DOD GUIDE FOR ACHIEVING

RELIABILITY, AVAILABILITY, AND MAINTAINABILITY

"Systems Engineering for Mission Success"

AUGUST 3, 2005

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. 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 as part of a robust systems engineering process to achieve satisfactory levels of RAM, successfully demonstrate them during operational test and evaluation, and sustain them through the system's life cycle.

The Guide supports the DoD's fundamental principles and procedures as documented in DoD Directive 5000.1 and DoD Instruction 5000.2, and the discretionary best practices in the *Defense Acquisition Guidebook*. Operations and Acquisition professionals should use this guide as a reference source supporting their management and technical responsibilities.

RAM capabilities are achieved through a collaboration of skilled people and organizations, with a clear mission and goal, armed with the right supporting information, adequately resourced, using effective technical tools and systems engineering management activities, and developing the necessary documentation at each product stage, throughout the acquisition process.

This Guide focuses on the four key steps necessary for building systems with the required levels of RAM:

1. Understand and document user needs and constraints,
2. Design and redesign for RAM,
3. Produce reliable and maintainable systems, and
4. Monitor field experience and sustain RAM performance.

Chapter 1 introduces RAM, what it is, why it is important, current RAM problems in the DoD, and activities appropriate to achieving satisfactory levels. It concludes with a guide for senior management. Chapter 2 provides an overview of the four-step model for achieving RAM. Chapter 3 focuses on Step 1 including RAM metrics, joint capabilities integration and development, and pre-acquisition activities. Chapter 4 focuses on Step 2 and scopes successful approaches for designing-in reliability and maintainability. Chapter 5 focuses on Step 3 and expands this discussion through the testing, production and fielding of capabilities. Chapter 6 focuses on Step 4 and addresses methods for sustaining RAM through the operational life and providing lessons learned for the following generation of capabilities. Throughout the document, the guide also highlights the integration of RAM activities with the defense acquisition management framework, the joint capabilities integration and development system, and the systems engineering technical reviews.

We encourage its wide spread use in the acquisition, testing, and supporting of defense systems. We also ask for your feedback on its utility by contacting our Office of Primary Responsibility, OUSD(AT&L)DS/SE/ED via ATL-ED@OSD.MIL.

JUN 2 0 2005

David W. Duma
Acting Director
Operational Test & Evaluation

AUG - 3 2005

Kenneth J. Krieg
Under Secretary of Defense
Acquisition, Technology, and Logistics

Chapter 1 Reliability, Availability, Maintainability, and the Department of Defense

1.1 Introduction

The primary objective of Department of Defense (DoD) acquisition is to acquire quality products (systems) that satisfy user needs with measurable improvements to mission capability and operational support in a timely manner, and at a fair and reasonable price.[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. This chapter introduces RAM, what it is, why it is important, current RAM problems in the DoD, and activities appropriate to achieving satisfactory levels. These topics are developed further in subsequent chapters.

1.2 RAM Defined

RAM refers to three related characteristics of a system and its operational support: reliability, availability, and maintainability.

1.2.1 Reliability

Reliability is the probability of an item to perform a required function under stated conditions for a specified period of time. Reliability is further divided into mission reliability and logistics reliability. For further information see Sections 3.2.2 and 4.4.8.

1.2.2 Availability

Availability is a measure of the degree to which an item is in an operable state and can be committed at the start of a mission when the mission is called for at an unknown (random) point in time. Availability as measured by the user is a function of how often failures occur and corrective maintenance is required, how often preventative maintenance is performed, how quickly indicated failures can be isolated and repaired, how quickly preventive maintenance tasks can be performed, and how long logistics support delays contribute to down time.

1.2.3 Maintainability

Maintainability is the ability of an item to be retained in, or restored to, a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair.

1.2.4 Factors Affecting RAM

Many factors are important to RAM: system design; manufacturing quality; the environment in which the system is transported, handled, stored, and operated; the design and development of the support system; the level of training and skills of the people operating and maintaining the system; the availability of materiel required to repair the system; and the diagnostic aids and

[1] DoD Directive 5000.1, The Defense Acquisition System, May 12, 2003, Paragraph 4.2, page 2.

tools (instrumentation) available to them. All these factors must be understood to achieve a system with a desired level of RAM. During pre-systems acquisition, the most important activity is to understand the users' needs and constraints. During system development, the most important RAM activity is to identify potential failure mechanisms and to make design changes to remove them. During production, the most important RAM activity is to ensure quality in manufacturing so that the inherent RAM qualities of the design are not degraded. Finally, in operations and support, the most important RAM activity is to monitor performance in order to facilitate retention of RAM capability, to enable improvements in design (if there is to be a new design increment), or of the support system (including the support concept, spare parts storage, etc.).

Although significant improvements have been made in increasing the reliability of basic components such as microelectronics, these have not always been accompanied by corresponding gains in the reliability of equipment or systems. In some cases, equipment and system complexity and functionality have progressed so rapidly that they negate, in part, the increased reliability expected from use of the higher reliability basic component. In other cases, the basic components have been misapplied or overstressed so that their potentially high reliability is not realized. In still other cases, program management has been reluctant or unable, due to program budget shortfalls or highly aggressive schedules, to devote the time and attention necessary to ensure that the potentially high reliability is achieved. However, in many areas of the commercial sector, such as the computer, electronic and automotive industries, increased system complexity has not negated system reliability. In fact, often products with increased system complexity are provided with increased system reliability. This is an area the defense sector must also strive to improve.

1.3 Importance of RAM

Achieving specified levels of RAM for a system is important for many reasons, specifically the affect RAM has on readiness, system safety, mission success, total ownership cost, and logistics footprint.

1.3.1 Readiness

Readiness is the state of preparedness of forces or weapon system or systems to meet a mission, based on adequate and trained personnel, material condition, supplies/reserves of support system and ammunition, numbers of units available, etc. Poor RAM will cause readiness to fall below needed levels or increase the cost of achieving them. Effective diagnostics helps assure both system/mission readiness and efficient repair/return to ready status.

1.3.2 System Safety

Inadequate reliability or false failure indications of components deemed Critical Safety Items (CSI) may directly jeopardize the safety of the user(s) of that component's system and result in a loss of life. The ability to safely complete a mission is the direct result of the ability of the CSI associated with the system reliably performing to design intent.

1.3.3 Mission success

Inadequate reliability of equipment directly jeopardizes mission success and may result in undesirable repetition of the mission. The ability to successfully complete a mission is directly affected by the extent to which equipment needed to perform a given mission is available and operating properly when needed. Mission aborts caused by false failure indications can have the same impact as hard failures.

1.3.4 Total Ownership Cost

The concept of Total Ownership Cost (TOC) is an attempt to capture the true cost of design, development, ownership and support of DoD weapons systems. At the individual program level, TOC is synonymous with the life cycle cost of the system. To the extent that new systems can be designed to be more reliable (fewer failures) and more maintainable (fewer resources needed) with no exorbitant increase in the cost of the system or spares, the TOC for these systems will be lower.

1.3.5 Logistics Footprint

The logistics footprint of a system consists of the number of logistics personnel and the materiel needed in a given theater of operations. The ability of a military force to deploy to meet a crisis or move quickly from one area to another is determined in large measure by the amount of logistics assets needed to support that force. Improved RAM reduces the size of the logistics footprint related to the number of required spares, maintenance personnel, and support equipment as well as the force size needed to successfully accomplish a mission.

1.4 The Current RAM Problem with Military Systems

While the speed, range, firepower, and overall mission performance of weapons systems has improved dramatically over the years, RAM problems have persisted. RAM problems slow the development and fielding of systems, drive up the total ownership cost, and degrade operational readiness and mission accomplishment at the strategic, operational and tactical levels. New complex digital designs have increased software development and integration issues and the importance of integrated diagnostics.

A number of studies and reports indicate that the problems are not limited to a few systems; they often arise in the initial definition of requirements; and they have a significant impact on the DoD budget. RAM data collection and analysis are part of the problem.

A study[2] of some defense systems provides an example of the breadth of the reliability problem (Figures 1-1 and 1-2). Data came from operational tests of systems from 1985-1990 and 1996-2000, respectively. The percentage of systems meeting reliability requirements decreased from 41 percent to 20 percent.

[2] Reliability Performance Today, presented at ATEC/PEO C3T Day, AEC R&M Directorate, 27 Jul 01.

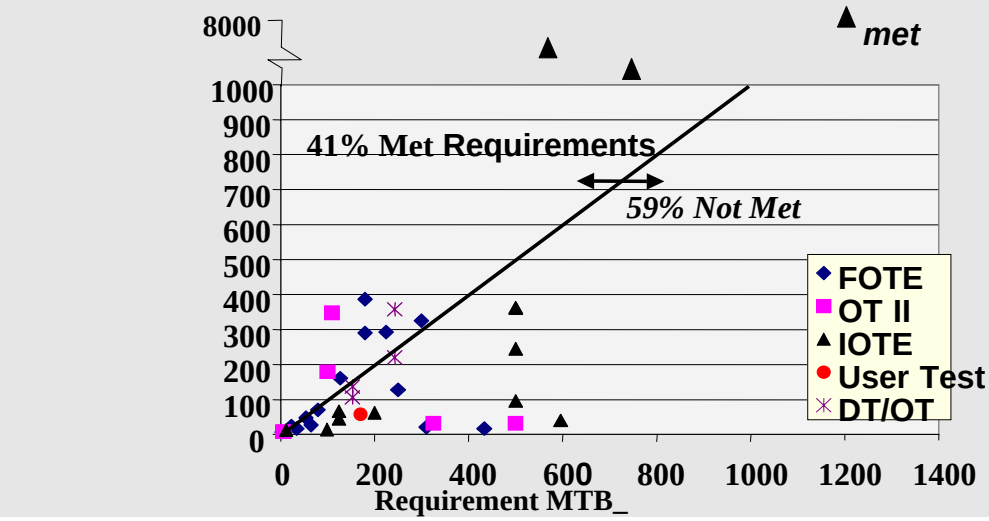


FIGURE 1-1: Demonstrated Reliability vs. Requirements for Operational Tests, 1985-1990[3]

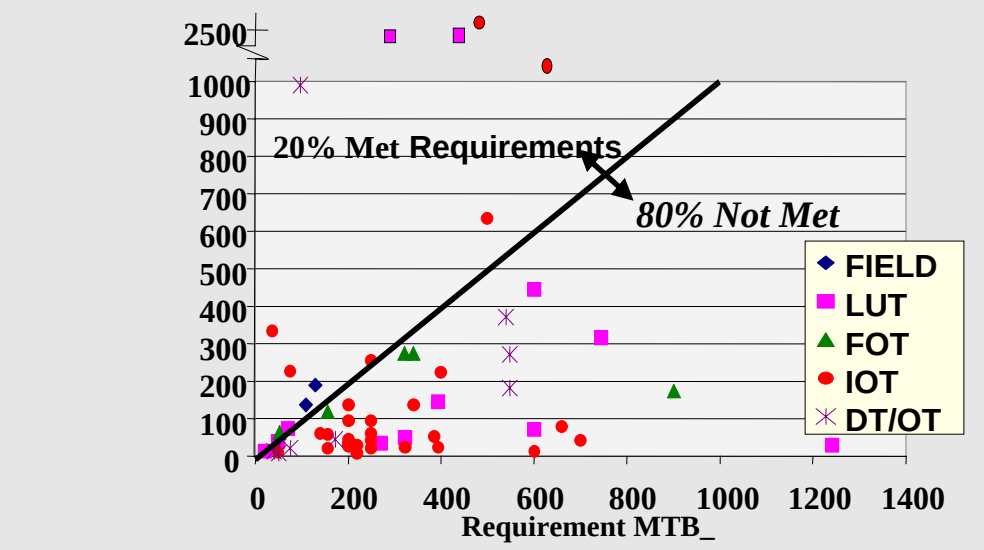


FIGURE 1-2: Demonstrated Reliability vs. Requirements for Operational Tests, 1996-2000[4]

[3] MTB_ means mean time between _ (where _is failure, critical failure, etc). FOTE: Follow-On Test and Evaluation, OT II: Operational Test II, IOTE: Initial Operational Test and Evaluation, DT/OT: Developmental Test/Operational Test

[4] LUT: Limited User Test, FOT: Follow-On Test, IOT: Initial Operational Test

In both periods (1985-1990 and 1996-2000), a large percentage of systems failed to meet needed levels of operational reliability. Further, the trend worsened. As a result, DoD conducted a series of studies on these programs to determine the causes. They concluded[5] that defense contractor reliability design practices may not routinely be consistent with best commercial practices for accelerated testing, simulation-guided testing, and process certification and control. Physics-of-failure approaches with physics-based computer-aided design tools may not have been used on a regular basis. A Failure Modes, Effects, and Criticality Analysis (FMECA) and a Failure Reporting, Analysis, and Corrective Action System (FRACAS) were generally not effective in correcting problem failure modes. A FRACAS generally is effective only if a technical Failure Analysis Program is funded and implemented. In addition, DoD found that inadequate testing was conducted at the component and system level. Testing time was limited, and sample sizes were too small. Component stress testing was frequently inadequate or not conducted. Proper accelerated life testing was rarely accomplished. Adequate Reliability Program Plans that provided a roadmap to realization of reliability program objectives and requirements were lacking as well.

A 2003 General Accounting Office (GAO) analysis reported that persistent low readiness rates and costly maintenance problems contribute to increases in the total ownership cost of DoD systems[6]. The GAO report offered several reasons: 1) weapons system requirements focused on technical performance, with little attention to operations and support (O&S) costs and readiness, especially early in development; 2) using immature technologies to meet performance goals weakened the ability to design weapon systems with high reliability; and 3) there was limited collaboration among organizations charged with requirements setting, product development, and maintenance.

Another study, by the National Academy of Sciences, recommended improvements to data collection and analysis to confront RAM problems: "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."[7] The study also recommended "Military reliability, availability, and maintainability testing should be informed and guided by a new battery of military handbooks . . .."[8]

In summary, these studies and the corporate experience of the DoD over the past decade suggest the following reasons why systems fail to achieve RAM requirements:

- Poorly defined or unrealistically high RAM requirements.

[5] Conclusions of the studies were published in two papers: a. AEC-AMSAA paper, "Making Reliability a Reality" published in the Army AL&T magazine in March 2003, and b. AEC-AMSAA paper, "Five Key Ways to Improve Reliability" published in the RAC Journal in 2Q 2003.

[6] GAO final report; *BEST PRACTICES: Setting Requirements Differently Could Reduce Weapon Systems' Total Ownership Costs*; February 11, 2003; [GAO Code 120092/GAO-03-057]

[7] *Statistics, Testing, and Defense Acquisition: New Approaches and Methodological Improvements*, Michael L. Cohen, John B. Rolph, and Duane L. Steffey, Editors, National Academy Press, Washington D.C., 1998.

[8] This Guide does not fully replace DoD 3235.1H (the RAM Primer) which will continue to be available to users at http://www.dtic.mil/whs/directives/corres/html/32351h.htm. It should be used with caution because the limitations associated with the concepts and techniques presented are not clearly defined in the Primer.

- Lack of priority on achieving R&M
- Too little engineering for RAM. Among engineering process failures, these stand out:
  - Failure to design-in reliability early in the development process.
  - Inadequate lower level testing at component or subcomponent level.
  - Reliance on predictions instead of conducting engineering design analysis.
  - Failure to perform engineering analyses of commercial-off-the-shelf (COTS) equipment.
  - Lack of reliability improvement incentives.
  - Inadequate planning for reliability.
  - Ineffective implementation of Reliability Tasks in improving reliability.
  - Failure to give adequate priority to the importance of Integrated Diagnostics (ID) design influence on overall maintainability attributes, mission readiness, maintenance concept design, and associated LCC support concepts.
  - Unanticipated complex software integration issues affecting all aspects of RAM.
  - Lack of adequate ID maturation efforts during system integration.
  - Failure to anticipate design integration problems where COTS and/or increment design approaches influence RAM performance.

1.5 The Steps to Achieving Satisfactory RAM

The key to developing and fielding military systems with satisfactory levels of RAM is to recognize it as an integral part of the Systems Engineering process and to systematically manage the elimination of failures and failure modes through identification, classification, analysis, and removal or mitigation. Additionally, strengthened ID design maturation tasks will enable RAM design attributes to be realized. These activities start in pre-systems acquisition and continue through development, production, and beyond into operations and support.

There are four key steps that can be taken to achieve satisfactory levels of RAM. Figure 1-3 shows the four key steps with the current DoD 5000 series acquisition management framework[9] to illustrate the time frame at which the four key steps should be conducted. Unlike the DoD 5000 series acquisition management framework there are not milestone decisions to signify the beginning and end of each key step. Instead, the beginning and end of each step is illustrated within Figure 1-3 as a flexible time period depending on each system acquisition process.

[9] The current DoD 5000 series acquisition management framework is outlined in DoD Instruction Number 5000.2 issued on May 12, 2003.

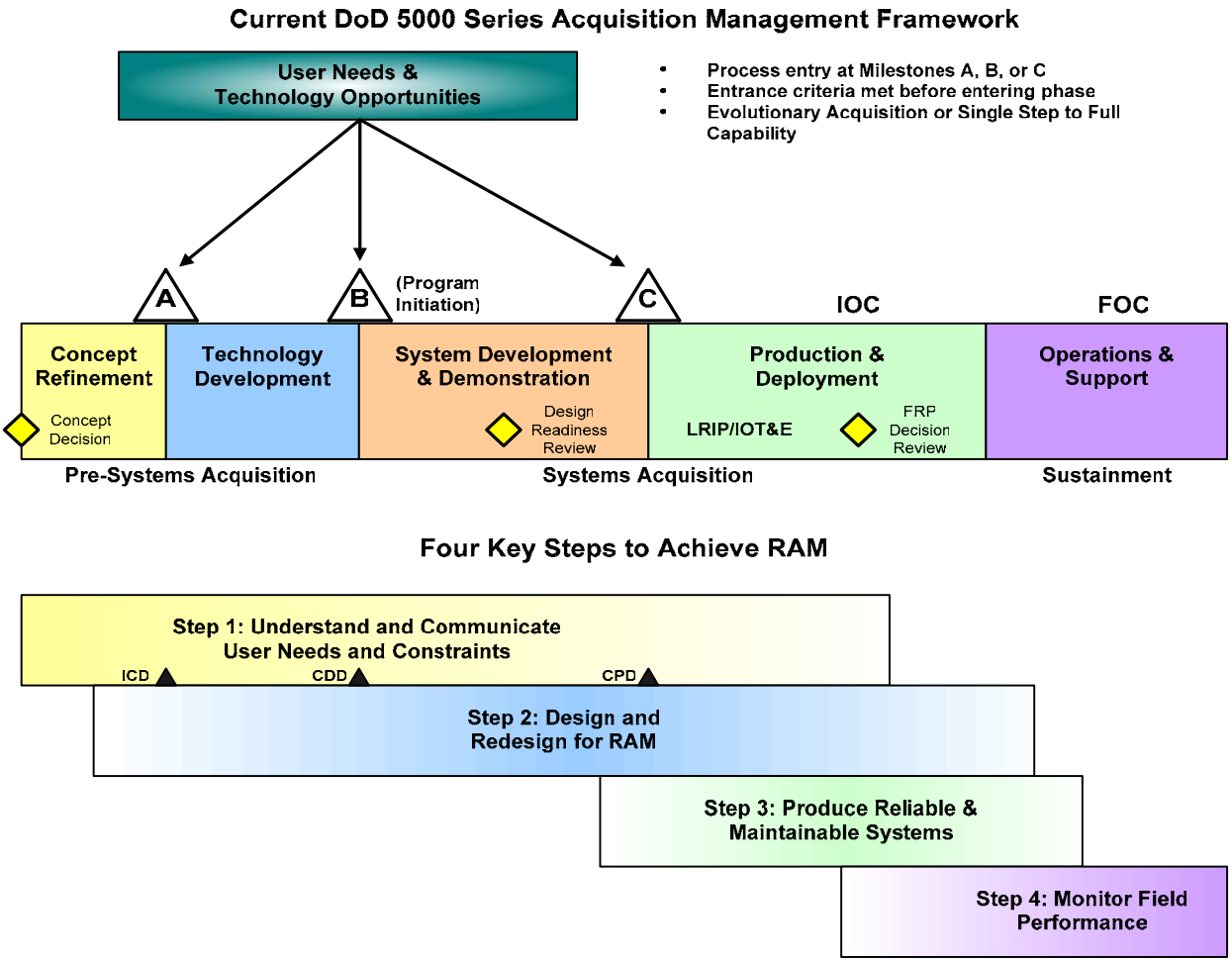


FIGURE 1-3: Four Key Steps to Achieve RAM within DoD 5000 Series Acquisition Management Framework

1.5.1 Step 1: Understand and Document User Needs and Constraints

The first priority in an acquisition program is to thoroughly understand what the customer needs and expects (the customer includes those who will operate, maintain, and support the capability being acquired). Step 1 involves the following:

- The user and acquisition communities collaborate to define desired capabilities to guide development. The definition of capability includes the mission, system performance, force structure, readiness and sustainability, as well as constraints such as logistics footprint and affordability.
- Within this overall capability, determine the reliability, availability and maintainability needs of the user, in operational terms, for the operational concept, in the expected operational environment and conditions, considering peacetime and wartime use. A multidisciplinary team of users (operators and maintainers), system and design engineers, manufacturing engineers, and testers collaboratively develop a RAM Rationale which establishes bounds on the trade space and guides the entire program. This analysis will likely require the use of modeling to ensure performance is achieved across the required

scenarios. The analysis considers the interaction of many elements, e.g., system reliability with the logistic support concept (the support structure used to maintain and repair the system, the number of spares, and spare parts) and operation in an integrated diagnostics environment where additional facilities, support equipment or ground stations play a major role in achieving operational requirements. User constraints on the number of people available to operate and maintain the system will affect availability of the fleet. Throughout the analysis, the probability of mission success should be a fundamental metric. Mission failure due to the system's failure to operate properly in its intended environment is a reliability failure as well as a mission failure whether caused by hardware (component failures) or software (Built-in-Test (BIT) false alarms). Since component reliability is dependant on the environment, the reliability of commercial-off-the-shelf (COTS) items may differ significantly in the military application.

- Compare the needed levels of RAM to the RAM performance of current systems/capabilities performing the mission. Assess the feasibility of achieving the needed levels of RAM with available technology. Initiate technology development and risk reduction efforts to achieve user RAM needs.
- Develop a Request for Proposal (RFP) that addresses all aspects of system performance. The RFP should clearly identify all constraints, assumptions, and definitions needed for the contractors to put the RAM situation in context, derive the inherent levels of RAM (those that are determined by design and manufacturing), determine the best approach for achieving satisfactory RAM, and state the operational RAM requirements (e.g., operational availability). (See Appendix A for further information on this topic)
- Translate the operational RAM terms into suitable RFP and contractual terms for the material development contractor to pursue. Develop the mission and logistics reliability specification requirements and the maintainability and integrated diagnostics specification requirements. These and associated RAM program and acceptance test requirements become part of the RFP and contract. Specification development requires conversion of the operational RAM parameters to an equivalent contractual measurement. This process has been recognized as a weak link.
- Provide reliability and maintainability incentives in contracts. To achieve the levels of RAM the user needs, the Program Manager has to put requirements and incentives in the contract, pay for them, conduct program reviews, and provide effective oversight. Contract requirements and the vendor selection process must reflect explicitly the need for reliable systems. Contracts should provide clear incentives to design and build reliable, maintainable systems versus allowing significant profit from follow-on replenishment spares. Both monetary and non-monetary incentives can be used to assess and measure contractor RAM performance. If properly formulated, RAM performance requirements stated in performance-based contracts can ensure that the contractor or supplier will focus on the system or product RAM performance requirements of primary interest. This approach allows incentives to be awarded realistically based on the RAM performance measurements that are made during design and development. RAM performance requirements (for example, mission reliability, logistics reliability, testability, diagnostics) on which the incentives are based must be realistic, measurable, and unambiguous to permit valid demonstration and verification within stated confidence bounds. The RAM incentive program should flow with the normal system development activities and schedules. Some DoD contracts have included the requirement for a RAM

demonstration before full-rate production, with rewards and penalties, to ensure that RAM gets appropriate attention during development.

The Program Manager initiates three RAM management processes during Step 1: Understand and Document User Needs and Constraints. The RAM management processes include the RAM Program Plan (RAMPP), the Data Collection, Analysis, and Corrective Action System (DCACAS), and the RAM Case. The PM also initiates the Test and Evaluation Master Plan (TEMP), which includes RAM test and evaluation planning. These processes continue through the system's life cycle. All are addressed in more detail in later chapters.

Inadequately addressing Step 1 has been identified as one of the primary reasons for test difficulties and the failure to meet user needs. The definition should include specifying values for the appropriate RAM parameters, or metrics, (to be attained under operational conditions) needed to provide a measurable improvement in mission success and operational support at a fair and reasonable price.

1.5.2 Step 2: Design and Redesign for RAM

During this phase the key objectives are to:

- Develop a comprehensive program for designing and manufacturing for RAM that includes people, reporting responsibility, and a RAM Manager.
- Develop a conceptual system model, which consists of components, subsystems, manufacturing processes and performance requirements. Use the model throughout development to estimate performance and RAM metrics.
- Identify all critical failure modes and degradations and address them in design.
- Use data from component-level testing to characterize distribution of times to failure.
- Conduct sufficient analysis to determine if the design is capable of meeting RAM requirements.
- Design in: diagnostics for fault detection, isolation and elimination of false alarms; redundant or degraded system management for enhanced mission success; modularity to facilitate remove-and-replace maintenance; accessibility; and other solutions to user-related needs such as embedded instrumentation and prognostics.

To meet these objectives, Step 2: Design and Redesign for RAM, requires the following key activities:[10]

1.5.2.1 Implement the right activities at the right time in the right way

As important as it is to select the right activities, it is equally important to conduct the activities at the right time. An analysis intended to support design improvement, for example, is of little value if it is begun near or after the critical design review. For maintainability, it is of little value to require explicit levels of system testability for accurate and dependable BIT fault detection and isolation during the design phase, if ID software maturation efforts to utilize these testability

[10] Many of these are based on Crow, L. H., "Achieving High Reliability, *The Journal of the Reliability Analysis Center, Fourth Quarter, 2000,* 1-3.

features and minimize false alarms are not also considered. ID maturation processes are included in the overall RAM program plan and implemented throughout platform integration testing.

Finally, even if an activity is conducted at the correct time, the results will be misleading or will be of little use in achieving the requisite level of RAM if it is not conducted properly. Standards, guides, and textbooks are available that provide the correct procedure for conducting nearly every type of analysis or test related to designing for RAM.

1.5.2.2 Conduct Formal Design Reviews for Reliability and Maintainability

Conduct formal reviews for RAM that promote an understanding of the tactical operational environment in which the system or subsystem will operate and to assure progress toward achieving RAM requirements. Formal RAM reviews should be conducted at least once each during preliminary design and during final design and should be an integral part of the System Requirements Review (SRR), System Functional Review (SFR), Preliminary Design Review (PDR) and Critical Design Review (CDR). These reviews occur during the System Development and Demonstration (SDD) phase. RAM reviews should begin early in the system development process and continue through production and deployment. RAM reviews might even be appropriate during Technology Development (TD).[11] These reviews assure that the RAM model, the current design configuration, and the engineering design agree.

1.5.2.3 Use an Impartial, Competent Peer to Perform the Design Review

The engineer who performs the RAM analyses is usually the judge of the attributes to be examined and their exact depth of examination. The analyst also selects the analytical approach. All of these decisions are a function of the analyst's experience, wisdom, and perception of the user needs and constraints. For these reasons it is very possible that omissions or inadvertent errors will be occasionally made. Experience has shown that approximately 40 percent of all analyses contain significant shortcomings when performed for the first time.[12] Approximately half of these are defects or omissions in the analysis alone and are not design defects. The remaining 20 percent actually represent design defects, the severity of which ranges from minor to mission catastrophic. Experience has also shown that about five percent of all released manufacturing designs contain potential mission jeopardizing defects. The only proven method for detection of these defects is an independent review of the design details by an impartial, objective, competent peer in the appropriate technical field.

1.5.2.4 Use a Closed-Loop Design Review Process

The review process uses a closed-loop system that identifies each design defect, enters it into a tracking system, and requires resolution by either a design change or a program waiver. The process differentiates between analysis omissions and defects or design deficiencies. Analysis deficiencies are also tracked to assure timely updates, which may identify additional design deficiencies and serve as an accurate historical record of the design activity.

[11] DoD Instruction 5000.2, Operation of the Defense Acquisition System, May 12, 2003.
[12] NASA Preferred Reliability Practices: Practice No. PD-AP-1302, "Independent Review of Reliability Analyses."

1.5.2.5 Emphasize Systems Engineering Design Analysis and Rely Less on RAM Predictions

Systems engineering is a logically sequenced, consistent set of technical activities that translates a customer's needs and requirements into a balanced solution. Unfortunately RAM predictions often do not provide the balanced solution systems engineering design analysis strives to obtain. RAM prediction is any method used to assess the level of RAM that is potentially achievable, or being achieved, at any point. Achieving metrics via a RAM prediction will not ensure that the best system design is developed. Too often the following is forgotten about RAM predictions:

- RAM predictions are a process, not a one-time activity, which should begin in early development and continue throughout the life of the system, with different methods used at varying times.
- No one method of RAM prediction is right for every item at all times. The "right" method is the one for which the requisite data are available and that is appropriate for the intended use of the RAM prediction (i.e., comparison, spares computations, contractual verification, part characterization, system field performance, etc.).
- RAM predictions stated at a confidence level are more meaningful than a point estimate.
- An understanding of the method itself, the maturity of the design, and the fidelity of the data must temper the results of any method used to perform RAM predictions.

Systems engineering ensures that the solution that satisfies the requirements of a RAM prediction will also be the best overall solution with regards to multiple programmatic and technical considerations. Systems engineering expands the evaluation criteria to select criteria that best balance program requirements, such as system performance, total ownership cost, schedule, supportability, risk, etc. The criteria are selected based on the stated problem as well as the level and complexity of the analysis required.

1.5.2.6 Fully Understand the Implications of Using COTS Equipment

The use of commercial-off-the-shelf (COTS) items in military systems has definite advantages over developing a new, comparable item. In addition to saving the cost of development, COTS items often have a proven track record in commercial products, come with warranties, and may be available from multiple sources. Perhaps most importantly, the technology used in electronic COTS items rapidly changes. By buying COTS, the program can take advantage of the newest technologies being used by the manufacturer of the COTS item. COTS items usually include computers, displays, power supplies, input/output devices, communications equipment, and so forth. Even some system-level items, such as cargo trucks, have been purchased off-the-shelf.

Despite the advantages of using COTS equipment, it should not be used without fully understanding the implications of using it in a military environment. Before deciding to buy COTS for a military application, the program should carefully weigh important factors including the environment, integration, maintenance, long-term support, warranty, and integrated diagnostics. These factors and additional details on the use of COTS are addressed in Chapter 3, section 3.5.

1.5.2.7 Focus on Maintainability (Especially Diagnostics) and Provide Sufficient Resources to Mature the Diagnostic Capability

Effective ID designs reduce maintenance time and increase system availability. Vendor maintainability demonstrations effectively support maturing subsystem fault detection and isolation capabilities. Overall system maintainability demonstrations including fault insertions enable verification of accessibility, provide data to calculate remove and replace times, and confirm the degree of technical skill and adequacy of technical documentation required to perform maintenance. As every failure provides the opportunity to improve reliability, it also provides the opportunity to evaluate and improve maintainability characteristics.

1.5.2.8 Link Design Testing and Reliability Testing

Every test should also be a reliability test. Early testing often focuses on performance of the system, a subsystem, or a component. Nevertheless, every time a system is tested, reliability data should be collected. Early testing may not be in the stressful operational environment or under realistic conditions. However, when a failure occurs, consider that particular failure mode explicitly, whether a true component failure or a built-in test indicated system failure. Consider every failure an opportunity for better system understanding, characterization, and ultimately for system improvement. Early in the development process, failure mode removal is almost always easier and less costly than later in the development life cycle. Development must deal with every failure mode, not just those that appear in specially designed reliability tests. For complex systems, it is possible that the demonstrated reliability at the end of the final design phase may still fall short of the RAM design specifications. A target minimum value of the initial reliability, to be achieved by the end of development, should be established during the pre-acquisition. In order to conform to the stated purpose of DoD Acquisition, the target minimum value should represent a measurable improvement to mission capability and operational support at a fair and reasonable price.

1.5.2.9 Manage the Failure Mode Mitigation Process

A closed-loop process deals with failure modes when they are found. Every failure mode, potential modes that surface during design analysis as well as those identified during performance or other tests, should go through a process to determine how to deal with the failure mode. It is important to assess the risk to mission success that the problem poses. Experts who are familiar with similar systems or the operational environment may be able to identify potential failure modes and resolutions as early as the system concept model.

Use a failure modes and effects analysis (FMEA) to identify failure modes and potential problem areas affecting the mission, hardware reliability, and safety. The FMEA provides a structured process for addressing and mitigating failure modes. Experience has shown that it is easy to be overly optimistic about the effectiveness of failure mode mitigation. Corrective actions (fixes) are rarely 100 percent effective. Methods for determining reliability growth are addressed in Chapter 4.

The FMEA should be a living document during the development of hardware design. The primary benefit of the FMEA is the early identification of all critical and catastrophic subsystem or system failure modes so they can be eliminated or minimized through design early in development. It is important that the FMEA is continually updated to keep pace with the evolving design so it can be used effectively throughout development and sustainment.

1.5.2.10 Assess the Risks and Operational Impacts Before Trading RAM for Cost, Schedule, or Other Requirements

If the system does not achieve good RAM, mission performance and life cycle cost are at risk. End-to-end modeling of the system life cycle helps to evaluate the impact of changes in RAM. A model of the logistics support concept quantifies the implications of RAM levels on the elements and costs of support over the long term. The pressures of budget or schedule can cause Program Managers and contractors to consider reducing or eliminating RAM activities, in particular the task of ID maturation since it occurs near the end of system development just prior to technical or operational evaluation . An objective analysis of risk and impact should be made. Specifically, any potential negative impact on the system's ability to provide measurable increases to mission capability or operational support should be weighed against any potential short-term savings. Unless a programmatic, systems engineering and total life-cycle perspective is taken in making such decisions, the net result can be decreased mission performance and increased costs over the long term.

1.5.2.11 Address RAM Considerations in Pre-Systems Acquisition Technology Development Activities

RAM personnel assist in the evaluation of technological capabilities and assess the risk and cost impacts on achieving RAM needs. Modeling the logistics support program helps quantify the RAM impacts on the size and cost of the life cycle support program and indicate where technology development, specifically for reliability and maintainability, is needed to meet acquisition objectives.

1.5.2.12 Avoid Delaying Corrective Actions

Estimates of reliability in the presence of delayed corrective actions tend to significantly over estimate reliability. Delaying corrective actions enables failure modes to continue and may lead to implementation prior to verifying the effectiveness of the proposed fix. This is particularly important for ID software corrective actions implemented late in development. If diagnostics false alarms are corrected by software, they (like component failures) require adequate test time to verify effectiveness of the proposed fix.

1.5.2.13 Provide Meaningful Oversight in Executing the Contract

The best practice in executing oversight responsibility is based on the following four principles.

- Treat RAM as an integral part of the systems engineering process. Assess RAM in each phase of development. In early phases the reliability allocation among components is

important and its realism and empirical basis must be reviewed carefully. The design of the support system must be checked to ensure it is consistent with known operational constraints.

- Find deficiencies as early as possible. These deficiencies can be in any of three areas: technology and its application in the design, the operational concept, and the support concept. Untested technologies should be tested in the stressful operational environment. Logistics drivers such as high failure rate modules, inaccurate fault diagnostics, and mismatches between required maintenance skills and the actual planned maintenance workforce need to be identified as early as possible. It is important that the supporting system be developed concurrently with the system development and demonstration. It is important to develop and assess associated support equipment, both hardware and software, in concert with the host platform in order to identify and correct RAM problems with RAM integration prior to Initial Operational Capability. The government has special knowledge of the operational environment and the realities of the planned maintenance workforce which also should be integrated.
- Correct deficiencies in the most appropriate phase. As a rule of thumb, the earlier the better.
- Coordinate and integrate RAM testing and evaluation across all phases. The context for evaluation is always the performance in the operational environment and expressed in operational terms. Early RAM consideration might be based, in part, on expert opinion, or modeling of the system. Later, real test data comes in and the evaluation should be modified to reflect the new information. Areas of uncertainty are areas of risk. Ways to reduce the uncertainty need to be devised as appropriate. Tests of components in stressful operational environments may be appropriate. Many of these actions will require government participation. For example, carrying a proposed sensor package on a surrogate vehicle that simulates the vibration and thermal environment may be appropriate. Another example pertains to new avionics design for an existing airframe: experience has shown that measuring the actual environment (temperature, vibration, power stability, g-forces) in an aircraft avionics location is more effective for achieving RAM than relying on the environmental design specifications of the aircraft. Only by staying informed on the reliability aspects of engineering can the government contribute to the success of the product.

1.5.3 Step 3: Produce Reliable and Maintainable Systems

The purpose of the Production and Deployment phase of acquisition is to achieve an operational capability that satisfies mission needs. There are two major parts of this phase: Low-Rate Initial Production (LRIP), and Full-Rate Production and Deployment. Before beginning this phase, the user operational capability is updated. LRIP quantities are normally limited to no more than 10% of the total contemplated production. The LRIP effort completes the manufacturing development process and generates the units for Initial Operational Test and Evaluation (IOT&E). The IOT&E provides information on how well the system meets user needs including RAM. Full-Rate Production and Deployment provide the systems, supporting materiel and services to the users. Finally users attain Initial Operational Capability (IOC).

The emphasis of Step 3 shifts to process control, quality assurance, and environmental stress screening, which is also visible in the RAM activities expected during this phase. In addition, data collection from production articles deployed to operational units provides insight into how well production units are performing in the operational environment. Optional RAM activities during the Production and Deployment phase include a failure prevention and review board (examines DCACAS results to improve design by eliminating problems), production reliability qualification/acceptance tests, lot acceptance testing, and participation in software change review board (SCRB) to insure proposed ID corrective actions are incorporated and do not degrade overall RAM. The RAM activities that are recommended for follow-up after initiation during the engineering and development phase include reliability growth testing, maintenance/maintainability demonstration and evaluation, continued ID maturation efforts, and DCACAS. Required RAM activities include continued support of the DCACAS process and subcontractor controls as well as implementation of stress screening to precipitate known failures prior to delivery. Another goal of Step 3 is achieving the system's initial operational capability.

