communication equipment may be affected by interference or sun spot activity, and the vessel's power plant and other essential systems may have failures. It takes a lot of experience and great skill to cope with such risks and still bring the ship safely to its destination.

How does the acquisition manager navigate through the risks associated with a weapon system program? Risk management has always been an implicit part of the manager's job. It had its origins in the insurance industry, where the tools of the trade included actuarial tables. In the 1970s and 1980s, risk management started to gain recognition in other industries. Initially, the focus of risk management in these industries was similar to that of the insurance industry: protecting against catastrophe and evolved to protecting unaffordable potential losses. In the 1980s, total quality management had become formalized as a means for improving the quality of business processes. Today, modern risk management is widely implemented as a means of protecting the bottom line and ensuring long-term performance. For the acquisition manager, this translates into bringing a program in on schedule, on budget, and with all technical requirements satisfied.

Risk management consists of the following activities:

- Identify concerns.
- Identify risks and risk owners.
- Evaluate the risks as to likelihood and consequences.
- Assess the options for accommodating the risks.
- Prioritize the risk management efforts.
- Develop risk management plans.
- Authorize the implementation of the risk management plans.
- Track the risk management efforts and manage accordingly.

A variety of tools are available to help the acquisition manager. Some have evolved from the actuarial approach used in the insurance business. Others have been developed and tailored to specific fields of endeavor. These include Risk Ranking Tools, Probabilistic Risk Assessment (Reference 4), and Risk Software. NASA has developed a formal probabilistic risk assessment program (References 5-6).

Another important tool that can help in managing risk is an effective reliability program. This article explores the ways in which a reliability program can contribute to effectively managing risk. Although the focus is on managing risk in a military acquisition program, the discussion applies equally to the acquisition of any new product.

Managing risk may begin with acquisition but continues through the life of a system. Table 1 outlines some of the risk management activities associated with the three major phases of the life cycle.

What is an Effective Reliability Program?

An effective reliability program during system acquisition includes the following:

1. A documented process for developing requirements that meet customer needs, are realistic, and achievable within budget and schedule constraints.
2. Activities for designing for reliability. This includes the use of analytical techniques such as Failure Modes and Effects Analysis, Finite Element Analysis, Failure Analysis, and Root Cause Analysis. It also includes Robust Design Techniques.
3. Testing conducted to identify failure modes; support reliability growth through improving reliability by identifying design weakness, analyzing these weaknesses, and changing the design to eliminate or minimize the effect of failures; and to validate whether or not the reliability requirements have been met.
4. A strong quality assurance program during manufacturing and production to translate the design into an actual system with as much fidelity as possible. Such a program includes statistical process control and periodic testing to ensure that the last product off the line has the same level of reliability as the first.

An effective reliability program cannot stand alone; it must be incorporated into the overall systems engineering and design effort. Thus, activities such as configuration management and control, design trades, cost-benefits analysis, and so forth apply to the reliability effort as much as to other performance parameters. The results of reliability analyses and tests, in turn, can be useful to the safety analyst, maintenance planner, and logistics staff. They can also be used as part of an overall risk management effort.

Table 1. Risk-Related Objectives of Life Cycle Phases (Based on a Table in Reference 7)

Life Cycle Phase	Objective
Concept definition, design, and development	• Identify major contributors to risk. • Assess overall design adequacy. • Provide input for establishing procedures for normal and emergency procedures. • Provide input for evaluating acceptability of proposed hazardous facilities or activities.
Construction, production, installation, operation, and maintenance	• Gauge and assess experience to compare actual performance with relevant requirements. • Update information on major risk contributors. • Provide input on risk status for operational decision-making. • Provide input for optimizing normal and emergency procedures.
Disposal (decommissioning)	• Provide input to disposal (decommissioning) policies and procedures. • Assess the risk associated with process disposal (decommissioning) activities so that appropriate requirements can be effectively satisfied.

(Continued on page 10)

Consider...

Your product is having major problems at a key customer site and your customer is losing faith.

Your warranty costs doubled last month and your VP calls to ask you why.

Your customer is asking for reliability and availability numbers and your reliability expert just left the company.

Do you have a solution?

www.relexsoftware.com

Risk Management . . . (Continued from page 7)

In NAVSO P-3686 (Reference 8) dated October 1998, the importance of systems engineering to the management of technical risk is stated as follows.

> The Integrated Process/Product approach to technical risk management is derived primarily from the Critical Process approach and incorporates some facets of the Product/work breakdown structure (WBS) approach. The systems engineering function takes the lead in system development throughout any system's life cycle. The purpose of systems engineering is to define and design *process and product solutions* in terms of design, test, and manufacturing requirements. The WBS provides a framework for specifying the technical objectives of the program by first defining the program in terms of hierarchically related, *product oriented elements* and the *work processes required* for their completion.
>
> This emphasis on systems engineering, including processes and technical risk, along with process and product solutions, validates and supports the *importance of focusing on controlling the processes*, especially the prime contractor and subcontractors [sic] critical processes. Such a focus is necessary to encourage a proactive risk management program, one that acknowledges the importance of understanding and controlling the critical processes especially during the initial phases of product design and manufacture.

As an important part of the overall systems engineering approach, the reliability program can be a valuable contributor to the management of risk.

Reliability as a Risk Management Tool

Few people in acquisition debate the need for an effective reliability program as part of a risk management program. The question is how can such a program assist in risk management? Let us examine the various tools of reliability and see how they can be used to help identify, prioritize, and manage risk.

Analytical Reliability Tools. These include the Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Root Cause Analysis (RCA), Worst Case Analysis, and Sneak Circuit Analysis (SCA).

1. <u>FMEA</u>. The FMEA is an analytical tool used throughout the design process. It can be used to examine increasing levels of indenture, usually starting at the assembly level and progressing up. Briefly, the analysis is conducted to identify:

   a. The various functions of the item being analyzed.
   b. The possible ways that the item could fail to perform each of its functions (failure modes).
   c. The likelihood of each failure mode occurring.
   d. The effect, should the failure mode occur, on the item and system operation.
   e. The root cause of each failure mode.
   f. The relative priority of each failure mode.
   g. Recommended actions to reduce the likelihood, effect, or both of the failure modes, beginning first with the highest priority modes.

Different standards are available that define the FMEA process. Although they may differ in the details, they all include similar steps. One of these is some way of prioritizing failure modes. The old military standard (MIL-STD-1629) describes a Failure Modes, Effects, and Criticality Analysis (FMECA) in which failure modes are prioritized based on their relative criticality, a function of the probability of occurrence and severity of effect. The Automobile Industry Action Group (AIAG) standard uses a risk priority number, also based on probability of occurrence, severity of effect, and other factors.