1.5.3.1 Testing

It is important to continue development testing of oversight of evolving RAM attributes to determine if the system has a satisfactory level of reliability, availability, and maintainability. The purpose of test and evaluation is learning. Though operational assessments are conducted through Steps 1 and 2, LRIP is normally the first opportunity for dedicated operational tests, using production representative units, operationally representative support systems (including peculiar support systems), representative support personnel, and an operationally realistic environment. The final judgment will require that the system "satisfy user needs with measurable improvements to mission capability and operational support in a timely manner, and at a fair and reasonable price." This is also the opportunity to verify that fixes from previous phases have been developed, incorporated, and correct the RAM problems without introducing new ones. Often, there are not enough time or test units at the conclusion of normal development or during OT&E to demonstrate achievement of high reliability with high confidence. As a result, all relevant RAM data should be exploited for possible use in the overall evaluation.

1.5.3.2 Quality Assurance

A primary RAM concern during manufacturing is to prevent degradation of the inherent reliability, availability, and maintainability designed into the system during the design phase. The Quality and Product Assurance activities work closely with the RAM development team to assure a full understanding of the impact of the manufacturing processes on end item RAM and to develop value added manufacturing processes that assure the integrity of the product. A stable base of certified vendors and appropriate component acceptance testing is essential. Involvement of RAM engineering in the review/approval loop for the selection of parts and materials, manufacturing processes and procedures, and assembly procedures further ensures that RAM concerns are addressed. By participating in SCRB and Engineering Change Proposal (ECP) reviews RAM engineers assure RAM and ID goals are not compromised. During the transition from development to production there is often significant pressure to redesign for the

purpose of saving costs. Including the RAM team in the review process can eliminate changes that compromise achieving RAM performance.

1.5.3.3 Achieving Initial Operational Capability

During the second part of this phase (full-rate production and deployment), units are receiving trained manpower, systems, equipment, and support; and they are working toward achieving initial operational capability and the required readiness (operational availability) and sustainability levels. There are many opportunities during this transition for RAM-related problems to arise, such as inadequate maintenance training, unanticipated failure modes, and differences in the operational environment or use profile from that anticipated during design. The RAM team should anticipate this opportunity, monitor this transition, and identify resources to rapidly assess and resolve problems that may arise. Timely identification of RAM design problems during this transition can expedite the development and incorporation of fixes into the production process for remaining units.

1.5.4 Step 4: Monitor Field Performance

Ensure that the needed levels of RAM are sustained during the life of the system, since O&S costs are typically more than half of the TOC. Reliability and maintainability drive the elements of support and the costs of support through the life cycle. The elements of support generally include maintenance at all levels; manpower and personnel to operate and support the system; supply support; support equipment and tools; technical data; training and training support; computer resource support; facilities; and packaging, handling, storage and transportation. Three performance measurements provide overall indications of field experience: mission success rates, operational availability, and operations and support costs. However, in themselves, they do not necessarily indicate the specific cause of problems. A robust data collection and analysis program, such as a continuation of the RAM review boards and DCACAS from earlier steps, will help identify and prioritize specific RAM problems for resolution.

1.5.4.1 RAM Capabilities Mature Over the Operational Life

There are several effective techniques for projecting (and sustaining) the reliability, durability, and maintainability of systems. The "lead-the-fleet" concept often is used for aircraft and ground vehicles. A few systems are used at a much higher usage rate than the fleet average and closely monitored to anticipate and correct the kinds of failures that may develop as the fleet ages. Other forms of accelerated testing of early articles can identify and correct failure modes early in the life cycle. End to end value chain modeling is an effective method of understanding the relationship of key system parameters and performing sensitivity analysis and trade studies. A reliability-centered maintenance approach provides opportunities to sustain and maximize effectiveness of preventive maintenance.

1.5.4.2 Sustaining RAM and Trending

To support and sustain RAM capabilities, the collection, analysis, and maintenance of data continues into the operational environment with sufficient detail and visibility to identify RAM

performance problems as they begin to emerge. To achieve this, it is important that experiences development engineers and member of the RAM team, who were assigned to development and demonstration of the product, be tasked to continue into the operational phase. Often, normal service data collection systems are inadequate to provide the needed RAM detail; and special or augmented data collection programs are developed and fielded along with the system. These data collection efforts take full advantage of embedded instrumentation, diagnostics, and unique identification (UID) of items.

1.6 Senior Management's Role

The Defense Acquisition Executive has the responsibility for supervising the Defense Acquisition System. The Milestone Decision Authority is the designated individual with overall responsibility for a program including advancement to the next phase. The Program Manager is the designated individual with responsibility for development, production, and sustainment to meet the user's operational needs. These senior managers assure that programs achieve the needed levels of RAM by ensuring that:

- Realistic user needs are identified,
- User needs are properly translated and incentives are placed in contracts,
- Adequate contractual and organic resources are identified and allocated,
- Sufficient funding and schedule are allocated to achieve RAM objectives,
- Contractual requirements are satisfied, and
- User needs are demonstrated in OT&E and sustained during operations.

Execution of an acquisition program is the responsibility of the Program Manager. However, senior management plays an essential role in providing guidance and support to ensure that long-term goals are not compromised because of the short-term pressures of schedule and cost. By encouraging careful attention to RAM from the beginning, management can reduce the risks of failing to "satisfy user needs with measurable improvements to mission capability and operational support in a timely manner, and at a fair and reasonable price."

Table 1-1 provides questions pertaining to RAM to help senior managers influence the achievement of the RAM capabilities the user needs. The questions are based on the four key steps to achieve RAM previously illustrated in Figure 1-3. The purpose of the questions associated with each step is defined in the following statements.

1. Determine if the user needs and constraints are well understood.
2. Determine if the program will design and redesign effectively for RAM.
3. Determine if manufacturing will yield systems with desired levels of RAM.
4. Determine if field data will help sustain and improve the capabilities of the system.

TABLE 1-1: RAM Questions and Desired Responses for Senior-Level Reviews

Step	Question	Character of Response
1	**Is there an appropriate, relevant, well-justified RAM Rationale?** (What is the rationale for the user's RAM expectations?)	Demonstrate an understanding of the RAM aspects of the mission/desired capability and way in which the operational test agency and user measure it.
	Will the planned RAM for this system provide a measurable improvement in mission capability and operations support? (Identify the critical failure modes and mechanisms based on previous systems or versions as well as any identified in the current development. Explain how failure modes and mechanisms were identified.)	Demonstrate knowledge of current RAM performance of similar systems. Address specific activities, technologies, and other measures for achieving the higher RAM levels. Based on TOC, technological constraints, or other factors. Address impact on O&S, footprint, and readiness. Show how design is being improved.
	Do RAM design specifications reflect the RAM Rationale and RAM Program Plan? (Identify the RAM design specifications. Identify action(s) being taken or previously taken to reduce risk.)	Understand how RAM design specifications were derived from user needs. Demonstrate that sound engineering is being conducted to address failures. Provide evidence of adequate investigation.
2	**How is RAM addressed in the contract?** (Outline the rewards and penalties structure for the system prior to production and deployment.)	Provide contractor's process and rationale. Highlight design analyses and tests. A RAM demonstration before production and fielding. Are there a RAM Manager, a team, a process and adequate resources? How are the RAM activities being selected? The contract should identify all analytical, test, and data collection activities conducted for or related to RAM, identify the purpose of each, how they will be conducted, and how and when they will be integrated into the overall systems engineering process. The contract should explain how failure modes and degradations and effects would be identified, prioritized, and addressed during design. The government should have a role in this. The contract should describe the testing planned at each level of design, how data will be used for RAM purposes (e.g., assessment, improvement, characterization), and the associated analytical tools and methods. The contract should provide the government management, test, and technical data rights (e.g. ICD) to support system understanding and RAM data analysis and archival through the system life cycle.
	What does the RAM Program Plan contain? (Identify problems experienced in demonstration /acceptance testing as well as whether or not problems were anticipated and how they are being corrected.)	There is a reliability program that has resources and capability to achieve satisfactory reliability. The RAM Program Plan contains provisions to eliminate false BIT indications. Explain nature and implications of problems found. Explain how previous analyses and tests are being re-examined and updated. Provide the "get-well" plan. Plan for sufficient testing to demonstrate achievement of RAM requirements.
	Are there adequate funds to perform RAM activities? What are the projected TOC savings associated with the RAM Program?	The program budget has funds identified to accomplish the RAM activities, such as maturing reliability and incorporating BIT fixes. The program has done the TOC analysis that justifies a robust RAM program in development as well as sustainment.

TABLE 1-1 (Continued): RAM Questions and Desired Responses for Senior-Level Reviews

Step	Question	Character of Response
2 Cont'd	**Is the timing of these activities such that the results can influence the design process?**	The detailed program schedule shows that the results of the RAM activities will be available in sufficient time to be considered as part of the design trade studies and reviewed at the preliminary and critical design reviews (PDR and CDR). This should be clearly visible in the Integrated Program Schedule.
	Is the RAM testing documented in the Test and Evaluation Master Plan?	Identify contents of TEMP pertaining to RAM testing. Describe use of demonstration testing or accelerated life testing to satisfy RAM requirements.
	Is there meaningful contract oversight of the RAM program?	The levels of RAM achieved in design are demonstrated and assessed at each engineering and programmatic design review and at milestone reviews. There is a systematic process in use for identifying, tracking, determining the cause, and implementing corrective actions to eliminate or mitigate failures and failure modes. The PM is using trained RAM engineers, on staff or matrixed, to provide leadership for an effective RAM program.
	If COTS is being used, what is the RAM level in commercial applications? (Determine anticipated change in RAM using the COTS in a military application. If the anticipated change is negative, identify what responsive actions are planned.)	Demonstrate that RAM was a criterion for selection. Understand the effects of a new application/environment. If COTS is to be modified, what will be the implications for warranty and support? Identify changes to the maintenance and support concepts if COTS is used. Determine whether the costs of required changes to the support system are reasonable and affordable.
	If software is being implemented within system, how is its reliability being assessed? What processes will be implemented to sustain operational capability?	The software development team: (1) has Software Engineering Institute certification or equivalent, (2) utilizes proven development processes and metrics, and (3) has software integration facilities. Software anomalies are identified throughout the development and demonstration. There is a close, effective interaction of the RAM and software teams and their activities.
3	**Are the subcontractors stable?** (Identify possibilities for parts obsolescence and/or diminishing manufacturing sources.)	Explain how vendors/subcontractors were chosen. Identify how vendors/subcontractors are continually evaluated to determine stability of items they supply. Describe process used to evaluate alternative parts and/or materials.
	What is the quality assurance program?	Identify all process controls and production reliability acceptance tests implemented as part of quality assurance program.
	What are the contract incentives to ensure RAM?	For example, outline the use of an initial period of Contractor Logistics Support on a firm fixed price contract or RAM demonstration requirements linked to contract incentives.
	Has IOT&E performance demonstrated achievement of satisfactory levels of RAM?	There is enough data, from IOT&E and all other relevant demonstrations to indicate that satisfactory mission reliability and RAM will be achieved in the field. Deficiencies have been identified and corrective actions are funded and scheduled.
4	**What provisions will ensure system RAM matures early and the system is durable throughout the operational life?**	There is a "lead-the-fleet" program and accelerated testing of early articles to identify and correct failure modes early as the system enters operation phase and continuing as the fleet ages.
	Is there a formal RAM data collection and review process, after the system is fielded? How will the RAM Team be resourced when the system is fielded?	Data capture, analysis, and archival planning include collection of Unique Identification (UID) for repairable items and exploits failure, environmental, and usage information through embedded instrumentation. The government has rights to the data. Program Manager has the responsibility to plan for and resource RAM in the sustainment phase of the life cycle.

Chapter 2 Achieving RAM in Military Systems

2.1 Introduction

Chapter 1 addressed RAM from the perspective of top-level managers: the Milestone Decision Authorities and Program Managers. This chapter provides an overview of the four key steps for achieving RAM. It is intended for a broader audience including system users who develop capability documents, development and acquisition staffs, the testing community, and contractors. The chapter focuses on the management and the technical processes for achieving satisfactory levels of RAM. Chapters three through six will address each of the four key steps in greater detail.

As stated earlier, the process of achieving satisfactory RAM depends on four key steps, which are illustrated in Figure 2-1 and discussed in the subsequent paragraphs.

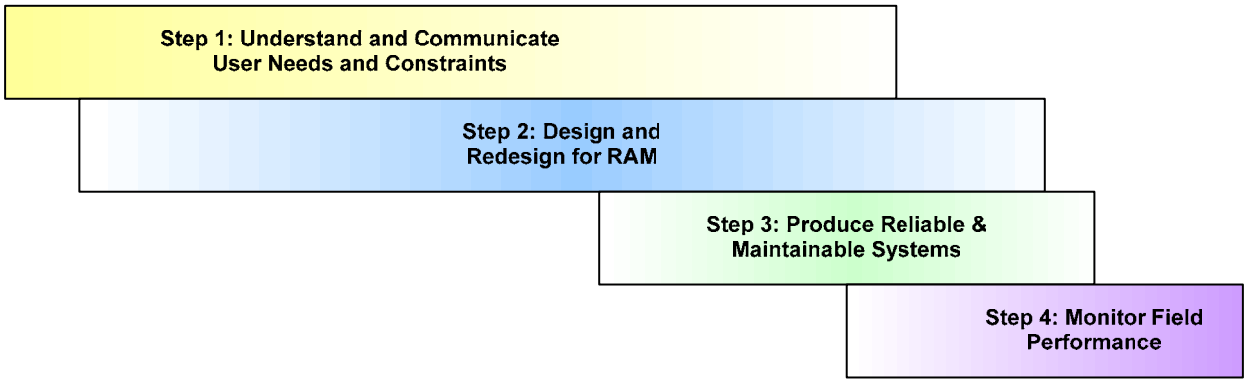


FIGURE 2-1: Key Steps to Developing Reliable, Available, and Maintainable Systems

- 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. Step 1 is outlined briefly in Section 2.2 and is the focus for Chapter 3 of this guide.
- 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. All the while the RAM requirements are balanced against the effectiveness of the other performance requirements associated with the system. Section 2.3 of this chapter provides a simple explanation of the activities encountered during Step 2, whereas Chapter 4 provides more breadth and depth on this topic.
- After the needs and constraints of the user are "built-in" the system through design and redesign, the system must now be manufactured in such a manner that designed reliability and maintainability remain intact throughout production. Step 3 ensures that a reliable and maintainable system is produced, which contributes to improved system availability. This will be discussed further in Section 2.4 and Chapter 5.
- Historically the development of many systems has accounted rather well for the first three steps required to achieve RAM requirements, but may have often overlooked (with

adverse results) the final step of the process, which is monitoring field experience. The cost to operate and support systems has increased over time throughout the DoD, therefore Step 4 should not be forgotten because, without monitoring field performance, the strong RAM foundation developed during the first three steps may degrade. Captured field experience allows for better-maintained systems, identifies necessary improvements to the system, and provides much needed "lessons learned" to future systems. A brief overview of Step 4 is given in Section 2.5 with a comprehensive synopsis in Chapter 6.

Each step comprises five components 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 steps are consistent with robust system engineering practices, and are compatible with any general acquisition process. The guide will focus on how they apply to the Department of Defense acquisition framework.

The four key steps identified in Table 2-1 focus on addressing the many reasons why system RAM degrades over time. Since system RAM is often difficult to accurately assess until the system is deployed or fielded many of these factors that result in degraded system RAM do not appear until this final step, which places a great importance on Step 4: Monitor Field Experience. Although most system RAM degradation is not observed until Step 4, the previous 3 steps are often as much, if not more, to blame for the observed degradation in the field (i.e., a change in operating concept or environment is observed when the system is fielded, but there may have been signs in Step 1: Understand and Document User Needs and Constraints that should have been addressed to prepare for this possibility). Table 2-2 describes some of the reasons why system RAM degrades.

TABLE 2-2: Some Reasons Why System RAM Degrades Over Time

Reason	Discussion
Change in operating concept	If system is used in a manner different from that originally allowed for in the design, new failure modes can occur, and the overall frequency of failures can increase. In such cases, corrective actions can be expensive or impractical. If the new operating concept is essential, decreased RAM levels may have to be accepted.
Change in operating environment	If a system is used in an environment different from that originally allowed for in the design, new failure modes can occur, and the overall frequency of failures can increase. In such cases, corrective actions can be expensive or impractical. If the system must operate in the new environment, decreased RAM levels may have to be accepted.
Inadequate training	Inadequate operating or maintenance training usually increases the number of failures induced by improper operation or maintenance. The corrective action is to improve the training.
Wearout / Inadequate Reliability Centered Maintenance Program	As systems age, the number of failures per unit time for parts having wearout characteristics will increase. A preventive maintenance program to replace or overhaul such parts will prevent wearout from becoming a problem. Ideally the preventive maintenance program is based on the reliability characteristics of the parts (i.e., a reliability-centered maintenance program based on the field data within the DCACAS).
Inadequacies of design analysis and test	All engineering models, analytical tools, and test methods are imperfect. It is also impossible to perfectly model or simulate the actual operational environment during design and test. Finally, the time and funds available for analysis and testing are limited. For all of these reasons, failure mechanisms may go undetected until after the system is fielded.
Lack of understanding the role of software in RAM performance.	Most modern weapons systems are digital in design. The mission success, availability, and supportability are largely governed by software. Previously, classical RAM levels were component failure intensive. Currently, software plays a more important role. Personnel managing, developing, and producing these new systems need to understand that software intensive systems require a different approach to failure detection, isolation and ultimate repair or corrective action.
Change in supplier	If a supplier chooses to stop manufacturing a part or material, goes out of business, or no longer maintains the necessary levels of quality, an alternate source of supply is needed. If RAM is not a major consideration in selecting the new supplier, system reliability may degrade. If there are a limited number of new suppliers to select from, lower RAM levels may have to be accepted.
Poor configuration control	Over a system's life, there is the temptation to reduce costs by substituting lower-priced parts and materials for those originally specified by the designer. Although the purchase price may be lower, life cycle costs will increase, and the mission will suffer if the "suitable subs" do not have the necessary RAM characteristics. Strong configuration management and a change control process that addresses all factors, including RAM performance, are essential throughout the life of the system.
Manufacturing problems	Although the manufacturing processes may have been qualified and statistical processes implemented at the start of production, changes can occur during the production line that degrade RAM. This possibility increases as the length of the production run increases; therefore, constant quality control is essential.
Inadequate funding	Inadequate support funding can affect many factors, including availability of repair parts, support equipment, and maintainer training, which can have a profound effect on RAM.

DoD Directive Number 5000.1 issued on May 12, 2003 states, "Acquisition programs shall be managed through the application of a systems engineering approach that optimizes total system performance and minimizes total ownership costs." The *Defense Acquisition Guidebook*, released in October 2004, provides even more depth to this issue of using a systems engineering approach. It states:

"The Program Manager should implement a robust systems engineering approach to translate operational needs and capabilities into operationally suitable increments of a system. Systems engineering permeates design, production, test and evaluation, and system support. Systems engineering principles should influence the balance among the performance, cost, and schedule parameters and associated risks of the system. Program Managers exercise leadership, decision-making, and oversight throughout the system life cycle. Implementing a systems engineering approach adds discipline to the process and provides the Program Manager with the information necessary to make valid trade-off decisions throughout the program's life cycle."

"Systems engineering is typically implemented through multi-disciplined teams of subject matter experts (often formally chartered as an Integrated Product Team (IPT)). The systems engineering working-level IPT translates user-defined capabilities into operational system specifications consistent with cost, schedule, and performance constraints. While the program office usually has a Chief Engineer or Lead Systems Engineer in charge of implementing the system engineering process, personnel from non-systems engineering organizations or from outside the program management structure may also perform activities related to systems engineering. Most program personnel should see themselves as participants in the systems engineering processes."

"Early and effective employment of systems engineering, applied in accordance with a well-structured Systems Engineering Plan, and monitored with meaningful systems engineering technical reviews, will reduce program risk and identify potential management issues in a timely manner."

Therefore, DoD is adopting a systems engineering approach to acquisition to ensure that the Program Management Office pursues RAM as it has been proven to be crucial to reducing the total ownership cost of a system and improving operational readiness, but at the same time the pursuit of RAM can not be achieved at the expense of other programmatic or technical considerations.

Improved RAM will drive down support costs, since a reliable system will require fewer repairs and fewer spare parts; thus reliability improves and support costs decrease. A maintainable system translates into the ability to make repairs quickly, lowering the delay times and the total number of systems that DoD must own to accomplish a goal; therefore with fewer systems required and quicker repair times, support costs decrease. An available system provides increased mission capability; as downtime decreases so do support costs.

While improved RAM lowers support costs, it is often more expensive to acquire a system with improved RAM. Therefore, achieving the desired system RAM is often a tradeoff with the

product acquisition price. Although RAM and product acquisition price must be balanced it is important to note that good RAM saves money in the out-years of the system's life cycle.

Total ownership cost (TOC) and life cycle cost are nearly interchangeable terms used to define the sum of all financial resources necessary to organize, equip, and sustain military forces sufficient to meet national goals in compliance with all laws, all policies applicable to DoD, all standards in effect for readiness, safety, and quality of life, and all other official measures of performance for DoD and its components. TOC is comprised of the costs to research, develop, acquire, own, operate, and dispose of defense systems, other equipment and real property, the costs to recruit, retain, separate, and otherwise support military and civilian personnel, and all other costs of business operations in the DoD.

Figure 2-2 illustrates the typical total ownership cost or life cycle cost associated with a system's life cycle. Notice that acquisition costs are only a fraction of the total ownership cost for the system. This "tip of the iceberg" effect is not the exception, but instead is the rule for system acquisition programs.

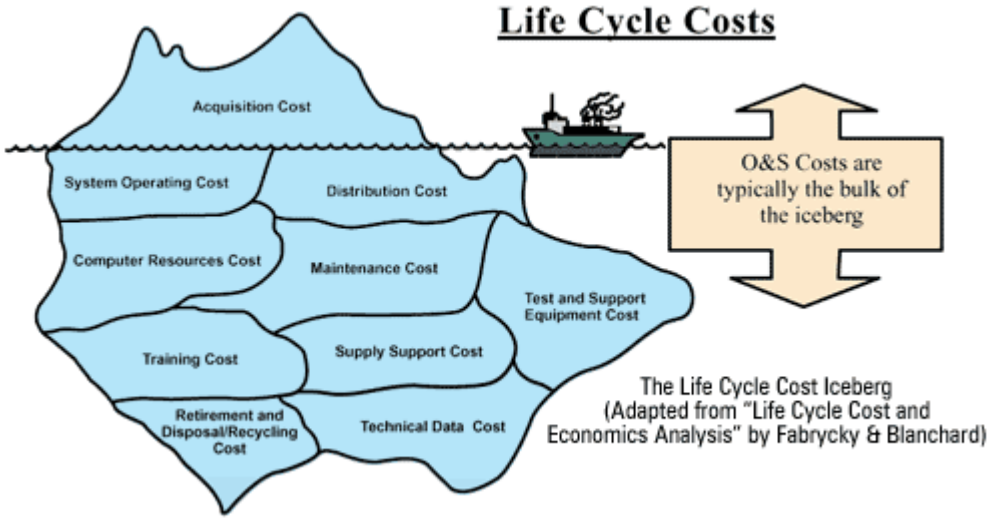


FIGURE 2-2: Life Cycle Cost Iceberg

Figure 2-2 identifies the following costs associated with the life cycle cost iceberg:

- System Operation Cost: Base cost to operate the system including paying the users, fuel for the system, and so on.
- Distribution Cost: Cost to ship the product to its destination.
- Computer Resource Cost: Often when deploying a new system, personnel will be deployed with the system and the personnel will need new computers. New complex systems will require extensive computing capability to accommodate on-board recorded data for various disciplines. Therefore no matter how simple the new system may be there will be some computing time added to the O&S costs.
- Maintenance Cost: Costs to conduct routine maintenance, at whatever level, including compatibility using Automated Maintenance Environment (AME) tools and resources.

- Test and Support Equipment Cost: Costs associated with developing and acquiring diagnostic equipment and tools required for the new system.
- Training Cost: All systems require some level of costs to train users and maintainers on how to use and maintain the new system.
- Supply Support Cost: Costs associated with shipping spare parts, returning faulty parts to the depot for repair, etc.
- Retirement and Disposal/Recycling Cost: Eventually the new system will reach the end of its useful life and must be appropriately discarded to comply with Federal regulations and to ensure public safety.
- Technical Data Cost: Developing a library of technical data is vital for any complex system and there will be costs associated with collecting, maintaining, and analyzing this technical data.
- In-Service Engineering and Logistics Cost: The cost associated with the management and execution of the above life cycle requirements.

Section 2.6 addresses the integration of the four key steps for achieving RAM through a systems engineering approach within the current DoD acquisition management processes.

2.2 Step 1: Understand and Document User Needs and Constraints

The first priority in an acquisition program is to thoroughly understand what the customer needs and expects (the customer includes those whom will operate, maintain, and support the capability being acquired). The user needs should include the wartime and peacetime usage rates, the use environments, the non-operating duration and conditions, the operational constraints of the maintenance and supply system, and the logistics footprint. In cases of an equipment or capability replacement situation, it should identify limitations of the current capability or system and its support concept, define the current RAM burden[13], propose or document desired changes, identify design constraints (from manpower, training, etc.), and define expected system stress (environmental, usage, etc.). Potential threats to the capability should be addressed during this phase of the acquisition life cycle also.

The role that the customer (i.e., individual or organization that commissions the engineering of a system or the prospective buyer of system/capability) plays in acquisition is in defining the operation, maintenance and support concepts; developing the doctrine, training, personnel and leadership elements of the capability; and providing data from fielded systems performing missions similar to those planned for the new capability. The more completely a developer understands the user needs and constraints, the more likely the end result will satisfy the user. It has been said that it is much more difficult to hit a moving target; therefore, the more the developer understands the user needs and constraints, the better the final design should be.

Systems engineering is the process that controls the technical system development effort with the goal of achieving an optimum balance of all system elements. The process transforms a

[13] The purpose of acquisition is for the new capability to improve upon the current capability. Therefore, the RAM burden can be defined as the penalty that a system pays in terms of operation and support costs, in maintenance manpower, in downtime, or in the supply chain due to the unreliability, unavailability, or unmaintainability of the existing capability versus what acquiring a new capability could provide.

customer's needs into clearly defined system parameters and allocates and integrates those parameters to the various development disciplines needed to realize the system products and processes. Systems engineering attempts to optimize effectiveness and affordability as the system/capability is developed. The systems engineering process fulfills two fundamental purposes:

1. Makes sure that the question (What are the user needs and constraints?) is answered before designing the answer.
2. Coordinates, focuses, and balances the technical efforts of all involved throughout the acquisition process.

2.2.1 Mission and Goals for Step 1

The mission of Step 1: Understand and Document User Needs and Constraints, is to develop an understanding of the needs for the given system capability so that the acquisition process can fulfill those needs. By the end of this step the following goals should be addressed.

- The levels of RAM that the user requires are defined, quantified, documented, and assessed as achievable.
- The rationale for RAM requirements is explained to guide trade-off studies and evaluations.
- The top-level program plan for achieving RAM is developed in a manner that ensures that RAM requirements are achievable.

Through understanding user needs and constraints, the required RAM for the new capability begins to be defined. A series of analyses are conducted early in this step to establish the case for a materiel approach to resolve a gap in capability. The primary focus of Defense acquisition is to acquire quality products that balance the process of satisfying user needs (while improving mission capability and operational support) as well as adhering to scheduling constraints and justifiable acquisition costs[14]. The current mission capability and operational support are the baseline against which the new system will be measured, so those performance factors need to be defined and documented. During capability analysis[15], time and resources need to be set aside to measure and characterize current operational experience, organize and record RAM data as well as supply chain performance data, interpret the data, and draw conclusions about the causes of shortfalls. It is also imperative to understand and document software design complexity and influence on RAM.

[14] DoD Directive Number 5000.1 states, "The primary objective of Defense 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."

[15] Capability analysis and development was previously called the requirements process. Currently in the DoD, the Joint Capabilities Integration and Development System (JCIDS) is the activity that defines new capabilities. The primary focus of JCIDS is to ensure that the joint force is properly equipped and supported to perform across the range of military operations. The capabilities-based approach leverages the expertise of all government agencies, industry and academia to identify improvements to existing capabilities and to develop new warfighting capabilities. The JCIDS process defines needed capabilities through an analysis of doctrine, organization, training, materiel, leadership, personnel and facilities (DOTMLPF). Needed levels of RAM are defined within this framework, principally in the category of materiel.

Thus the goal of this first step is to inform and share information among those who will have to design, buy, use, and support the system. The information they need to share includes the users' needs, how the system will be used or potentially misused, the environment of use and support, the constraints on what support is available for the system, what information will be available to decision makers, and how that information will be verified.

2.2.2 Organizations and People for Step 1

Many different organizations and a multitude of personnel must collaborate effectively to define and then to achieve the needed capability. The partnership starts in Step 1 and continues throughout the life cycle of the capability. For DoD capabilities, joint and service users, technology developers, acquisition program offices, systems engineering IPT, supporters, testers, and senior leaders work together to develop the capability and apply the four steps to yield the required levels of RAM. Government offices form partnerships with industry contractors to achieve this goal. The heaviest use of contractors is during the activities of steps two and three (i.e., design/redesign and produce). Contractors can also perform important functions in Step 1 (i.e., by developing technologies with high RAM, and providing expert judgment on RAM requirements and realism) as well as in Step 4 (i.e., by supporting and continuing the improvement of RAM levels during the operating phase of the life cycle).

The individual responsible for RAM should have the necessary authority to fully participate in the system acquisition process and obtain the resources for achieving satisfactory levels of RAM.

2.2.3 Supporting Information for Step 1

A vast majority of the required information to support the completion of Step 1 is taken from existing information pertaining to the system that the capability being acquired will improve upon. This information includes field experience, current logistics and manpower requirements, current user "wish lists," and technical improvements needed for the current system. However, if the replacement system incorporates more complex technology (software for example) than the system being replaced, any analysis will take those differences into account.

Characterizing the total life cycle environment is essential during Step 1. Characterization is the process of identifying relevant parameters (i.e., temperature, humidity, vibration, etc.) of the expected environments for the capability and the realistic changes of values and durations for these parameters. The total life cycle environment characteristics include:

- Storage
- Shipping and handling
- Installation/Deployment
- Operation
- Maintenance

2.2.4 Tools and Activities for Step 1

The tools needed to satisfactorily complete this step include: User Panels, Expert Judgment Panels, and Preliminary RAM models. The activities may include: (1) developing a concept system, (2) constructing a model of the system, (3) using the model and expert judgment to make preliminary RAM estimates, (4) developing the RAM Rationale, (5) planning the RAM program, and (6) beginning the RAM Case. All are addressed in more detail in later chapters. These last three activities are closely related as identified in the bullets below. Although the RAM Rationale, RAM Program Plan, and RAM Case can all be important tools when completing Step 1: Understand and Document User Needs and Constraints, their utilization may vary from acquisition to acquisition. Almost always there will be a need for a RAM Program Plan and often there is a strong desire to develop the RAM Rationale, but the benefit of the RAM Case may often be overlooked.

- The RAM Rationale defines the needed RAM characteristics, mission profile and use environment. The RAM Rationale identifies the RAM requirements, and their analytical basis, to be documented in the government's RFP.
- The RAM Program Plan lays out the strategies, processes, resources, and organization to achieve the RAM requirements. The RAM Program Plan manages the activities required to achieve a reliable, available, and maintainable system.
- The RAM Case provides the record of how well requirements have been demonstrated at each stage of the program. The RAM Case provides the evidence that the contractor achieved RAM requirements. Therefore, without the RAM Case and the presentation of the contractor's evidence, some level of uncertainty is possible in terms of the contractor's ability to satisfy the RAM requirements as defined by the DoD personnel (i.e., within RFP, contractual documents, etc.).

The systems engineering approach to the acquisition process recommends technical reviews to confirm outputs of the acquisition phases and major technical efforts within the technical phases. During Step 1: Understand and Document User Needs and Constraints the following technical reviews should be conducted.

- Initial Technical Review (ITR): Multi-disciplined technical review to support a program's initial Program Objective Memorandum submission. This review ensures that a program's technical baseline is sufficiently rigorous to support a valid cost estimate (with acceptable cost risk), and enable an independent assessment of that estimate by cost, technical, and program management subject matter experts. If COTS equipment or a Non-Developmental Item (NDI) is being considered, pertinent data must be obtained to assess feasibility of using the system. The ITR assesses the preliminary RAM estimates, RAM Rationale, and RAM Program Plan.
- Alternative System Review (ASR): Multi-disciplined technical review that ensures that the system's requirements agree with the customers' needs and expectations and that the system under review (including COTS/NDI) can proceed into the Technology Development phase of the acquisition process. The ASR verifies the feasibility of RAM

requirements with the aid of comprehensive risk assessments[16] as well as trade studies/technical demonstrations.

- System Requirements Review (SRR): Multi-functional technical review that ensures all system and performance requirements derived from the Capability Development Document are defined and consistent with cost, schedule, risk, and other system constraints. The review determines the direction and progress of the systems engineering effort and the degree of convergence upon a balanced and complete configuration. The SRR provides the preliminary allocation of system requirements (RAM) to hardware, human, and software subsystems. It also verifies that test methods and acceptance criteria, based on use of agreed-to verification methods, are incorporated into schedules, facilities requirements, manpower needs, and other programmatic imperatives.
- Integrated Baseline Review (IBR): The IBR should be conducted throughout the acquisition process when Earned Value Management is required as the focus of the IBR is financial, but should include important technical considerations as well. The IBR identifies project milestones and resources as well as ensuring objective and rationale system measurements (RAM) are identified.

2.2.4.1 Develop a Conceptual RAM Model of the System

Based on the needs defined by the user and mission analysis, the system developer creates a conceptual model of the system. The first iteration of the conceptual model identifies the major subsystems, and probable manufacturing processes, and makes an estimate of the potential system performance. The conceptual model evolves as information is gained during the development process and serves as the framework for analyzing, allocating, and achieving RAM requirements.

The portion of the conceptual model for analyzing, allocating and achieving RAM often takes the form of a logic model, such as a reliability block diagram. Computer-based logic models facilitate the computation of the expected system-level RAM metrics, trade-offs among competing designs on the basis of their RAM metrics, and the identification of weaknesses in the various designs.

Reliability modeling[17] has numerous benefits in addition to reliability allocation among subsystems. It is useful in all phases of the life cycle. Using reliability modeling can:

- Improve understanding of the equipment,
- Allow an early evaluation of design alternatives,
- Identify critical subsystems, components, and parts as well as their interactions, and
- Guide resource allocations to portions of the equipment most needing improvement.

Before finalizing a formal definition of user needs for acquisition (for example in a Capability Development Document), an analysis of RAM technical feasibility is needed. This provides a high level review of the RAM risks associated with the program and identifies areas of concern

[16] Various checklists can assist in risk identification. Naval Air Systems Command uses their Systems Engineering Technical Review Checklist which identifies risk by program phase.
[17] More information on reliability modeling and the reliability block diagram is in Chapter 4, Section 4.5.2.5.

that require greater developmental resources, technical investigation or closer management attention. This is particularly important if the proposal includes integration of COTS/NDI equipment. If the risk level is high, alternative courses of action (technological development, alternative requirements or different strategies) should be formulated, which can proceed in parallel.

2.2.4.2 Elicit Expert Judgment

While much data and knowledge about subsystems can be found in the reliability literature, the information and wisdom necessary to put it all together in a system that works will come from people who have worked similar problems before. Though it may be premature to predict system level RAM this early, consulting experts (the more independent the better) can reveal risk areas, failure modes, and risk reduction activities for design consideration. Statisticians and researchers have developed formal techniques to elicit expert judgment, structure questions to learn what is known and unknown about components, failure modes, and reliability of similar components, subsystems and systems. They have also developed techniques to calculate reliability by combining different types of data from these sources. It is also important to examine lessons learned from other programs using similar technology or design approaches. All these sources can help the conceptual design process and provide a foundation for engineering design. For example, high-risk components should be identified for design improvement, parallel development or special testing, and qualification activities

2.2.4.3 Calculate Initial Reliability

Using the system model and information about reliability, availability, and maintainability of the system elements from expert judgment panels or other sources, calculate an initial estimate of system reliability. Identify potential and likely failure modes and causes, and then plan how to implement design, assessment, and test activities to avoid, remove, or mitigate the unacceptable risk failure modes and causes.

2.2.4.4 Develop the RAM Rationale

A RAM Rationale documents the results of analyses conducted during Step 1. This information becomes the basis for developing RAM related portions of the request for proposal and contract(s) to design, develop, test, produce, deploy and operate the capability. The RAM Rationale also supports: trade-off studies to balance cost and performance; development test planning and evaluation; and operational test and evaluation. The core elements of the RAM Rationale are:

- Quantitative measures of the levels of reliability, availability and maintainability needed by the user, in operational terms, as well as corresponding quantitative measures in contractual terms for use in the RFP and contract.
- An operational mode summary and mission profile, which quantifies how and in what environments the capability will be used throughout the life cycle.

- The hardware and software failure definitions and scoring criteria for assessing mission failures and logistics failures during modeling, simulation, test and other activities used for estimating, verifying, or predicting levels of RAM.

The RAM Rationale also:

- Explains why the RAM levels are needed and how they interact and relate to other aspects of the capability (such as performance, force structure, affordability, support concept/plan, logistics footprint); and
- Documents RAM performance of current capability to provide the basis for assessing measurable improvements to mission capability and operational support.

The RAM Rationale flows into the Joint Capabilities Integration and Development System (JCIDS) process to define RAM-related aspects of the needed capability. JCIDS documentation provides a formal communication of capability needs between the joint operator and the acquisition, test and evaluation, and resource management communities. The first product of the JCIDS process is the Initial Capabilities Document (ICD). The Analysis of Alternatives (AoA) is an evaluation of the operational effectiveness, operational suitability and estimated costs of alternative systems to meet a mission capability. The focus of the AoA is to refine the selected concept documented in the approved ICD.

2.2.4.5 Develop the RAM Program Plan

The RAM Program Plan[18] (RAMPP) provides a comprehensive compendium of the RAM activities, functions, processes, test strategies, measurement, data collection, resources and timelines required to ensure system RAM maturation. The RAMPP supports demonstration of both contractual and operational requirements. The plan provides visibility into the management and organizational structure of those responsible (both contractor and government) for the conduct of RAM activities. Additionally, the plan provides information on proven design techniques to be used in the program; test strategies (for surfacing failure modes and for requirement demonstration); a description of the activities and processes to ensure retention of requisite RAM levels in production; and future plans for monitoring RAM in the field and the mechanisms for incorporating needed corrective actions (design and/or manufacturing) in the field. Resources to execute the program are well defined and a schedule developed for the conduct of RAM activities within required program acquisition timelines. A RAMPP should be developed both by the contractor, delineating those activities supporting the attainment of the system specification, and the government program office which provides an expansion of contract activities to include government developmental and operational test activities supporting and confirming attainment of operational requirements. The plan is tailored to each system. For those systems that are totally Non-Developmental Item (NDI) acquisitions, the RAMPP focuses on contractor verification of RAM claims and manufacturing processes in place (given item is not yet in production), which will ensure item retains its inherent RAM design characteristics

[18] Based on "Reliability Program Plan (RPP) Guidelines," Submitted as requirements for DA RAM Panel, Stephen P. Yuhas, Chair, Validation Subgroup, March 28, 2001.

during production and operations. The contractor provides evidence, based on verification test data, that the system meets RAM contract requirements and the RAM Rationale.

2.2.4.6 Translate Operational RAM Metrics into Contractual Terms

It is imperative that the operational RAM metrics associated with the system are translated into contractual terms that become system RAM requirements within the RFP and contract. For acquisition of an overall weapons system, an overall RAM requirement including Integrated Diagnostics should be imposed in the contract and demonstrated. A lesson learned from previous system procurements is that the prime contractor is reluctant to expend valuable resources late in development, to refine integrated system anomalies, unless there is an overall requirement to be met. Individual system BIT performance is often directed to primary computers or controllers, which may be acceptable from a vendor or developer's standpoint, but to a user's standpoint, the overall integrated system output is what is seen and used to effect repair. This is particularly true for multi-component integrated systems such as fuel, propulsion and environmental control on complex airborne weapons systems. RAM metrics take many forms, e.g., mean time between failure (MTBF). MTBF is commonly used, but it is frequently not the best choice. For one-shot devices, a probability of mission success is more appropriate. See Section 3.2 for more information on RAM metrics. Whatever metrics are used, operational requirements can be converted into contractual requirements by several methods, including:

- Apply a Formal Translator: Formal translators are the equation used to convert operational jargon into contractual jargon and vice versa. The Reliability Analysis Center developed many translators for the DoD, which are included in its **Reliability Toolkit: Commercial Practices Edition**. Another translator used in Naval Aviation is the **NAVAIR (4.9.4) Audit Trail**[19], which considers many of the variables used to convert operational metrics to contractual requirements.
- Apply Systems Engineering Approach: A systems engineering approach can be applied to determine how much mean time between failure (MTBF) is necessary to protect the user's required mean time between maintenance (MTBM) for reliability. This determination is somewhat based on the definition of "time" and "failure" as stated in the contract specification. A MTBF value should be determined that can be placed in the specification that will protect the user's interest.
- Apply Cost, Schedule, and Other Constraints: This method translates the operational requirements into contractual requirements based on a specified budget or a specified period of time. (i.e., Given a specified budget, how much MTBF can we afford to buy? Given a specified period of time, how much MTBF would the contractor be able to incorporate into the design?)
- Ask the Contractor "What is the best that can be done?" Translating requirements from operational to contractual based on what the contractor can provide will often not relate well to what is specified in terms of the user's needs and constraints.

[19]The NAVAIR (4.9.4) Audit Trail is a model that can be tailored to various equipment/platform applications and uses internal application programs that provide factors proven through lessons learned from other programs. The output provides realistic and achievable quantitative Operational, TEMP and Equipment Specification requirement recommendations.

- Apply a Policy: If a DoD or Service RAM translation policy is in existence when RAM contractual requirements are being formulated, that policy needs to be considered as part of the translation effort. That is not to say the policy should be applied blindly without the application of sound engineering judgment. Like any other policy statement, its applicability and effectiveness must be judged in the context of the program to which the policy is being applied, otherwise, it could drive up costs unnecessarily, and/or may be technically unachievable.

2.2.4.7 Begin to Build the RAM Case

The RAM Case is a reasoned, auditable record to document how well a defined system supports the RAM requirements. It provides progressive assurance that RAM requirements are being developed, implemented, verified, enforced and that the requirements can be achieved. The case evolves between the customer and supplier as the project evolves. Initially the customer is the government acquisition organization; eventually, it is subsequently the user. Reliability analyses are not an after-the-fact documentation of what resulted during the design process, but an active integral part of the design process. Immediate action should be taken if unacceptable analysis results are found. See Chapter 3 for more information on the RAM Case.

2.2.5 Outputs and Documentation for Step 1

Outputs from Step 1 document the user needs and inform the subsequent activities.

- Documentation of the model provides the baseline for subsequent assessments.
- Initial RAM projections provide the basis for technology development, fault mitigation, and risk reduction activities in pre-systems acquisition.
- The RAM Rationale describes the level of reliability, availability, and maintainability the user needs in order to achieve TOC, system readiness, and mission performance goals. In DoD acquisition framework, the RAM Rationale is summarized in the Analysis of Alternatives (AoA), and later updated in the Capability Development Document (CDD) and the Capability Production Document (CPD).
- The RAM Program Plan describes the structured series of RAM related activities that will achieve the needed RAM levels.
- The RAM Case is the accumulated evidence, at any point in the program, of demonstrated progress toward achieving the users' RAM needs.

Formal documentation is essential for recording user-needed capabilities, guiding the program, and providing the rationale for the selected levels of RAM. It also makes the analysis readily available for peer review or independent audit.

2.3 Step 2: Design and Resign for RAM

Designing for RAM begins with sound analyses, involves implementing sound design approaches, addresses RAM at successive levels of integration starting at the system and working through the indentures down to the individual components, and includes RAM-related

developmental testing. A good design process will aid in the reduction and elimination of risks to mission success at a point where the costs of such efforts are at their minimum.

Designing for RAM should address not only the system but also: the processes used to manufacture the system, the expected maintenance system, logistics system, and the operational constraints. Manufacturing can introduce flaws, which in turn can lead to failures in the field. The RAM aspects of design and manufacturing should be an integral part of the system engineering process, so that RAM requirements will be addressed concurrently with other performance requirements. As discussed in previous sections, systems engineering activities can be directed to designing and manufacturing reliability and maintainability into the system, but availability is the function of this inherent reliability and maintainability as well as the system's supportability and producibility. It is essential that reliability/maintainability activities be integrated into the overall design effort, thereby avoiding duplicative effort and making the best use of the output and results of analyses and tests. RAM considerations should be a part of all design decisions, trade-offs, and activities from the beginning of the design effort. In this respect, RAM is the same as any other design characteristic.

User constraints are also design constraints. The way in which a user measures the RAM of a system may not be directly meaningful or suitable as an engineering design specification. Although some factors may not be under the developer's control, they should still be accounted for in establishing the design RAM requirements and in the design of the system itself. For example, the developer usually can anticipate that many failures affecting RAM performance could be caused (or prevented) by the design, whereas other failures could be caused during manufacturing, use, or repair. During the design phase it is best to assume all failures are design related. That is if a design can be assembled incorrectly, it will be misassembled. If the design allows the system to be used improperly, it will be so used. If a repair can be done wrong, a part inserted backwards, for example, it will eventually be done wrong. For complex weapons systems, software anomalies may only surface when an unlikely set of circumstances occur simultaneously. In an operational environment, these circumstances are found to occur much more than anticipated and become a liability to overall RAM attributes.

2.3.1 Mission and Goals for Step 2

The mission of Step 2: Design and Redesign for RAM, is to develop the design to satisfy the requirements for the desired capability. The design must satisfy all design specifications and be producible. When the design is produced and deployed it must also meet all user requirements. A systems engineering approach using an interdisciplinary team ensures that required performance characteristics including RAM requirements are achieved. Performance will not be met without a continued focus, which an interdisciplinary team provides as each team member "champions" a design specification to satisfy the user requirements. The design's RAM is achieved no differently as it involves an iterative process that will: (1) eliminate the expected failure modes of the design to maximize reliability, improving RAM, (2) actively pursue a design that can not only be maintained, but maintained efficiently, and (3) acquire availability through the combination of high reliability and high maintainability as well as the availability of adequate logistics support (i.e., maintainer, spares, test equipment, procedures, publications, managements, etc.). Targeted levels of RAM are more likely to be achieved when designers

accurately anticipate and accommodate the operational, environmental and support factors that will be applicable to the fielded system.

Beginning with the design of the system, RAM should be considered explicitly:

- Examine the design and its detail.
- Examine subsystems, assemblies, subassemblies, and components: identify "knowns" and "unknowns" about each indenture level within the system (mitigate risk to success).
- Find, analyze, and mitigate failure modes and failure mechanisms.
- Avoid delaying corrective action in development.
- Account for manufacturing. The design can contribute to minimizing quality control problems that will cause mission failures in the field.
- Evaluate the maintainability and supportability of the system such as the accessibility of components that might need to be replaced, the completeness of the built-in test equipment, the presence of on-board instrumentation, or consider issues of sparing and support
- Develop a (ground) maintenance support system to support maintenance decisions in the User's environment using data recorders to support tasks such as maintenance planning, scheduling, configuration management, operator debrief, and usage data collection such as operating hours or cycles. Some modern designs must be supported in the Automated Maintenance Environment (AME) and must be designed for this support concept.
- Develop a representative prototype of the system, and, where possible, identify composition of subsystems, assemblies, subassemblies, and components.
- Verify that RAM is achieved in representative conditions, using developmental testing or similar activities.

2.3.2 Organizations and People for Step 2

During the design phase of the system acquisition the DoD will assign a relevant Program Manager, Chief Engineer or Lead Systems Engineer and team members, including end users and maintainers, with various responsibilities (including RAM). The contractor will have at least a Project Manager, but may have staff relevant to RAM requirements, such as a Lead Systems Engineer, Logistics Engineering Manager, and a RAM Manager. The development contractor will utilize an interdisciplinary team with RAM being just one part of the team's focus.

The individual responsible for RAM should have the appropriate understanding and authority to incorporate RAM into each phase of acquisition. This person should fully participate in development decisions, design and performance reviews, trade studies and support planning.
This function works best as part of an interdisciplinary team that includes operational, test, and support staff. The reason all these people are necessary is that the selection of specific activities by the RAM Manager and the implementation of those activities requires a solid understanding of design, the system requirements, and the relative value of a given activity in achieving the required levels of RAM. Achieving required RAM is a team effort of contractor and defense personnel working together with a unified and determined aim of producing an effective system.

2.3.3 Supporting Information for Step 2

The outputs of Step 1 (i.e., reliability model documentation, initial RAM predictions, RAM Rationale, RAMPP, and RAM Case) are the basis of the supporting information for Step 2. Each of those outputs becomes inputs during this phase and should be refined during Step 2.

As stated earlier targeted levels of RAM are more likely to be achieved when designers accurately anticipate and accommodate the operational, environmental, and support factors applicable to the fielded system. Designers rely on documentation from previous acquisition phases as well as their preliminary RAM Program Plan (RAMPP), System Engineering Plan (SEP), and Test and Evaluation Master Plan (TEMP). Other documentation that is referenced for the constraints and boundaries which the design must operate and be sustained include:

- Operational concept documentation
- Logistics and maintenance support (concept) documentation
- Life cycle environmental information
- Integrated diagnostic software functional design and operation documentation.

The system's design and support concept should be an iterative process that starts with the initial development of this concept with refinement in the subsequent steps. The system's design should be updated based on the output from the RAM model, information from component and vendor performance, detection of failure modes, and the results of analyses and mitigation plans.

2.3.4 Tools and Activities for Step 2

The majority of tools and activities traditionally discussed in textbooks on RAM are utilized during the design (and redesign) process. They include:

- Contractor Incentives - The contract shapes how the work is actually performed.
- Good Systems Engineering – Consists of reliability roadmaps and looking at every aspect from the operations concept to manufacture with a continued focus on RAM. Link design and reliability testing. Conduct operational assessments that translate RAM into the broader context of force structure, mission success, cost/budgets, and readiness (i.e., developing RAM specifications). Assess impacts on operations in general and more specifically before completing a trade-off that will affect RAM.
- RAM Design Tools - Conduct formal design reviews and use the specific tools for addressing RAM such as FMEA, FTA, RBD, WCCA, LCC, and Testability Analysis (TA) (all will be described later), reliability tests, embedded diagnostic and prognostic instrumentation in the design, and a logistic support analysis. Apply appropriate Protocols and Standards/Military Specifications.
- Reliability Growth Testing (RGT) Analysis Methodology: RGT analysis monitors improvements in reliability while deficiencies are being identified and fixed. Methodology also can assess the impact of design changes and corrective actions on the reliability growth rate of the system, specifically during O&S design changes to the deployed system.

Technical reviews continue in Step 2 as the Systems Engineering Plan is updated. The following technical reviews are conducted during Step 2: Design and Redesign for RAM.

- System Functional Review (SFR): Technical review determines if system under review can proceed into preliminary design. SFR ensures that functional performance requirements derived from the Capability Development Document are defined and are consistent with program budget, program schedule, risk, and other system constraints. The SFR includes updated risk assessments (identifying critical items) and an approved Product Support Plan (aimed at reducing logistics footprint). SFR determines whether RAM functional performance requirements are fully defined and consistent with the performance specification. The SFR is the ideal forum to assess the prime Contractor's proposed diagnostics concept and other supportability aspects that are not generally available through acquisition documentation. This information can then be discussed as design relevant topics in the following reviews.
- Preliminary Design Review (PDR): A successful PDR is predicated on the Integrated Product Team's determination that the subsystem requirements, subsystem preliminary design, results of peer reviews, and plans for development and testing form a satisfactory basis for proceeding into detailed design and test procedure development. The PDR must determine if the design will be operationally suitable and effective (i.e., development testing and operational testing). PDR assesses whether the preliminary RAM design will satisfy end user and maintainer requirements.
- Critical Design Review (CDR): The purpose of this design review is to ensure that the system under review can proceed into system fabrication, demonstration, and test while meeting the stated performance requirements within cost, schedule, risk, and other system constraints. The Program Manager should tailor the review to the technical scope and risk of the system, and address the CDR in the Systems Engineering Plan. CDR success is based on the ability to satisfy the Capability Development Document, identify critical safety items/applications, identify key product characteristics impacting RAM, and ensuring overall system success. CDR assesses whether the final RAM design will satisfy user requirements.
- Test Readiness Review (TRR): A multi-disciplined technical review to ensure that the subsystem or system under review is ready to proceed into formal test. The TRR assesses test objectives, test methods and procedures, scope of tests, and safety as well as confirming that required test resources have been properly identified and coordinated to support planned tests. TRR assesses the ability of tests to confirm RAM requirements.

2.3.4.1 Contractor Incentives

Contractors should understand and implement sound RAM design processes to satisfy military needs. A well thought-out approach will reduce cost and risk. The developers of this approach must understand that a contractor can only deliver that which is in the contract. Therefore, there should be incentives in the contract to ensure that the contractors utilize the desired approach. Some examples of contractor incentives include: incentive fees, requirements for RAM demonstrations before the full rate production decision, and, where applicable, contracts that include multiple years of maintenance support at a fixed fee.

2.3.4.2 Good System Engineering Design Tools for RAM

The most important thing is to have a good closed-loop system of data collection, analysis and dissemination to identify and correct failures of a product or process. This closed-loop system is commonly referred to as a Data Collection, Analysis, and Corrective Action System (DCACAS). The DCACAS process will be discussed in detail within Chapter 4 of this guide.

A DCACAS process contributes to every other process in the development and deployment of the system. Because all of the RAM analyses tend to be interwoven, they should utilize a common database comprised of realistic assumptions and estimates and be initiated early in the design phase. The program office and prime contractor should jointly develop detailed RAM parameter definitions, including anticipated RAM performance reports. DCACAS data and reports should be easily accessible to all program participants, for example, through a web based portal.

2.3.4.3 Determining Uncertainty and Risk Associated with the Design;

This also involves prioritizing among design options and maturing the design for Production and Deployment. There are activities appropriate to assessing the system design itself, even before anything is assembled. These include using expert, independent judgment to determine the level of uncertainty associated with the design. Using lessons learned and other programs' available information and expert judgment, a reliability model can be used to assess the risk (expected loss) associated with the design. Such assessment can be used to refine the design if the level of risk is unacceptable. The assessments can also guide where further testing and information gathering is necessary. At any given point in the development of a system there will be many different sources of information on the current RAM status and the projected (expected) ultimate RAM performance. Combining these diverse sources of information is a highly technical subject. Therefore, experts on such integration of information sources should be part of the RAM Manager's team. The RAM Manager's team must determine what additional resources are needed in order to reduce the uncertainty or risk associated with the design. This involves assessment of the operational risks for the design too.

Some basic activities of assessing the design, maturing the design, implementing the design into hardware and software, and maturing the implementation of the design, are included in Table 2-3 below. The total system end-to-end assessment, done as an operational test, is discussed later. The preferred viewpoint is that other forms of total system end-to-end assessment should begin as early as possible.

TABLE 2-3: RAM Assessment Methods

Objective	Stage of Development	Activity	Test/Analysis
1. Assess the Design	Conceptual Model of system or design plans	Identify similarities and differences with current system. Identify failure modes known to similar systems.	• Failure Modes and Effects Analysis • Fault Tree Analysis (FTA) • Finite Element Analysis (FEA) • Thermal Analysis • Electromagnetic Interference Analysis (EMI) • Worst Case Circuit Analysis • Durability Assessment • Software Architecture • Testability Analysis • Comparative Analysis
		Calculate the RAM using similar components or expert judgment.	• Reliability Predictions • Durability Assessment • Simulation • Maintainability Analysis • Dormancy Analysis
2. Mature the Design	Design plans and candidate components	Component testing in realistic environment.	• Reliability Testing • Maintainability (BIT) fault insertion testing
	Component Choice	Screen components to eliminate latent part and manufacturing process defects.	• Environmental Stress Screening (ESS) • Highly Accelerated Stress Screening (HASS)
3. Implement the Design	Prototype or breadboard	Test functional operation to identify design limits, constraints, and integration anomalies.	• Highly Accelerated Life Testing (HALT) - Thermal • HALT - Vibration • HALT – Combined (Thermal/vibration/ shock/ humidity/ dust / electrical power instability) • System integration and software development laboratories
4. Mature the Implementation	Prototypes/initial production items	Additional screening and test for quality control.	• HALT • HASS • Integration and software development laboratories
		Quantify reliability improvement for redesigned components, etc.	• Reliability Growth Testing (RGT)
		Verify the ease of maintenance for production systems. Verify fault detection and isolation design attributes	• Maintainability Demonstration • Initial BIT assessments • Fault insertion testing

		Verify the ability of production systems to perform within specification for extended period of time.	• Durability Testing

Assessment is a process. Early in a program, the quality of the assessment will be coarse. Such an assessment is adequate for making comparisons and making very general conclusions, but is totally inappropriate for determining compliance, projecting spares, determining operational suitability, etc. As additional information is gained through analysis, and the elicitation of expert judgment, the assessment is improved.

2.3.4.4 Measurement

Measurement is needed for a variety of reasons including:

- Evaluating alternative choices of parts, materials, and processes,
- Providing a quantitative basis for design trade-offs,
- Comparing established RAM requirements with state-of-the-art feasibility,
- Providing guidance in budget and schedule decisions,
- Providing a uniform basis for proposal preparation, evaluation, and selection,
- Determining progress in meeting the RAM goals and requirements,
- Identifying and ranking potential problem areas and suggesting possible solutions,
- Providing a basis for selecting an economic warranty period, and
- Determining spares requirements.

2.3.4.5 Testing

There are many guides to good testing; this Guide will not include the depth of those guides, but instead provide a top-level overview. This Guide will note what can be unique or important to RAM testing. The most important thing to realize about the testing is that the testing should be designed and integrated into the development to *get a good system, not just a good number*. RAM testing is discussed within Chapter 4.

2.3.4.6 Design of Experiments

Design of Experiments (DOE) is a method for optimizing the parameters for a defined use environment or to find a robust design (i.e., one well suited for a range of use environments). DOE refers to a collection of methods for collecting and analyzing data under controlled conditions. This collection includes methods for the design and analysis of simple experiments as well as strategies for moving from one experiment to the next based on previous results. The goal of all these methods is to maximize the information contained within and available from relatively little data, this is accomplished by:

- Selecting factors and determining factor levels (sometimes called the treatments),
- Selecting the specific combination(s) of factor levels at which to run the experiment (called interactions),

- Selecting responses, and
- Precisely specifying the experimental procedure to be followed.

Each of these activities is governed by the experiment's purpose. Methods for analyzing experimental data are discussed in more detail in subsequent chapters.

Many factors can influence the operation and RAM performance of an item. These can include environmental factors (temperature, vibration, and humidity), threats (e.g., electromagnetic pulse), and operational concepts. Characterizing these environments is an important part of a comprehensive RAM strategy. Characterization is the process of identifying the relevant parameters (temperature, humidity, etc.) of the environments and the realistic ranges of values and durations for these parameters.

RAM reviews should be routine, but two points are particularly important, the Preliminary Design Review (PDR) and the Critical Design Review (CDR). At those points a thorough assessment of the system's RAM metrics must be conducted.

2.3.5 Outputs and Documentation for Step 2

The most important output of a successful Step 2 is the system design, and all of the tasks within Step 2 should be directed towards the culmination of that design. Documentation centers on the following aspects:

- Development process management,
- Documentation of design/development process,
- Documentation of results, and
- Establishment of contract deliverables.

The starting point for the tasks of Step 2 concentrates on how the user will challenge the system when in use. Any initial design should be evaluated with a formal documentation by a panel of experts who must comment on what is known and unknown about the RAM implications of each of the design choices. A model of the system's RAM metrics can be used to document the results. If the risks are unacceptable (i.e., too much unknown about a technology or a design), an alternative might be explored either alone or in parallel.

PDR documents should contain or refer to these evaluations. They should also consider the maintenance concept and the Integrated Logistic Support Concept. In other words, the PDR should look at the whole system, including the interactions that the system will have with other systems.

A successful approach will have all the activities integrated together. There will be a RAM Program Plan, highlighting the relevance of each activity to achieving needed levels of RAM. The main points of the RAM Program Plan, especially at the system level, will be summarized in the Test and Evaluation Master Plan (TEMP). The RAM Program Plan, as discussed in Chapter 4, will outline the whole process of maturing RAM.

The TEMP should provide the picture of how all the testing fits together and how the testing produces a system that can confirm not only the system's effectiveness at meeting the performance objectives for the capability, but the required reliability, availability, and maintainability as well.

2.4 Step 3: Produce Reliable and Maintainable Systems

The acquisition of a capability starts with the identification of the desired capability, followed by a definition of the technology required to create the capability, and then the design, development and demonstration of a system that will provide the capability. Throughout this acquisition process particular attention is given to providing a capability that will be reliable, available, and maintainable. This attention must continue as the capability is produced and deployed. The quality and fidelity of production cannot improve the inherent RAM of a product, but poor quality manufacturing or system integration can reduce the system's inherent RAM when it is deployed to the field.

2.4.1 Mission and Goals for Step 3

Manufacturing must be a controlled process that does not adversely affect the item with production defects. During this phase, the production organization seeks to build production units, demonstrate acceptable performance of these units, and have them pass acceptance testing, without degrading the designed-in RAM levels of the system.

The goal here is to maintain designed (inherent) levels of RAM during production. All production systems (prototype, low-rate initial production, and full-rate production) must strive to meet the RAM objectives. Component choice, vendor choice, manufacturing technique, and system integration are all important considerations that must be closely monitored during production.

Unless the design is translated into a tangible system with a high degree of fidelity, the levels of RAM observed in earlier analysis and discovery testing would not be seen in field use. Manufacturing processes can introduce quality-related failures that will decrease reliability and therefore, availability. There are two basic objectives of testing during the production phase of system acquisition/development:

- Ensure that the RAM aspects of design are not negatively impacted by manufacturing processes or functional software updates,
- Take appropriate action when RAM is negatively affected.

As pointed out earlier, the appropriate actions to improve RAM may include changes to the manufacturing processes, improved manufacturing quality systems, changes to both hardware and/or software designs, selection of better parts and materials, and additional training for machine and process operators.

The quality of the RAM analyses is significantly increased when worked in a coordinated manner, using realistic assumptions, and when verification testing is part of the qualification procedure.

2.4.2 Organizations and People for Step 3

In Step 3 management, engineering, and manufacturing must work together to deliver a quality product. The people and organizations involved in the Production and Deployment phase are an evolution of the staff team. The DoD program team that manages the design and development of the capability often also has the responsibility of managing the production of the system that has been developed to provide the capability. There must be a Quality Control Manager with a strong voice during manufacturing (backed up by a design that allows for easy assessment of reliability in the product) as well as a Production and Reliability Engineering Manager for the retention of RAM capabilities developed in the prior acquisition process phases. Operational Test and Evaluation (OT&E) staff, specifically a Project Office T&E Manager, will be needed during production as government representation that can clearly state the acceptance testing and criteria as well as the stock pile testing protocol.

2.4.3 Supporting Information for Step 3

Many of the outputs of the System Development and Demonstration phase become inputs to the Production and Deployment phase of the acquisition life cycle. Design records, hardware and software specifications and requirements, and procedures are just some of the documentation that will be used during the system production. Statistical quality control charts are often used to ensure that the manufacturing process is within contractual acceptance testing specifications as defined in the design documentation. If production changes, from the preliminary production processes and procedures that were documented in the design phases, are required due to an affect on the form, fit, function, and interface of the manufactured item, it would necessitate formal configuration review procedures to officially make the production changes. It is important to ensure that these changes are also provided to supportability design groups in order to keep them abreast of the evolving design.

2.4.4 Tools and Activities for Step 3

The RAM Program Plan shifts from design and pre-build metrics to assuring and verifying that the required RAM characteristics are attained and retained throughout production. A system to capture field data (i.e., DCACAS) must be in place and used to provide feedback to the production process regarding the RAM characteristics. The DCACAS process is extremely important in conducting fleet RAM assessments as well as identifying and addressing engineering change proposals.

Contractor incentives remain a key motivational tool in Step 3 as they were in Step 2. Incentives are directed to design–in reliability, ease maintenance, and reduce the logistic burden. Tying a fixed price and fixed year support contract to the production contract provides an incentive for high RAM designs. Quality control is a key manufacturer response desired during the Production and Deployment phase.

Programs for improving quality rely on statistical techniques such as control charts to analyze a process or its outputs so as to take appropriate actions to achieve and maintain a state of statistical control and to improve the process capability. Popular statistically based programs for quality assurance include Taguchi, Six Sigma, and Deming. Statistical techniques for quality control are addressed in Chapter 5, Section 5.5.13.

The emphasis of the production and manufacturing phase shifts to process control, quality assurance, and environmental stress screening, which is also visible in the RAM activities expected during this phase, such as:

- Environmental Stress Screening (ESS): Defined as the removal of latent part and manufacturing process defects through application of environmental stimuli prior to fielding the equipment. ESS and HASS will be used to ensure that reliable, available, and maintainable systems are produced and deployed that will be devoid of latent part and manufacturing process defects.
- Lot Acceptance Testing: Binomial and Poisson sampling has long been associated with acceptance testing. Such sampling is carried out to provide an adequate degree of assurance to the buyer that no more than some specified fraction of a batch of systems is defective.
- Production Reliability Assurance Testing (PRAT): Performed to ensure that the reliability of the hardware is not degraded as the result of changes in tooling, processes, workflow, design, parts quality, or any other variables affecting production.
- Continuation of Growth/Test-Analyze-Fix-Test (TAFT): The process of growing reliability and BIT performance, and testing the system to ensure that corrective actions are effective was started in Step 2. In Step 3, the focus becomes ensuring that the corrective actions are producible and equate to improved RAM in the produced system.
- Reliability Growth Testing Analysis Methodology: RGT analysis monitors improvements in reliability while deficiencies are being identified and fixed. This methodology also can assess the impact of design changes and corrective actions on the reliability growth rate of the system, specifically during O&S design changes to the deployed system.
- Continued Maintenance/Maintainability Demonstration and Evaluation: Continuing this assessment from Step 2 during Step 3, or OT&E, may be necessary and ensures that the maintainability of the system has not changed from the preliminary design to the production design or that the system has not been degraded by software updates. Effective system BIT and overall system ID maturation is important to achieve OT&E goals.
- Continued Reliability Quality Testing (RQT) and Acceptance Testing: The RAM activities started in Step 2 shift from qualifying the proposed design to ensuring that the manufacturing process is repeatable in producing acceptable system during the Production and Deployment phase of Step 3.
- DCACAS: The biggest change in the DCACAS process from Step 2 to Step 3 is where the input data is captured. Instead of developmental testing being the primary source of data, information can be captured from OT&E, other field sources, and ongoing PRAT.

Several technical reviews are conducted during Step 3: Produce Reliable and Maintainable Systems including:

- System Verification Review (SVR): The purpose of the SVR or Functional Configuration Audit is to evaluate the system under review to determine if it can proceed into Low-Rate Initial Production and Full-Rate Production within cost, schedule, risk, and other system constraints. SVR assesses the system final product to determine if it meets the functional requirements, including RAM, documented in the Functional, Allocated, and Product Baselines.
- Production Readiness Review (PRR): The PRR examines a program to determine if the design is ready for production and if the producer has accomplished adequate production planning to ensure designed-in RAM levels are not degraded. At this review, the Integrated Product Team should review the readiness of the manufacturing processes, the Quality Management System, and the production planning (i.e., facilities, tooling and test equipment capacity, personnel development and certification, process documentation, inventory management, supplier management, etc.).
- Operational Test Readiness Review (OTRR): The Program Manager may conduct another TRR prior to Initial Operational Test and Evaluation (IOT&E). The OTRR focuses on ensuring that the "production configuration" system can proceed into IOT&E with a high probability of successfully completing the operational testing. The Full Rate Production Decision may hinge on this successful determination. OTRR assesses the ability of operational tests to confirm RAM requirements.
- Physical Configuration Audit (PCA): The PCA is conducted in conjunction with the Full Rate Production Decision as the PCA examines the actual configuration of an item being produced to verify that the related design documentation matches the item as specified in the contract. The PCA also confirms that the manufacturing processes, quality control system, measurement and test equipment, and training are adequately planned, tracked, and controlled in order to ensure that RAM is not degraded in the production process. Additional PCAs should be performed throughout the system life cycle as necessitated by changes in item design, manufacturing process and source of supply dictate.

2.4.5 Outputs and Documentation for Step 3

There will be numerous outputs and documentation at the conclusion of the Production and Deployment phase of the system acquisition life cycle including:

- Production process management
- Acceptance test results
- Production contract deliverables

The outputs and documentation are often customized to the program, project, and/or contract requirements.

2.5 Step 4: Monitor Field Experience

Once a system is deployed, the RAM program focuses on monitoring and sustaining the inherent RAM that has been "designed in" the system. The system will have an inherent RAM potential when it is produced, but without adequate knowledge about the operations and support concepts the system RAM will be degraded. Therefore, much effort is required prior to deployment to eliminate any known impediments that will degrade system RAM. Unfortunately not all impediments will be known at the time of deployment, which increases the importance of data collection when the system is deployed.

Collecting data from fielded systems is not simple unless the ability and means to collect field data has been developed prior to fielding the system. The DCACAS used during testing (in System Development and Demonstration as well as Production and Deployment phases) should be the same as compatible with the DCACAS for collecting field data. The key issue is the manner in which data will flow from the field into the DCACAS. For modern complex equipment containing on-board data recorders, it is important to obtain all relevant data from the recorder and retain it within the DCACAS for engineering evaluation and possible corrective action. Other DCACAS inputs may include data from other equipment (e.g., hour meter, voltmeter, speedometer, temperature gauge, pressure gauge, fuel gauge, etc.). Field incident reports, combined with on-board data recorders, if available, can identify the how, what, where, when, and why of each failure. However, if desired information is not on the field incident report or data recorders are not available, it will never make it to the DCACAS database. Losing meaningful information increases the importance of knowing what field data to collect, which is often based on what an analyst may need in the future. With the "right" field data an analyst can not only assess, but perform trend analysis of field RAM metrics, thus providing much needed feedback to the user, design team, and manufacturer to correct RAM related problems so that corrective actions can be implemented (either on the current system or future system).

2.5.1 Mission and Goals for Step 4

The goal of Step 4: Monitor Field Performance is to:

1. Maintain RAM performance during operational life,
2. If shortfalls are found early, identify RAM deficiencies for correction in the current configuration, and
3. Provide a good baseline for the development of future systems (i.e., lessons learned).

Monitoring field performance enables the user to perform corrective actions as needed, but the continuous monitoring of the deployed system enables the user to respond quickly and effectively, thus improving their corrective action process. Monitoring field performance also maintains RAM performance during operational life and feeds RAM deficiencies into the next increment of evolutionary acquisition. Tracking RAM performance over time is an important part of an overall strategy of achieving and sustaining required levels of RAM. If a problem persists and RAM performance degrades below an acceptable threshold, then the problem must be addressed, whether it is localized to a single system or across all systems. Over the life of a system, many factors can affect RAM performance.

2.5.2 Organizations and People for Step 4

The Program Manager is responsible for the total life cycle system management. As systems are deployed and the acquisition life cycle moves to the Operations and Support phase, the responsibilities of the development contractor and government design/system engineering team decrease and those of the in-service organizations increase. The in-service organizations that assume responsibilities during the Operations and Support phase include defense military and civilian personnel, civilian contractors, and often a combination of both depending on the program.

Lessons learned have shown that the experienced Systems Engineering RAM Team should stay involved with monitoring field performance until the system no longer requires engineering design, development, or test and evaluation, that is, until all RAM parameters and goals are being met in the users' environment. By combining the skills and knowledge of the System Engineering RAM Team with that of the field engineering effort, the transition will become much more smooth and cost effective. The presence of contractor field engineers at locations where the system is being operated enhances communication between the user and the product development and manufacturing team. As the new product meets the real deployed environment, the potential for problems is high. A good field engineering effort, combined with the experience of the system engineering RAM team, will provide understanding to operators and maintainers as well as provide feedback of unanticipated problems to the development team to speed the resolution of initial RAM and support problems. A robust field engineering effort should be supported throughout the life cycle of a fielded system as new failure modes will present themselves through all phases of field experience. This is particularly true for systems with frequent incremental development and complex software controlled systems that are continuously updated where changes may affect RAM.

An in-service manager with the support of a professional engineering team will take control of the Failure Prevention and Review Board, failure analyses relating to the DCACAS, and logistics responsibilities (spares support, logistics initiatives, modeling, and analysis).

2.5.3 Supporting Information for Step 4

Outputs of the Production and Deployment phase support the transition of the system into the Operations and Support phase, specifically in the areas of in-service management and engineering. Supporting production data includes:

- Configuration data
- FMEA results
- Critical Safety Item lists
- Fault Tree Analysis results
- Reliability Centered Maintenance (RCM) Analysis information
- DCACAS summaries
- Test results

2.5.4 Tools and Activities for Step 4

There are several tools and activities that are used during the Operations and Support (O&S) phase to assess and assure RAM. Many of the tools and activities were started in previous phases of the acquisition life cycle, but must adjust to the change in focus in regards to assessing and assuring RAM during the O&S phase. The tools and activities include:

- DCACAS Process: Backbone of assurance technologies (reliability, availability, maintainability) as it provides the data needed to monitor system performance and identify corrective actions to ensure RAM is not degraded after the system is deployed.
- Reliability Growth Testing Analysis Methodology: RGT analysis monitors improvements in reliability while deficiencies are being identified and fixed. This methodology also can assess the impact of design changes and corrective actions on the reliability growth rate of the system, specifically during O&S design changes to the deployed system.
- Life Data Analysis: Supports overhaul decisions, changes to the maintenance concept, and risk mitigation activities through statistical analysis of component, assembly, or system data.
- Repair Strategy: Continually reviews maintenance and support concepts to ensure that repair strategy is not introducing defects into the deployed system that degrade its inherent RAM. This includes refinement of the on and off equipment maintenance processes including the automated maintenance environment support strategy.
- BIT/ID Maturation: Defines the continuous process of eliminating false alarms and improving fault detection and isolation as the system matures.
- RCM: Logically determines (with the aid of life data analysis results) if preventive maintenance makes sense for a given item and, if so, determining the appropriate time and manner in which to conduct the preventive maintenance. As field performance is monitored during O&S the focus is determining whether changes need to be made to the preventive maintenance program.
- Condition-Based Maintenance: Defines optimal maintenance point that maximizes the expected results (in terms of increased product output, decreased maintenance costs, etc.) with the costs (both short-term and long-term) of implementing the maintenance. It is important during O&S to verify that condition-based maintenance program is acceptable based on the monitored field performance of the system.
- Parts Obsolescence and Diminishing Manufacturing Sources: Attempts to avoid potentially expensive and time-consuming problem of searching for suitable replacement parts for parts that are no longer manufactured or are no longer viable to produce according to the current specification. Subcontractors and vendors need to be continually contacted to ensure that parts obsolescence and diminishing manufacturing sources will not affect the system during the O&S phase.

There is a technical review that is completed during Step 4: Monitor Field Performance, which is the In-Service Review (ISR). The ISR is conducted periodically to ensure the system under review is operationally deployed with well-understood and managed risk. This review documents in-service RAM, operational system risk, system readiness, costs, trends, aging equipment and out of production issue. Analysis identifies opportunities for refinement.

2.5.5 Outputs and Documentation for Step 4

Use of a structured and controlled data acquisition process provides the necessary information to perform trend analyses on the behavior of the subject equipment/system and to support root cause analyses of failure situations. Application of RAM tools and techniques is extremely data-dependent and the root of: (1) oversight/insight into program or system behavior, (2) validation decisions made earlier during the System Development and Demonstration phase and (3) the identification of modifications/actions needed to sustain the program. For example, if reliability centered maintenance (RCM) were used during design, operations will provide the opportunity to validate or revise the maintenance decisions (redesign, condition monitoring, or run to failure) that were made during the System Development and Demonstration phase. For the purpose of capturing lessons learned that can be utilized on future programs, even one-shot item operation provides the capability to explore what did and did not go well. The most essential ingredient that will help guarantee the success of any operational RAM program is management's continuing commitment and support.

All RAM analysis activities are dependent on the available RAM data. It is important to consider the desired outputs of the RAM analysis at the start of the RAM program, so that a data collection system can be designed to capture the necessary inputs.

2.6 Acquisition Framework and Program Integration

This section addresses the four key steps for achieving RAM. These four steps, and the activities supporting them, constitute a model for achieving customer needs for RAM over the system life cycle. The steps have been evolved from successful, and unsuccessful, experiences in many different product development environments. The model captures the essential management and technical activities to ensure achieving the level of RAM needed by product users. The steps are most effective when employed in a robust systems engineering environment.

In the Department of Defense, JCIDS and the Defense Acquisition System as defined in DoD Directive 5000.1 and DoD Instruction 5000.2 provide the framework for how user needs or requirements are defined, how products are acquired, and how funding is planned, programmed, and budgeted. No matter how they change, the four key steps for achieving RAM can be accommodated within them and provide the preferred approach for meeting these aspects of user needs. The rest of this section summarizes the current defense processes for defining user needs (JCIDS), and for acquiring materiel solutions to these needs (DoD 5000 Series), followed by an approach for implementing the four key steps within these processes.