Whether the FMEA process described in the AIAG standard, the FMECA process described in MIL-STD-1629, or the process as documented in other standards is used, they share the common element of prioritizing risk. As such, the FMEA/FMECA process is an excellent tool for identifying technical risk. By tracking recommended actions for high-risk failure modes, and ensuring that the recommended design (or other) changes are effective, the technical risk can be managed.

2. <u>FTA</u>. Whereas the focus of the FMEA is on a subassembly, an assembly, and so forth, the FTA focuses on a specific event, usually and undesired event (i.e., a failure). By creating what are known as fault trees, one can then trace all of the possible events or combinations of events that could lead to the undesired event.

Not only can the FTA directly contribute to identifying design risks, but it can also reduce risk during operation. By its very nature, the FTA can help in developing the diagnostics so necessary to the maintenance of a system. (The FMEA can also contribute to the development of diagnostics).

3. <u>RCA</u>. Given the limited funds and schedule facing each program manager, it is critical that item and money is not expended ineffectively. When high-risk failures occur during testing, design changes usually are required to reduce the risk to an acceptable level. This reduction is achieved by eliminating a failure mode, reducing the frequency with which the mode will occur, minimizing the effect of the mode, or some combination of these alternatives.

To arrive at an effective design change, the underlying cause of each failure must be determined. This underlying cause is not the failure mode. A failure mode, such as an open in a resistor, can be compared to a symptom. When we are ill, our doctor (we hope) does not treat our symptoms. Instead, the doctor tries to determine the underlying reasons for our illness. To do so requires experience, good judgment, and the use of diagnostic tools, such as X-ray, blood tests, and so forth.

Just as doctors search for the underlying cause of an illness, engineers must determine the underlying reason for a failure mode.

These reasons are often referred to as failure mechanisms. They are the physics of failure. A primary tool used to identify these failure mechanisms is Root Cause Analysis (RCA). RCA is experience, judgment, and specific activities applied in combination. The activities include non-destructive and destructive inspections. Table 2 lists just a few of these activities conducted for RCA.

Table 2. Typical Activities for Determining Root Cause

• Physical examination of failed item	• Mechanical testing
• Fracture mechanics	• Macroscopic examination and analysis
• Nondestructive evaluation - X-ray - Thermography - Magnetic flux - Penetrant dye - Computerized tomography - Ultrasonics	• Microscopic examination and analysis • Comparison of failed items with non-failed items • Chemical analysis • Finite element analysis

4. Worst-Case Analysis. As part of the reliability and design programs, analysis can be performed in worst case conditions to assure adherence to the specification requirements, reducing the risk of failure due to inadequate operating margins.

The design is examined to identify circuit tolerance to parameter drift of critical parts that may lead to out-of-specification conditions over the system's operating life.

The analysis demonstrates sufficient operating margins for the operating conditions of the circuits, taking into consideration:

- Parts parameter variations
- Initial tolerances
- Temperature
- Aging effects
- Radiation effects
- Power input line voltage variations
- Operational mode effects
- Circuit parameter variations due to loading & stimulus

5. SCA. Many system failures are not caused by part failure. Design oversights can create conditions under which a system either does not perform an intended function or initiates an undesired function. Such events in modern weapon systems can result in hazardous and even dire consequences. A missile, for example, may be launched inadvertently because of an undetected design error.

A significant cause of such unintended events is the "sneak circuit." This is an unexpected path or logic flow that, under certain conditions, can produce an undesired result. The sneak path may lie in the hardware or software, in operator actions, or in some combination of these elements. Even though there is no "malfunction condition," i.e., all parts are operating within design specifications, an undesired effect occurs. Four categories of sneak circuits are listed in Table 3.

Table 3. Categories of Sneak Circuits

Category	Characteristics
Sneak Paths	Unexpected paths along which current, energy, or logical sequence flows in an unintended direction.
Sneak Timing	Events occurring in an unexpected or conflicting sequence.
Sneak Indications	Ambiguous or false displays of system operating indications conditions that may cause the system or an operator to take an undesired action.
Sneak Labels	Incorrect or imprecise labeling of system functions - e.g., system inputs, controls, displays buses - that may cause an operator to apply an incorrect stimulus to the system.

Sneak circuit analysis is a generic term for a group of analytical techniques employed to methodically identify sneak circuits in hardware and software systems. Sneak circuit analysis procedures include Sneak Path Analysis, Digital Sneak Circuit Analysis, and Software Sneak Path Analysis.

Reliability Testing.

1. Reliability growth testing. The term Reliability Growth Testing (RGT) usually refers to a process by which the following three objectives are achieved:

a. Failures are identified and analyzed.
b. The design is improved to eliminate the failures, reduce the probability of their occurrence, reduce the effects of the failures, or some combination of these alternatives.[1]
c. The progress being made in the growth process is tracked with quantitative estimates of the reliability. Models, such as the Duane and AMSAA, are used for making the estimates.

When all three of these objectives are being pursued, the RGT is a formal program for achieving growth. Growth can also be achieved by analyzing the failures from any and all testing and developing design changes to address the failures. However, quantitative estimates of reliability may not be able to be made due to statistical limitations of combining data from different tests. For our purposes, we will refer to this latter process as Test-Analyze-And-Fix (TAAF).

Whether RGT or TAAF is used, the process of identifying and addressing failures helps reduce technical risk. The RGT also provides a quantitative means of assessing the risk of not meeting a specific reliability goal within budget and schedule.

2. Life testing (Reference 9). Every product and system consists of hundreds, perhaps thousands, or hundreds of thousands of parts. The system reliability depends on how these parts are connected together, how they are applied, and the reliability of each. Some parts may have little impact on system reliability due to their application. Others may be critical to the continued and safe operation of the system.

[1]Economic and other factors also bear on the decision to address or accept a given failure.

It is obvious that selecting the "right" parts is important. A "right" part is one that:

- Performs the correct function
- Has sufficient reliability
- Meets other criteria such as support, obsolescence, and cost

Determining whether a part has the requisite reliability for a given application is an element of part characterization. Life testing is one method for characterizing a part from a reliability perspective. By testing a sample of parts, recording the times to failure for the parts, and analyzing these times to failure, the reliability of the population represented by the sample can be estimated[2]. As importantly, some insight into the category of failure (wearout, infant mortality, random failure[3]) can be gained. One common technique for analyzing the times-to-failure data is Weibull analysis (Reference 10).

Using life testing, engineers can determine if the reliability of each part is adequate[4] and, if not, what changes might be necessary to attain the required level. By ensuring that the "right" parts are selected, technical risk is reduced.

3. Validation testing. Validation testing helps confirm whether the efforts during design have paid off or not. It can be done at the part level or at higher level of indenture. The types of test often used for validation are listed in Table 4.