2.6.1 Current Process for Defining User Needs

The current DoD process for defining user needs is the Joint Capabilities Integration and Development System (JCIDS), defined in the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01D, dated 12 March 2004 and the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3170.01A, dated 12 March 2004. The JCIDS implements a capabilities based approach which leverages the expertise of government agencies, industry and academia to identify improvements to existing capabilities and to develop new warfighting capabilities. The approach uses a collaborative process that utilizes joint concepts to identify capability gaps and

integrated materiel and non-materiel solutions to resolve those gaps. The JCIDS requires substantially more analytical effort early in the process of capability definition in order to provide a well-developed, integrated and supportable solution to the warfighter. The JCIDS process provides the right environment for defining and documenting user needs and constraints at the front end of the acquisition process. However, it does not directly force required levels of RAM capability and logistics footprint in the ICD. The AoA refines the selected concept documented in the ICD and evaluates the operational effectiveness and suitability and estimated cost of alternative systems to meet a mission capability. Traditionally the requirements generation process focused narrowly on the materiel system to be acquired. In addition to materiel, the new JCIDS process also explicitly addresses the doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) aspects of the needed capability.

2.6.2 Current Acquisition Framework

The current defense acquisition process is defined by two documents: DoD Directive Number 5000.1, The Defense Acquisition System, and DoD Instruction Number 5000.2, Operation of the Defense Acquisition System, both dated May 12, 2003[20]. The Defense Acquisition (5000 Series) process and JCIDS were developed together to provide a better integration of user needs and the process used to satisfy those needs. The stated primary objective of Defense 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. As with JCIDS, this 5000 Series framework provides the opportunity to focus on achieving the user's needs for RAM over the life cycle. Both also stress a collaborative team of users, technologists, acquisition personnel and testers, from government, industry, and academia, which is a key to implementing the four steps for achieving RAM.

Figure 2-3 illustrates the current DoD 5000 series acquisition phases and decision points. User needs come from the collaborative process defined in JCIDS. Needs are defined for both the materiel and the non-materiel elements of capability. Depending on the level of definition, maturity, and feasibility, there are three phases and milestone decision points to enter the pre-systems acquisition or systems acquisition process. The three phases are Concept Refinement, Technology Development and System Development and Demonstration. The milestone decision authority (MDA) can authorize entry into the acquisition system at any point consistent with phase criteria and statutory requirements. DoDI 5000.2 lists specific entrance criteria and statutory requirements.

[20] The defense acquisition process has changed numerous times over the years in terms of how the various phases of the acquisition life cycle are identified (i.e., a single Concept and Technology Development phase in DoD 5000 series circa 2001 versus separate Concept Refinement and Technology Development phases in DoD 5000 series circa 2003). No matter how the acquisition life cycle phases are defined, the goals, activities, processes, and documentation that accompany them will remain, as will the four key steps to achieve RAM. Therefore, this guide will reference the DoD 5000 series circa 2003 as the most current, but due to the likelihood of this being altered in the future, more emphasis should be placed on the activities being carried out in each phase and on how the phases interact with the four key steps than the names of the phases.

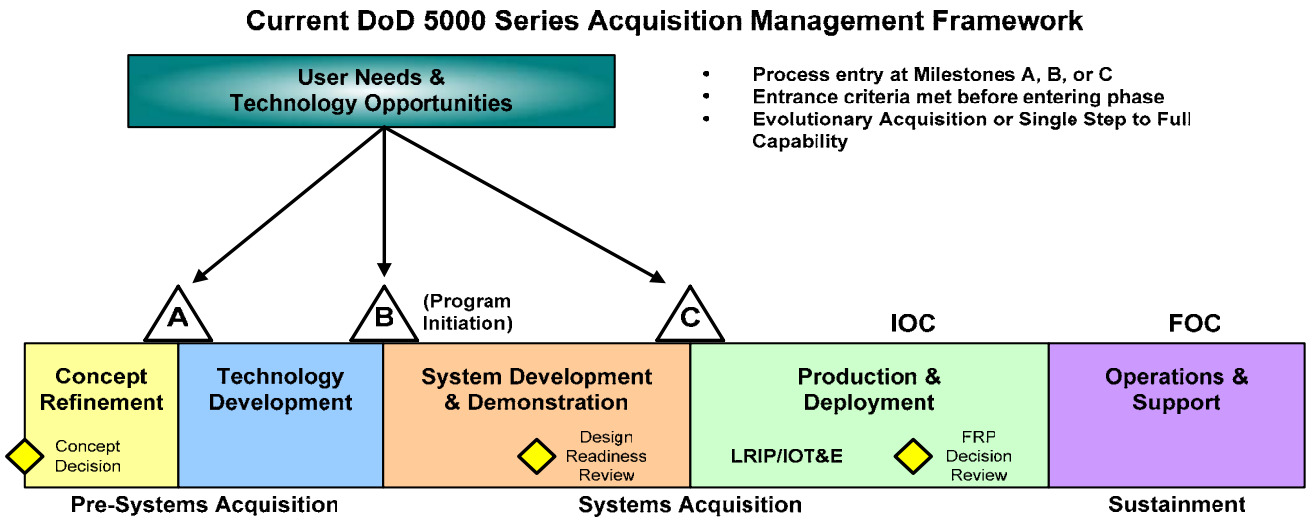


FIGURE 2-3: The Defense Acquisition Management Framework

Concept Refinement (CR) starts with the approved ICD and concept decision as the first of the three decision support processes in the acquisition management framework. The AoA is used to assess critical technologies and demonstration needs. The result of the AoA is the basis for the Technology Development Strategy (TDS). The TDS documents the program strategy, overall program goals, and specific program goals and a test plan for the first incremental technology demonstration. The MDA approves the TDS at Milestone A and the ICD is finalized for future use in the Technology Development phase.

The purpose of the Technology Development (TD) phase is to assess the viability of technologies and refine user requirements. The AoA guides the activity. The project exits this phase when a useful capability has been defined, technology demonstrated, and systems can be developed in a short (5 year) period of time. Technology, including software, is to be demonstrated in a relevant environment, preferably an operational environment, sufficient to be considered mature enough to be used in the following phase. Also during this phase, the user prepares the Capability Development Document (CDD) to support program initiation at Milestone B, better define program capability, and define the Key Performance Parameters (KPP) to guide the next phase. The CDD builds on the ICD and provides detailed operational performance parameters necessary to define the proposed system. TD ends with JROC approval of the CDD and a Milestone B decision to begin system development.

The purpose of the System Development and Demonstration (SDD) phase is to develop the system or improve the capability, reduce manufacturing risk, ensure operational suitability and reduce logistics footprint, and demonstrate system integration. The approved CDD guides the process. Entrance into this phase depends on technology maturity (including software), approved requirements, and funding. Some programs enter the acquisition framework directly at Milestone B, the beginning of SDD, without going through CR and TD if the MDA judges that all Milestone B entrance criteria have been met. There is no shortcutting the development of user needs.

The Design Readiness Review, the second management level review, in mid SDD addresses a number of important factors with respect to RAM accomplishment including planned corrective actions to hardware/software deficiencies, adequate development, a completed failure modes and effects analysis, and an estimate of systems RAM based on demonstrated RAM levels. Critical activities during system demonstration include early operational assessments and successful developmental test and evaluation (DT&E). The Capability Production Document (CPD) is approved before the Milestone C acquisition decision. The CPD is the sponsor's primary means of providing authoritative, testable capabilities for the Production and Deployment phase of an acquisition program.

The purpose of the Production and Deployment (PD) phase is to achieve an initial operational capability (IOC) that satisfies mission needs. The phase begins with the Milestone C decision. The sequence of activities in this phase are: (1) low-rate initial production (LRIP), which produces the products for initial operational test and evaluation (IOT&E), (2) the Full Rate Production Decision Review (FRPDR), (3) full rate production, and (4) deployment. RAM related criteria for entry into PD include acceptable performance in DT&E and Operational Assessment (OA), mature software capability, acceptable operational supportability, and demonstration that the system is affordable through the life cycle. Deficiencies encountered in testing prior to Milestone C will be resolved before proceeding beyond LRIP and any fixes verified in follow-on operational test and evaluation (FOT&E). The Director of Operational Test and Evaluation (DOT&E) determines the number of production or production representative test articles required for IOT&E and the Live Fire Test and Evaluation (LFT&E). For programs that are not on the DOT&E oversight list, the service OTA determines the number of test articles.

The purpose of the Operations and Support (O&S) phase is to execute a support program that meets operational support performance requirements and sustains the system cost effectively over the total life cycle (full operational capability or FOC). Effective sustainment begins at the start of the system acquisition process, with the design and development of reliable, available, and maintainable systems. Program Managers are required to optimize the operational readiness achieved in this phase through affordable, integrated, embedded diagnostics and prognostics, embedded training and testing, serialized item management, automatic identification technology, and iterative technology refreshment.

The user-generated documentation (ICD, CDD, and CPD) provides a continuing and evolving user influence throughout the acquisition process Figure 2-4 illustrates how the JCIDS documents support the decision milestones. The ICD supports the Concept Decision; the CDD supports the Milestone B acquisition decision, and the CPD precedes the Milestone C decision at the end of the System Development and Demonstration phase. The initial formulation of user RAM needs and constraints occurs first in the Analysis of Material Approaches (Figure 2-4) which supports the ICD. During this early definition of capability, the RAM Rationale may consist of top-level qualitative statements about mission reliability, logistics footprint constraints, and Total Ownership Cost. The understanding expressed in the RAM Rationale continues to develop as more is learned about system capability and feasibility through pre-acquisition and acquisition.

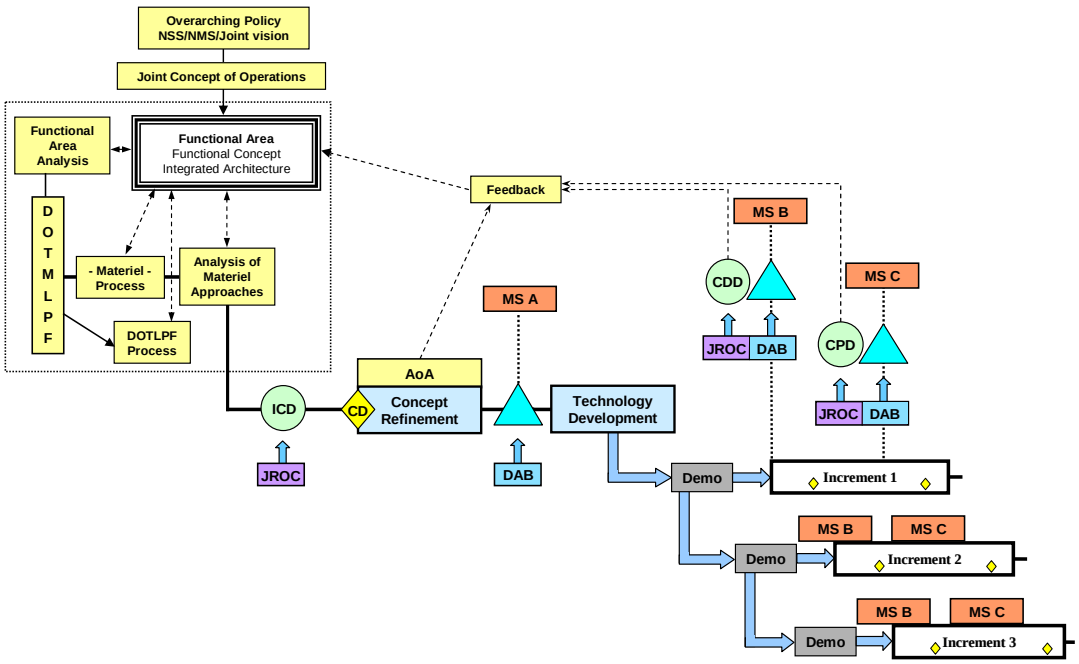


FIGURE 2-4: Defense Acquisition Management Framework and Joint Capabilities Integration and Development System

Figure 2-5 illustrates the how the system engineering technical reviews integrate the four key steps to achieve RAM into the acquisition management framework. The four key steps overlap each other significantly to emphasize continuing interaction between them. The beginning and end points of the four key steps are not rigid may vary from program to program.

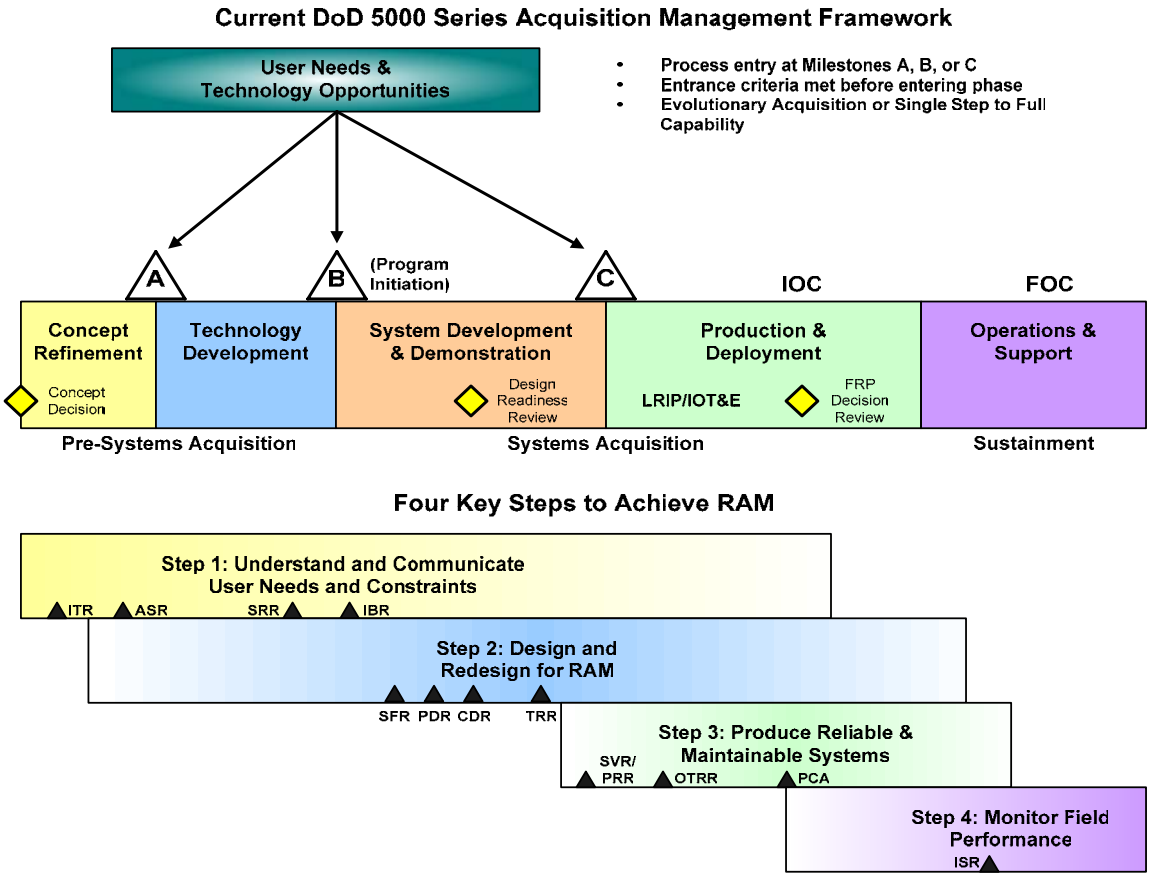


FIGURE 2-5: The System Engineering Technical Reviews Assess Progress Toward Achieving RAM

Chapter 3 Understand and Document User Needs and Constraints

3.1 Introduction

The first priority in an acquisition program is to thoroughly understand what the customer needs and expects (the customer includes those whom will operate, maintain, and support the capability being acquired). The user needs should include the wartime and peacetime usage rates, the use environments, the non-operating duration and conditions, the operational constraints of the maintenance and supply system, and the logistics footprint. It should identify limitations of the current capability or system and its support concept, define the current RAM burden[21], propose or document desired changes, identify design constraints (from manpower, training, etc.), and define expected system stress (environmental, usage, etc.). Potential threats to the capability should be addressed during this phase of the acquisition life cycle also.

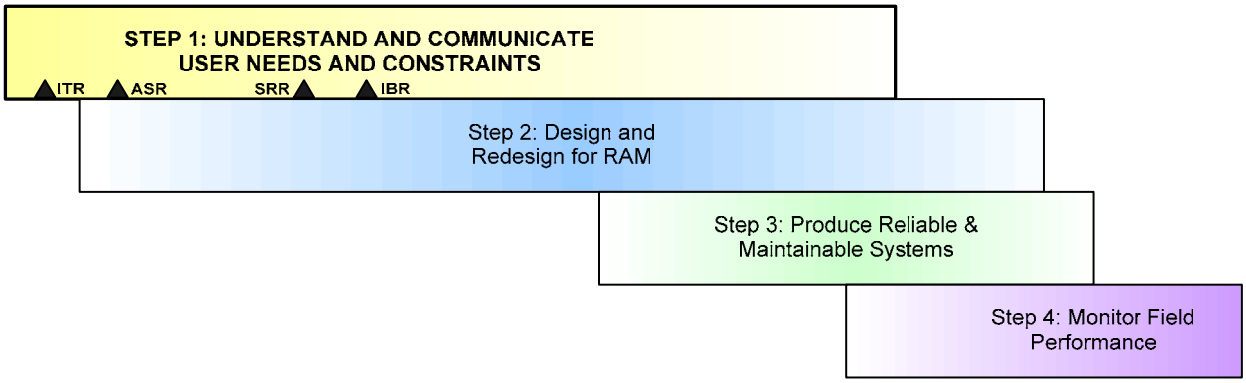


FIGURE 3-1: Understand and Communicate User Needs and Constraints

The primary objective of understanding and documenting user needs and constraints is identifying the system/capability requirements. A requirement can be defined as (1) a characteristic that identifies the performance levels needed to satisfy specific objectives within a given set of conditions and (2) binding statement in a document or in a contract. There are three basic types of requirements: functional, performance, and constraint. Functional requirements identify (1) the necessary task, action, or activity that must be accomplished or (2) what the system/capability must provide. Performance requirements characterize how well the system/capability must perform a function when subjected to expected conditions. Constraint requirements are subject to the restrictions placed on a system/capability through legislative, legal, political, policy, procedural, moral, technology or interface conditions. The source of requirements is the customer (i.e., commissioning agent or prospective purchaser or system/capability) as well as stakeholders, which can include the acquirer, user, customer, manufacturer, installer, tester, maintainer, Executive Manager, and Program Manager. User requirements are often not adequate for design purposes as they are usually stated in non-technical terms (i.e., needs, wants, desires, and expectations). The user requirements become

[21] The purpose of acquisition is for the new capability to improve upon the current capability. Therefore, the RAM burden can be defined as the penalty that a system pays in terms of operation and support costs, in maintenance manpower, in downtime, or in the supply chain due to the unreliability, unavailability, or unmaintainability of the current capability.

clear, unambiguous, and measurable as they are derived into technical requirements. Technical requirements balance what is acceptable to the stakeholders versus what is achievable through the application of technology.

Requirements development/management activities include:

- Eliciting requirements from customers and potential product/service users,
- Validating and prioritizing customer/user requirements,
- Defining requirements in a manner that is executable and verifiable,
- Identifying alternative solutions to achieve requirements,
- Isolating balanced and robust solutions that "best" meet requirements, and
- Verifying implemented solutions satisfy requirements.

A February 20, 2004 Under Secretary of Defense Acquisition, Technology and Logistics (USD AT&L) memorandum[22] stated, "All programs responding to a capabilities or requirements document, regardless of acquisition category, shall apply a robust systems engineering approach that balances total system performance total ownership costs within the family-of-systems, systems-of-systems context. Programs shall develop a Systems Engineering Plan (SEP) for Milestone Decision Authority (MDA) approval in conjunction with each Milestone review and integrated within the Acquisition Strategy. This plan shall describe the program's overall technical approach, including processes, resources, metrics, and applicable performance incentives. It shall also detail the timing, conduct, and success criteria of technical reviews."

Systems engineering can be defined as an iterative process of top-down synthesis, development, and operation of a real-world system that satisfies, in a near optimal manner, the full range of requirements for the system. Systems engineering can also be characterized as a number of processes that work together on a set of inputs to achieve the desired output where the desired output is a system/capability that meets the user's needs and requirements in a near optimal manner. Systems engineering must account for the entire life cycle of the system/capability acquisition. The life cycle functions that systems engineering accounts for are development, manufacturing/production/construction, deployment (fielding), operation, support, disposal, training, and verification. Systems engineering ensures that the correct technical tasks are accomplished during the acquisition process through planning, tracking, and coordinating. Lead Systems Engineers are responsible for the:

- Development of a total system design solution that balances cost, schedule, performance, and risk,
- Development and tracking of technical information required for decision making,
- Verification that technical solutions satisfy customer requirements,
- Development of a system that is cost-effective and supportable throughout the life cycle,
- Adoption of the open systems approach to monitor internal and external interface compatibility for the systems and subsystems,
- Establishment of baselines and configuration control, and
- Proper focus and structure of interdisciplinary teams for system and major subsystem level design.

[22] The USD (AT&L) memorandum will be included in the next revision to DoD Instruction 5000.2.

3.2 Mission and Goals:

Understanding user needs encompasses determining: (1) how a customer describes RAM: (2) the conditions of use under which the RAM is expected to be delivered; and (3) the constraints on what the user can do in the field to achieve RAM. This understanding is typically expressed with RAM metrics as described in the next four sections. The program management office (PMO) engineers translate user needs into system level RAM metrics suitable for inclusion in the development contract.

3.2.1 General Considerations in Developing Metrics

The RAM metrics should be chosen based on the type of system under consideration (i.e., one-shot systems or repairable systems), the support concept, and the system's use.

- One-shot systems are expendable systems that only get used once and are then replaced, for example an automotive air bag is a one-shot system. The reliability may be characterized by a single probability (e.g., 99.9% reliability when 999 out of 1000 air bags fired and deployed properly when voltage was applied). Alternative reliability characteristics might be storage reliability and reliability under conditions before use (i.e., vibration conditions of transportation).
- Repairable systems are repaired upon failure. The reliability could be measured in miles between failure, time between failure, on-demand functioning (i.e., pulled the trigger five times and fired four times). In these cases the units used to express reliability are different: per mile, per hour, per demand. Alternatively, reliability could be measured as the frequency of unscheduled maintenance. In each of these cases, the reliability metric also could be recast as a probability: the probability of some number of miles without a failure; the probability of so many hours without a failure; the probability of some number of trigger pulls without a failure; the probability of some number of weeks without an unscheduled maintenance action. The dimension of how the failure is perceived could also be included by restating the reliability metrics as, e.g., the probability of some number of miles without "indicating and recording" a failure.

The definition of failure might be even more difficult for complex systems where success is not "all or nothing." Care must be taken in defining failure to ensure that the failure criteria are unambiguous. Failure should always be related to a measurable parameter or to a clear indication. A seized bearing indicates itself (as a failure) clearly, but a leaking seal might or might not constitute a failure, depending on the leak rate or whether or not the leak can be rectified by a simple adjustment. Electronic equipment may have modes of failure which do not affect function in normal operation, but which may do so under other conditions. For example, the failure of a diode used to block transient voltage spikes may not be apparent during functional test and will probably not affect normal function. Defects such as changes in appearance or minor degradation that do not affect function are not usually relevant to reliability. However, sometimes a perceived degradation is an indication that failure will occur and therefore such incidents can be classified as failures. It is important to recognize that the operator cannot observe most electronic equipment functional failures. These failures are

reported by the Integrated Diagnostic system and as such, will include both real hardware faults and 'indicated faults' that are subsequently classified as false alarms. Engineers working in design and verification need to recognize that system availability, mission reliability, and the 'logistic footprint' are influenced by both equipment reliability and Integrated Diagnostic false alarms. Similarly, a repair can be complete (returned "good as new") or incomplete. The main point to express here is that not all failures encountered in the field are within the control of the developers or the design itself. System modeling should account for these considerations if requirements that are contractually bound will be affected by these considerations.

In all cases the nature of the failure mechanism will be important in properly characterizing the reliability. For example, the reliability of a piece of aircraft avionics could be characterized best by calendar time to failure, flight hours between failure, on-time between failure, or number of aircraft landings between failure.

For any product, the key RAM issues, from the user's perspective, are:

- What measures of operational RAM are important?
- What levels of operational RAM are required?
- How and when will the achievable levels of operational RAM be assessed?
- How will progress toward meeting the required levels of operational RAM be measured?
- How and when will the achieved levels of operational RAM be determined?
- How can the user's operational RAM requirements be "translated" into contractual requirements?

The failure mode is a function of the type of system, complexity and technology used, maintenance concept, and the ease with which the failure mode can be detected. It is critical to account for all known failure modes in establishing design reliability metrics and goals. Requirements should be verifiable. User requirements are often tougher than what is really needed; therefore, it is important to ask, "How were those requirements determined?"

Military commanders must report the status of their forces in terms of readiness. Reliability and maintainability are two important design parameters, measures of system performance, and inputs to readiness. The maximum availability that can be achieved is a function of the reliability and maintainability designed and manufactured into an item as well as other factors. The next three subsections discuss specific metrics for each of these areas.

3.2.2 Reliability Metrics

Reliability is the probability that an item can perform its intended function(s) without failure for a specified time under stated conditions. Reliability is a measure of whether or not an item will function properly when used by typical users in its operating environment. The specification of reliability, and the design for reliability, requires the identification of the conditions of use and what constitutes proper functioning (i.e., when is a failure a failure). For some systems that are repairable, the rate of recurrence of a problem is an important characteristic. For systems or components that are replaced when they fail, the lifetime of the component is important. Analysis of recurrence data from repairable systems and analysis of lifetime data for components

and non-repairable units require different statistical models and methods of analysis. However, in all cases, reliability should be defined with respect to a well-defined mission and conditions of use. Reliability is a function of the environment and the stresses it places on a system. The conditions of use include, but are not limited to, the environment of operation (such things as temperature, season of the year, operating time, dust, vibration, acoustic environment, geographic location), maintenance as specified, and operation within the design specifications. (If users consistently operate a system outside the design specifications (e.g., higher than designed for speeds), often this operation will lead to reliability problems when the system is in use.) An operational perspective must be present as early as possible in the design reviews. A reliability specification requires a description of what constitutes mission success or failure for the equipment when it is operational. Table 3-1 identifies several popular reliability metrics.

TABLE 3-1: Reliability Parameters

Parameter	Description
Failure Rate (λ)	The total number of failures within an item population, divided by the total time expended by that population, during a particular measurement interval under stated conditions.
Hazard Rate	Instantaneous failure rate. At any point in the life of an item, the incremental change in the number of failures per associated incremental change in time.
Mean Time Between Failure (MTBF)	A basic measure of reliability for repairable items. The average time during which all parts of the item perform within their specified limits, during a particular measurement period under stated conditions. (RAC Toolkit)
Mean Time Between Maintenance (MTBM)	A basic measure of reliability for repairable fielded systems. The average time between all system maintenance actions. Maintenance actions may be for repair or preventive purposes. (RAC Toolkit) An alternative definition: The time (i.e. operating hours, flight hours) between the need for maintenance actions to restore a system to fully operational condition, including confirmation that no fault exists (a No Defect maintenance action) This parameter provides the frequency of the need for maintenance and complements the labor hour parameter to project maintenance workload. This parameter is also used to identify unscheduled maintenance (MTBUMA) and Scheduled maintenance (MTBSMA)
Mean Time Between Repair (MTBR)	A basic measure of reliability for repairable fielded systems. The average time between all system maintenance actions requiring removal and replacement or in-situ repairs of a box or subsystem.
Mean Time Between Critical Failure (MTBCF)	A measure of system reliability that includes the effects of any fault tolerance that may exist. The average time between failures that cause a loss of a system function defined as "critical" by the customer. (RAC Toolkit)
Mean Time Between Operational Mission Failure (MTBOMF)	A measure of operational mission reliability for the system. The average time between operational mission failures which cause a loss of the system's "mission" as defined by the customer. This parameter may include both hardware and software "failures."
Mean Time To Failure (MTTF)	A basic measure of reliability for nonrepairable systems. Average failure free operating time, during a particular measurement period under stated conditions.

There may in fact be several different ways to view the reliability of a system depending on its function and complexity. One perspective focuses on the probability that no failure will occur during a mission that would prevent the system from successfully completing its operational mission (i.e., MTBOMF), while other perspectives focus on failures that require maintenance (i.e., MTBR). The first case emphasizes mission capability, and the latter illustrates operational support. Both measures are important and both are a direct result of how the system and its

constituent elements were designed, manufactured, and how their maintenance support is structured.

3.2.2.1 Full Mission Capability, Degraded States, Partial Mission Capability and Failure

Most military systems have multiple missions. Not all of the items that comprise the system are needed to perform every mission. An aircraft may have an air-to-air offensive mission, an air-to-ground offensive mission, and a reconnaissance mission. An item may support the air-to-air mission, whereas it is not needed for the reconnaissance mission. Operational commanders are usually interested in having equipment that is fully mission capable because it gives them maximum operational flexibility. Thus from the perspective of achieving reliable, available, and maintainable equipment the full mission capability is the capability to design for and monitor the effectiveness of the equipment for all potential operational scenarios. In operational use, failures may be induced by the act of repairing a failed item, removing and replacing a failed item, or during preventive maintenance. From the user's perspective, an induced failure is still a failure. By understanding the importance of specifically addressing the human element in a system, designers can minimize induced failures. Again, in the design phase of system, the period in which the foundation for achieving RAM is being developed, systems that allow or encourage induced failures are in fact poor designs with respect to RAM. Many tools exist to check that parts are accessible for repair or replacement and that diagnostics will detect and isolate faults reliably for quick repair. (For example, connectors that induce noise into electrical circuits, or make it difficult to seat components properly induce reliability problems and should be dealt with in the design phase.) Alternatively, a poorly developed BIT design can introduce false BIT detections (false alarms) that are processed identically to real component failures. To define reliability in some instances we need to describe what it means to succeed and to fail. The following identify considerations for developing a definition of failure:

- Not all failures impact the mission, but can impact the operational support, maintenance, and logistics system.
- Not all failures at lower-levels of indenture cause a mission failure. So a localized failure may or may not constitute a failure at a higher level. For example, a system may have redundant components so that a failure of one may not cause a mission failure. A failure may result in a total loss of function or may just produce a degradation of the function.
- In many cases an event occurs that degrades the performance of an item below some desirable level, but does not cause total loss of the item's function. For example, a failure of some electronic components in early-warning radar may reduce the ability of the radar to detect objects of a given size. The radar is still operating, but in a degraded or less effective mode. Has the radar failed? In another case, a function may be distributed among two or more "black boxes." It is possible that when a failure occurs to one box, computers can reroute signals to allow the function to continue to be performed albeit at a degraded level.

In each of the preceding examples, the function continues to be performed by the system, but the ability of the system to perform the function has degraded. The question is, of course, whether or not degraded performance constitutes a failure. The answer will vary depending on the mission, the function, system-specific requirements, and user-specific requirements. The definition should be clear and it should be specific, otherwise there is a real danger that the

equipment developed will not truly satisfy the needs of the user. The definition should also be specific regarding false alarms since they can impact the user the same way actual failures do, and often the user cannot determine whether the indicated failure is a true failure or a false alarm.

3.2.2.2 Reliability Related to Operational Support

All indicated and recorded failures, even those that do not affect successful completion of the mission, eventually result in some corrective action. Corrective action often includes some level of repair or inspection to mitigate the failure. Logistics reliability (sometimes called basic reliability) deals with all failures. Repair (called corrective maintenance), in this case, can consist of removal and replacement, in-place repair, or some combination thereof for the failed item. The cost of high failure rates can be:

- The need for more spares,
- The need for additional maintenance personnel,
- More system downtime,
- Larger logistics footprint,
- Decreased readiness to perform missions or increased force size, and
- Higher life cycle cost.
- The need for corrective action on poor reliability or BIT false alarms.

A logistics reliability specification requires a good definition of the use profile, similar to mission reliability. The use profile addresses peak or wartime usage rates, peacetime rates and conditions, as well as non-operating times and conditions. In addition to determining the maintenance needed to address failures, the reliability characteristics of a design also help determine the preventive maintenance that should be performed. Using an approach called Reliability-Centered Maintenance, candidates are identified for preventive maintenance. Factors such as safety and economics then are used to select which candidates to include in an initial preventive maintenance plan. This plan is then updated, ideally, throughout the operating life of the system with the aid of life data collected from the deployed systems.

3.2.3 Maintainability Metrics

Chapter 1 defined maintainability as the probability that an item can be retained in, or restored to, a specified condition in a given time when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair.

Many different parameters are used for maintainability. They include quantitative measures such as mean time to repair (MTTR), max time to repair (M_{Max}), and maintenance ratio (MR). Table 3-1 lists some of these quantitative measures that are mainly concerned with *time*. Maintainability also is a function of finding failures therefore diagnostics is important and is characterized with metrics such as built-in-test (BIT) effectiveness, fault detection, isolation and false alarm rates. Some programs have found a more recent metric, mean operating hours between false alarm (MOHBFA), to be more meaningful than the classic false alarm rate. Maintainability is also concerned with economical considerations and ease of maintenance. The

ease of maintenance is indirectly indicated, or measured, by accessibility, accuracy of diagnostics, level of standardization, and human factors-related considerations. Features of the design, such as the level and accuracy of embedded diagnostics instrumentation and prognostics, can increase the maintainability of the system. Some of the more commonly used maintainability metrics are identified in Table 3-2.

TABLE 3-2: Quantitative Measures of Maintainability

Parameter	Description
Mean Time to Repair (MTTR). Also called Mean Corrective Maintenance Time ($\overline{M}_{ct}$)	For a sample of repair actions, a composite value representing the arithmetic average of the maintenance cycle times for the individual actions.
Maximum Active Corrective Maintenance Time (M_{max})	That value of maintenance downtime below which one can expect a specified percent of all corrective maintenance actions to be completed. Must be stated at a given percentile point, usually the 90^{th} or 95^{th}. Primarily related to the lognormal distribution.
Mean Preventive Maintenance Time ($\overline{M}_{pt}$)	A composite value representing the arithmetic average of the maintenance cycle times for the individual preventive maintenance actions (periodic inspection, calibration, scheduled replacement, etc.) for a system.
Median Active Corrective Maintenance Time (M_{ct})	That value of corrective maintenance time that divides all downtime values for corrective maintenance such that 50% are equal to or less than the median and 50% are equal to or greater than the median.
Mean Active Maintenance Time ($\overline{M}_{ct}$)	The mean or average elapsed time needed to perform maintenance (preventive and corrective), excluding logistic and administrative delays.
Mean Time to Restore System (MTTRS)	For highly redundant systems, the mean or average time needed to switch to a redundant backup unit.
Mean Downtime (MDT)	The mean or average time that a system is not operational due to repair or preventive maintenance. Includes logistics and administrative delays.
Maintenance Labor Hours per Hour or per Cycle, per Action or per time period, e.g. Month	A labor hour factor based on operating or calendar time, maintenance actions, or operating cycles.
Maintenance Ratio (MR)	A measure of the total maintenance labor burden required to maintain an item. It is expressed as the cumulative number of labor hours of maintenance expended in direct labor during a given period divided by the cumulative number of life units during the same period.
Percent BIT Fault Detection (Pfd)	The ratio of the number of faults detected by the system BIT to the total number of faults experienced by the system, expressed as a percent.
Percent BIT Fault Isolation (Pfi)	The ratio of detected faults that was unambiguously isolated to a single replaceable unit or other rule identified in the procurement specification (i.e. to a group of 3 or less replaceable units).
Percent False Alarms (Pfa)	The ratio of detected (indicated) failures to the total indicated failures plus verified failures, expressed as a percent.. For both DT and OT communities, this parameter has now been replaced by MOHBFA
Mean Operating Hours between False Alarm (MOHBFA)	The mean or average time (i.e. operating hours, flight hours) between indicated (detected) faults where no fault could be confirmed. (e.g. False alarm)

3.2.4 Availability Metrics

Chapter 1 stated that availability is a measure of the degree to which an item is in an operable state and can be committed at the start of a mission when the mission is called for at an unknown (random) point in time. Simply, availability is the probability that the system will be able to perform its mission profile (or some part of it) when required. Availability is primarily a

function of how often failures occur or corrective/preventive maintenance is required (reliability), and then how quickly indicated or recorded failures can be confirmed and repaired or preventive maintenance performed (maintainability). Factors such as the logistics and maintenance support can also affect availability, but these aspects are outside the intended scope of this guide, therefore for further reference on the effects of logistics and maintenance support consult:

- **Department of Defense Handbook: Acquisition Logistics**, MIL-HDBK-502, USAMC Logistics Support Activity, May 30, 1997.
- **Designing and Assessing Supportability in DoD Weapon Systems: A Guide to Increased Reliability and Reduced Logistics Footprint**, Prepared by the Office of Secretary of Defense, February 12, 2003.

More specific ways of defining availability can depend on the nature of the system:

- The probability that a system is in an operable state at an arbitrary point in time.
- The proportion of time that a system is in an operable state.
- For aircraft, sortie generation rate can be used.

As with reliability, availability requires a description of how the item is to be used. This description includes how often the item will be operated, maintenance policy, maintenance concept, and adequacy and responsiveness of the supply system. Availability is one of the most widely used parameters in system acquisition and also one of the most difficult to understand because of the many factors involved in measuring it. Availability is affected by how often a system becomes unusable and how long it takes to restore it to service. A system that never experiences any failures or requires any preventive maintenance would always be available for use; regardless of how long any maintenance action might take. Conversely, if corrective or preventive maintenance could be performed in zero time, the system would always be available for use (although mission reliability might not be acceptable). In either case, availability would be a perfect 100%. In practice, the availability of systems is never perfect because failures do occur and it always takes a finite (non-zero) amount of time to make repairs or to prevent them.

If an ideal support system, with infinite spares and maintenance personnel, could be developed, then availability would be a function only of the number of failure repair actions in a given time interval and the time it took to make repairs or remove and replace a failed item, and the time required for preventive maintenance actions. That is, it would solely depend on the levels of reliability and maintainability inherent to the system.

Since the support system is never ideal, other factors affect the availability of systems in operational use. These factors include the availability of spare and repair parts, tools, support equipment, and maintenance personnel; the skill and knowledge of maintenance personnel; and the throughput capacity of repair facilities. Nevertheless, need for repair and time to repair, reliability and maintainability are key design factors that determine the maximum level of availability that a system can achieve.

For non-repairable or one-shot systems availability is often measured in terms of operational readiness since maintainability measurements are not applicable. Operational readiness is the

probability that the system is either available at the beginning of the mission or can be brought to operationally ready state by the beginning of the mission within a prescribed period of time.

3.2.4.1 Elements and Measures of Availability

As already discussed, many elements determine the level of availability. Depending on what elements are being considered, different methods for measuring availability are used. The basic elements that determine availability can be divided into three categories: failures, maintenance, and resources. Table 3-3 describes these three categories.

TABLE 3-3: Categories of Elements Determining Availability

Category	Description
Reliability	Mission and non-mission failures that require repair. The lower limit on the number of failures is determined by the inherent level of reliability deigned and built into the system. However, poor manufacturing, inadequate maintenance, operations in conditions beyond those specified for the design, and "acts of God" can increase the number. In addition to determining a lower bound on failures, the reliability characteristics of an item should be considered in determining the number and types of preventive maintenance actions that are either required or are economically desirable.
Maintainability and Maintenance	Maintenance actions include both corrective maintenance (i.e., repairs as a result of failures) and preventive maintenance. The time required for and inherent ease and economy with which a maintenance action can be performed is a direct function of how well maintainability was considered in design. The length of time required for a given maintenance action is also affected by the skill of the maintenance personnel, the maintenance policy and concept, and effectiveness of maintenance manuals and procedures.
Resources	Resources include the number of maintenance personnel available as well as the number and availability of spare and repair parts, support equipment, repair manuals, tools, etc.

3.2.4.2 Inherent Availability

When only the effect of design on availability is being considered, then Inherent Availability, or A_i, is the appropriate measure. The equation usually associated with A_i is given in Table 3-4. This equation is called the steady-state equation for inherent availability. The steady-state equation is only appropriate over long periods of time, when the system reaches steady state. When considering a short duration, such as a warfighter's three or seven day mission, the inherent availability equation will not be applicable as steady state is not likely to be achieved. Thus inherent availability should be calculated using simulation for this example.

3.2.4.3 Operational Availability

When the effects of design and the support system on availability are being considered, then Operational Availability, or A_o, is the appropriate measure. The equation usually associated with A_o is given in Table 3-4. This equation is called the steady-state equation for operational availability. The steady-state equation is only appropriate over long periods of time, when the system reaches steady state. When considering a short duration, such as a warfighter's three or seven day mission, then availability will most likely not achieve steady state. Therefore, it

would be inappropriate to use this closed form equation for operational availability. Simulation should be used to calculate operational availability for this example.

TABLE 3-4: **Comparing Inherent and Operational Availability**

Measure	Equation (Steady-state)	Factors
Inherent	$A_i = \frac{MTBF}{MTBF + MTTR}$	MTBF is the mean time between failures. MTTR is the mean time to repair and is a function of maintainability. It includes: • Diagnostic time (time to detect and isolate failure) • Time to repair (in-place repair or removal and replacement of the failed item) • Time required to validate the repair (e.g., functional check)
Operational	$A_o = \frac{MTBM}{MTBM + MDT}$	MTBM is the mean time between maintenance. MTBM includes all maintenance actions, including repairing design/manufacturing failures and maintenance-induced failures, performing preventive maintenance, and other actions (e.g., remove an item to facilitate other maintenance). MDT is the mean downtime and includes the time: • For platform preparation (connecting safety devices, external power, air conditioning, support equipment etc.) to conduct maintenance. • For maintenance instruction consultation • During which maintenance is being performed • During which a maintenance action is awaiting parts, personnel, or equipment • Diagnostic time (time to detect and isolate failure) • To repair (in-place repair or removal and replacement of the failed item) • Required to validate the repair (e.g., functional check) • Due to administrative and other logistics delays

Availability is measured in terms of uptime and downtime. After a system is developed and is put in test or in field use, the number of hours that the system is "up" (i.e., capable of performing all required functions) and the total number of hours that it was supposed to be up in any given calendar interval can be measured. The operational availability can then be measured by dividing the time the system was up by the total time it was supposed to be up.

Operational availability can be described by the following equation:

$$A_o = \frac{\text{Uptime}}{\text{Total Time}}$$

- Uptime is the time during which the system was capable of performing all required functions in a given calendar interval.
- Total Time is the total time during which the system was supposed to be up during a given calendar interval. (Total Time = Uptime + Downtime)
- In practice Downtime has at least two components. The first component is the time waiting for spare parts to arrive via the supply chain, called logistic down time. The second component is the time to repair, which may consist of maintenance time (i.e.,

MTTR), and in addition, any time that is spent in the queue waiting for the maintenance persons to begin working. (Downtime = Active Repair Time + Administrative Delay Time + Logistics Delay Time where the administrative and logistics delay times are also referred to as Operational Availability).

Although this equation is an accurate expression of A_o for a system as observed in operation, it has two major deficiencies:

- Uptime and downtime can only be measured for a system in an operational inventory and are not measurable for a system in development.
- If the measurement period is short compared with the reliability and maintainability parameters of the system, the equation will not give a true indication of the availability being achieved.

Table 3-5 illustrates the impact that reliability (as one element of Uptime) and maintainability (as one element of Downtime) can have on operational availability. The table represents R&M factors that should be considered for specific parameters having an effect on A_o, and, therefore, provides the user with alternatives to obtain greater inherent (designed-in) operational availability, or solutions for unacceptable operational availability, in the customer's field environment.

TABLE 3-5: Impact of R&M on Operational Availability

Reliability Parameter (e.g., MTBF)	Maintainability Parameter (e.g., MTTR)	Impact on Operational Availability	R&M Considerations
Increase	No Change	Increase	Operational availability can increase due to: • Improved design reliability (hardware and software) • More efficient screening tests at product manufacturer • Reduction in the number of induced failures • Reduction in the number of incidents where an apparent failure cannot be verified • Increased time between preventive maintenance actions
Decrease	No Change	Decrease	Operational availability can decrease due to: • Design modifications having negative impact on reliability • Reduced efficiency of screening tests at product manufacturer • An increase in the number of maintenance-induced failures • An increase in the number of unverified failures • Shorter time between preventive maintenance actions
No Change	Increase	Decrease	Operational availability can decrease due to: • Use of lower-skilled repair personnel • Increase in delays due to paperwork or unavailability of repair parts • Reduced efficiency in detecting and isolating failures during repair • Improper correlation between product performance limits and test equipment measurement limits • Induced failure caused by mishandling of the product during repair
No Change	Decrease	Increase	Operational availability can increase due to: • Increased training and/or learning by repair personnel • Readily available repair parts and reduction of paperwork • Increased efficiency in correctly verifying and isolating failures • Proper handling of product during repair • Improved correlation between product performance limits and test equipment measurement limits

3.3 Organizations and People

To understand and document user needs and constraints from a government and industry perspective, warfighters, users, developers, technologists, reliability engineers, designers, testers, budgeters, and sustainers must be involved in a meaningful way. During Concept Refinement and Technology Development, even before an acquisition program office is assigned, a knowledgeable individual, responsible for RAM, is needed to support development of the

conceptual system (and alternatives), formulate the RAM Rationale, structure RAM requirements in the request for proposal, and bring relevant RAM "lessons learned" to the program. An Integrated Product Team (IPT) provides a communication forum for achieving an understanding in this early stage and later assessing progress to achieve RAM performance throughout the acquisition life cycle. Industry plays a crucial role in achieving RAM performance and is often a partner during this stage of defining a new capability and assessing the feasibility of current technology to meet material needs. During this phase, the operational test agency drafts an evaluation concept paper, which begins to formulate the strategy for evaluating the new capability.

3.4 Supporting Information

The key pieces of information needed during this first step are: field experience with existing systems, current logistic and manpower requirements, user desires, technical possibilities and experience. Much of this information comes in the form of the Initial Capabilities Document (ICD), Analysis of Alternatives (AoA) Plan, exit criteria for the various acquisition phases, and alternative maintenance and logistics concepts. With all of the various participants and information supporting Step 1 it is best to establish a forum in which a careful and objective discussion of the supporting information can be conducted. A formal document that provides the rationale is a very helpful way to insure the discussion is complete. It is important to identify the limitations of the current system and its support concept, to define the current RAM burden, to propose and document desired changes, and to identify the design constraints (from manpower, training, etc.).

Designing for reliability will require a careful and complete use profile that includes wartime usage rates, peacetime usage, the spectrum of environments in which the system could be used, non-operating time and conditions, and the operational constraints of the maintenance and supply systems. The total life cycle environment can include:

- Storage
- Shipping and handling
- Installation/Deployment
- Operation
- Maintenance

Characterizing these environments is important supporting information. Characterization is the process of identifying the relevant parameters (temperature, humidity, vibration, etc.) of the environments and the realistic ranges of values and durations for these parameters.

3.5 Tools and Activities

The activities that should be conducted to understand and document user needs and constraints include:

1. Development of a conceptual system,
2. Consideration of COTS/NDI
3. Construction of a representative system model,

4. Preliminary assessment of RAM using the system model and expert judgment,
5. Formation of the RAM Rationale,
6. Conception of the RAM Program Plan (RAMPP), and
7. Development of the RAM Case.

As part of the systems engineering approach to the acquisition process the following technical reviews will be utilized within Step 1: Understand and Document User Needs and Constraints to ensure that RAM is achieved. The purpose of these reviews is to provide the Program Manager with an integrated technical assessment of program technical risk and readiness to proceed to the next technical phase of the effort. Results of these reviews should be used to update the Systems Engineering Plan.

- Initial Technical Review (ITR)
- Alternative System Review (ASR)
- System Requirements Review (SRR)
- Integrated Baseline Review (IBR)

3.5.1 Development of a Conceptual System

The Joint Capabilities Integration and Development System (JCIDS) analysis implements a capabilities-based approach that requires a collaborative process that utilize joint concepts and integrated architectures to identify prioritized capability gaps and integrated doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) solutions (materiel and non-materiel) to resolve those gaps. The first step in the JCIDS process is the sponsor-led performance of a functional area analysis (FAA), which identifies operational tasks, conditions, and standards needed to achieve military objectives. The output of the FAA is the tasks to be reviewed in the follow-on functional needs analysis (FNA). The FNA is also sponsor-initiated and its purpose is to assess the ability of the current and programmed joint capabilities to accomplish the tasks that the FAA identified within the full range of operating conditions while adhering to the designated standards. The FNA will produce a list of capability gaps or shortcomings that require solutions as well as identifying the time frame in which those solutions are needed. The third step of the JCIDS process is the functional solution analysis (FSA), which is an operationally based assessment of potential DOTMLPF approaches to solving/mitigating one or more of the capability gaps/needs identified in the FNA. The results of the FSA are potential needs solutions, which include: (1) integrated DOTMLPF changes; (2) product improvements to existing materiel or facilities alone; (3) adoption of interagency or foreign materiel solutions that have limited non-materiel DOTMLPF consequences; and (4) new materiel starts that have limited non-materiel DOTMLPF consequences.

The documentation developed during the JCIDS process provides a formal communication of capability needs between the operator and the acquisition, test and evaluation, and resource management communities. The first product of the JCIDS process is the Initial Capabilities Document (ICD). The ICD may include the baseline RAM and supportability characteristics of current capability, the operational modes and summary mission profile for the new capability, the logistics support concept for the new capability and inputs to the request for proposal to contract for development of the new capability. The ICD becomes the basis for development of

the Capabilities Development Document (CDD). The CDD aids the translation of RAM into the broader context of force structure, mission success, cost/budgets, and readiness specifically in developing RAM specifications. The purposes of developing reliability goals (or "requirements") are to:

- Establish product-level specifications that will ensure the RAM performance of the system will meet the users' functional needs.
- Allocate the system-level requirements down to a level (i.e., subsystem, component, or assembly level) meaningful to the design and manufacturing engineers.

User needs are expressed in operational terms that explicitly or implicitly address many factors influencing RAM. Some of these factors are beyond the control of the designer, whereas others are not design-related, but instead are determined by policy, funding, and other non-technical issues. It is important, then, that user needs be translated into design (specification) parameters that are meaningful to a designer, and, if met, will ensure that the desired field performance will be achieved. Designers must account for five sets of factors relating to the system's mission profile that will affect RAM performance. The mission profile includes a definition of functions the system will perform; a description of the environments in which the system will be stored, transported, operated, and maintained; a statement of the RAM and the skill level requirements of users; and a definition of system failure relative to its function. The five mission profile factors include:

- Inherent Design Factors: The design characteristics of the system determine its RAM performance (i.e., the frequency of failures and the time required to fix these failures affect system availability, mission reliability, and demand for maintenance). Resources like spares and labor will also affect inherent design characteristics. Inherent factors are a function of the time and money available for design and test, the robustness of design analyses, the available technology, and other competing requirements.
- Other Performance Factors: Trade-offs between competing requirements are made to reach "optimal compromises." For example, it is extremely difficult to optimize both of two inversely related engine requirements for an aircraft, such as high reliability and high thrust-to-weight ratio. A trade-off is made that produces an engine design that is reliable enough to ensure safety and an acceptable aircraft availability, but which still has an adequate thrust-to-weight ratio.
- Support Infrastructure Factors: The operating and support concepts will affect RAM performance. Specialization of skills and other personnel policies will affect the operating and support concepts. The number of required spares (as well as pipeline times) within the support concept can be directly affected by the maintenance concept (i.e., levels of repair, a single location/base performing maintenance for several locations, etc.) and policy (i.e., cannibalization, safety, inspection, etc.). Spares buys are determined not only on the basis of the maintenance concept and reliability, but on available funding, economic order quantities, and other factors.
- Operating Concept Factors: The RAM performance of any system can and will be affected by the operations concept that will govern the system when it is deployed. The operations concept must accurately account for the types of mission that the system will be subjected to, deployment requirements, the need for operations at austere bases, etc.

- Operating Environment Factors: RAM performance is obviously a function of the type and severity of the environment in which it will be operated. Operations from bases in the desert will impose different stresses on a system than those imposed by operations for bases in tropical areas. Sand, dust, salt water, heat, cold, humidity, thermal and mechanical shock, and vibration will directly affect the system's RAM performance.

Systems engineering is a logically sequenced, consistent set of technical activities that translates a customer's needs and requirements into a balanced solution. These technical activities are outlined in Chapter four of the Defense Acquisition Guidebook. Systems engineering emphasizes the concept of concurrency, in which the requirements and approach for test, production, and logistics support, are integrated with those for development so that the solution is best suited for the entire life cycle. The fundamental approach to systems engineering involves the integration of all factors (i.e., five sets above that affect RAM) in a coordinated effort to provide a balanced product or service solution. Figure 3-2 illustrates the requirements of the systems engineering process.

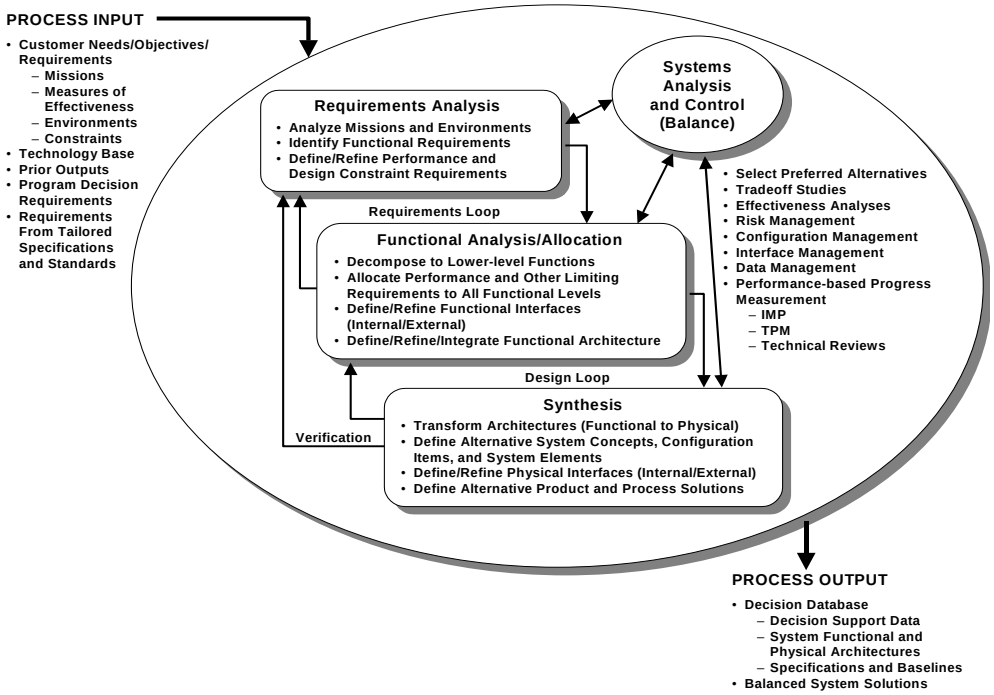


FIGURE 3-2: Systems Engineering Process Requirements

The Program Manager for the capability needs to implement a sound systems engineering approach to translate approved operational needs and requirements into operationally suitable blocks of systems. The top-down, iterative approach will consist of a requirements analysis, functional analysis and allocation, design synthesis and verification, and system analysis and control. Systems engineering should be an integral part of design, manufacturing, test and evaluation, and support of the product as systems engineering attempts to balance performance, risk, cost, and schedule. These activities are shown throughout the Integrated Defense Acquisition Technology & Logistics Life Cycle Management Framework, using V Charts for each acquisition phase.

The overwhelming measure of a successful system is that it works, is reliable, available, and maintainable, and is cost-effective over time. The conceptual system lays the foundation for achieving this success, therefore decisions made as the user needs and constraints are manipulated into this conceptual system can make or break the ability of the deployed system to achieve desired RAM performance.

3.5.2 Consideration of COTS versus New Development

Use of commercial items offers significant opportunities for reduced development time, faster insertion of new technology, and lower life cycle costs. COTS items are usually less expensive to buy (larger customer base), quicker to obtain (no development), and usually incorporate the latest technology (and are regularly updated with new technology). These advantages are very attractive. However, COTS should not be blindly used in military applications without considering possible problems and disadvantages. Particular attention should be paid to the intended usage environment and understanding the extent to which this differs from (or is similar to) the commercial usage environment; subtle differences in usage can have significant impact on system safety, reliability, and durability. Table 3-6 lists some of the problems and disadvantages of COTS related to RAM performance.

TABLE 3-6: Potential RAM Problems/Disadvantages of COTS.

Factor	Discussion
Environment	If the environment of the military application is more severe than the commercial application, reliability may be significantly less in the military environment.
Integration	COTS items may require new and different support requirements, i.e. special support equipment, item interface adaptors, the use of materials or fluids that are currently banned in that service etc. The acquisition activity and user should conduct a thorough analysis and risk assessment of integrating the COTS item into the user's environment.
Maintenance	For a true COTS item, the only military repair is to remove the failed item from the system and replace it with new. The manufacturer must do all maintenance of the COTS item for two reasons: • Usually commercial suppliers will not sell the data needed to repair the item. To obtain such data, the government usually has to do reverse engineering and generate the data at considerable cost. • Government attempts to do maintenance will normally void the warranty and the supplier will may refuse to incorporate whatever technology updates are being made to new production items in the modified items.
Long-term support	Suppliers not obligated to support an item for a specific length of time. They may not provide much notice of plans to discontinue supporting an item. The government may: • Choose to make a life-of-type buy. • Use reverse engineering to develop a “make-to-print” specification and develop repair procedures. • Identify another COTS item that is a “suitable substitute.”
Warranty	Warranties of commercial items are usually null and void if the user attempts to modify or repair the item. The user should determine if existing policy and procedures are adequate for the return of warranted items or if new policy and procedures are needed, especially for items that fail while the system is deployed to an overseas location.
Integrated Diagnostics	Proposed COTS systems and units need to provide system status and functional information in compatible format to on-board and off system maintenance environments

3.5.3 Representative System Model Construction

Once sufficient system requirements have been identified, a basic top-level RAM concept model can be developed with data from similar technology, analogous developments, and extrapolations where necessary.

The system model becomes the framework for analyzing, allocating and achieving RAM requirements. Computer based models facilitate the computation of system reliability and maintainability. Creating a representation (usually pictorial, graphical, or mathematical) of the system allows designers to estimate the expected system RAM, perform trade-off analyses among competing design on the basis of RAM, and to identify weaknesses in the design. Models also can be used in the requirements development process and to allocate system-level reliability requirements to lower assembly levels. Models provide a means to determine the degree of appropriate fault tolerance as well as insights into the impact of lower-level failures on the system.

The most common model used for reliability is the Reliability Block Diagram (RBD). An RBD consists of blocks that represent individual items. The represented items can be components, subassemblies, assemblies, subsystems, and so forth. The blocks are connected through topologies, which represent the relationships among the blocks from a reliability perspective. The two basic types of topologies are series and parallel. In a series configuration, the failure of any block causes the failure of the system defined by the items. In a parallel configuration (built in redundancy), as long as a given number of alternative paths are functioning, the system will function. An RBD can consist of series and parallel topologies and combinations of these two basic topologies. This deals well with failure modes, but may be difficult to use when exploring degraded performance. A much more in-depth discussion of RAM modeling is included within Chapter 4 of this guide.

3.5.4 Perform Preliminary RAM Assessment

RAM assessment is the continuing process of determining the value of the level of RAM being achieved at any point in time. The ability to make an assessment, and the quality of the assessment, depends on the information available. Therefore, preliminary RAM assessment which are based primarily on historical data are usually very rough estimates, but as the acquisition program progresses, knowledge of expected field RAM performance becomes more refined as system RAM models move from qualitative inputs to more quantitative inputs.

Although preliminary assessments are limited in their accuracy, these early assessments can and should be used to determine technological feasibility, refine requirements, improve the concept model, support design trade-offs, identify design weaknesses for improvement, mitigate failure modes and track progress toward achieving needed RAM capabilities. Since preliminary assessments should not be considered accurate measures of the expected operational RAM performance the RAM estimates should not be used prematurely as the sole basis for major decisions such as sparing levels and/or budgeting.

Assessment at early stages of development is achieved through eliciting and applying expert judgment, comparative analysis and system modeling. Initial estimates of RAM for the various system blocks should also be conducted at this time if the information is available. Some uses for assessments have already been mentioned. Table 3-7 lists many applications for assessments.

TABLE 3-7: Applications for RAM Assessments

Application	Timing	Cautions
Compare established requirements with state-of-the-art feasibility	Part of process of determining system requirements	Optimistic requirements drive costs and increase program risk
Provide a uniform basis for proposal preparation, evaluation, and selection	Guidance in preparing assessment needed in RFP	Incorrect or unrealistic assumptions allow bidders to make optimistic assessments
Evaluate alternative choices of parts, materials, and processes	Begin in earliest stages of design Continue through life cycle	Be consistent in method used and use for comparison only. Early emphasis is on design improvement, not absolute measurement
Provide a quantitative basis for design tradeoffs		
Identify and rank potential problem areas and suggest possible solutions		
Provide guidance in budget and schedule decisions	When amount and quality of data justify – an assessment based on test data preferred over one based solely on analyses	Assessments, especially analytical predictions, should never be sole basis for major decisions
Provide a basis for selecting economic warranty period		
Determine spares requirements		
Determine compliance with requirements	When design is stable	Usually by formal demonstration/ acceptance testing – most "accurate" assessment prior to deployment to the extent that the actual operating environment can be simulated

Assessment begins at the earliest program stages and continues throughout the life cycle (Figure 3-3). The fidelity of the assessment increases as analyses are performed, design evolves, and data is collected from tests at component, subsystem, and system levels, and then from operation.

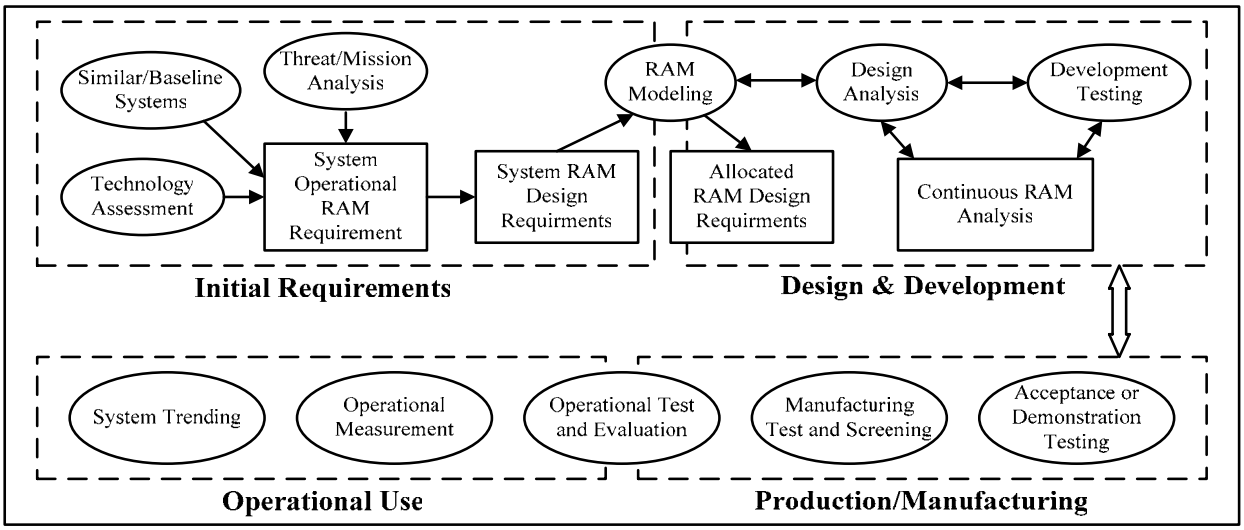


FIGURE 3-3: Assessment is a Process that Begins with Developing Requirements and Continues throughout the Design, Development, Manufacture, and Use of a System

One of the most basic RAM assessment techniques utilized is the similar system or comparative analysis method. Comparative analysis has been developed as a means of performing a preliminary assessment of a system before the system is fully defined. At the conceptual stage in system development there is little specific RAM information available, which forces analysts to base their analysis on assumptions and similar systems. The primary characteristic of the comparative analysis is to evaluate new equipment with information and RAM characteristics for similar equipment already in use. This evaluation should be done at the system, subsystem, assembly or component level depending on where the analogies are most appropriate. The assumption that becomes the foundation of this method is that equipment will behave or evolve in a predictable manner, causing similar equipment to exhibit similar reliability. Factors that must be considered include system design, mission performance needs, manufacturing, physical comparison, operational employment and environmental factors, and process similarities. If possible, the data collected from existing equipment should have similar environmental and operating conditions, but there are methods available to convert the data if the new system has different environmental and/or operating conditions. If COTS/NDI equipment is being considered, the comparative analysis needs to consider the problems/disadvantages presented in Table 3.6. A COTS item may have considerable R&M field experience but the analysis needs to address differences in environment in commercial or other applications. With modern equipment, particularly those employing new technologies, though it may be difficult to find "similar" designs (whether electronic, mechanical / hydro-mechanical, or structural) it is usually possible to compare functions.

The primary uses of a comparative analysis are to:

- Identify reliability and maintainability related risk areas and implement failure mitigation and technology development efforts so that user needs are met.
- Calculate initial reliability and maintainability estimates and redesign for reliability and maintainability.

The following guidelines are provided for completing a comparative analysis.

1. Define new equipment relative to type, operational mode summary and mission profile, and its intended operating environment. Other characteristics may also be helpful, such as size and output requirements, support concepts and technology differences.
2. Clearly define the existing equipment that is being considered the equivalent of the new system. Note obvious differences between the existing equipment and proposed system.
3. Collect any available reliability and maintainability data on the existing equipment, and note differences between old and new systems so that adjustments can be made to the reliability and maintainability data.
4. With the assumption that similar equipment will exhibit similar reliability in similar environments, determine the level of reliability that the new system can be expected to achieve. The accuracy of this estimate depends on the quality of the available reliability data, and the ability of the analyst to incorporate the necessary adjustments to the data that will reflect the true reliability potential of the new system.

Chapter 4 identifies additional information concerning RAM assessment methods, beyond comparative analysis, that should be used as the conceptual design matures.

3.5.5 Formulate RAM Rationale

RAM requirements for a system need to be developed with care. Unrealistically high requirements will drive costs and inappropriately skew the development program. Requirements set too low will lead to poor field performance and high operations and support costs. RAM requirements, like all requirements, need to be carefully balanced between technological feasibility and operational needs and desires. In addition, developers may need to trade-off some performance requirements to optimize overall system performance.

The requirements development process takes all inputs from relevant stakeholders and translates the inputs into technical requirements. DoD Lead Systems Engineers primarily respond to the JCIDS documents (ICD, CDD, and CPD) that identify gaps in need of a materiel solution. The Program Manager should work with the user to establish and refine operational needs, attributes, performance parameters, and constraints that flow from JCIDS-described capabilities and then ensure that all relevant requirements are addressed. Together with the user, the Program Manager should translate "customer needs" into the following program and system requirements:

- Performance parameter objectives and thresholds,
- Affordability constraints,
- Scheduling constraints, and
- Technical constraints.

With these factors in consideration, there is significant benefit for a project to have a clearly justified RAM Rationale that provides insight into the basis of the stated requirements. Documentation of the RAM Rationale provides a record of the basis of the RAM requirements development.

The RAM Rationale documents the results of analyses conducted to achieve RAM within Step 1: Understand and Document User Needs and Constraints. This information becomes the basis for developing RAM related portions of the request for proposal and contract(s) to design, develop, test, produce, deploy and operate the capability. Documentation of the RAM Rationale is strongly recommended so that clear and concise explanation of the RAM requirements is available to measure the attainment of these goals in the system being designed and manufactured by the contractor. The RAM Rationale also supports: trade-off studies to balance cost and performance; development test planning and evaluation; and operational test and evaluation. The RAM Rationale expresses quantitative measures of the levels of reliability, availability and maintainability needed by the user, in operational terms; as well as corresponding quantitative measures in contractual terms for use in the request for proposal (RFP) and contract. The core elements of a comprehensive RAM Rationale are:

- Operational Mode Summary: Description of the mission profile, the required functions, mission cycle and the environmental/operational conditions under which the system is expected to be used. The operational mode summary identifies the relative frequency of

the various missions or the percentage of the systems involved in each mission. It also expresses the percentage of time the equipment will be exposed to each type of environmental condition during its intended lifetime. The operational mode summary will not specify unscheduled downtime.

- Mission Profile: A time-phased description of the operational events and environments an item is subject to from the start to the end of a specific mission. Tasks, events, durations, operating conditions, and environmental conditions are identified for each mission phase. The mission profiles should state specific quantities of operation (i.e., hours, rounds, miles, or cycles) for each mission-essential function within the mission.
- Fault/Failure Definition and Scoring Criteria: Traditionally a fault is defined as any non conformance which requires an unscheduled maintenance action to correct it and a failure is defined as the loss of function. Clear, unequivocal definitions of fault and failure should be established for the system/equipment in relation to its functions and performance parameters. This is important in terms of providing the basis for a clearly defined scoring criteria and a contractual framework acceptable to both the purchaser and the contractor for the proper accounting of faults and failures (which will allow contractually meaningful RAM data to be derived). The contract should clearly state agreed failure definitions and specify any conditions under which faults are not the contractors liability such as battle damage, operations outside agreed upon limits, and user negligence. Fault/failure definitions are also addressed in the RAMPP (Section 3.5.6.)
- Program Management Office (PMO) Analysis: The primary purpose of the PMO analysis is to identify overall design and support options and levels of reliability and maintainability performance that are not only technically achievable, but that have acceptable cost, schedule, and risk characteristics proportionate to the user's RAM goals and constraints. A baseline comparison system (may be an actual system or hypothetical system comprised of assemblies having technology and complexity similar to those of the proposed capability) is used to estimate the reliability and maintainability characteristics of the proposed capability. The designer conducts a comparative analysis (discussed earlier), state-of-the-art analysis, and materiel developer proposal analysis as part of the RAM Rationale. The state-of-the-art analysis identifies design improvements of the proposed capability in relation to the baseline comparison system. The PMO analysis evaluates alternatives (i.e., Analysis of Alternatives or AoA) based on both performance and economic considerations to determine which proposal is superior in terms of realistic and cost-effective improvements to the top drivers of mission failure rate, manpower, and parts cost.
- User Representative Analysis: The user representative analysis sets the goals for the RAM program and validates the ability of the RAM requirements to successfully accomplish the mission. This analysis addresses operational effectiveness and supportability as well. The supportability analysis should address manpower requirements and administrative and logistics downtime (ALDT).
- Logistics Support Analysis: The logistics support analysis is the selective application of scientific and engineering efforts in an effort to assist in the compliance of supportability and integrated logistics support objectives. This analysis should also define how the proposed capability will have to integrate into the user's maintenance environment. In the case of Naval Aviation, this can mean an Automated Maintenance Environment

(AME) where a functionally complex ground station processes recorded data from the overall system and integrates numerous maintenance activities such as operator debrief, maintenance control functions such as configuration management, component accumulated time (i.e. flight hours, operating hours, cycles etc.) before removal, accumulates engine life use indices, vibration analyses (particularly on new Helicopters) and others. For such an integration to work, the RAM design team and the Logistics team will have to collaborate closely. A supportability strategy describes the overall program as well as the program requirements, tasks, and milestones. An interface should be developed between the personnel supporting the RAM requirements and those providing the supportability strategy to ensure that both sets of objectives can be effectively met.

- RAM Parameters: The purpose of the RAM parameters portion of the RAM Rationale is to declare: (1) all of the RAM parameters being used; (2) the procedure for calculating the parameter estimates; and (3) the underlying assumptions used as a basis for the calculations. The RAM parameters address mission success, operational readiness, maintenance manpower, and logistic support costs.
- Required Operational Capability Update: This update allows for any final adjustments that may be necessary to the RAM requirements prior to the release of the request for proposal (RFP). This final update takes advantage of the additional information provided by prospective contractors in their comments/feedback on the draft RFP.
- Translation to Technical Requirements: The translation of the RAM requirements to the contractual technical requirements sets the target for the proposed capability. All future design and development efforts will be focused on achieving these technical requirements. Translation techniques include applying: (1) a formal translation (via conversion equations), (2) a systems engineering approach (based on contractual definition of time and failure), (3) a policy, (4) cost, schedule and other constraints (what RAM can budget afford?), (5) and ask the contractor (what is the best that can be done?).

The RAM Rationale also:

- Explains why the RAM levels are needed and how they interact and relate to other aspects of the capability (such as performance, force structure, affordability, support concept/plan, logistics footprint); and
- Documents RAM performance of current capability to provide the basis for assessing measurable improvements to mission capability and operational support.

The RAM Rationale may consider certain qualitative RAM requirements such as:

- Requirements for the employment of certain materials/electronic components,
- Requirements for the observance of specific design and safety regulations,
- Transportation, handling, and storage requirements,
- Requirements concerning setup/arrangement/assembling of the units,
- Requirements concerning accessibility/exchangeability, and
- Application of RAM Lessons Learned for all these areas.

3.5.6 Construct Preliminary RAM Program Plan

The RAM Program Plan (RAMPP) is the means through which activities and progress in satisfying customer RAM requirements are monitored and controlled. The plan provides clear traceability to original customer RAM requirements and also shows activities together with any applicable success criterion relating to the generation of the associated RAM Case. The plan should be traceable to the broader planning activity for both system support and the acquisition/delivery arrangements for the overall fielded system. The plan should also be integrated appropriately with relevant system development and quality planning. The customer and supplier should mutually agree upon the plan before implementation. The RAMPP should be subjected to appropriate management reviews during its period of use as well. During Step 1 the plan is in a preliminary state and is utilized more as a planning tool than a documented plan to adhere to as it may be in subsequent steps.

The RAMPP identifies the RAM activities, functions, processes, test strategies, measurement, data collection, resources and schedule required to ensure RAM system maturation. The RAMPP should demonstrate both contractual and operational requirements at requisite confidence levels (when appropriate). The RAMPP will identify the management and organizational structure of those responsible for RAM activities. The RAMPP provides information on proven design techniques that will be used in the program; test strategies (both for identifying/mitigating failure modes and for requirements demonstration); a description of the activities and processes which will ensure retention of requisite RAM levels in production; and future plans for monitoring field RAM as well as the tools required to conduct corrective actions (design and/or manufacturing) in the field. In short, the RAMPP is the foundation upon which all four of the key steps to achieving a reliable, available, and maintainable system are based. The RAMPP content addresses these areas.

- System Description: Includes a technical description of the system with a thorough description of the system hardware and software elements, expected operational requirements, and how the operational requirements relate to system RAM. The system description should identify for the various equipment used within the system whether the contractor or government will supply the equipment. If applicable, historical information should be provided for legacy systems that are being replaced or upgraded including a comparison of the designs. If data exists that can be used to support current RAM tasks or activities from these legacy systems the data should be analyzed and reviewed to determine how it can best support the development of the proposed system/capability.
- RAM Requirements: Clearly defines RAM requirements for proposed system/capability as well as an explanation of the translation of contract requirements to operational requirements. Usage conditions and the expected operational environments in which the equipment will be operated are defined in this section. If applicable, contract warranty provisions or RAM-related contract incentives should be defined with the RAM requirements also.
- Design Guidelines, Tasks and Analysis: The design guidelines that will ensure that RAM is "built in" to the system/capability must be documented within the RAMPP. Achieving design assurance through an analysis of proposed conceptual designs and how they will satisfy contractual requirements is addressed in this section of the RAMPP. This section

will emphasize that using the proper design tools and activities up front instead of performing extensive test validation later will ensure RAM is "built in" to the system/capability. Associated RAM tasks and analyses to maximize RAM during design and maintain this inherent RAM throughout production and manufacturing will be discussed within this section as well. Some tasks and analyses that may be outlined here include (these tasks and analyses will be further discussed in Chapter 4):

- Physics of Failure: Technique used to identify and understand the physical processes and mechanisms of failure. The purpose of the physics of failure approach is to "design out" failures prior to testing and deployment.
- Critical Items Identification/Analysis: Specifically addresses items that require special attention due to complexity, application of state-of-the-art technology, high cost, single source, or single point failure potential. The analysis will identify the special controls required for these items to reduce the risk they pose to the system/capability.
- Identification of Potential RAM Problems: Outlines the hardware, software, or procedural problem areas as well as the impacts these problems would have on system RAM. Proposed solutions or corrective action plans should be identified for each problem area.
- Software Reliability Assessment: The contractor identifies the tools (metrics) that will measure the software reliability development process. Statistical tools or models will be identified to conduct the software reliability assessment.
- Redundancy: Allows a system to continue operation after a failure (increasing availability), assuming that the functionality of the failed item can be handled by another item within the system. A redundant design should be considered for systems with critical operations or where it may be cost-effective to utilize redundancy in place of more expensive redesigns. Trade-offs to consider include cost, increased maintenance, and space and weight increases for increased RAM and performance. When considering system redundancy special consideration should be given to identifying and mitigating common cause failures (i.e., a single failure that would eliminate the redundancy of system).
- Derating: The practice of limiting electrical, thermal, and mechanical stresses on parts to levels below their specified ratings to provide additional safety margins and improve RAM.
- Thermal Management: Steady-state temperature, temperature cycling and gradients must be understood to determine methods to control these effects so as to not degrade RAM. Testing will be required to verify that these effects have been accounted for within the system.
- Shock and Vibration Control: Conduct analyses on mechanical stresses and flexing/deflections produced within equipment's intended environment to determine appropriate protection/reduction measures. Testing will be required to verify that these effects have been accounted for within the system.
- Parts Control Program: The purpose of a parts control program is to maintain/increase inherent system RAM through minimization of the varieties of parts used though the establishment of a preferred parts list. The parts selection and control program should minimize the number of part varieties, but also be flexible enough to implement new technology when advantages are evident.