Table 4. Commonly Used Tests for Validation

Level of Indenture	
Parts	**Assembly and Higher**
• Weibull testing • Attribute testing	• Sequential testing • Fixed length testing • Attribute testing

RGT, TAAF, and part characterization is done as part of the design process, a process in which the design is changing. There is no pass-fail criterion for such tests; the objective is to identify and address weaknesses in the design from a reliability perspective. Validation testing, on the other hand, is ideally done on the "finished" design and is a "go-no-go" or "pass-fail" test. Validation testing provides the best measure of the level of reliability achieved before a full production decision is made.

When validation tests are included as part of the contractual requirements, it provides an added incentive to contractor and government alike to do the requisite engineering starting early in the program. Neither the customer nor the contractor wants the system to fail the validation test. Knowing that the test is a hurdle that must be passed provides incentive to control technical risk throughout the design process.

Production Reliability Testing. After the design is accepted, validation tests have been passed, and the production processes have been brought under control, Production Reliability Testing (PRT) may be conducted, especially when the production takes place over an extended period of time.

PRT is intended to detect any degradation in reliability performance that may result from changes in suppliers, design processes, configuration, and so forth. When degradation is detected, PRT provides an early warning so that corrective actions can be considered before a large number of systems are delivered to the customer. Many of the same techniques used for validation purposes can be used for PRT. Thus, PRT helps reduce the risk of sending systems with poor reliability to the customer. In addition, the earlier that problems are detected, the lower the cost to correct the problems.

Reliability Predictions and Assessments. Realistic and fact-based assessment of the level of reliability being achieved at any point in time is an important element of a comprehensive reliability program. The need for quantitative measures has been alluded to several times in this article (likelihood of a failure mode, reducing the probability of occurrence of a failure, and tracking growth in a formal RGT program).

The author distinguishes between a prediction and an assessment in the following way. A prediction is usually thought of as the quantitative output of a model, such as a parts count model, reliability block diagram, or simulation. An assessment is an overall evaluation of the reliability based on the output of models, test results, engineering judgment, and consideration of any assumptions and the limitations of the models and testing. The subject is much too broad and involved to cover here in detail. Two points, however, are important to the subject of risk management.

1. Point estimates versus confidence intervals (Reference 11). Predictions based on models and testing can always be expressed as a single, or point value. The output of some types of models, empirical models for example, can only be stated as point values. Point estimates are probably the most common way that technical people communicate predictions and assessments to management.

The problem with a point estimate is that it incorrectly conveys certainty. When one states that the MTTF of a part is 10,000 fatigue cycles or that the MTBF of a subsystem is 2,200 operating hours, it is often interpreted in the same way as stating that the part is 3.5 cm long or the subsystem weighs 450 pounds. The latter two measures are deterministic and, within the limits of our measurement equipment and changes in temperature and humidity, do not vary from day to day.

Reliability, however, is a probabilistic concept. Reliability testing consists of testing samples. Even when several samples are taken from a population with a given distribution with known parameters, the parameters obtained from the sample testing vary in value. Given that the distribution of the population is never known, the variation in results from testing different sam-

[2]This description is necessarily brief. For more information on life testing, see References 9 and 10.

[3]Every failure has an underlying cause. Random refers to the times to failure. This category of failures includes failures due to maintenance and human errors, "Acts of God," and a mixture of failure modes.

[4]Assuming that the system-level reliability requirement was properly allocated to lower levels of indenture.

ples can be very large. Thus, in accepting a point estimate as "gospel," we run the risk of being optimistic. Worse yet, we have no idea what the level of risk may be.

For those cases where a statistical model or test is used, we can provide confidence bounds on the point estimate. A confidence bound can be either one-sided (i.e., we are X% confident that the interval from the lower bound to infinity includes the true reliability) or two-sided (i.e., we are X% confident that the interval from a lower bound to an upper bound includes the true value of reliability). Consider the following statements concerning an item for which the MTBF requirement is 950 hours.

a. The estimate of reliability is 1,000 hours MTBF.
b. The 90% confidence interval for reliability is 700 to 1,500 hours MTBF.

Which does a better job of indicating that the estimate is inexact and carries with it a risk of being wrong (i.e., the achieved MTBF is less than the requirement)? If the manager desires a smaller interval, he or she must either be willing to invest in additional testing or accept a higher risk of being wrong.

2. The Reliability Case (Reference 12). The Reliability Case is an example of an assessment. It is a progressively expanding body of evidence that a reliability requirement is being met. Starting with the initial statement of the requirements, the "Reliability Case" subsequently includes identified, perceived, and actual risks; strategies; and an Evidence Framework referring to associated and supporting information. This information includes evidence and data from design activities and in-service and field data as appropriate.

The Reliability Case provides an audit trail of the engineering considerations starting with the requirements and continuing through to evidence of compliance. It provides traceability of why certain activities have been undertaken and how they can be judged as successful. It is initiated at the concept stage, and is revised progressively throughout the system life cycle. Typically it is summarized in Reliability Case Reports at predefined milestones. Often, it is expanded to included maintainability (The R&M Case). The Reliability Case is developed using:

- Calculations
- Testing
- Simulation
- Analyses
- Expert opinion
- Information from any previous use

Each Reliability Case report lists and cross references the parent requirements in the Evidence Framework, against which the evidence is to be judged, and is traceable to the original purchaser's requirement. The body of evidence traces the history of reviews and updates of the reliability design philosophy, targets, strategy and plan, which keep these in line with the changing status of the original risks and any new or emerging risks. The status of assumptions, evidence, arguments, claims, and residual risks is then summarized and discussed. Clearly, the Reliability Case can be an important part of the overall technical risk management effort.

Conclusions

Risk is always with us; there is no escaping it. However, we can deal with risk and keep it at an acceptable level by managing it. We can manage risk by using a variety of tools to:

1. Identify risks
2. Evaluate them as to likelihood and consequences
3. Assess the options for accommodating the risks
4. Prioritize the risk management efforts
5. Develop risk management plans
6. Track and manage the risk management efforts

One of the tools available to the manager for specifically addressing technical risk is an effective reliability program. Many of the activities conducted to develop a system having the requisite level of reliability can directly contribute to the management of technical risk. These include:

1. Analyses
2. Tests
3. Predictions and Assessments
4. The Reliability Case

By implementing reliability as part of a systems engineering approach, the results of reliability-focused activities can contribute to the many other activities that take place in a system acquisition program. The systems engineering approach capitalizes on the synergy of coordinated and synchronized technical activities. By eliminating duplicative effort and making maximum use of the results of activities, the systems engineering approach by its very nature helps minimize risk. Reliability, implemented as part of the systems engineering approach, can play a significant role in risk management.