- Reliability Allocation: Allocates system level requirements to subsystem, assembly, subassembly, or component levels. Preliminary reliability allocation is often based on historical baseline data with adjustments introduced based on technology type and applied usage rates.
- Reliability Prediction: Iterative analysis process that estimates reliability at the lowest level for which data is present. With the aid of reliability block diagram models these reliability estimates can be combined to derive the system level reliability prediction. Reliability predictions should be continually updated based on design changes and tests results.
- Failure Modes and Effects Analysis (FMEA): Identifies potential failure modes and their impact on the system as well as providing candidate failure modes for mitigation via corrective actions.
- Fault Tree Analysis (FTA): A top-down model graphically depicts all known events or combinations of events that can occur regarding a specific undesirable event (i.e., failure). The FTA and the FMEA tools are supportive techniques; the FTA focuses on catastrophic events at the system level, and the FMEA examines all potential failure modes regardless of severity.
- Testability Analysis: A comprehensive analysis of individual subsystem design for the use of BIT as a RAM concept to detect, isolate and report/record detected faults in the operational environment. For example, these outputs are generally provided to: the mission operator (pilot) for system/subsystem operational mission status, the maintenance control organizations to schedule and document subsequent repair actions to restore the affected system to operational status, and the RAM team through proper operational readiness reporting.
- Data Collection, Analysis, and Corrective Action System (DCACAS): Process by which system data (hardware and software indicated failures and successes) are tracked; analysis conducted to determine root cause of failure; and corrective actions identified and implemented to reduce failure occurrence.

- Test Activities and Data Collection: Testing ultimately has two purposes; (1) provide failure information about the system so that corrective actions may be developed to mature system RAM, and (2) determine compliance with RAM requirements in the form of qualification or demonstration testing. Testing should complement the design effort not replace it. The RAMPP should identify the types of test activities that will be conducted throughout the system's life cycle. Potential test activities include (once again these activities will be further discussed in Chapter 4):
  - Environmental Testing: Contractual qualification testing conducted to illustrate the equipment's ability to operate during and after exposure to environmental extremes. The government should provide within the RFP a comprehensive characterization of intended operational environments. Contractors will then develop tests to verify that system performs reliably in these environments.
  - Accelerated Testing: The purpose of these tests is to precipitate failure modes more quickly by increasing the component's/system's stresses. Accelerated life testing (ALT) usually focuses on temperature, vibration, humidity, and power stresses in either a continuous or step-wise manner. ALT is a different approach to testing that shortens the time needed to "grow" the reliability of a part using a formal growth program or to demonstrate the level of reliability achieved for an assembly. A major

requirement of ALT is to not induce failures that would not normally occur in the actual environment. The reason for this requirement is to ensure that correlation between the accelerated and normal environments is not lost so that the reliability at normal conditions can be projected based on the assessment made at the accelerated conditions. With highly accelerated life testing, HALT, there is no such requirement as HALT is conducted solely to identify the operational or destruct limits of the system. Therefore, no projection of actual reliability performance can be made based solely on the reliability observed during HALT.

- Reliability Development/Growth Testing: A test, analyze, fix, and test (TAFT) method used to obtain failure modes on prototypes and production subsystems or systems so that corrective actions can be applied to mature system RAM. This type of testing is primarily conducted during system development, but can be conducted during production and manufacturing to further mature system RAM. Sufficient test time, calendar time to implement fixes, test assets, and economic resources must be properly allocated to ensure an effectively conducted program. Properly structured, this activity addresses maturation of the integrated diagnostics capability and recognizes that integration of subsystems can be a significant source of unreliability.
- Reliability Qualification/Demonstration Testing: A fixed configuration test (no fixes allowed) exclusively conducted to demonstrate compliance with a RAM requirement with some level of confidence usually. Pre-production qualification tests and production qualification tests are examples of this test activity.
- Government Development Testing: This technical testing is similar to field environmental testing or tests to ensure achievement of technical performance, safety, supportability, durability and RAM. These tests may augment contractor system level integrated testing and operational testing. The Navy refers to government development testing as Technical Evaluation (TECHEVAL).
- Operational Testing: Equipment is subject to testing within operational environment according to the system's operational mode summary/mission profile with actual users according to approved doctrine and tactics, techniques, and procedures. The Navy refers to operational testing as Operational Evaluation (OPEVAL).

- Planning, Tracking and Assessment Methodologies: This section of the RAMPP addresses the methodologies used to measure and project RAM. Reliability growth/projection methodologies serve two purposes as they (1) measure requirement compliance and (2) identify potential problems to the developer and management early in the process. For systems that are conducting a reliability growth program, an idealized curve is constructed using all test phases that will be considered in the growth process. The idealized curve describes the overall reliability trend of the program. The objective of the idealized curve development is to ensure that reliability requirements are met with some degree of confidence at the end of the growth process. High reliability systems can have an MTBF requirement many times greater that the test time that can be allocated for demonstrating reliability of the item with some reasonable level of confidence. Testing multiple systems/items and combining results from multiple tests, even operational experience, can increase operating time and improve confidence.
- Production and Quality Control: Quality control efforts are documented during the manufacturing phase as well as during development. A quality assurance (QA) program for the prototype should be documented to address: organizational responsibilities;

engineering and planning for QA, vendor or subcontractor QA provisions, databases, inspections, material review actions for non-conforming hardware; and failure analysis. Quality during manufacturing is accomplished in much the same manner as RAM, where quality must be designed in during development through the creation of a robust design and then through process controls to ensure that the quality is not degraded.

- Follow-on Activities: This effort should focus on the identification of operations and support cost drivers and contribute to improvement efforts (i.e., candidate engineering change proposals and integrated diagnostic software updates). Field data collection in the Operations and Support phase provides information on warranty compliance and address RAM issues yet unresolved from earlier developmental and operational testing. This data may serve as a historical baseline in support of RAM requirements for future systems/capabilities.

3.5.7 RAM Case Development

From the very beginning of a new development or major modification program, the development team in conjunction with the user should employ a continuous assessment process to define and document the capability and limitations imposed by the level of reliability, maintainability, and availability with an emphasis on the operational impacts. Whereas the RAMPP takes a forward view by describing the activities together with any applicable success criterion that are to be undertaken to demonstrate that the RAM objectives have been achieved, the RAM Case provides a retrospective view. The RAM Case is a justification of the approach and documents evidence, throughout the acquisition, which verifies that the system meets its RAM requirements. This includes evidence that the RAM requirements are achievable and are properly understood by the developing organization. A well-documented RAM Case will greatly benefit any acquisition process, but the retrospective view (as compared to the forward view of the RAMPP) has historically allowed it to be neglected if the acquisition program has been successful at achieving the RAM requirements defined in the RAM Rationale. If the RAM requirements are not clearly achieved the benefits of the RAM Case increase immensely as the RAM Case documents the steps taken to meet RAM requirements. The RAM Case evolves from the direction of the customer and the supplier as the project matures. Initially the customer is the government acquisition organization; eventually, it is subsequently the user.

The RAM Case may be based on a variety of types of evidence, but they must be within the bounds of the stated assumptions. The method used in a particular instance may be chosen at the supplier's discretion, as appropriate to the nature of each requirement addressed. Suitable approaches are described below. Although they may be used in isolation, it is more common to use these approaches in combination to provide a more robust RAM Case.

- Quantitative Evidence: this approach is based on defined methods of analysis to generate metrics that demonstrate the required (or desirable) RAM features in the target system. This type of evidence also includes the results of any testing or demonstrations conducted as part of a RAM Program Plan.
- Qualitative Evidence: Focuses on processes used for development and support of the system. Qualitative evidence seeks to assure satisfaction of RAM requirements by

demonstrating quality, maturity, and integrity of the underlying engineering and management processes.

- Historical or Comparative Evidence: Includes systems already in use and supported for other customers. Comparative evidence could be relevant for a system that is a variant of an existing product, or is similar to an existing product produced by the same supplier. The information provided might include both quantitative and qualitative aspects of the product and the associated support services.

The body of evidence for the RAM Case is the cumulative information at any point in time, which may include the following:

- Product description
  - Part number/Manufacturing drawing number
  - Serial Number
  - Hardware and software revision level/modification level
  - Physical characteristics
  - Drawing number
  - Block Diagram
  - Interface boundaries, if applicable
- RAM requirements
  - Rationale for the requirements
  - Progress towards meeting
  - Latest estimate
- Risk Areas
  - Risk areas associated with the product satisfying the RAM requirements
  - Assessments of the risk severity and likelihood of occurrence
  - How these risks are being/have been managed
- A description of activities undertaken to assure the achievement of RAM requirements
- Results of analyses that provide
  - Insight into risks
  - Knowledge of failure modes and degradation mechanisms
  - Critical degradation and failures
  - Failure tolerance
  - Single Point Failures List
  - Critical aspects of the design
  - Critical Items List
  - Failure Detection, Isolation, & Recovery mechanisms
- Results of all testing that provide information on
  - Risks
  - Failure modes and degradation mechanisms
  - Critical degradations and failures

In general, the rationale for generating a RAM Case during development will apply similarly to maintenance of the case during later phases. The RAM Case will provide the basis for assurance that the original RAM requirements continue to be met in the face of ongoing evolution and change to the system.

The RAMPP and RAM Case may be required as deliverables contracted between a supplier and a customer. The RAMPP provides a forward view of intended processes and RAM Case looks back at decisions made. Therefore both of these key artifacts are created in the early stages of a project and it is to be expected that not only a RAMPP, but also a RAM Case should form part of any proposal in order to justify design and process decisions upon which the proposal is based. The RAM Case continues to be developed throughout the acquisition life cycle and provides visibility of progress. Iterations of the RAM Case may be linked to acquisition and funding milestones. Where deliverables of one phase are used as discriminators for future contract awards, care should be taken to distinguish between acceptance of deliverables from one phase and claims about future intentions.

The RAM Case can be a topic of discussion at design and management reviews. By assessing the robustness of the RAM Case at any given time, engineers and managers get a good sense of the level of RAM being achieved. Just as important, they gain insight into what actions may be necessary to correct any noted deficiencies or outstanding risks and problems.

The RAM Case approach represents a cooperative approach in stark contrast to the historic R&M prescriptive approach, heavily reliant upon the use of "hard-line standards." A RAM Case is closely linked with the RAM Program Plan and is the sum total of all RAM evidence that is generated by the engineering design activities, trials and testing, and in-service or field data.

To meet the RAM requirements, the RAM Case, in conjunction with the RAMPP, provides the evidence by which the following objectives are demonstrated:

- The RAM requirements of the customer are determined, demonstrated, and understood by both the customer and the supplier.
- Strategies are developed in the RAMPP resulting in a program of RAM activities together with applicable success criterion, which demonstrate that their implementation will satisfy the RAM requirements.
- The customer is provided with progressive assurance that the RAM requirements will be satisfied.
- The RAM risks and management strategy are clearly identified in meeting the RAM requirements.
- The creation of RAM Case (status) reports which record how the RAM requirements are met through all stages of acquisition through deployment for in-service operation.

3.5.8 Initial Technical Review (ITR)

The ITR ensures that a program's technical baseline is sufficiently rigorous to support a valid cost estimate (with acceptable cost risk), and enable an independent assessment of that estimate by cost, technical, and program management subject matter experts. The ITR assesses the capability needs and conceptual approach of a proposed program and verifies that the requisite research, development, testing, engineering, logistics, and programmatic bases for the program reflect the complete spectrum of technical challenges and risks. The ITR evaluates the preliminary RAM estimates, RAM Rationale, and RAM Program Plan.

3.5.9 Alternative System Review (ASR)

The ASR ensures that the system's requirements agree with the customers' needs and expectations and that the system under review can proceed into the Technology Development phase of the acquisition process. This review generally assesses the alternative systems that have been evaluated during the Concept Refinement phase (including COTS/NDI), and ensures that the preferred system alternative is cost effective, affordable, operationally effective and suitable, and can be developed to provide a timely solution to a need at an acceptable level of risk. The ASR also verifies the feasibility of RAM requirements with the aid of comprehensive risk assessments as well as trade studies/technical demonstrations.

3.5.10 System Requirements Review (SRR)

The SRR verifies that all system and performance requirements derived from the Capability Development Document are defined and consistent with cost, schedule, risk, and other system constraints. The review determines the direction and progress of the systems engineering effort and the degree of convergence upon a balanced and complete configuration. To be successful the SRR must identify an acceptable level of risk for the system under review. The SRR provides the preliminary allocation of system requirements (RAM) to hardware, human, and software subsystems. The SRR may occur more than once during the acquisition process as future SRR(s) may be required during Step 2: Design and Redesign for RAM.

3.5.11 Integrated Baseline Review (IBR)

The IBR should be conducted throughout the acquisition process when Earned Value Management is required as the focus of the IBR is the System Development and Demonstration contract. The IBR must also address important technical considerations as well, such as the identification of project milestones and required resources as well as ensuring objective and rationale system measurements (RAM) are in place. Similar to the System Requirements Review, the IBR may also be an iterative review that is repeated during Step 2 as well as Step 3: Produce Reliable and Maintainable Systems.

3.6 Outputs and Documentation

Outputs from Step 1 not only document the user needs, but also inform the subsequent activities.

- The conceptual system/capability documentation will direct the design as it matures through the subsequent acquisition phases.
- Documentation of the system model provides the baseline for subsequent assessments as it identifies critical items, redundancy, design limitations, etc.
- The preliminary RAM assessment provides the basis for technology development, corrective actions, and risk reduction activities in pre-systems acquisition; and for JCIDS/acquisition capability documents (ICD, CDD) as well as RFP and contractual requirements for Milestone B entry into systems acquisition.

- The RAM Rationale describes the level of reliability, availability, and maintainability the user needs. At the time of ICD approval, the RAM rationale may only be qualitative statements of mission reliability needs or logistics footprint limitations which constrain the new capability. In DoD acquisition framework, the RAM Rationale may be summarized in the ICD, and later updated in the CDD and the Capability Production Document (CPD). At the ICD
- The RAM Program Plan describes the structured series of RAM-related activities that will satisfy the RAM requirements of the system/capability. The RAMPP may be developed in conjunction with the Systems Engineering Plan (SEP) or as a stand-alone plan specifically addressing RAM.
- The RAM Case is the accumulated evidence, at any point in the program, of demonstrated progress toward achieving the RAM requirements.
- A preliminary Test and Evaluation (T&E) Strategy is developed.

Formal documentation is essential for recording user-needed capabilities, guiding the program, and providing the rationale for the selected levels of RAM. It also makes the analysis readily available for peer review or independent audit.

Chapter 4 Design and Redesign for RAM

4.1 Introduction

Achieving the required levels of reliability, availability, and maintainability (RAM) for a system begins with identifying the user needs and developing realistic requirements. RAM requirements can be achieved through system design and redesign. This chapter describes Step 2: Design and Redesign for RAM as illustrated in Figure 4-1.

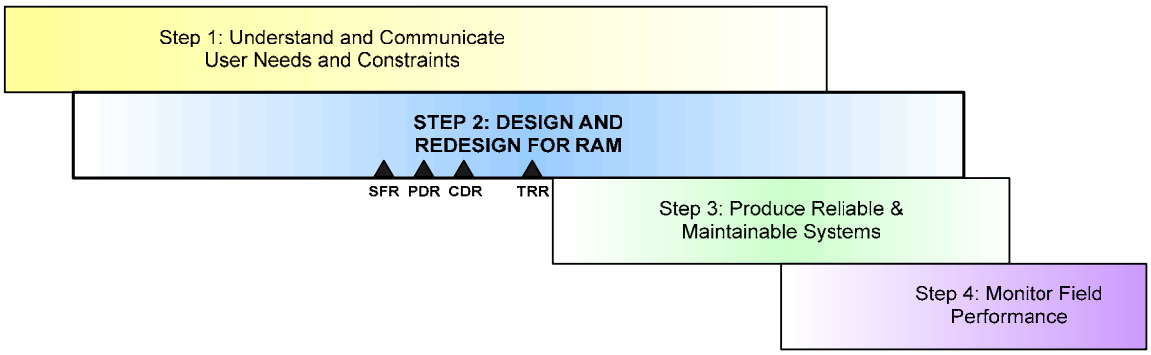


FIGURE 4-1: Design and Redesign for RAM

4.2 Mission and Goals

The mission of the System Development and Demonstration phase is to develop the system design, so that it meets all design specifications, is producible, and when produced and fielded, will meet user requirements.

Design and development are system engineering processes. Design synthesis that achieves high reliability involves a process that can be thought of as an iteration of design (design and redesign), where relevant failure modes are identified and removed. Reliability of a system arises from its resistance to failure, so during the design and development phase, an effective design process eliminates the system failure modes that would be encountered in the field. The removal of failure modes requires vigilant, informed, and sustained engineering effort.

Maintainability arises from ease of maintenance and involves a similar engineering effort to simplify and enable maintenance when it is required. To produce a maintainable design, designers and developers must actively pursue this end.

Operational availability of a system is a consequence of its actual reliability and maintainability (R&M) performance in the field, and the support provided. High levels of system availability can be achieved through the combination of high reliability and maintainability, and the availability of adequate logistics support (including maintainer, spares, required test equipment, procedures, publications, management, etc.). Targeted levels of RAM are more likely to be achieved when designers accurately anticipate and accommodate the operational, environmental and support factors applicable to the fielded system.

4.3 People and Organizations

The Step 2: Design and Redesign for RAM activity will often be managed within a development contract, with the development contractor pursuing contractual requirements that include a range of performance-based requirements and specifications including RAM requirements. These requirements were developed in the first step of the model and described in Chapter 3.

The service acquisition executives or component acquisition executives will normally assign a relevant Program Manager, Chief Engineer or Lead Systems Engineer and team members with responsibility for the engineering effort of a program, including the reliability engineering effort. Contractor organizations will vary, but would normally have a Program Manager responsible for achieving contractual requirements. Depending on the size and complexity of a project, positions and titles with elemental responsibility within a contractor organization will vary, but contractor staff relevant to RAM requirements could include the Lead Systems Engineer, the Logistics Engineering Manager, and possibly a RAM Engineering Manager. The development contractor will ensure the developing system is designed to have suitable RAM performance normally by utilizing an interdisciplinary team of designers that should also include operational, test and support staff.

Achieving required RAM is a team effort of contractor and defense personnel working together with a unified and determined aim of producing an effective system.

4.4 Supporting Information

4.4.1 Input Information

As noted earlier, system operational availability is a consequence of actual system R&M performance in the field, combined with the logistics support provided. Targeted levels of RAM are more likely to be achieved when designers accurately anticipate and accommodate the operational, environmental and support factors applicable to the fielded system.

Designers rely on and consider the documentation that is supplied within the contractual context from earlier life cycle phases. This documentation includes:

- Operational Concept documentation
- Logistics and Maintenance Support (Concept) documentation
- Life cycle environmental information

These documents provide the constraints and boundaries within which the design must operate and be sustained. The support and maintenance concepts are typically refined during this phase, as a result of gaining a better understanding of the technology, the technical solution, and operational constraints.

In response to the Request for Proposal (RFP), the contractor will normally have undertaken some preliminary system design and will have produced early design artifacts, usually including

preliminary system RAM models to enable basic system design parameters to be estimated and proposed.

The RFP should normally require a preliminary RAM Program Plan (RAMPP) be developed as part of the Systems Engineering Plan (SEP). The SEP should identify the RAM engineering techniques that will be applied to develop system or elemental RAM performance. The requirements for RAM demonstration, as appropriate, should be identified in the specification and relevant verification matrix, and normally outlined in the contractor's preliminary Test and Evaluation Plan (TEP).

Subsystem, configuration item, or component RAM data may be available to the development team through Government Furnished Information (GFI), lessons learned from other programs, field knowledge, company information services, Original Equipment Manufacturer (OEM) and suppliers, or defense industry data sources such as the Reliability Analysis Center (RAC). The contractor or a DoD organization may know relevant failure modes corporately for the technology.

4.4.2 Developed Information

Often the preliminary life cycle environmental information provided from previous phases or supplied within the contractual context is insufficient for detailed design and development and needs to be more comprehensively developed. This development is usually undertaken in the systems engineering, logistics engineering or reliability engineering process.

Corporate procedures and processes should have been referenced in the contractor's proposal (RFP response) and be utilized or customized for particular projects.

4.5 Tools and Activities

Project engineering activities will normally be managed within the Systems Engineering Plan, with more detailed RAM engineering techniques often managed under the RAMPP. As noted in Chapter 3, the contractor will typically have developed a preliminary RAMPP in the RFP response stage. Whichever plan (i.e., RAMPP or Systems Engineering Plan) it is included within, the activities needed to undertake and achieve RAM need to be carefully considered and documented. The RAM program design needs to consider the technology maturity, maturation, technical risk and demonstration needs of the technology and system.

4.5.1 Develop RAM Program Plan

Successful and efficient reliability program management comes from the ability to identify and tailor relevant "value-added" tasks that address the stated or implied needs of the customer while minimizing overall system or product life cycle costs. Knowing and understanding the needs of the customer serves as the basis for establishing realistic reliability and integrated diagnostics/BIT design requirements. Building inherent RAM into the design and ensuring that it is maintained throughout the development, manufacture and use of the product/system is the primary objective of an effectively managed RAMPP.

An effective RAMPP provides an overall cost benefit, particularly in terms of Life Cycle Cost (LCC). An effective program may include analysis tasks that supersede unnecessary tests, or may use a test strategy that has a more significant impact on inherent product RAM than analytical methods. In either case, the improved product/system RAM should be pursued at optimal cost. A well-planned development and test program will ensure that a design meets the user's RAM needs, and that potential defects that would otherwise be introduced during design or manufacture are removed before the product is delivered to the customer.

The choice of RAM tasks to be considered for a particular product design is a function of many factors: the challenge to the state of the technology, purpose of the overall effort, environmental characteristics, repair or service needs, safety considerations, and funding and schedule constraints. It is important that the contractor selects those tasks that are most effective given these factors and not simply implement a "standard" program used on prior efforts.

4.5.1.1 Maintenance/Support Concept Refinement

As noted earlier, the Operational Concept and Logistics and Maintenance Support Concepts identify the constraints under which the system is operated and supported. How a system will be supported and maintained are design constraints that will affect the system design. Refinement of the initial support and maintenance concepts is enabled through a better understanding of the technology, the technical solution and fielding constraints.

One of the most important aspects covered by the support concept is the identification of the maintenance levels (also known as repair or support levels). The classic support levels for military systems were organizational, intermediate, and depot support with associated line replaceable units, shop replaceable units, and piece parts. As the military services seek to reduce logistics footprint, increase mobility, and reduce costs, three-level maintenance has generally been replaced by two-level maintenance, namely organizational and depot. To support a two-level concept, adequate levels of reliability are essential. Otherwise, an inordinate number of spares will be needed to fill the pipeline or availability will suffer. The support concept needs to describe the system's support environment for sustainment which includes supply, maintenance, transportation, sustaining engineering, data management, configuration management, manpower, personnel, training, habitability, survivability, environment, safety (including explosives safety), occupational health, protection of critical program information, anti-tamper provisions, and information technology, including National Security Systems, supportability and interoperability functions (DODI 5000.2).

The Navy is using a support concept (Automated Maintenance Environment (AME)), where systems status and functional information recorded by on-board recorders is downloaded onto the AME ground station for operator debrief, and subsequent maintenance management, maintenance order distribution, hardware and software configuration management, special diagnostic and analytical trending programs such as engine life use indices, vibration analysis etc. For an effective integration of the new weapon system into AME, this requirement needs to be understood and communicated by the user and acquisition agent (step 1) and effectively implemented through the other 3 steps.

4.5.1.2 RAM Maturation through the Program

Throughout the acquisition process, management should be cognizant of the typical progress of RAM characteristics through a defense program. Systems that are more evolutionary in nature (i.e., that result in products that are basically similar to a predecessor and use the same basic technology) may have a level of RAM that is either adequate or inadequate from the start, but are unlikely to increase significantly over the course of development. Systems that are significantly developmental or have leading edge or novel technologies, on the other hand, are likely to show low RAM initially but increasing RAM performance as the development matures. Development of the technology and system should include increasing the RAM performance. As such, RAM may "grow" in phases through the program, brought about by targeted engineering activity to remove failure modes. Step changes of performance may also occur when each new "environment" is encountered, such as when the system is first fielded for Initial Operational Test and Evaluation (IOT&E). The RAM performance may be affected because of the difference in the way increasingly "real world" users and maintainers use and support the equipment rather than the more simulated and constrained world of the development environment. A similar step change may occur due to effects such as full rate production effects, or use by regular operational and support staff after equipment is distributed and fielded.

This concept of RAM maturation over the system life cycle is illustrated in Figure 4-2. Developers and managers should be aware that each program will have a unique curve that is a result of a number of factors, including the level of engineering effort applied to refine the design, the understanding of the real world usage and environment, knowledge identification and removal of failure modes, etc.

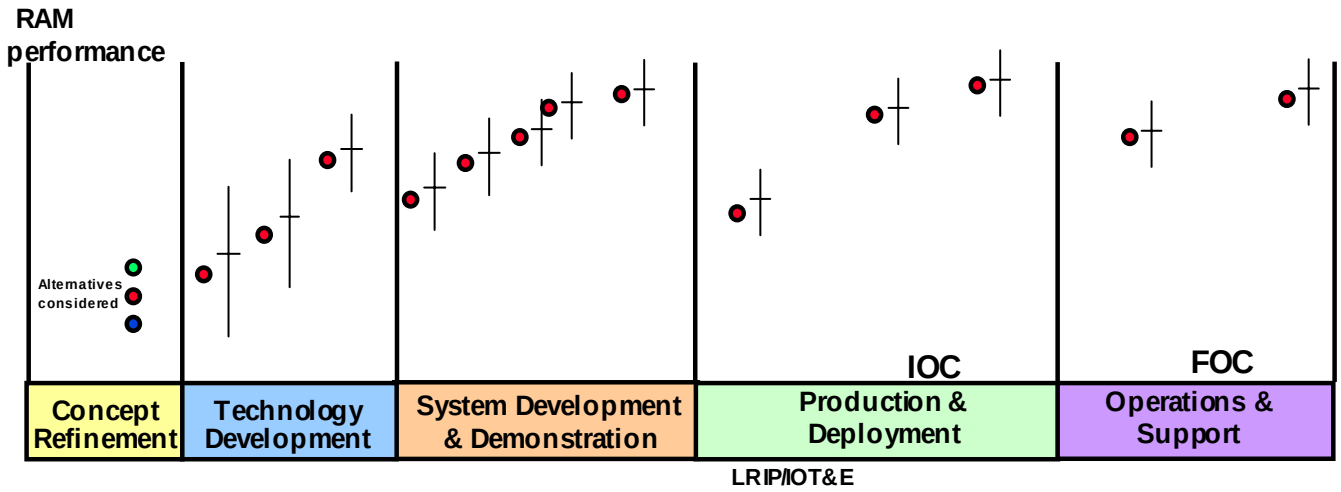


FIGURE 4-2: RAM Maturation May Occur Across the Entire Life Cycle

Similarly, a system in which commercial off-the-shelf (COTS) items have been integrated may need to grow RAM through the program by protecting or insulating the more susceptible items from the adverse stress, such as shock, temperature, etc. experienced in the defense environment. The severity of the field environment may not have been appreciated until later in the development program.

System operational availability in the fielded environment is also expected to differ from development projections, due to the effect of the actual logistics system and support factors, rather than theoretical or nominal figures. Factors such as the levels of spares and their distribution, maintenance staff availability, training, technical aptitude, competing tasks, and repair turn around times affect the operational availability achieved. Prior to the real world values being encountered, one should recognize that anticipated operational availability remains a projection.

4.5.2 RAM Design and Development Techniques

There are a number of techniques used within the systems engineering process to develop and assure the RAM performance of the system. These include the following techniques described subsequently:

- General RAM Design Considerations
- Mission Profile Definition
- Repair Strategy
- RAM Assessment
- Reliability and Availability Modeling
- Simulation (Markov Analysis)
- Data Collection, Analysis and Corrective Action System (DCACAS)
- Data Management Technique (PREDICT)
- Failure Modes and Effects Analysis (FMEA)
- Fault Tree Analysis (FTA)
- Ishikawa Diagram
- Benchmarking
- RAM Prediction Models
- Physics of Failure
- Reliability Growth Testing and Test-Analyze-Fix-Test (TAFT)
- Accelerated Testing Methods
- Life Data Analysis
- Component Testing
- Analysis of Repairable Systems
- Commercial-Off-the-Shelf (COTS) Assessment
- Reliability Centered Maintenance (RCM)
- Condition Based Maintenance (CBM)
- Maintenance/Maintainability Demonstration and Evaluation
- Analysis Demonstration and Test of Testability/Diagnostics
- Man-in-the-Loop Testing
- Sparing Models Assessment Methods
- Specific Models (i.e., ACIM/TIGER)
- Parts Obsolescence and Diminishing Manufacturing Sources
- Bayesian Techniques
- Fault Insertion Testing
- RQT and Acceptance Testing

- One Shot Device Testing
- Environmental Stress Screening (ESS)/Highly Accelerated Stress Screening (HASS)

4.5.2.1 General RAM Design Considerations

In general, the following basic techniques should be in the forefront of designers' minds during the design and development process as methods that will normally improve the RAM performance of items under design:

- Simplify the design
- Improve the design by eliminating failure modes
- Implement redundancy judiciously
- Design for fault-tolerance
- Design the items to be fail-safe
- Derate components or elements (i.e., practice of limiting electrical, thermal, and mechanical stresses on electronics to levels below their specified ratings)
- Provide early warnings of failure through fault diagnosis/condition monitoring
- Use standard parts and reduce variation in parts and components
- Adopt a modular design approach
- Use robust design techniques
- Use improved technology and better materials
- Make suitable performance trade-offs (e.g., less stress – some decrease in performance traded for longer life that still satisfies the system's promised capability)
- Use proven Testability guidelines for minimizing false alarms (thresholds, timing, n-of-n faults before reporting, etc.)

More comprehensive design guidance and techniques would normally be developed by the contractor for each project to assist the designer to avoid common traps and pitfalls. These may have entered the corporate culture, and have become corporate practices or standard methods.

4.5.2.2 Mission Profile Definition

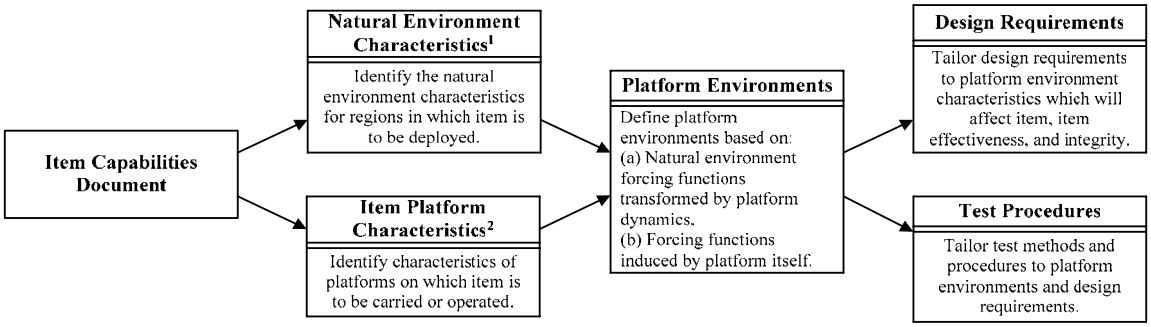
The environment in which a system is operated significantly influences the RAM performance of the system. For example, a desktop computer will achieve different levels of RAM in a mobile headquarters used in a desert environment compared with the same model operated in a fixed, air-conditioned office. Systems need to be developed to achieve the required performance in the required environment. Proper characterization of the mission profile and use environment allows the contractor to develop the system with sufficient robustness to sustain the envisioned use.

Initial environmental and mission documentation may be supplied within the development contract, but typically this will need to be refined as the system characteristics are better known.

All significant life stages, including storage and transportation, need to be considered in the use profiling and environmental characterization. Figure 4-3 illustrates this identification process. Systems experience stress during supply and initial deployment from the manufacturer. Some

systems may remain in storage for extended periods awaiting use while others are deployed and enter the field immediately after acquisition.

Large portions of safety critical embedded systems such as automotive electronics or safety equipment (fire alarm systems) spend the majority of their life in the non-operating state. The non-operating environment is characterized by items or systems that are connected to a functioning device where there is a reduction or elimination of the physical and electrical stresses compared with the operating condition. Non-operating environment conditions present different RAM issues that are sometimes overlooked since the effects of operating environment conditions are often a greater concern. Issues relating to non-operating failures need to be taken into consideration from the System Development and Demonstration phase of the system's life cycle. Furthermore, the relevant environmental concerns that need to be taken into consideration depend on the environmental factors associated with each different target environment (i.e., storage, receipt screening, repair/modification, testing, and shipping/transportation). To combat this, a physics of failure-based approach (discussed in-depth within Section 4.5.2.14) to the design cycle is popular.



Notes:
1. Conventional meteorological data is not collected with military hardware in mind. Great care must be taken to ensure that the meteorological data used is relevant to the specific hardware items.
2. In this context, a platform is any vehicle, surface, or medium that carries the hardware. For example, an aircraft is the carrying platform for an avionics pod, the land itself for a ground radar, and a man for a hand-carried radio.

FIGURE 4-3: Environmental Tailoring Process

Figures 4-4 and 4-5 illustrate the types of natural and induced environments that can be expected during the Operations and Support phase of the military equipment's life cycle.

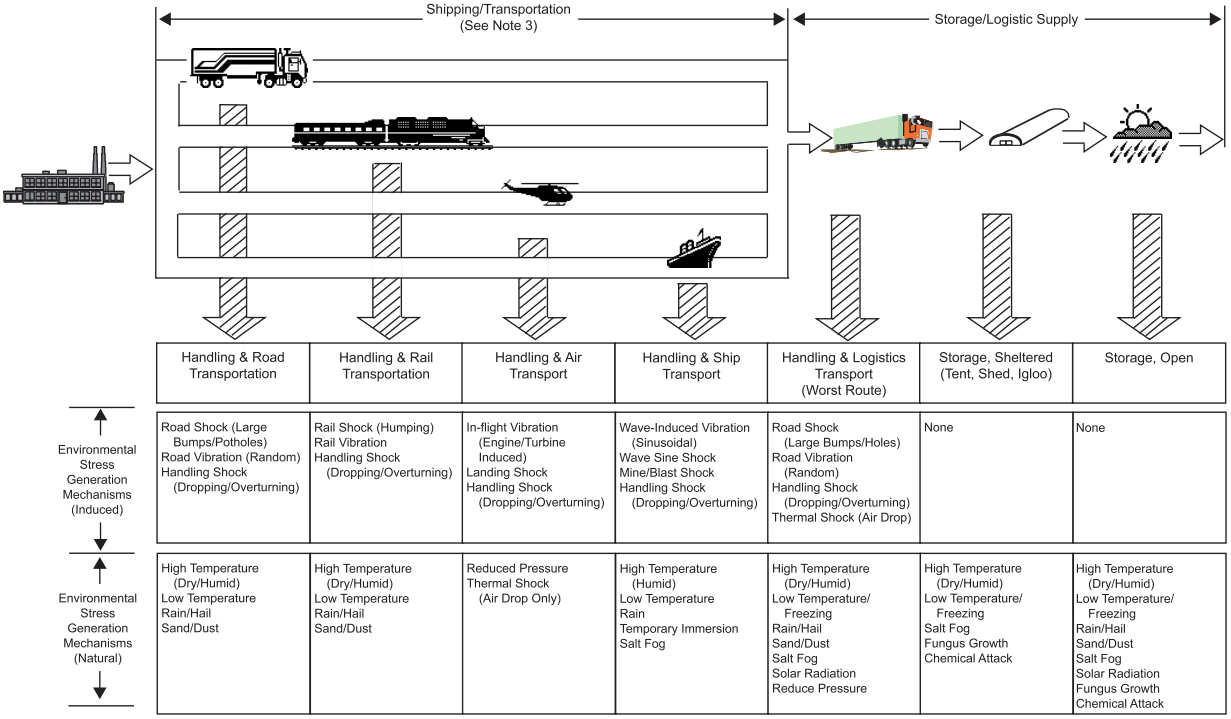


FIGURE 4-4: Generalized Life Cycle Histories for Military Systems Shipping/Transportation and Storage/Logistic Supply[1]

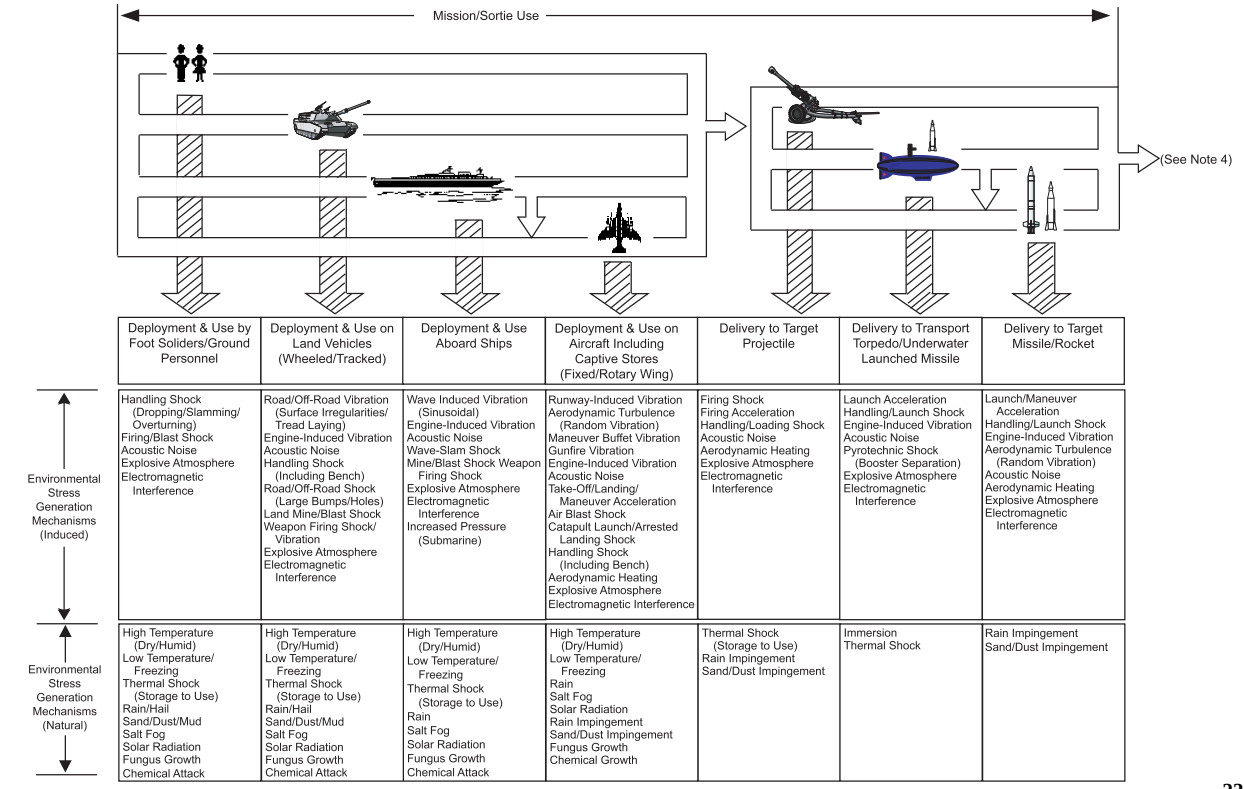


FIGURE 4-5: Generalized Life Cycle Histories for Military Systems – Mission/Sortie Use[23]

[23] Notes from Figures 4-4 and 4-5:

4.5.2.3 Repair Strategy

When a product fails it is desirable to restore it to operation in a fast and economical manner. It is also important that the repair activity does not degrade the inherent RAM of the product. To achieve these ends, it is necessary to formulate an appropriate repair strategy.