References

1. "Understanding Risk Management," CrossTalk, Software Technology Support Center, Ogden ALC, UT, February 2005, page 4.
2. Bolles, Mike, "Understanding Risk Management in the DoD," Journal of Defense Acquisition University, Volume 10, 2003, pages 141-154.
3. Ross, James P., "A Risk Management Model for the Federal Acquisition Process," Naval Postgraduate School Thesis, 1999, DTIC Document ADA368012.
4. Foote, Andrew J., "Is Probabilistic Risk Assessment the Answer?," Journal of the Reliability Analysis Center (RAC), First Quarter, 2003.
5. "The Inherent Values of Probabilistic Risk Assessment," Second NASA Probabilistic Risk Assessment Workshop, June 19, 2001.
6. "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners," Version 1.1, August 2002.
7. Dhillon, B.S., Design Reliability, Fundamentals and Applications, CRC Press, NY, 1999.
8. "Top Eleven Ways to Manage Technical Risk," NAVSO P-3686, October 1998.

9. Kalbfleisch, J.D. and Ross, L., Prentice, "The Statistical Analysis of Failure Time Data, Wiley, New York, 1980.
10. Abernethy, Robert, The New Weibull Handbook, 4th Edition, Published by R. Abernethy, 1996, ISBN 0 9653062 0 8.
11. RAC-HDBK-1210: "Practical Statistical Tools for the Reliability Engineer," RAC, Rome, NY 1999.
12. START 2004-2, "The R&M Case - A Reasoned, Auditable Argument Supporting the Contention that a System Satisfies its R&M Requirements," RAC, Rome, NY, 2004.

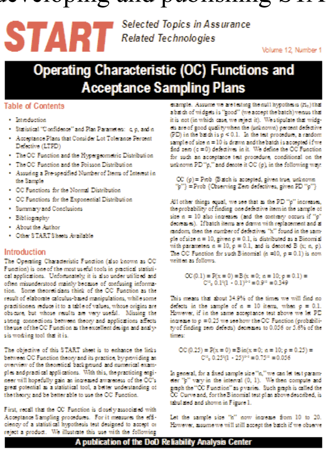
About the Author

Ned H. Criscimagna is a Science Advisor with Alion Science and Technology Corporation and RAC Deputy Director. Prior to joining Alion, he worked for ARINC Research Corporation. Before entering industry, Mr. Criscimagna served for 20 years in the U.S. Air Force, retiring with the rank of Lieutenant Colonel. Over his 39-year career, he has been involved in a wide variety of projects related to DoD acquisition, reliability, logistics, reliability and maintainability (R&M), and availability. He led the development of the last version of MIL-HDBK-470 and the last update to MIL-HDBK-338. He instructs the RAC's Mechanical Design Reliability Course.

Mr. Criscimagna earned his B.S. in Mechanical Engineering from the University of Nebraska-Lincoln in 1965 and his M.S. in Systems Engineering from the USAF Institute of Technology in 1971. He is a member of the American Society for Quality (ASQ), the National Defense Industries Association, and the Society of Automotive Engineers (SAE), and is a Senior Member of the International Society of Logistics (SOLE). He is a SOLE Certified Professional Logistician and an ASQ Certified Reliability Engineer. He is a member of the ASQ/ANSI Z-1 Dependability Subcommittee, the US TAG to IEC TC56, and the SAE G-11 Division. He is listed in the 27th Edition of Who's Who in the East, the 54th, 56th, and 57th, Editions of Who's Who in America, and in the 8th Edition of Who's Who in Science and Engineering.

START Sheets

For the past few years, the Reliability Analysis Center has been developing and publishing START Sheets. What, you may ask, is


START Selected Topics in Assurance Related Technologies
Volume 12, Number 1

Operating Characteristic (OC) Functions and Acceptance Sampling Plans

Table of Contents

- Introduction
- Statistical "Confidence" and Plan Parameters: c, p, and n
- Acceptance Plans that Consider Lot Tolerance Percent Defective (LTPD)
- The OC Function and the Hypergeometric Distribution
- The OC Function and the Poisson Distribution
- Assuring a Pre-specified Number of Items of Interest in the Sample
- OC Functions for the Normal Distribution
- OC Functions for the Exponential Distribution
- Summary and Conclusions
- Bibliography
- About the Author
- Other START Sheets Available

Introduction

The Operating Characteristic Function (also known as OC Function) is one of the most useful tools in practical statistical applications. Unfortunately, it is also under utilized and often misunderstood mainly because of confusing information. Some theoreticians think of the OC Function as the result of elaborate calculus-based manipulations, while some practitioners reduce it to a table of values, whose origins are obscure, but whose results are very useful. Missing the strong connections between theory and applications affects the use of the OC Function as the excellent design and analysis working tool that it is.

The objective of this START sheet is to enhance the links between OC Function theory and its practice, by providing an overview of the theoretical background and numerical examples and practical applications. With this, the practicing engineer will hopefully gain an increased awareness of the OC's great potential as a statistical tool, a better understanding of the theory, and be better able to use the OC Function.

First, recall that the OC Function is closely associated with Acceptance Sampling procedures. For it measures the efficiency of a statistical hypothesis test designed to accept or reject a product. We illustrate this use with the following example. Assume we are testing the null hypothesis (H_0) that a batch of widgets is "good" (we accept the batch) versus that it is not (in which case, we reject it). We stipulate that widgets are of good quality when the (unknown) percent defective (PD) in the batch is p < 0.1. In the test procedure, a random sample of size n = 10 is drawn and the batch is accepted if we find zero (c = 0) defectives in it. We define the OC Function for such an acceptance test procedure, conditional on the unknown PD "p," and denote it OC (p), in the following way:

OC (p) = Prob {Batch is accepted, given true, unknown "p"} = Prob {Observing Zero defectives, given PD "p"}

All other things equal, we see that as the PD "p" increases, the probability of finding one defective item in the sample of size n = 10 also increases (and the contrary occurs if "p" decreases). If batch items are drawn with replacement and at random, then the number of defectives "x" found in the sample of size n = 10, given p = 0.1, is distributed as a Binomial with parameters n = 10, p = 0.1, and is denoted B (x; n, p). The OC Function for such Binomial (n = 10, p = 0.1) is now written as follows.

$$OC(0.1) = P(x = 0) = B(x = 0; n = 10; p = 0.1) = C^{10}_0\, 0.1^0(1 - 0.1)^{10-0} = 0.9^{10} = 0.349$$

This means that about 34.9% of the times we will find no defects in the sample of n = 10 items, when p = 0.1. However, if in the same acceptance test above we let PD increase to p = 0.25 we see how the OC Function (probability of finding zero defects) decreases to 0.056 or 5.6% of the times:

$$OC(0.25) = P(x = 0) = Bin(x = 0; n = 10; p = 0.25) = C^{10}_0\, 0.25^0(1 - .25)^{10-0} = 0.75^{10} = 0.056$$

In general, for a fixed sample size "n," we can let test parameter "p" vary in the interval (0, 1). We then compute and graph the "OC Function" as p varies. Such graph is called the OC Curve and, for the Binomial test plan above described, is tabulated and shown in Figure 1.

Let the sample size "n" now increase from 10 to 20. However, assume we will still accept the batch if we observe

START 2005-1, OC CURVES

A publication of the DoD Reliability Analysis Center

a START Sheet? First, START is an acronym that stands for "Selected Topics in Assurance Related Technologies." A START Sheet is a current awareness periodical. Each START Sheet provides a "jump-start" on a topic of immediate interest to individuals in the reliability, maintainability, supportability, quality, and interoperability (RMSQI) fields. In addition to a concise write-up, each installment includes comprehensive lists of contacts, bibliographic references, and other sources for further information and action.

START Sheets are typically 6-8 pages long. A total of 49 START Sheets had been published as of 1 June 2005. Those published thus far in calendar year 2005 are:

- START 2005-1: Operating Characteristic (OC) Functions and Acceptance Sampling Plans.
- START 2005-2: Understanding Binomial Sequential Testing.
- START 2005-3: Developing Reliability Requirements.

START Sheets are free to the RMSQI community and can be downloaded as pdf files from the RAC web site at <http://rac.alionscience.com/rac/jsp/start/startsheet.jsp>.

New DDR&E Portal

A new DDR&E R&E Portal, sponsored by the Office of Director Defense Research & Engineering, is available to DTIC registered DoD employees and DoD support contractors. The portal provides access to: RDT&E Budget databases, S&T Planning documents, S&T Activities, S&T Workforce, and News.

To use the portal, you must register by going to <https://register.dtic.mil/DTIC/>. For more information on the portal, contact: <rdte_help@dtic.mil>

RMSQ Headlines

Revitalization of Systems Engineering in DoD, by Michael W. Wynne with Mark D. Schaeffer, Defense AT&L, published by the Defense Acquisition University, March-April 2004, page 14. Michael Wynne is the acting Under Secretary of Defense for Acquisition, Technology, and Logistics (USD/AT&L). Mark Schaeffer is the Principal Deputy, Defense Systems, and the Director, Systems Engineering (SE) in the Office of USD/AT&L. The authors describe the changes in policy and new initiatives in education and outreach being taken to revitalize SE within DoD. Although SE is usually considered from a technical perspective, the authors show how it is linked to cost and schedule.

New DoD RAM Guide

By: Ned H. Criscimagna, Alion Science and Technology and Michael Zsak, Decisive Analytics Corporation

Introduction

A new DoD Guide on Reliability, Availability, and Maintainability (RAM) is undergoing final coordination and will be released in the very near future. The Reliability Analysis Center served as the facilitator and lead developer for the team-based effort, which involved participants from DoD, the military services, and industry. The Introduction to the new guide succinctly states the purpose of the document:

> The primary objective of Department of Defense (DoD) acquisition is to acquire quality products that satisfy user needs with measurable improvements to mission capability and operational support in a timely manner, and at a fair and reasonable price (Reference 1). This guide supports that objective. It addresses reliability, availability, and maintainability (RAM) as essential elements of mission capability. It focuses on what can be done to achieve satisfactory levels of RAM and how to assess RAM.

Addressing a Fundamental Reliability Issue

Poor reliability in defense systems negatively affects the operational readiness rates required by commanders in the field. It also leads to larger logistics footprints that detract from mobility and increases operating and support costs that divert resources from necessary modernization. Reliability issues continue to cause problems for the Department. In 1998, the National Research Council wrote:

> *The Department of Defense and the military services should give increased attention to their reliability, availability, and maintainability data collection and analysis procedures because deficiencies continue to be responsible for many of the current field problems and concerns about military readiness.* (Reference 2)

The General Accounting Office (GAO) observed that in FY 2003, DoD asked for approximately $185 billion to develop, procure, operate, and maintain its weapon systems—an increase of 18% over FY 2001. A significant portion of these funds are needed to cover spare parts and support systems to meet required readiness levels, and the high cost of maintaining systems has limited DoD's ability to modernize and invest in new weapons. This led Government Accounting Office (GAO) to issue a report to the Senate Armed Services Subcommittee on Readiness Management Support in which one recommendation to DoD was to revise acquisition regulations to require a firm estimate of component and subsystem reliability at the production decision (Reference 3).

Latest Changes in Acquisition Policy Help

New Defense Acquisition Policy guidance, in the DoD 5000 series regulations, addresses part of the problem. For example, consider the following provisions.

- The new policy requires that acquisition programs be managed through the application of a systems engineering approach that optimizes total system performance, and minimizes total ownership costs.
- Entrance into the System Development and Demonstration phase depends on technology maturity (including software), approved requirements, and funding. Unless some other factor is overriding in its impact, the maturity of the technology shall determine the path to be followed.
- Reliability in the context of overall system performance, supportability, and affordability must be considered before proceeding into full rate production and deployment.
- New performance-based logistics strategies will optimize total system availability while minimizing cost and logistics footprints.

Policy alone is not enough. Processes and procedures are needed to help change the behavior of the acquisition system to improve up-front design. Finally, technical guidance must be made readily available on how to "do the job right."

Providing Better Technical Guidance

Under acquisition reform, many military specifications, standards, and handbooks were cancelled to force the DoD to rely more on the commercial world and thereby accelerate the adoption of commercial best practices and technologies which would improve capability at lower cost. Unfortunately, in the RAM area, a void formed. The National Research Council (NRC) recognized this situation in the aforementioned 1998 report where it recommended:

> *Military reliability, availability, and maintainability testing should be informed and guided by a new battery of military handbooks containing a modern treatment of all pertinent topics in the fields of reliability and life testing, …*

As a result of this void, many programs do not execute RAM tasks effectively. Recent studies concluded that defense contractor reliability design practices may be inconsistent with best commercial practices for accelerated testing, simulation guided testing, and process certification/control. Other studies found component- and system-level testing is inadequate, testing time is limited, and sample sizes are too small.

Component stress testing was frequently missing or inadequate. Proper accelerated life testing was rarely accomplished. Early system level modeling and simulation was inadequate to enter

(Continued on page 17)

New DoD RAM ... (Continued from page 15)

tests with acceptable levels of reliability. This situation leads to inefficiencies e.g., reinventing the wheel, errors, greater costs, stovepipes, inadequate data, limited data sharing, and reuse.

As part of a call to action, the NRC Committee on National Statistics convened a workshop on reliability issues for DoD systems in June 2002 (Reference 4). The workshop focused on seven topics.

- Global reliability test designs to direct defense system development
- Recent developments in reliability growth modeling
- Use of statistical modeling for combining information, with applications to developmental and operational testing
- Methods for estimating reliability from field performance data
- Modeling of fatigue
- Reliability of software-intensive systems
- Assessment of life-cycle costs through the use of reliability analysis

The broad goal of the workshop was to foster greater interaction between the academic and defense acquisition communities to:

- Generate greater interest from the academic community in reliability issues facing defense acquisition.
- Inform decision makers about ways of dealing with constraints that may hamper the application of statistical techniques in obtaining test and field data and in the use of testing for the development of reliable systems.
- Acquaint the defense community with state-of-the-art techniques applicable to the problems they face.