A repair strategy should be one of the first considerations used in the planning and design of a product. Therefore, it is one of the first efforts in the Concept Refinement phase of the acquisition process. It can be based on market survey to determine the customer needs, and should be redone if the needs change. The repair strategy and product design should be compatible. The repair strategy should be modified as required, which may come in the form of maintainer feedback, design changes due to modification or upgrade, safety concerns associated with performing repair(s), etc.

The painstaking effort to produce a reliable product can be for naught if defects are introduced in the maintenance process. Defects can be introduced in many ways. If maintenance requires more powerful test equipment or a higher skilled maintenance person than is actually available, attempts at repair may do more damage than good. A lack of guidance or inadequate repair procedures may cause maintenance errors that introduce latent defects into the product. A well-conceived repair strategy attempts to preclude the degradation of RAM, as well as provide the fastest and most economical restoration of service.

The repair strategy should be formulated to respond to the following basic questions:

- **Who?** Who will be doing the repairs and what are their skill levels? The repair strategy should not require higher repair skills than those available or the repair process will degrade RAM. A repair strategy for unskilled technicians could include repair by replacement of plug-in modules to reduce handling, built-in-test to eliminate the need to troubleshoot, and expert systems to guide the repair actions of the technician.
- **Where?** Will repairs be done at the user's site, the producer's plant, or a third party location? What resources should they be expected to have? In some systems, some repair can actually be performed during, rather than after, the mission
- **How?** Will the repair require special tools or skills? Will a maintenance manual be included with the system? The need for special tools should be avoided, as a lost tool means the product may be damaged during repairs made using improper tools. Note that a tool or skill not considered special by some users may be special to others. The maintenance manual, if any, should match the skills of the user and the tools available.
- **What?** Will components be designed for replacement or repair? At what level of assembly will replacement be preferred? Is this consistent with the user's needs? When products are designed to be repaired by module replacement, but are used by users who

1. The environmental stress events experienced by actual hardware may not always occur in the sequence shown in this profile.
2. The generalized profile provides only representative decision-making information.
3. Hardware may be subjected to any or all of the shipping/transportation modes shown.
4. The generalized profile shows only areas of environmental concern and does not attempt to show operational use patterns.

repair the modules rather than replace them, achieved RAM is almost invariably degraded through induced damage. Such cases often arise when the user cannot wait for a replacement module to resume operation. Solutions include the encapsulation of the modules to preclude repair, on-site spares to permit continued operation of the product while awaiting replacement parts (including the provision of built-in spare modules), provision for expedited spares delivery (i.e., just-in-time), or the design of modules for repair by the available technicians and tools. Modern digital designs often contain provisions to reload computer programs to eliminate a software anomaly impacting the mission.

- **When?** Is preventive maintenance (PM) needed? How often? On what basis (e.g., "hard" time or on condition)? When should periodic inspections be performed, if appropriate? The wear out of mechanical products and failures of electronic products that are not obvious (i.e., the corruption of data) can result in poor operational RAM metrics. In non-critical cases these situations may be found by periodic inspection. For critical applications, means should be provided to make repair needs obvious. PM schedules should fit into the user's schedule. If not, PM may be ignored, with resulting damage further degrading the achieved system RAM.

4.5.2.4 RAM Assessment

RAM assessment is the continuing process of determining the value of the level of RAM being achieved at any point in time. The ability to make an assessment, and the quality of the assessment, depends on the information available. Because of the stochastic nature of RAM, the assessment of RAM becomes more tightly bounded with greater information. RAM statistics are always an estimate. Actual RAM performance can never be known exactly until the item has completed service, which is patently too late. In addition to the stochastic aspect, as the acquisition program progresses, knowledge of expected field RAM performance becomes more refined as system RAM models move from qualitative inputs to more quantitative inputs.

As previously discussed in Step 1, assessment at early stages of development is achieved through eliciting and applying expert judgment, lessons learned, comparative analysis and system modeling. As design and development progresses (i.e., Step 2), additional information is gained through analyses and tests, the data becomes more quantitative, the assessment becomes more refined, and eventually the assessment becomes a more tightly bounded indicator of the RAM performance, both the inherent level that has been achieved in design and the expected level that will be achieved in use.

Modern systems have increasingly utilized software to meet the requirements of the user to ensure the capability is achieved in a state-of-the-art technological fashion. Software is needed to integrate the high-tech items selected for modern systems. When these systems have complex functional operational integration issues, design and development of the Integrated Diagnostic software often lags the operational software. The result is often a delayed or inadequately matured ID software suite that impacts both developmental test time and RAM, particularly the false alarm impact on the mission, platform availability, system maintenance, spares, etc. Therefore, assessing the functional reliability of the BIT and ID software must also be conducted

as part of the RAM assessment. Software reliability is discussed in Appendix B of the RAM Guide.

Although assessments are needed throughout the development of a system, and often are stated in what appear to be very "accurate" terms, it must always be remembered that reliability and maintainability are probabilistic concepts and that operational availability is a function of not only reliability and maintainability but of many other factors. For that reason, any assessment will have a margin for error, and results should be stated using a confidence intervals rather than simply point estimates. Data from all these tests and assessments should be archived throughout the system life to support effective technical management throughout the life cycle and influence the development of successive systems. There are statistical techniques available (described later in this section) for combining data from different tests and types of tests and assessments to provide more robust estimates of reliability and maintainability. Assessment is a continuous process as illustrated in Figure 4-6.

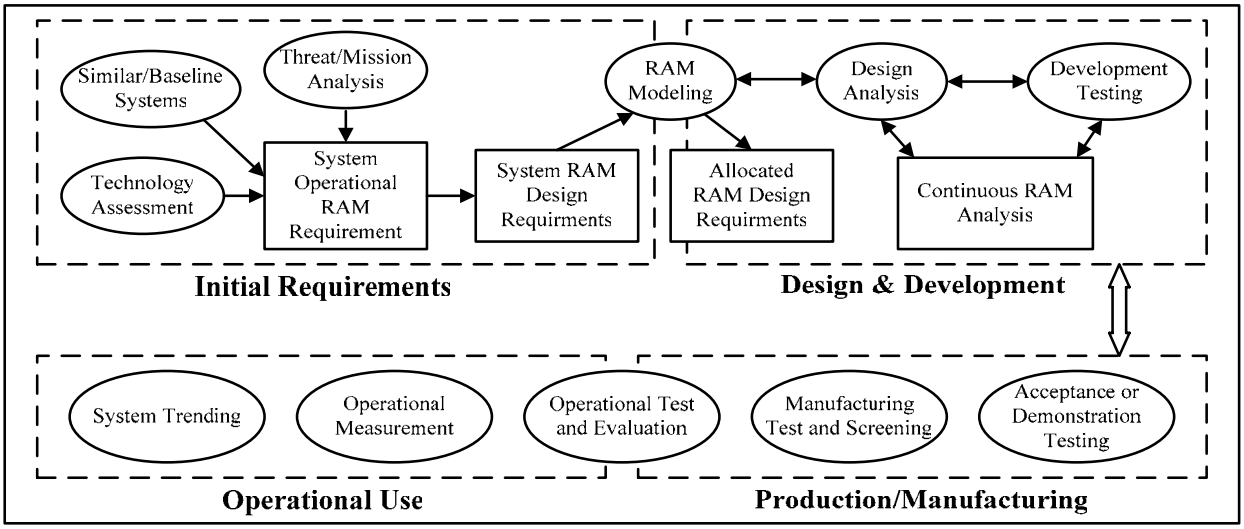


FIGURE 4-6: Assessment is a Process that Begins with Developing Requirements and Continues Throughout the Design, Development, Manufacture, and Use of a System

Limitations of Assessment: All assessments will have limitations. They may be caused by insufficient sample size, inadequate testing under required conditions (both technical and operational), or immature system functionality. Limitations should be clearly identified and reported as part of an assessment, as well as their effects on test results, parameter estimates, and any inferences on requirements compliance.

Combining Data/Results from Different Assessments: All data requires expert evaluation before sets from different conditions are combined. Reliability analysts strive to gather as much data on a product as possible to make assessment of the acceptability of the product as accurately as possible. Consequently, there is often a desire to combine predicted, test, and operating data for current, new, modified and similar products. Problems will be encountered when non-homogeneous or heterogeneous data are combined to represent a new product. One of the important engineering tasks for improved reliability is identifying design or product defects prior

to production and operation. Data analysis is one of the features used to determine the shortcomings of the process, which is why accurate and proper data combinations are necessary.

Combining similar data sets in order to establish confidence intervals, estimate or forecast values, model data or establish distributions (goodness of fit) is very appealing. Larger data sets provide more information, allowing better estimates and more refined values to be obtained. But this is only true if the information is consistent, of good quality and comes from similar populations.

Analysts need to ensure that only suitable data is combined, and that the exercise does not become a case of adding "apples and oranges," for the data may be similar only in appearance. For example, "field data" from a particular device needs to be considered prior to combining it with its laboratory data. If these data sources described system reliability performance in different conditions and developed from different levels of product maturity, simply combining these data may be counterproductive. By combining such data, additional "noise" may be introduced into the data set. The extra "noise" can increase the variance and therefore, also may increase the uncertainty and the size of the confidence interval. In such cases, it may be worse to combine the data sets than to analyze them separately.

To correctly combine several data sets, an in-depth analysis of each data set under consideration should be performed. That is, using an Exploratory Data Analysis (EDA) approach (introductory data analysis via tabular, graphical and descriptive statistics) one assesses the data characteristics. This assessment establishes whether the population appears symmetric and unimodal or skewed. Then, prospective statistical distributions for the parent population are established and estimates of the parameters are determined.

Using the estimated parameters, theoretical and qualitative differences and similarities between environments, operational profiles, product maturity, methods of testing and other factors are established. These differences and similarities are identified via confidence intervals and hypothesis test for the parameters, such as the mean, variance, median, etc. Finally, in-depth statistical analyses on each data set (such as analysis of variance, of covariance, regression modeling, goodness-of-fit tests, etc.) are performed to establish and quantify any statistical difference between the sets.

As a result of all the aforementioned analysis, only those data sets that do not show large statistical differences between their distributions and their parameters, and where other similarities can be established should be combined. For example, data sets from different laboratory tests, that appear to come from the same distribution, such as a normal distribution, with the same mean and variance, when the tests are performed on similar devices in approximately equal time epochs, may be combined.

A summary of the implementation procedure for combing data is provided below. The first two steps are always conducted when combining data sets, whereas the remaining steps are dependent upon the circumstances encountered while combining the data sets.

1. Perform an Exploratory Data Analysis (EDA)

2. Perform graphical analysis
3. Perform goodness of fit analysis
4. Perform analysis of variance
5. Perform regression analysis
6. Quantify statistical differences

Several important caveats regarding combining data from several sources to develop statistical models, in general, and regression models, in particular, have been noted. The two most important are that (1) data should only be combined when the engineering and statistical analysis support such combinations, and that (2) the statistical model should always follow reality, not the other way around. If care is not taken, an engineer might end up modeling the data and not the problem.

One final and very important note regarding combining the results of different tests should be kept in mind. Regardless of the test being conducted, all failure indications should be analyzed, the root cause determined, and an informed decision made as to whether it is technically, economically, and necessary given the user needs, to try to eliminate (or reduce the effect or probability occurrence) of the failure mode. The preceding statistical tests are needed only when a quantitative assessment is to be made based on the test results.

Design Reviews: Consistent with the systems engineering process, RAM performance should be included within the standard design review process for the project. This means that at critical points of the system development and maturation, that the development methods, results and projects are reviewed and considered by external authorities. It is essential that the independent review process be based on purely technical grounds and avoids any connotation of being personal or punitive in nature. The reviewers should maintain an objective, constructive, and professional dialogue with the analysts to aid in the resolution process. Experience on numerous projects has shown that this independent review process does work and the resultant quality of both the analyses and the designs is enhanced. The absence of an independent review of RAM analyses results in the very real possibility of not detecting a design defect. Furthermore, the process rapidly degenerates if the design analyst feels that the analysis task is performed simply to satisfy a project milestone.[24]

Modeling and Simulation: A RAM model presents a clear picture of functional interdependencies and provides the framework for developing quantitative product level RAM estimates to guide the design trade-off process. RAM models are helpful for the following:

- Allowing summarization of all factors affecting system RAM
- Making numerical allocations and assessment
- Easy identification of single points of failure
- Evaluating complex redundant configurations
- Showing all series-parallel and other topological relationships

RAM models are derived from and traceable to system functional requirements. They may take inputs from comparative analysis, RAM predictions, test data, field data, as well as customer

[24] Taken from NASA Preferred Reliability Practices, PD-AP-1302.

requirements and use profiles (including mission, threat, operating, and support concepts). Models may vary from being relatively simple to going into great detail by taking into account duty cycles, service life limitations, wearout items, varying environments, dormant conditions, human reliability, software, etc. The scope of the model usually depends on the type and amount of information available for use and the criticality of the product under consideration. Even a simple model may help guide concept refinement and design decisions to improve overall RAM, assuming appropriate judgment is used. Just as RAM assessments must account for the affects of software within the system, RAM modeling must include the system's software as well as its interaction(s) with the system (see Appendix B). RAM modeling is more comprehensively described in section 4.5.2.5.

As RAM models are developed to include more detail, the calculation of overall system RAM performance becomes more complex and difficult to solve analytically. Solutions can be determined through modeling tools such as simulation. Simulation involves mimicking some or all of the behavior of one system particularly with computers, models, or other equipment. The most popular simulation technique is Monte Carlo simulation, where the performance of the logical model of the system under analysis is repeatedly evaluated using RAM parameter values selected from designated probability distributions. The lower level parameter values are randomly selected with their probabilities constrained by the relevant distribution functions. Since Monte Carlo simulation can be performed without complex mathematical analysis, it has become a popular means to model system reliability and availability. Complex systems are relatively easily modeled using Monte Carlo simulation and input algorithms are straightforward. Input assumptions for parameters such as failure and repair rates are not constrained, which provides analysts the freedom to use non-constant values for these parameters. (Of course, as is true for other modeling techniques, the quality of the output directly depends on the quality of the input data and the realism of the simulation model.) Monte Carlo simulation effortlessly handles other model aspects like queuing rules for repairs, repair priorities, and the use of serviceable spare parts from unserviceable systems (cannibalization).

Reliability assessment using RAM demonstration and reliability growth methodologies are dealt with in later sections.

4.5.2.5 Reliability and Availability Modeling

RAM modeling is a very powerful and informative tool and very useful for activities in addition to its utility as an assessment tool. As discussed in Section 4.5.2.4, a reliability model presents a clear picture of functional interdependencies and provides the framework for developing quantitative product level reliability estimates to guide the design trade-off process.

There are several basic reliability and availability models used when analyzing a system. The basic series reliability model, illustrated in Figure 4-7, consists of two independent components (each exhibiting a constant failure rate); the failure of either component will result in a system failure.

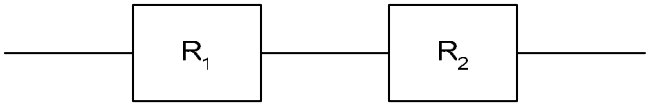


FIGURE 4-7: Basic Series Model

The reliability of a system with a basic series model is the combined probability of no failure of either component over the modeled time interval, therefore for a series of n, s-independent components reliability can be expressed as: $R = \prod_{i=1}^{n} R_i$

When redundancy is introduced between the components, the reliability models become more complex. The active redundancy model is used for simplest redundant system, which consists of two independent components that can still achieve system success as long as one component is functioning. Figure 4-8 shows a dual redundant system.

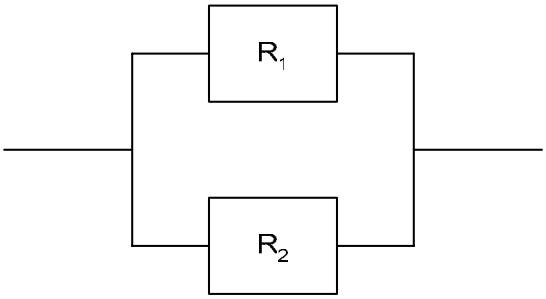


FIGURE 4-8: Dual Redundant System

For an active redundant combination of n s-independent elements, the reliability of an active redundant system can be expressed as: $R = 1 - \prod_{i=1}^{n} (1 - R_i)$

The m-out-of-n redundancy model is used when m units out of the n independent components with similar reliabilities are required to achieve system success. The binomial reliability function is used to calculate the reliability for the m-out-of-n redundancy model, which is expressed as: $R = 1 - \sum_{i=0}^{m=1} \binom{n}{i} R_i^i (1 - R_i)^{n-i}$

Standby redundancy is the process in which one unit does not operate continuously, but instead only becomes active when the primary unit fails. When modeling a system with standby redundancy the reliability of the standby and primary units is needed as well as the reliability of the sensing and switching system that controls the system's operation. As an example, n equal units in a standby redundant configuration (assuming perfect switching) that are non-maintained with equal constant operating hazard rates (λ) and no dormant failures the general reliability formula (assuming homogenous exponential process) for time, t, is: $R = \sum_{i=0}^{n-1} \frac{(\lambda t)^i}{i!} \exp(-\lambda t)$

Active, m-out-of-n, and standby redundancy models represent the basic redundant systems, but there are many systems that utilize redundant features with far more variety and complexity. Examples include:

1. Dual or triple active redundant hydraulic power systems used in aircraft as well as an additional emergency (standby redundancy) back-up system in case all primary circuits fail.
2. Fire detection and suppression systems consist of detectors (often in parallel active redundant configurations) and a suppression system that is triggered by the detectors.

When designing a system with redundancy additional care should be taken to ensure that single-point failures are considered. Single-point failures can partly eliminate the redundant capability of a system as some failure modes can affect the operation of all parts of a redundant system.

It is important to note that although redundancy increases mission or functional reliability, it decreases what is referred to as basic or logistics reliability. That is, the total number of failures, mission and non-mission, will increase because more items have been added to the design. In the case of standby redundancy, where switching and detection is involved, additional failure modes are introduced. Similarly, redundancy can increase the complexity of the manufacturing process and thereby increase the risk of introducing quality problems during production. Thus, it is essential that redundancy be used judiciously and only when no other approach can ensure an adequate level of the reliability for critical functions.

Commercial software packages are available to assist with reliability modeling. Information is available on the DoD-sponsored Reliability Analysis Center (RAC) web site, http://rac.alionscience.com.

4.5.2.6 Simulation

As stated in Section 4.5.2.4, simulation is defined technically as, "mimicking some or all of the behavior of one system particularly with computers, models, or other equipment."

The key to a successful simulation model is to thoroughly define the problem definition and accurately build the model, which is the beginning of an eight-step process. The remaining steps of a simulation study process are data collection, programming, verification, experimental design, model implementation, and documentation. It is important when completing these steps to re-visit previous steps to validate that recent discoveries do not change prior beliefs. Validation adds credibility to the study and ultimately verifies the likelihood that simulation-based recommendations are believable and suitable to be accepted.

A limitation of Monte Carlo analysis is the expense associated with computer time since a simulation of large systems can require hours of computer run-time. Simulation results vary due to the probabilistic nature of simulated events, therefore it is usually necessary to perform numerous runs to obtain estimates of performance measures as well as quantify the variances associated with desired results.

Monte Carlo simulation techniques are often used in collaboration with reliability modeling to assess or consider the reliability, availability, and maintainability of various systems. Several of the software packages identified in Section 4.5.2.5 utilize Monte Carlo simulation techniques.

Markov Analysis: Markov analysis looks at a sequence of events and analyzes the tendency of one event to be followed by another. Using this analysis, we can generate a new sequence of random but related events, which appear similar to the original. IEC Standard 61508 **Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems** has significantly re-vitalized Markov analysis by requiring the analysis of various disparate failure modes from a safety perspective. The methods also are receiving more attention because today's software tools make computationally complex Markov analyses easier to perform today than in the past. Markov analysis can be used to determine reliability and availability metrics if they are defined as the variables of interest. Events or states can be given a failure probability (failure rate) and the probability of being restored to an available state (repair rate) to determine desired reliability and availability metrics. There are two basic Markov analysis methods: the Markov Chain and the Markov Process.

A Markov Chain assumes discrete states and a discrete time parameter, which may be described as Homogeneous or Non-Homogeneous. A Homogeneous Markov Chain is characterized by constant transition rates between the states. A Non-Homogeneous Markov Chain is characterized by the fact that the transition rates between the states are functions of a global clock (e.g., elapsed mission time).

The Markov Process assumes states are continuous and can be completely characterized by their transition probability matrix. Markov models are frequently used in RAM-related activities where events, such as the failure or repair of a module, can occur at any point in time. The Markov model evaluates the probability of transitioning (transition rate) from one known state into the next logical state (i.e., from everything working to the first item failed, and from the first item failed to the second item's failed state, and so on) until, depending upon the configuration of the system being considered, the system has reached the final or totally failed state. The basic assumption of a Markov Process is that the behavior of a system in each state is "memory-less." A "memory-less" system is characterized by the fact that the future state of the system depends only on its present state. A stationary (Homogeneous) system is one in which the transition rates from state to state remain constant with time. In other words, the probability of transitioning from one state to another state is the same regardless of the point in time that the transition occurs. The states of the model are defined by system element failures. The transition rates between states are a function of the failure rates of the various system elements. Transition rates are subject to the assumed distribution of failure and repair times as well as the "memory-less" system assumption.

Repairs can be accounted for in Markov models by repair rates permitting the return from any given failed state to the preceding working state. This results in a complex diagram of bubbles, representing each state, and directed lines, with arrows, showing the movement from one state to the next, or to the preceding state. As the Markov Diagram is drawn, the failure rate values and the repair rate numbers can be entered into an $n \times n$ matrix (where "n" is the number of states being considered) commonly called the "transition matrix."

Semi-Markov Process models are also frequently used in reliability theory. The semi-Markov Process model is a probabilistic model useful in analyzing complex dynamical systems. Its behavior is similar to that of a pure Markov model. With semi-Markov Process models, however, the transition times and the transition rates (distributions) depend on the time at which the system reached the present state. This means that the transition rates in a particular state depend on the time already spent in that state (sojourn time) but that they do not depend on the path by which the present state was reached. Thus transition distributions in the semi-Markov Process can be non-exponential. The most important statistics of the semi-Markov Process are the interval transition rates.

Markov methods offer significant advantages over other RAM modeling techniques, some of these advantages are:

- Simplistic Modeling Approach: The models are simple to generate although they do require a more complicated mathematical approach.
- Redundancy Management Techniques: System reconfiguration required by failures is easily incorporated in the model.
- Coverage: Covered and uncovered failures of components are mutually exclusive events. These are not easily modeled using classical techniques, but are readily handled by the Markov mathematics.
- Complex Systems: Many simplifying techniques exist which allow the modeling of complex systems.
- Sequenced Events: Often the analyst is interested in computing the probability of an event resulting from a sequence of sub-events. While these types of problems do not lend themselves well to classical techniques, they are easily handled using Markov modeling.

The advantage of the Markov Process is that it neatly describes both the failure of an item and its subsequent repair. It develops the probability of an item being in a given state, as a function of the sequence through which the item has traveled (an iterative process in which the probability of being in a future state is based on the existing state). The Markov Process can thus easily describe degraded states of operation, where the item has either "partially" failed or is in a degraded state where some functions are performed while others are not. Competing techniques (i.e., failure modes and effects analysis and fault tree analysis) have a difficult time dealing with degraded states as contrasted with outright failures.

There are at present two international standards dealing with the Markov approach. They are IEC 61165, **Application of Markov Techniques,** and the previously mentioned IEC 61508.

4.5.2.7 Data Collection, Analysis and Corrective Action System

Figure 4-9 illustrates a typical Data Collection, Analysis and Corrective Action System (DCACAS) process. Several different data sources (failure, maintenance, success, service, and warranty data) are collected and analyzed as part of the DCACAS process illustrated in Figure 4-9, but not every DCACAS will utilize all of these data sources, whereas others may collect and analyze data sources that are not identified in Figure 4-9.

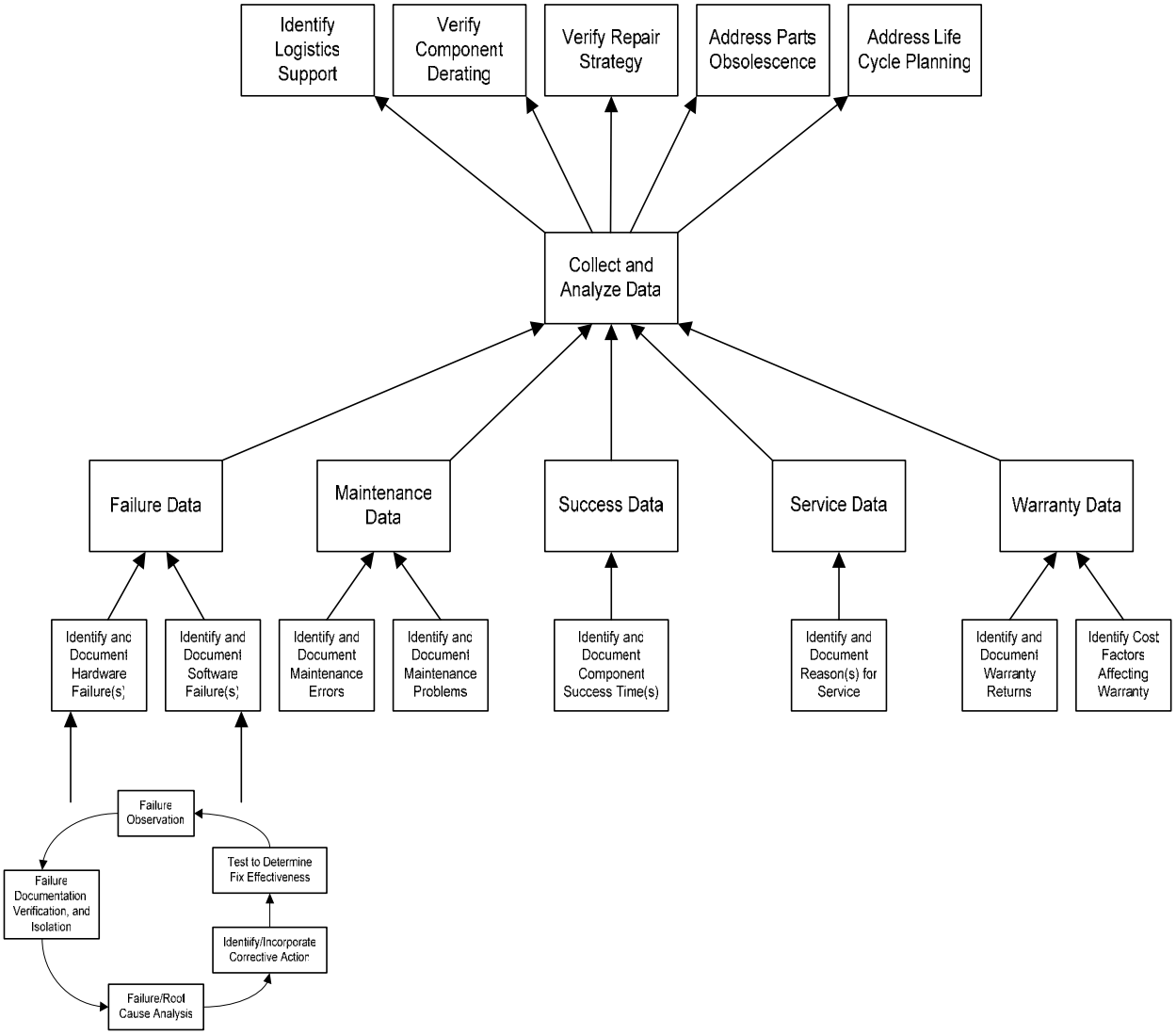


FIGURE 4-9: DCACAS Process

The basic concept of a Data Collection, Analysis and Corrective Action System (DCACAS) is simple to understand; yet it is often difficult to successfully implement in the context of an effective RAM program. The biggest difference between a traditional Failure Reporting, Analysis and Corrective Action System (FRACAS) and the DCACAS process is increasing the focus of the process from failures and problems to also include success data, as the success data is as important to the RAM program as the failure information. Similar to the FRACAS process some of the fundamental characteristics of the DCACAS process are:

- Identifying, selecting and prioritizing failures and problems for follow-on analysis to determine their root cause.
- Identifying, implementing and verifying corrective actions to preclude recurrence of the root cause failure or problem.
- Providing all appropriate personnel with access to the failure, analysis and corrective action information to support reliability growth and proactive decisions to prevent similar problems from occurring in future products or services (i.e., 'closing the loop').

- Collecting all operating and failure data to allow system performance to be assessed and trended.

The primary objective of DCACAS is to provide the mechanism for the documentation of pertinent data (failures and successes) of an RAM program as well as providing access to this data in a closed-loop format. The data collected is most useful when it can be disseminated in a usable form so that effective corrective action can be identified, implemented and verified as quickly as possible to avoid the negative impact (cost, schedule, decreased customer satisfaction, etc.) of recurring failures or faults.

The effectiveness of the DCACAS is limited to the quality and accuracy of the information that is originally documented whether it identifies a failure or success. The data must include enough details to make the information further usable, especially when the details of the failure are needed to facilitate root-cause determination. As a minimum the following information must be included for the DCACAS record:

- Who observed the data record (failure or success)
- The outcome of data record (i.e., identify specific indications of failure)
- Location where data was recorded
- When data was documented
- Under what conditions (environment, stress, etc.) data was collected

The goal of any DCACAS process is to continually address both the short- and long- term customer needs. The following elements should be considered in planning how the DCACAS process will operate:

- DCACAS planning should include the technical personnel involved with reliability, maintainability, human engineering, safety, testing, parts, materials, process control, configuration management, and supportability strategy.
- DCACAS planning should also include the involvement of the administrative functions that will control the resources necessary to effectively support DCACAS development and operation.
- The method of establishing, incorporating and using operating time or cycles within the DCACAS for quantifying experienced reliability should be clearly defined.
- If cost accounting information is to be included in the DCACAS, the appropriate people should also be involved.
- If the DCACAS is to be automated, computer programmers and administrators should be included in the earliest part of the planning stages.
- DCACAS planning typically involves the preparation of written procedures for the initiation of failure reports (and their required contents), processes for analyzing failures to determine root failure cause, and the feedback of corrective action information into the appropriate design, manufacturing, test and/or administrative processes.
- The DCACAS process should include provisions to ensure that corrective action is identified and implemented on a timely basis.
- DCACAS procedures should include flow diagrams that depict failed items and failure data flow. Methods for tracking the status of unresolved failures and suspended

corrective actions should be described, including the use of periodic audits. If the formality of the DCACAS suggests the use of Failure Prevention and Review Board (FPRB), its structure (i.e., participants), schedule and responsibilities should be defined. The FPRB focuses on the traditional role of failure review, but also concentrates on failure prevention by addressing potential problem failure modes as well as the actual problem failure modes. A FPRB can also support the failure modes and effects analysis (FMEA) to ensure potential problem failure modes are mitigated before they cause failures in testing or customer use.

The initial inputs to the DCACAS process should come from the source most closely associated with the original point that the data event was observed, which is dependent on when in the product cycle the DCACAS is initiated. During the System Development and Demonstration phase, the inputs to the DCACAS consist of information taken from a laboratory environment, which primarily takes the form of entries in an engineer's or technician's job notebook. The incidents or successes that occur during the development of a product, process or service can be captured as a means of early detection and correction of inherent design problems before manufacturing begins.

4.5.2.8 Data Management Technique

Frequently system reliability must be calculated based on a host of different kinds of data; this is particularly the case if only a small number of system tests can be performed and analysts are forced to rely upon both component and system tests to construct estimates. Los Alamos National Laboratory's Statistical Science Group (D-1) has developed methods to address this problem. In the past, D-1 worked with Delphi Automotive to develop a commercial, proprietary tool called PREDICT[25] (Performance and Reliability Evaluation with Diverse Information Combination and Tracking). PREDICT was the recipient of a 1999 R&D 100 Award.

More recently, D-1 is expanding upon the private sector PREDICT method to develop tools for conventional DoD and nuclear weapons stockpile management efforts. Under the title of Information Integration Technology (IIT), this effort focuses on development of improved models for reliability by:

1. Integrating component performance data with system test results, and
2. Calculation of system reliability in terms of all available covariate, component, testing, and expert judgment information.

Through IIT methods, D-1 has been able to significantly improve certainty and lifespan estimates for systems currently in service without causing any additional testing, through increased efficiency in using existing data sets.

IIT is primarily a method of analysis; however a number of tools are presently being developed. These include:

[25] PREDICT: A New Approach to Product Development and Lifetime Assessment Using Information Integration Technology, Los Alamos National Laboratory, LA-UR-00-4737, 2000.

- YADAS: A new software system written in Java for Markov chain Monte Carlo analysis of statistical models. YADAS is intended to be extensible to handle new models that researchers devise, and to make it easy to implement these models. It emphasizes use of Metropolis steps, relieving the user of the responsibility of calculating full conditional distributions. YADAS contains a versatile library for expressing relationships between parameters, as well as a library for proposing parameter updates that improve the mixing properties of the chain. YADAS is available at http://yadas.lanl.gov.
- GROMIT: A system behavioral modeling tool written in Python for system description and structural modeling. GROMIT helps users understand how measures of system or component behavior connect together, checks the logic and consistency of different system descriptions, and helps users create an integrated fault tree or Bayesian network structure that can be traced back to system descriptions. Work is underway to allow GROMIT to provide input information into YADAS. GROMIT, presently under beta development, is currently in use by D-1 as part of system analysis efforts and will be made available to IIT partners as appropriate.

Figure 4-10 illustrates the steps utilized as part of the IIT process.

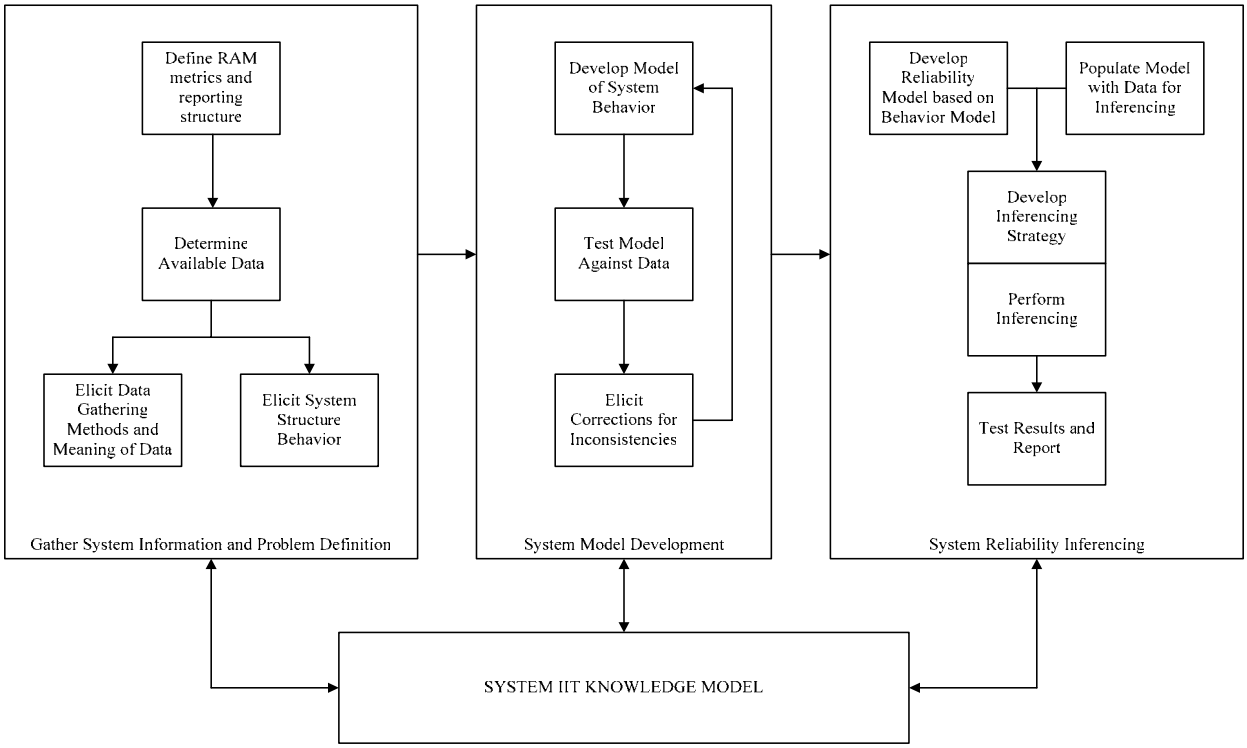


FIGURE 4-10: IIT Implementation Steps and Flowchart

4.5.2.9 Failure Modes and Effects Analysis

A failure modes and effects analysis (FMEA) is a reliability evaluation and design review technique that examines the potential failure modes within a system or lower indenture level, to determine the effects of failures on equipment or system performance. Each hardware or software failure mode is classified according to its impact on system operating success and

personnel safety. FMEA uses inductive logic (a process of finding explanations) on a "bottom up" system analysis. This approach begins at the lowest level of the system hierarchy and traces up through the system hierarchy to determine the end effect on system performance. The maximum benefit of completing an FMEA is realized from an early application in the system's life cycle rather than after the system's design is finalized.