Accordingly, the NRC workshop recommended that the cancelled DoD Handbook, DoD 3235.1-H *Test and Evaluation of Systems Reliability, Availability, and Maintainability: A Primer* (RAM Primer), last updated in 1982, be upgraded and replaced. The objective of such an effort was to improve communication on the most readily applied and broadly applicable statistical techniques between (1) those in DoD who have the responsibility for reliability of defense systems and (2) academic researchers with significant expertise in such statistical techniques.

Specifically, the NRC workshop determined that the treatment of the following subjects in the revised RAM Primer should be updated with more modern approaches.

- Methods for combining information across test environments
- Methods for incorporating subjective assessments
- Fatigue modeling
- Statistical methods for software engineering
- Wider use of nonparametric methods, specifically for reliability growth
- Alternative methods for modeling reliability growth

In addition, the workshop indicated that the material on the following subjects in the RAM Primer was deficient.

- Discussion of physics of failure models
- Robust methods
- Variance estimation
- Stress testing
- Accelerated testing
- Decision analytic issues
- Repair and replacement policies
- Methods for dependent components
- Current methods in experimental design
- Baysian approaches

The National Research Council recommendations were provided to a multi-organizational team chartered to develop the RAM Guide.

The New Guide

The new RAM guide provides information on reliability, availability, and maintainability throughout the system lifecycle. The content of the guide is organized into six chapters and four appendixes. The chapter and appendix titles are:

Chapter 1: RAM and the Department of Defense
Chapter 2: Achieving RAM in Military Systems
Chapter 3: Understand and Document User Needs and Constraints
Chapter 4: Design and Redesign for RAM
Chapter 5: Produce Reliable and Maintainable Systems
Chapter 6: Monitor Field Performance
Appendix A: Proposals and Contracts
Appendix B: Software Reliability
Appendix C: Reliability Growth Management
Appendix D: Field Assessment and System Trending

Chapters 3 through 6 develop in detail a four-step model for achieving RAM. The model, introduced in Chapter 1 and overviewed in Chapter 2, is shown in Figure 1. A brief explanation of the key steps shown in the figure follows.

- Before a system can be designed the needs and constraints of the user must be understood and documented. Therefore this first step is the foundation required to achieve RAM performance for a system.
- After the user needs and constraints are accounted for the acquisition process shifts to Step 2 which focuses on ensuring RAM requirements are “built-in” the system first in the design phase and then improved during the redesign phase for the system. RAM requirements are balanced against other system performance requirements.
- After the needs and constraints of the user are addressed through design and redesign, the system must be manufactured in such a manner that the designed-in RAM performance remains intact throughout production. Step 3 ensures that a reliable and maintainable system is produced.

(Continued on page 19)

New DoD RAM ... (Continued from page 17)

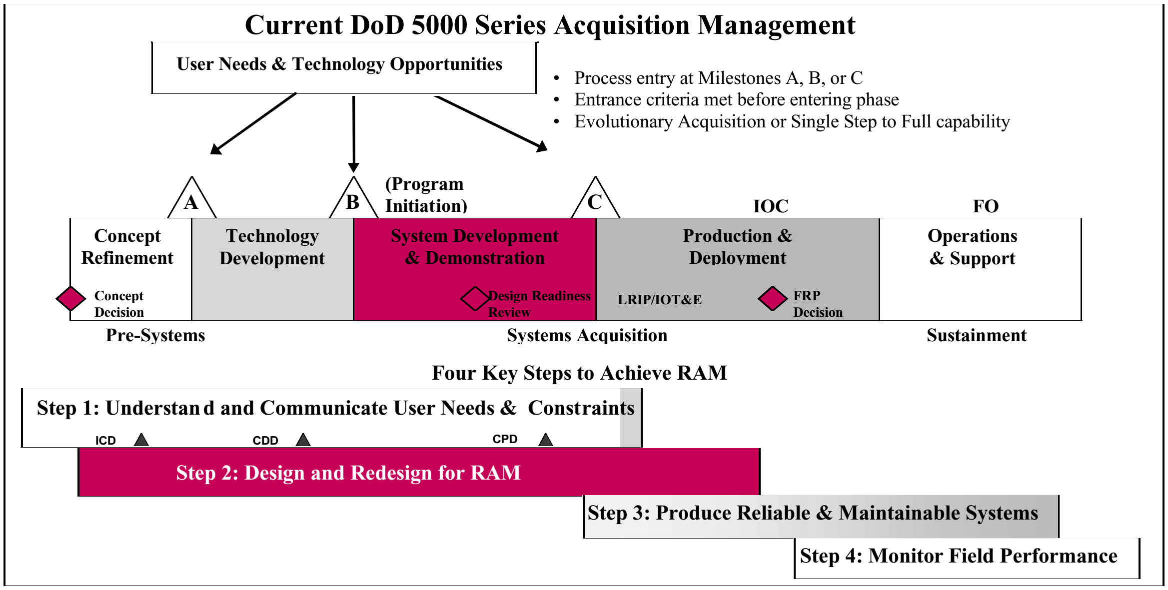


Figure 1. Model Showing the Key Steps to Developing Reliable, Available, and Maintainable Systems in the Context of Current Acquisition Policy. The four-step model was conceptualized by Dr. E. Seglie, OSD/OT&E.

- Often, the final step of the process, which is monitoring field experience, is overlooked, with adverse results. Since the cost to operate and support systems is so high in Defense systems, Step 4 is necessary because without monitoring field performance, the strong RAM foundation formed during the first three steps may degenerate. Field experience can be used to improve maintenance, identify necessary improvements to the system, and provide much needed "lessons learned" for future systems.

These steps are consistent with robust system engineering practices and are compatible with any general acquisition process. Each step consists of five elements, each of which is needed to be successful: (1) a clear goal for the step; (2) the right organizations and people involved; (3) adequate supporting information; (4) available tools, funds, and time to support the appropriate activities for that step; and (5) a good record of the results. The guide focuses on how the four steps of the model apply within the DoD acquisition framework.

The RAM Guide supports the DoD acquisition objective of acquiring quality products that satisfy user needs with measurable improvements to mission capability and operational support in a timely manner and at a fair and reasonable price. It certainly is consistent with and supports the stated imperatives of Undersecretary of Defense (Acquisition, Technology and Logistics) [USD(AT&L)] to:

- Provide a context within which I [USD(AT&L)] can make decisions about individual programs.
- Achieve credibility and effectiveness in the acquisition and logistics support processes.
- Help drive good systems engineering practice back into the way we do business.

The new RAM Guide does not seek, in one publication, to address all the deficiencies that the NRC identified. It places RAM in context as an important system performance parameter, it provides insight into what can be done to achieve satisfactory levels of RAM and it identifies how to assess RAM. It provides insight into issues that system developers need to consider and address. It introduces and explains topics, places them within the most recent Defense Acquisition framework, and provides the reader with further references for more detailed coverage. If there is sufficient demand, more detailed subsequent volumes may be developed to address in greater depth the issues identified by the NRC.

The RAM Guide will be available on the Systems Engineering Web Site, <http://www.acq.osd.mil/ds/se/index.html>. Feedback on the utility of the RAM Guide and suggestions for improvements should be provided to the Office of Primary Responsibility, OUSD(AT&L)DS/SE/ED via E-mail <atled@osd.mil>.

References

1. DoD Directive 5000.1, The Defense Acquisition System, May 12, 2003, Paragraph 4.2, page 2.
2. National Research Council, *Statistics, Testing, and Defense Acquisition: New Approaches and Methodological Improvements*, Panel on Statistical Methods for Testing and Evaluating Defense Systems, Michael L. Cohen, John B. Rolph, and Duane L. Steffey, Editors, Committee on National Statistics; Washington D.C., National Academy Press, 1998.
3. GAO Final Report, Best Practices: Setting Requirements Differently Could Reduce Weapon Systems' Total Ownership Costs, February 11, 2003, (GAO Code 120092/GAO-03-057).
4. National Research Council; *Reliability Issues for DoD Systems*, Report of a Workshop; Francisco Samaniego and Michael Cohen, Editors.; Committee on National Statistics; Washington D.C., National Academy Press; 2002.

(Continued on page 23)

Future Events in Reliability, Maintainability, Supportability & Quality

Computerized Maintenance Management Conference 2005
July 26-29, 2005
Indianapolis, IN
Contact: NetexpressUSA Inc.
PO Box 07070
Fort Myers FL 33919
Tel: (239) 985-0317
Fax: (309) 423-7234
E-mail: <info@netexpressusa.com>
On the Web: <http://www.maintenanceconference.com/cmms/index.htm>

2005 International Military & Aerospace COTS Conference
August 2-4, 2005
Norfolk, VA
Contact: Edward B. Hakim
The C3I, Inc.
Spring Lake, NJ 07762
Tel: (732) 449-4729
Fax: (775) 655-0897
E-mail: <e.hakim@att.net>
On the Web: <www.cotsconference.com/Callforpapers.html>

The Integrated Systems Health Management (ISHM) Conference
August 8-11, 2005
Cincinnati, OH
Contact: Ms. Cathy Griffith
Anteon Corporation
5100 Springfield Pike, Suite 509
Dayton, OH 45431
E-mail: <cgriffith@anteon.com>
On the Web: <http://www.usasymposium.com/ishm>

World Tribology Congress III Contact Mechanics and Friction Interfacial Phenomena in MEMS
September 12-16, 2005
London, ON
Contact: Dr. Richard S. Cowan
Georgia Tech
Manufacturing Research Center
P.O. Box 0560
Atlanta, GA 30332
Tel: (404) 894-3270
Fax: (404) 894-8336
E-mail: <rick.cowan@me.gatech.edu>
On the Web: <http://www.conferencetoolbox.org/WTC05/CallForPapersDetail.cfm>

Predictive Maintenance Technology Conference & Expo
September 19-22, 2005
Atlanta, GA
Contact: Reliabilityweb.com
Ft. Myers, FL
Tel: (888) 575-1245, Ext 112
Fax: (309) 423-7234
On the Web: <http://www.maintenanceconference.com/pdm/index.htm>

Materials Science & Technology 2005
September 25-28, 2005
Pittsburgh, PA
Contact: The Minerals, Metals & Materials Society
Warrendale, PA 15086
Tel: (724) 776-9000, Ext: 243
Fax: (724) 776-3770
E-mail: <tmsgeneral@tms.org>
On the Web: <http://www.matscitech.org>

IMAPS 38th Annual Symposium on Microelectronics
September 29 - October 1, 2005
Philadelphia, PA
Contact: IMAPS
Washington, DC 20002
Tel: (202) 548-4001
Fax: (202) 548-6115
E-mail: <imaps@imaps.org>
On the Web: <http://www.imaps2005.org>

SAE AeroTech Congress & Exhibition
October 3-6, 2005
Dallas, TX
Contact: Rebecca Wiley
Warrendale, PA 15096-0001
Tel: (724) 772-7116
Fax: (724) 776-0210
E-mail: <beckyf@sae.org>
On the Web: <http://www.sae.org/aerotech>

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

The appearance of advertising in this publication does not constitute endorsement by the Department of Defense or RAC of the products or services advertised.

SMRP Annual Meeting
October 23-27, 2005
St. Louis, MO
Contact: Society for Maintenance & Reliability Professionals
PO Box 51787
Knoxville, TN 37950-1787
Tel: (800) 950-7354
Fax: (865) 558-3060
E-mail: <info@smrp.org>
On the Web: <http://www.smrp.org>

8th Annual Systems Engineering Conference
October 24-27, 2005
San Diego, CA
Contact: Phyllis Edmonson
NDIA
Arlington, VA 22201
Tel: (703) 247-2588
Fax: (703) 522-1885
E-mail: <pedmonson@ndia.org>
On the Web: <register.ndia.org/interview/register.ndia?PID=Brochure&SID=_1GA0LCKpedmonson@ndia.org>

Aircraft Survivability 2005
October 31 - November 3, 2005
Monterey, CA
Contact: Christy O'Hara
NDIA
Arlington, VA 22201
Tel: (703) 247-2586
Fax: (703) 522-1885
E-mail: <cohara@ndia.org>
On the Web: <http://register.ndia.org/interview/register.ndia?PID=Brochure&SID=_1HH0UP6DG&MID=6940>

CMMI Technology Conference & User Group
November 14-17, 2005
Denver, CO
Contact: Phyllis Edmonson
NDIA
Arlington, VA 22201-3061
Tel: (703) 247-2588
Fax: (703) 522-1885
E-mail: <pedmonson@ndia.org>
On the Web: <http://register.ndia.org/interview/register.ndia?PID=Brochure&SID=_1GH0WZWpedmonson@ndia.org>

From the Editor

DoD and Standards

The memorandum issued by then Secretary of Defense William Perry in June of 1994 is well-know to anyone familiar with military acquisition. The activities and actions that ensued were collectively referred to as Defense Acquisition Reform. One of these activities addressed military specifications, standards, and handbooks. A review of the tens of thousands of these documents resulted in documents being:

- Cancelled
- Replaced with Non-Government Standards (NGS)
- Converted to Performance Specifications
- Converted to Handbooks
- Updated

Thousands of specifications have been converted by the Society of Automotive Engineers (SAE), the American Society for Testing and Materials (ASTM) International, or other non-government entities to commercial specifications. Organizations such as SAE and the Institute of Electrical and Electronic Engineers (IEEE) rushed to develop standards to replace documents such as MIL-STD-785, often duplicating each other's efforts.

It might have seemed to some that DoD and the military services had gotten out of the standards and specifications business. Even the promise that the government would participate in the development of NGS seemed destined to be an empty one, as funding severely limited participation by government personnel and fewer government people were now involved, even indirectly, with the standardization world.

Anyone who attended the 2005 Standardization Conference in March, held by the Defense Standardization Program Office (DSPO) knows that DoD is still very much in the standards business. The role of DoD and the military services is actually broader than it was prior to the famous June 1994 memorandum. That role includes the traditional one of developing specifications and standards. Now, however, these documents are either those that are unique to military systems and purpose and have no commercial equivalents, such as those dealing with nuclear weapons, or performance-based standards.

In addition to developing its own unique and performance-based standardization documents, DoD and the military services are deeply involved with commercial and other government organizations that develop standards and specifications. The 2005 Standardization Conference included speakers from the:

- US Army, Navy, and Air Force
- Federal Aviation Administration
- Defense Logistics Agency
- ASTM International
- SAE
- National Association of Corrosion Engineers (NACE) International
- ASTM International
- American National Standards Institute

Ned H. Criscimagna

Clearly DSPO is working hand-in-hand with many government and commercial organizations, here and abroad, to ensure that the specifications and standards needed to meet defense requirements are available. Consider the stated purpose, mission, and vision of the DSPO for the Defense Standardization Program (DSP):

PURPOSE: We champion standardization throughout DoD to reduce costs and improve operational effectiveness.

MISSION: We identify, influence, develop, manage, and provide access to standardization processes, products, and services for warfighters, the acquisition community, and the logistics community to promote interoperability, reduce total ownership costs, and sustain readiness.

VISION: DSP is a comprehensive, integrated standardization program linking DoD acquisition, operational, sustainment, and related military and civil communities. It is universally recognized for advancing DoD's Joint Vision 2010 and acquisition goals.

DSPO's own measures of its effectiveness include:

1. Improved interoperability of joint and coalition forces.
2. Standardized parts that have lowered costs, reduced inventories, shortened logistics chains, improved readiness, and furthered civil-military integration.
3. A DSP that is a single source for information exchange and coordinating all defense standardization efforts.
4. Institutionalized development and use of performance and non-government standards in DoD.
5. A DSP that is a vital technical resource and that actively participates in military, civil, and international standardization activities.
6. Prioritized set of standardization domains and a core cadre of experts in those domains.
7. System requirements documents (Mission Needs Statement/Operational Requirements Document (MNS/ORD)) that reflect standardization requirements.
8. Senior managers and program managers who view standardization as an essential element of acquisition program development.

Therefore, it is safe to state that DoD remains a positive and influential player in the world of standards and specifications.

New DoD RAM ... (Continued from page 19)

About the Authors

Ned Criscimagna's biography appears at the end of the article on Risk Management in this issue.

Michael G. Zsak, Jr. has over 34 years of detailed knowledge and practical experience in the technical and management aspects of DoD acquisition obtained while working in support of Army, Air Force, Office of the Secretary of Defense (OSD), Defense Logistics Agency, and Navy acquisition efforts. He now is a Systems Engineer with Decisive Analytics Corporation. He provides technical support to the Deputy Director, Systems Engineering and the Director, Test, Systems Engineering and Evaluation. Early in his career, Mike worked at the US Army Electronics Command, Fort Monmouth, NJ, where he worked in the Product Assurance Directorate and was assigned product assurance engineering responsibility for development of systems in the communications/avionics and surveillance, target acquisition and night observation area.

Mr. Zsak was assigned to HQ Air Force Systems Command in 1981, where he held various positions culminating in his appointment as the Director, Systems Engineering, Deputy Chief of Staff for Engineering and Technical Management. Mike left AFSC in 1991 and accepted the position of Director of the Weapon Systems Improvement & Analysis Division, Weapon Support Improvement Group, Assistant Secretary of Defense (Economic Security). After leaving that office, Mike served with the US Navy as the Deputy Program Manager for Tomahawk.

Mr. Zsak served as the DoD Advisor to the International Symposium on Product Quality & Integrity; the DoD representative to the US Technical Advisory Group for ISO/IEC JTC 1/SC7; Chaired the Reliability Analysis Center Steering Committee; was Vice Chair of the SAE International Division on Reliability, Maintainability, Logistics, and Supportability; and has been a guest lecturer at the University of Maryland and the Defense Systems Management College.

Mike received his BS in Mechanical Engineering from the New Jersey Institute of Technology, his MS in Management Science from Fairleigh Dickinson University, and completed the US Army Material Command Career Management Intern Training Program as a Quality and Reliability Engineer.

PRISM Column

How to Share Data

The sharing of system information is as simple as sharing a file. In the directory where the PRISM tool is installed, there are ".RSE" files. These files hold the information as it relates to a specific system. All the information (i.e., which process grade set has been applied, the order of components, the breakdown of the assemblies, etc.) is stored in this file. To share this information copy the file into a publicly shared directory (i.e., on a file server) or attach the file to an E-mail. The recipient then must copy the file to their local machine to open and use the file.

The building block of a system file is the component. Sharing component level information (i.e., Industry Part Number, OEM Number, Component Category, Component Type, etc.) can be done with some coordination. Using "Export Component Library" from the File drop down menu, the non-proprietary contents of a user's library can be extracted to a text file. These same entries can then be added to another user's library file using the "Import Component Library" function on the File drop down menu. *Note: Experience information is not exported.*

It is possible to create a separate component library for each system. Prior to adding any components to the component library, the "CL.GDB" file must be copied from the PRISM tool installation folder to a safe directory for later retrieval. After completing the system and adding the components to the library, the library file should be renamed. The copied "CL.GDB" file then should be copied back into the original folder. *Note: PRISM requires the component library file it is using to be named "CL.GDB."*

Sharing systems and component libraries is most efficient when it is done using a system coordinator who will act as a data administrator for compiling data to be added to the library. Each user will rely on this data administrator/coordinator to act as the custodian for a composite library. If users add components, change component information, or remove a component, they would need to advise the data administrator so that the composite library can be updated.

If users have added the components to their systems without adding them to the library, simply sharing the system with the data administrator will allow a library update. The data administrator would open the system and using the PRISM tool's "Add All to Library" function, add to the component library. The composite library can then be added to each user's library using the steps previously mentioned.

Additional information on sharing system files and component libraries can be found in the PRISM user's manual Appendix K. This appendix also illustrates best practices for implementing PRISM usage in team environments.

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>).

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