FMEA is an effective technique that:

- Determines the effects of each failure mode on system performance.
- Emphasizes identification of single-point failures.
- Provides data for developing fault tree analysis and reliability block diagram models.
- Provides a basis for identifying root failure causes and developing corrective actions.
- Facilitates investigation of design alternatives to consider high reliability at the conceptual stages of the design.
- Aids in developing test methods and troubleshooting techniques.
- Provides a foundation for qualitative reliability, maintainability, safety and logistics analyses.
- Uses a documented, systematic, and uniform method.
- Can provide an early identification of single failure points and system interface problems.
- Provides a mechanism for verifying that switching between redundant elements is not jeopardized by postulated single failures.
- Provides an effective method for evaluating the effect of proposed changes to the design on mission success.
- Provides the criteria for early planning of tests to characterize the weaknesses of the design.
- Provides a basis for the safety analysis that is done as part of evaluating the safety characteristics of the design.
- It is also a basis for operational troubleshooting and for locating performance monitoring and fault-detection devices within the system.

A properly prepared FMEA report will indicate a number of important features that include:

- Highlighting areas needing corrective action,
- Ranking failures according to severity of equipment operation and personal safety,
- Identifying reliability and safety critical components,
- Visibility of system interface features and problems, and
- Locating performance monitoring and fault sensing test equipment or test points.

Many FMEAs that are performed are completed in accordance with an accepted military methodology, which is outlined in the RAC publication "Failure Modes, Effects, and Criticality Analysis (FMECA)." Nevertheless, there are other generally recognized FMEA guideline documents that may be of interest to the reader. They are:

1. SAE J1739, "Potential Failure Modes and Effects Analysis in Design (Design FMEA) and Potential Failure Modes and Effects Analysis In Manufacturing and Assembly

Processes (Process FMEA) Reference Manual," Society of Automotive Engineers (SAE) International, July 1994.
2. FMEA-3, "Potential Failure Mode and Effects Analysis (FMEA Third Edition), Automotive Industry Action Group (AIAG), July 2001.
3. SAE ARP5580, "Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications," SAE International, July 2001.
4. IEC 60812, "Analysis Techniques for System Reliability – Procedure for Failure Mode and Effects Analysis (FMEA), International Electrotechnical Commission (IEC), TBD.

4.5.2.10 Fault Tree Analysis (FTA)

A fault tree analysis (FTA) is a systematic, deductive methodology for defining a single specific undesirable event and determining all possible reasons (failures) that could cause that event to occur. The undesired event constitutes the top event in a fault tree diagram, and generally represents a complete or catastrophic failure of the product. The FTA focuses on a select subset of all possible system failures, specifically those that can cause a catastrophic "top event." On the other hand, a FMEA progresses sequentially through all possible system failure modes regardless of severity.

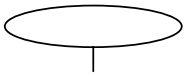
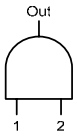
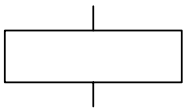
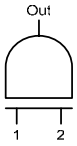
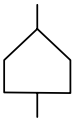
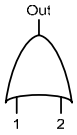
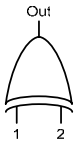
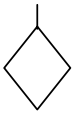
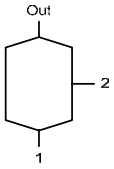
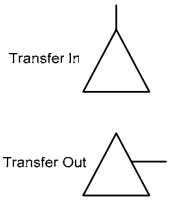
When properly applied, an FTA is extremely useful during the initial product design phases as an evaluation tool for driving preliminary design modifications. After a product becomes available in the market, the results of the FTA can be used as a troubleshooting tool. Through an FTA, a product can be evaluated from both a reliability and fault probability perspective. From a reliability perspective, the FTA can estimate whether a product will or will not meet performance reliability requirements. Through probabilistic evaluation, the FTA emphasis shifts to the likelihood of the occurrence of the undesired event, which is beneficial in quantifying risk regarding potential safety hazards that could result from the undesired event.

Fault tree analysis can be used for all of the following:

- Functional analysis of highly complex systems,
- Observation of combined effects of simultaneous, non-critical events on the top event,
- Evaluation of safety requirements and specifications,
- Evaluation of system reliability,
- Evaluation of human interfaces,
- Evaluation of software interfaces,
- Identification of potential design defects and safety hazard,
- Evaluation of potential corrective actions,
- Simplifying maintenance and troubleshooting, and
- Logical elimination of causes for an observed failure.

The symbols used in constructing an FTA to describe events and logical connections may vary between different national and international standards. A typical set of symbols is shown in Table 4-1.

TABLE 4-1: FTA Symbols

 **Top Event:** Contains description of the system-level fault or the undesired event. Input to the ellipse is from a logic gate.	 **AND Gate:** Output is to any Fault Event block or Transfer Out function. Inputs are from any Fault Event block or Transfer In function. Output occurs only if all inputs exist.
 **Fault Event:** Contains description of the lower-level fault. Fault Events receive inputs from and provide outputs to a logic gate.	 **Ordered AND Gate:** Output is to any Fault Event block or Transfer Out function. Inputs are from any Fault Event block or Transfer In function. Output occurs only if all inputs exist and the inputs occur in a specific order.
 **Input Event:** Contains a normal system operating input which has the capability of causing a fault to occur. The input event is used as an input to the logic gate.	 **OR Gate:** Output is to any Fault Event block or Transfer Out function. Inputs are from any Fault Event block or Transfer In function. Output occurs only if one or more of the input events occur.
 **Basic Event:** Contains a failure at the lowest level of examination which has the capability of causing a fault to occur. The basic event is used as an input to a logic gate.	 **Exclusive OR Gate:** Output is to any Fault Event block or Transfer Out function. Inputs are from any Fault Event block or Transfer In function. Output occurs when one, and only one, of the input events occur.
 **Undeveloped Event:** Contains a failure at the lowest level of examination which can be expanded into a separate fault tree. The undeveloped event is used as an input to a logic gate.	 **Inhibit Gate:** Output is to any Fault Event block or Transfer Out function. Inputs are from any Fault Event block or Transfer In function. One input is a lower fault event and the other input is a conditional qualifier.
 **Transfer Function:** Signifies a connection between two or more selections of the fault tree to prevent duplicating sub-branches at multiple tree locations or to signify a location on a separate sheet of the same fault tree.	

The following rules apply when constructing a fault tree:

1. State each fault clearly and write it in each event block.
2. Clearly define each failure as a component or product failure.
3. If a failure is attributable to normal operating conditions, that part fails normally.
4. All inputs to a given combination gate are fault events or basic inputs.
5. A branch is completely described down to the basic level before another branch is begun.
6. The fault tree has no redundant sections.
7. The fault tree should be completed before beginning the analysis.

The results of a fault tree analysis are expressed either qualitatively or quantitatively. Qualitative results include minimum cut-sets (combination of element failures capable of causing system failure), qualitative importance (qualitative ranking of various contributions to system failure), and common cause potentials (minimum cut-sets vulnerable to a single failure cause). Quantitative results consist of numeric probabilities (probabilities associated with system failure

and cut-set failures), quantitative importance (quantitative ranking of individual contributions to system failure), and sensitivity evaluations (effects of model changes and data errors).

Additional information about FTA can be found in various military handbooks (i.e., MIL-HDBK-338) as well as more in-depth information in NUREG-0492, the US Nuclear Regulatory Commission's **Fault Tree Handbook**, IEC 61025 **Fault Tree Analysis**, and the RAC's **Fault Tree Analysis Application Guide**.

4.5.2.11 Ishikawa Diagram.

The Ishikawa Diagram, also called the cause-and-effect diagram or fish bone chart, relates causes to effects. It can be used to hypothesize the factors that resulted in an unwanted condition, such as defects in a product, or to identify factors essential for a desired result, such as increased sales. The Ishikawa Diagram is created by listing major factors and subdividing these to the extent useful. The main problem is indicated on a horizontal line, and possible causes are shown as branches, which in turn have sub-causes, indicated by sub-branches, and so on. Once the factors are identified, other methods, such as the use of statistically designed experiments, can be used to determine the most important factors.

Some basic suggestions for the use of the Ishikawa Diagram or cause-and-effect method are:

- Involve people from different disciplines during the generation of list of causes.
- Do not be critical of others' opinions.
- Highlight the most likely causes that the team agrees upon. If there is confusion as to which factors are causes and which factors are effects, it may be necessary to use the matrix model technique. Often the resources will not be available to investigate all the opinions on the list, therefore narrowing down the original list should be conducted to prioritize or focus the thinking.
- Keep the viewpoint positive. Focus on problem solving rather than on finger pointing.

The following figure, Figure 4-11, illustrates a preliminary Ishikawa Diagram for defects introduced in a wave solder process. In this case major factors contributing to defects are identified as methods, manpower, material, and machinery (with various subdivisions).

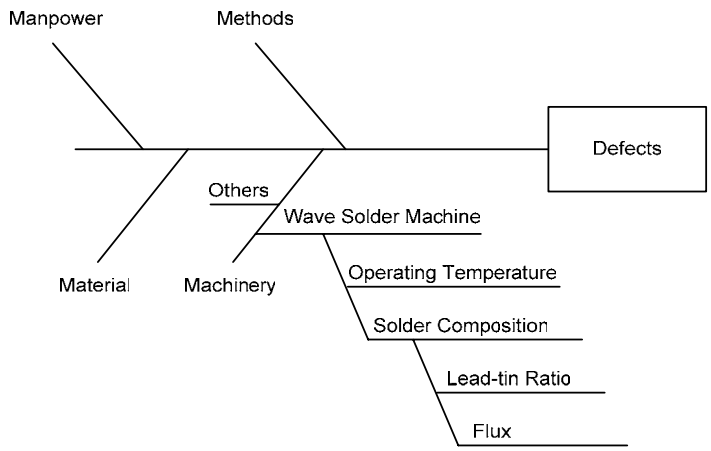


FIGURE 4-11: Ishikawa Diagram

Ishikawa Diagrams are one of the seven basic tools used in Total Quality Management (TQM) analyses. Other tools include flow charts (shows process steps from concept to end user), checklists (simple, but effective means of providing factual data to build improvement plan), Pareto charts (separates few critical factors from many trivial factors), histograms (groups data into equal size bins to determine central tendencies and variation in data), scattergrams (plot of paired data to determine correlation), and control charts (depicts measured values of data samples taken over time).

4.5.2.12 Benchmarking

Benchmarking has been utilized to identify products and processes for improvement and to produce systems with desirable RAM characteristics. Benchmarking can identify opportunities for improvement. Benchmarking is the procedure for finding the world-class standards for a product, service, or process and then adjusting one's own products, services and processes to exceed those standards. These world-class standards can be found by looking at competitors who are recognized leaders for the product, service, or process. For example, a company making computer monitors may compare the reliability of its products with other monitor makers and also with makers of conventional television receivers. If any outside organizations make a similar and significantly better product, there is room for improvement. Services may also be bench tested, including internal services such as order processing.

The following types of benchmarking are widely used:

- Competitive or Strategic: Benchmarking is done using competitors as models.
- Internal: Operating units or functions within a company are used as the model.
- Functional: Done using companies that are the best practitioners of a particular function, regardless of what industry the exemplar is in.
- Normative: Consultant collects data from group of companies on a product, service, or process and delivers statistics to the companies, with company name withheld.

When Xerox Corporation introduced benchmarking, it developed the following ten-step process:

1. Identify what is to be benchmarked
2. Identify comparative companies
3. Determine data collection method and collect data
4. Determine current performance levels
5. Predict future performance levels
6. Communicate benchmark findings and gain acceptance
7. Establish functional goals
8. Develop action plans
9. Implement action plans and monitor progress
10. Recalibrate measurements

A Reliability Analysis Center (RAC) study performed in 1993-1994 identified several "benchmarks" commonly found in the reliability program plan for successful businesses. These "benchmarks" include:

- Failures are analyzed thoroughly to identify the root cause of the failure and determine the necessary corrective action. All failures should be analyzed regardless of when or where the failures occur in development.
- Engineering development testing should be emphasized to better comprehend the design as well as validate the design process and models. Demonstrations are only recommended when focused on new components or assemblies or the application of old items in a new way. Accelerated testing is recommended to "age" high reliability items in an effort to determine their failure mechanisms.
- Reliability should be assigned to an Integrated Product Team (Product Development Team). Team should be given authority to determine reliability requirements and select design, analysis, test, and manufacturing activities required to achieve the reliability requirements.

4.5.2.13 RAM Prediction Methods

Reliability and maintainability prediction are forecasting methods that involve analysis of system characteristics and the use environment to estimate the reliability and maintainability of a system, prior to the item being developed, built or fielded. The availability prediction would then be modeled from these inputs combined with the relevant support information. Reliability predictions can be developed from a number of sources. Some of these sources, ranked in order of preference, are:

1. Past test or field data based on similar equipment
2. Engineering analyses, failure mechanism modeling, and/or accelerated life testing
3. Subject matter expertise based on known reliability levels for comparable equipment and technologies
4. Handbooks

Each of these approaches has limitations. Most important is to recognize that high reliability is not achieved through predictions. A reliability prediction may have little or nothing to do with the actual reliability of the product and can actually encourage poor design practices.

Organizations that frequently quote predictions may not understand the engineering and design considerations necessary to minimize risk and to produce a reliable design. In many cases, the person producing the prediction may not be a direct contributor to the design team. The historic focus of many organizations on the accounting of predictions versus the engineering activities needed to eliminate failures during the design process has significantly limited our ability to produce highly reliable products.

Reliability predictions are useful for a variety of reasons, including:

- Estimating the relative merits of competing designs.
- Selecting different components or limit applied component stresses (i.e., identify need for derating).
- Helping to understand life-limiting failure mechanisms.
- Assessing new component technologies when no historical data exists.
- Investigating the generic cause of a failure (i.e., wearout or an escape defect).
- Identifying whether a commercial-off-the-shelf component may achieve the required reliability when stresses are expected to exceed the commercial rating(s).
- Estimating types and quantities of spares needed for operation.

The four approaches listed earlier can be used to produce deterministic or probabilistic predictions for reliability. The use of existing test or field data from similar equipment is the most desirable approach. Also, predictions stated at a confidence level are always preferred to point estimates. However, in many cases, products may have no predecessors or may incorporate new technologies where no prior reliability data exist.

Lacking test or field data, the second preference is to use engineering analyses, failure mechanism modeling, or accelerated life testing to establish a reliability prediction. Through the FMEA process or based on past engineering experience, designers often know the leading potential causes of failure. Failure mechanism models exist for many of these causes. The expected life associated with fatigue, corrosion, diffusion, wear, fracture, and many other types of failure can be estimated through engineering modeling and analysis.

The third preference is to turn to subject matter experts. Often engineers and technicians can develop a range of likely reliability values for a given product. These estimates, which can be developed very inexpensively in a matter of minutes or hours, can turn out to be as accurate as estimates developed from any of the other sources. In many cases, a combination of the first three methods is the best way to produce an accurate prediction for product reliability.

A fourth method is to use methods described in reliability prediction handbooks or implemented in software tools. Such handbooks and tools include the following.

- MIL-HDBK-217, **Reliability Prediction of Electronic Equipment**
- Bellcore TR-TSY-000332, **Reliability Prediction Procedure for Electronic Equipment**
- British Telecom, **Handbook of Reliability Data for Components Used in Telecommunications Systems**

- Nippon Telegraph and Telephone Corporation, **Standard Reliability Table for Semiconductor Devices**
- France's National Center for Telecommunication Studies (CNET), **Collection of Reliability Data from CNET**
- PRISM (RAC) <http://rac.alionscience.com/prism/>

Through the years, the RAM and engineering communities have heatedly debated the effectiveness of the various prediction methods. Most parties do agree that any analyst using any prediction method must be very knowledgeable as to the source of the data and model used, their relevance for the given application, as well as the limitations and necessary assumptions. Those who use predictions to determine compliance, develop spares quantities, and so forth, must ensure that they understand the assumptions and limitations associated with the specific method used to make the prediction. Lack of understanding of a specific method can lead to misuse, excessive product costs, or inadequate reliability.

4.5.2.14 Physics of Failure

Physics of Failure (PoF) is a science-based approach to reliability that uses modeling and simulation to design reliability into a product, perform reliability assessments, and focus reliability tests and screens where they will be the most effective and productive. The PoF approach involves modeling the root causes of failure, often called failure mechanisms, such as fatigue, fracture, wear and corrosion. The basis of PoF is that it is not only important to understand how things work but also equally important to understand how things fail. Computer-Aided Design (CAD) tools have been developed to address various loads, stresses, failure mechanisms, and failure sites. Using PoF, engineers can use their knowledge of basic failure processes to prevent product failures through robust design and manufacturing practices. The PoF approach involves the following seven steps.

1. First, select the subsystems or components to analyze. This selection involves determining which subsystems or components are most functionally critical to the operation of the system. Once these subsystems or components are identified, then the subsystems and components that have the highest likelihood of failure are identified.
2. After the subsystems or components are selected, examine the operational and environmental loads and the preliminary design to identify potential failure mechanisms, failure sites and failure modes. Failure mechanisms are the chemical, electrical, physical, mechanical, structural, or thermal processes leading to failure. The term failure mechanism should not be confused with the term failure mode. Failure modes result from the activation of failure mechanisms. For electronics, failure modes are usually identified as shorts, opens, or electrical deviations beyond specifications. For mechanical components, the failure mode may be low-cycle fatigue.
3. Once the failure mechanisms are identified, perform an analysis on the stresses that affect the potential failure mechanisms. Potential stresses include thermal extremes, thermal cycling, vibration, mechanical shock, humidity, humidity cycling, voltage and current.
4. Next, identify the appropriate failure models (i.e., stress-life relationships) and their input parameters. The input parameters are associated with material characteristics, damage properties, relevant geometry at failure sites, manufacturing flaws and defects, and

environmental and operating loads. In this step, the variability for each design parameter is identified when possible.

5. After the model is developed, predict the time-to-failure, or lifetime, of the potential failure mechanisms in the test, operational, or usage environment. If possible, probabilistic time-to-failure estimates should be calculated that account for the variability of input parameters and process characteristics.
6. Perform physical testing to validate the modeling process. This validation could include life testing, accelerated-life testing, instrumented terrain tests, instrumented drop tests, or other tests. The objective of the testing is to validate the stress analysis, to verify that the identified failure mechanisms will occur, and to determine if there are unexpected failure mechanisms.
7. Finally, redesign to eliminate the failure mechanisms[26], or, during operational use, plan a preventive maintenance program to replace the affected items before they cause a system failure.

A central premise of the PoF approach is that reliability modeling (i.e., time-to-failure modeling) must be based on an understanding of root-cause failure processes or mechanisms. Failure-mechanism models explicitly address the design parameters that have been found to strongly influence hardware reliability. These parameters include material properties; defects; and electrical, chemical, thermal and mechanical stresses. The PoF approach can be used in designing new systems because generic failure models are as effective for new materials and structures as they are for existing designs. The goal is to keep the modeling, in a particular application, as simple as feasible without losing the cause-effect relationships that advance useful corrective action.

The use of a PoF process leads to improvements in system reliability, which can substantially reduce operation and support cost. The benefits of a PoF analysis include:

- Identification of design flaws
- Identification of weak or problem parts
- Determination of whether commercial-off-the-shelf parts and products are suitable for a given application
- Identification of destruction limits
- Development of effective accelerated tests
- Identification of wearout limits
- Estimation of failure-free operating periods

Also, by improving reliability early in the design process, reliability growth testing (i.e., test-analyze-fix-test process) can be greatly reduced. By knowing the most critical reliability problems, testing can be focused, producing significantly more cost-effective and beneficial results.

Physics of Failure analyses can take many forms. Examples of PoF analyses include:

[26] Ideally, we want to eliminate failure mechanisms. Often, that is technically infeasible or economically impractical. In such cases, we want to at least reduce the frequency of occurrence of the failure mechanism or reduce the impact of its occurrence on system operation.

- Thermal and vibrations modeling of circuit cards and linking the results to electronics failure-mechanism models to increase the failure-free operating period and eliminate expensive maintenance
- Performing dynamic analysis modeling to determine loads and accelerations at various points in mechanical structures so that loading can be reduced, geometries adjusted, and better components selected so that components (e.g. vehicle suspension elements) do not fail
- Performing finite-element analysis and fatigue analysis on commercial-off-the-shelf electronics to ensure that failure will not occur during storage, transportation, and launch for a given application
- Developing appropriate accelerated life tests using PoF models that accurately relate accelerated, high-stress conditions to the anticipated product usage environment
- Using fatigue modeling and analysis and finite-element analysis to address the specific geometries and loading so that stress-based prognostics algorithms can be developed to predict failures before they occur during operation for mechanical and electronics systems
- Using failure-mechanism models to isolate the true causes of product failure so that cost-effective strategies can be implemented to reduce the chance of subsequent failure

This list is not comprehensive, but does represent some of the types of PoF-based engineering activities that can substantially improve product reliability.

PoF represents the application of the best engineering design and analysis practices for a wide range of products based on an understanding of failure mechanisms. The analyses are based on peer-reviewed and published failure mechanism models and engineering tools. PoF can substantially improve reliability, reduce the time to field systems, reduce testing, reduce costs, and significantly increase customer satisfaction. It is an important engineering design tool.

4.5.2.15 Reliability Growth Testing and Test-Analyze-Fix-Test (TAFT)

Initial prototypes of complex weapon systems will invariably have reliability and performance deficiencies that generally could not be foreseen and eliminated in early design stages. To uncover and mitigate these deficiencies, early prototypes and later more mature units are normally subjected to a series of development and operational tests. The tests are specifically designed to expose the system components to the range of stresses that they are expected to encounter during the weapon's life cycle. Failures are analyzed, corrective actions are implemented, and modifications are tested to verify the effectiveness of the corrective actions. This development approach has been referred to as the test-analyze-fix-test (TAFT) procedure. In such a fashion one attempts to increase, or grow, the reliability of the prototypes to the stated requirement reliability, and the process is often referred to as a reliability growth program.

The success of a reliability growth program is determined by many factors. First, the intended missions of the weapon system must be clearly known and stated. The anticipated mission duration and stresses associated with each intended mission scenario should be specified or identified. Appropriate reliability requirements should be established. This may entail having separate reliability requirements that address system abort (i.e., mission) failures as well as all

failures that incur a logistics burden. Additionally, separate reliability requirements could be placed on different mission scenarios or elements of the system. Once this has been accomplished, the development and mapping of the planned reliability test and evaluation program can be undertaken.

The planned test and analysis program must be comprehensive enough to include the envelope of anticipated tactical operating conditions. To the extent feasible, the test conditions should cover the edges of the envelope for each identified type of stress and for each combination of stresses deemed significant. The reliability results under the extreme envelope conditions should be compared to the results obtained under more nominal stress levels. Such a comparison helps address whether the system reliability design is sufficiently robust. Identifying the potential dominant failure modes for each of the major subassemblies through analysis, by considering data from systems that utilize similar subassemblies, and lower level testing should guide the selection of these test events and associated stress levels to help ensure adequate coverage for the anticipated tactical stress envelope. This initial planning should be accomplished prior to the System Development and Demonstration (SDD) test phase. Although such activities typically do not utilize a statistical reliability growth model, these activities are an important contributor to the success of a reliability growth program and the necessary resources planned for and budgeted.

The resulting battery of planned test events to be conducted in the Technology Development (TD) test phase with the prototype units will help ensure that the early prototype reliability has the potential to grow to a reasonable level by the start of the following SDD phase. A set of test events, supplemented by analysis where needed, that provides adequate failure mode coverage provides the potential for reliability growth. To actually realize this potential, a second ingredient is necessary, namely the incorporation of effective corrective actions to the failure modes discovered by test or potential failure modes indicated by test or analysis. The proposed corrective actions (termed fixes) require time to formulate, obtain Failure Prevention and Review Board (FPRB) approval, and physically implement. Additional time is required to verify the implemented modifications. The fixes should be incorporated into the initial SDD units to increase the reliability maturity of these units. Not all the failure modes are typically addressed. Modes associated with commercial-off-the-shelf (COTS) or government furnished equipment (GFE) may not be fixed. However, if the assessed unreliability of the portion of the system comprised of the COTS and GFE is sufficiently large relative to a system requirement in the application environment, at least a portion of such modes will have to be addressed. Planning should consider this possibility.

Reliability growth modeling allows the analyst to estimate the current or projected system reliability performance and estimate the time required to develop specified levels of reliability. The emphasis or focus of the reliability growth activity is the identification and removal of failure modes, hence the technique has a fundamentally different attitude towards failures than acceptance testing, and as such, the combination of growth testing with acceptance testing is discouraged.

Reliability growth testing is typically modeled using either the Duane Model or the Army Materiel Systems Analysis Activity (AMSAA) Model developed by Dr. Larry H. Crow. Each

model has its advantages. The AMSAA (Crow) Model has exactly the same parameters and reliability growth pattern as the Duane Model. Therefore, the parameters for both models have equally recognizable physical interpretations. Estimation for the Duane Model uses a simple regression fit. The AMSAA (Crow) Model, however, utilizes more rigorous statistical procedures with the benefits of confidence intervals, Goodness-of-Fit tests, and other statistical tools and procedures. The appropriate model should be based on selecting the simplest one that does the required job. MIL-HDBK-189 suggests the Duane Model for planning and the AMSAA (Crow) Model for assessment and tracking. If a reliability qualification test (RQT) is performed the reliability growth testing should be planned and tracked using the Duane Model. Otherwise, the ability to calculate confidence limits around the data when using the AMSAA Model makes it more attractive for tracking.

The underlying assumption of the Duane Model and AMSAA (Crow) Model is that the plot of MTBF versus time is a straight line when plotted on log-log paper. The regression fit that estimates reliability growth within the Duane Model makes this model easy to use, which has also made it more commonly used. The Duane Model also assumes that fixes are incorporated immediately after a failure occurs (before additional test time is accumulated), but since this is rarely the case, this assumption is a disadvantage of using the Duane Model. The following equations are used with the Duane Model (K is a constant that is a function of the initial MTBF, α is the growth rate, and T is the test time).

- Growth Rate: $\alpha = \dfrac{\Delta MTBF}{\Delta Time}$
- Cumulative MTBF: $MTBF_C = \dfrac{1}{K} T^{\alpha}$
- Instantaneous MTBF: $MTBF_I = \dfrac{MTBF_C}{1-\alpha}$
- Test Time: $T = \left[(MTBF_I)(K)(1-\alpha) \right]^{\frac{1}{\alpha}}$

The scope of the up-front reliability program, severity of the use environment and level of technology introduced into the product can affect initial reliability and the test time required. The manufacturer's ability to aggressively ensure that fixes are developed and implemented can have a substantial affect on growth rate and test time. When planning a growth test based on the Duane Model the following should be considered.

- Calendar time should be estimated to be approximately twice the number of test hours to account for product down time.
- A minimum test length of five times the predicted MTBF is recommended (if Duane Model estimates less time). Various sources identify test lengths between 5 to 25 times the predicted MTBF.
- If the initial MTBF is very low, it may be that the equipment is entering reliability growth testing too soon (i.e., the pure design process is being terminated prematurely).
- For large MTBF systems (i.e., MTBF greater than 1000 hours), the preconditioning period equation is not accurate and 250 hours is commonly used instead.

- The growth rate experienced is a function of the design team's ability to identify and implement effective corrective actions.
- The starting point of the growth curve can greatly influence the calculated growth rate during the early phases of the growth analysis. When the starting point for the growth curve cannot be estimated based on expert judgment, lessons learned, or other means, a rule of thumb is to assume the starting point is 10% of the predicted reliability.
- The upper limit on the growth rate should be 0.5, since growth rates above 0.4 are rare.

The US Army Materiel Systems Analysis Activity (AMSAA) or Crow Reliability Growth Model employs the Weibull intensity function to model reliability growth during a development test phase. The model has been proved to be an adequate representation of reliability improvement during development for numerous systems. The AMSAA (Crow) Reliability Growth Model is applicable to systems for which usage is measured on a continuous basis (i.e., time in hours or distance in miles). A key element of the AMSAA (Crow) Reliability Growth Model is that it is designed for tracking the reliability within a test phase and not across test phases. The model evaluates the resulting reliability growth from introducing design fixes into a system during test and not the reliability growth that may occur at the end of a test phase due to delayed fixes.

The AMSAA (Crow) Reliability Growth Model assumes that within a test phase failures occur according to a Non-Homogeneous Poisson Process (NHPP). The failure rate or intensity of failures during the test phase can be represented by the Weibull function, $p(t) = \lambda\beta t^{\beta-1}$ where $\lambda>0$, $\beta>0$ are parameters and t is cumulative test time. Under this model the function $m(t) = \left[\lambda\beta t^{\beta-1}\right]^{-1}$ is interpreted as the instantaneous MTBF of the system at time. If t represents the total cumulative time for the system, then *m(t)* is the demonstrated MTBF or the MTBF of the system in its current configuration. With a failure rate or intensity function that may change with test time, the non-homogeneous Poisson process provides a basis for describing the reliability growth process within a test phase. The AMSAA (Crow) Model provides an estimate for assessment purposes, determines confidence bounds on the estimate, and uses an objective goodness-of-fit test for the data.

Another advantage of the AMSAA (Crow) Model is the ability to handle grouped data (i.e., the time to each failure in the system is not known). This capability is important when not all failures of interest are system-level failures that cause a test to stop. The start and end of each interval, they need not be equal, can be determined by a system failure. When at least three intervals of observations are made, the total failures in each interval can be determined by inspection. Using statistical methods, a reliability assessment can be made.

A common limitation identified by users of the AMSAA (Crow) Model is the procedures that are required prior to utilizing the model. First, the data must be analyzed to determine if a trend exists (i.e., Laplace Statistic). The parameters of the AMSAA (Crow) Model must then be calculated based on the sample size and test type (i.e., failure truncated or time truncated). Then, Goodness-of-Fit parameters must be calculated and compared with the "critical value" of the Cramer-von Mises Statistic. If the calculated Goodness-of-Fit value is less than the "critical value" the AMSAA (Crow) Model must be rejected, otherwise the model is accepted. If the AMSAA (Crow) Model is accepted, the system failure rate is then determined for the time of

interest (i.e., period in which AMSAA (Crow) Model is being applied). The upper and lower bounds of the calculated failure rate are then determined.

Table 4-2 compares the AMSAA (Crow) Model with the Duane Model,

TABLE 4-2: Comparison of AMSAA (Crow) and Duane Models

	Duane Model	AMSAA (Crow) Model
Basis of Model	Empirical model	Statistical model
Confidence Bounds	Confidence bounds cannot be determined	Confidence bounds can be determined
Trending	Significance of trend cannot be tested	Significance of trend can be tested
Data Fit	Least squares fit to the date	Maximum likelihood fit to the data
Popularity/Complexity	More popular/less complex (simple)	Less popular/more complex
Graphical Representation	Straight line on log-log paper	Straight line on log-log paper

A more recent development is the modeling of fix effectiveness. It is a common error for models to assume that fix actions are totally effective. Dr. Crow has developed a methodology for a measure of fix effectiveness, using terminology of failure modes within process control. To be considered in control, "fixed" failure modes are considered against three criteria; namely 1) there is a numerical calculation of the failure rate; 2) the numerical calculation is substantiated by at least one of the following: analysis, analogy or test; and 3) the failure rate is acceptable, given the system reliability specification and rationale. When system reliability is estimated, failure modes that do not meet the full criteria receive only partial credit for achieving the estimated reliability through use of an effectiveness factor, for example 0.7. As more failure modes are mitigated and come within the reliability process control, the estimate of system reliability increases and so does the confidence in that estimate. As a rule of thumb, the period of time to verify the effectiveness of a design change should be at least three times the frequency of the failure mode being corrected.

Other reliability growth models include:

- Cox-Lewis (Cozzolino) model or log-linear model, which uses NHPP to estimate parameters from test data. Cozzolino uses the Initial Defects Model to explain that new systems contain errors (defects) committed during the production process or of unintended structural weakness that will eventually manifest as failures. Repair will then eliminate this defect from reappearing.
- McWilliams model is based on a sequence of independent but non-identically distributed data. The McWilliams model considers the test to failure of a prototype, which will allow for the root cause determination of the failure and system redesign will reduce the potential for recurrence of this failure.
- Braun-Paine model based on rate of occurrence of failures that is dependent on the number of failures that have already occurred instead of the operating time the system has accumulated.
- Singpurwalla model attempts to adaptively estimate the current reliability when the interarrival times are independent, but not identically exponentially distributed. The current estimate of reliability for the system is based on the expected value of the posteriori distribution of the parameter of the exponential distribution (where the posteriori distribution is based on the prior distribution and test results).

- IBM model uses differential equations to calculate reliability growth of electronic equipment by assuming that failures without assignable causes occur at a peril rate and a fixed but unknown numbers of design, manufacturing, and workmanship defects are present in the system at the beginning of testing. The IBM model assigns failures to two categories; residual failures, which are a function of the number of expected failures that is not time dependent, and correctable cause failures, which are a function of the number of expected time-dependent failures.
- Jelinski-Moranda model is considered one of the earliest software reliability models, which assumes that a system starts with a known number of faults and each fault contributes the same amount to the overall unreliability of the system. This model assumes the times between failures are exponentially distributed.
- The Littlewood model questioned the idea of every fault having the same effect on the overall system reliability from the Jeliniski-Moranda model. Littlewood assumes that the components with higher failure rates are detected earlier in the growth process and those components with lower failure rates are detected later in the growth process. Littlewood focused on different occurrence rates for each fault with each fault assumed to have exponentially distributed times to failure.
- Lloyd-Lipow model considers a system with a single failure mode in which a test program is conducted with all tests conducted on items with a fixed probability of success. At the completion of the test program, a growth curve was created to fit the groups of success-failure data.
- Pollock model presents a reliability growth model using Bayesian techniques for both discretely and continuously failing systems. The system failure rate is dependent on the current state that changes in the following restrictive manner. After every failure, if the system is in the unrepaired state it 1) goes to the repaired state based on some known repair probability or 2) remains in the unrepaired state. If the system is in the repaired state it remains so with a probability of one. Models are then derived to estimate the projected system reliability at a specified time in the continuous failing system and after the observation of a specified number of trials in the discrete failing system.

For one-shot systems where there is an efficient TAFT loop, growth may be a fairly smooth process and a growth model, such as the Duane Model, may be used as the basis for the growth plan. On many one shot systems where hardware tends to be tested in batches, reliability growth may take the form of a series of steps or jumps between successive hardware design standards. MIL-HDBK-189 describes the various types of growth patterns and available growth models, which can be used to model reliability growth of one-shot systems.

For reliability growth testing or TAFT testing to be successful it is important that the testing program:

- Requires that each failure is analyzed fully and action is taken in the product's design or production to ensure that the failures do not recur. Failures should not be identified as being "random" or "non-relevant" during the testing program, unless a conclusive demonstration can be completed that illustrates that such a failure cannot occur on fielded production units.

- Provides for completing each corrective action as soon as possible on all units in the development program. Delaying corrective action only delays the reliability growth, which in turn means potential failure modes at the "next weakest link" may not be highlighted and the fix effectiveness of the corrective action will not be adequately tested.
- Ensures that, when failures occur, the failure investigation verifies the accuracy of the reliability predictions, stress analyses and failure modes and effects analyses (FMEAs) performed on the product. If discrepancies exist in these analyses, they should be identified and corrected.

More details on reliability growth are included in Appendix C of the RAM Guide. Other sources include: MIL-HDBK-189, **Reliability Growth Management,** MIL-HDBK-781D, **Reliability Test Methods, Plans and Environments for Engineering Development; Qualification and Production**, and International Electrotechnical Commission (IEC) 61014 - **Ed. 2.0 Programmes for Reliability Growth** for additional information on reliability growth and TAFT testing.

4.5.2.16 Accelerated Testing Methods

The test time required to determine accurate reliability metrics for some products under normal operating conditions may be excessively long and thus expensive or impractical to demonstrate. Ideally, collecting the data required to determine the reliability of a product should not hold up development and should be as economical as practicable, so it is imperative that tests are developed that can accelerate the time required to accurately measure product reliability. Accelerated life testing employs a variety of high stress test methods that shorten the life of a product or quicken the degradation of the product's performance. The goal of such testing is to efficiently obtain performance data that, when properly analyzed, yields reasonable estimates of the product's life or performance under normal conditions.

There are many accelerated test plans, some targeted to very specific technologies, and other tests developed for broader applications. All of which, however, typically fall into one of two general methods of testing: constant stress tests or step stress tests.

- Constant stress tests are commonly defined by one or two stress factors, such as temperature, voltage, humidity, etc., at only a few levels. The stress levels are predetermined and are generally well above the operational limits of the unit. The groups are operated under the defined stress conditions for a set amount of time. The failure data obtained is then utilized for the modeling and predictions by using applicable empirical relationships (i.e., Miner's rule, Arrhenius model, etc.). Probability plots can be used to evaluate the test results by relating the failure distribution parameters with the expected operating conditions using the cited empirical relationships.
- Step stress testing is conducted at progressively higher levels of stress in a sequential manner. The tests are initialized near the upper limit of the operational environment with all units placed on test together. The units are operated for a short duration (basically given a chance to fail) then the stress is indexed to the next higher level. The stepping procedure is often continued until all units have failed. Probability plots for step stress test results utilize a stress-time axis instead of a time axis to determine the probability of failure at a stress-time value.

When developing an accelerated test, it is critical that the higher stresses of the test do not precipitate unrealistic failure modes to occur. The physics of the materials being tested and a failure analysis should indicate whether or not unrealistic failure modes have been produced. If failure modes that can occur only at stresses well above the maximum operating stress are observed then the test will need to be redesigned to ensure results of interest are obtained. When conducting accelerated life tests it is important to ensure that the failure modes of the product are accelerated at the same rate. Another concern developers encounter when designing accelerated tests are interactions between separate stresses that combine to weaken the product being tested at a greater rate than expected from a simple additive process. Accelerated tests that combine environmental stresses should be supported by experimentation that provides the knowledge only garnered through empirical data to ensure that the amount by which the separate stresses are increased is related to the separate and combined effects of the environmental stresses.

Highly Accelerated Life Testing (HALT) is a form of accelerated testing in which the sole purpose of the test is to determine if the product can withstand the stresses it is being subjected to, if the test unit survives it passes the test, otherwise corrective actions will be taken to improve the product's design in order to eliminate the cause(s) of failure. In general, HALT will not quantify the life (or reliability) characteristics of the product under normal use conditions; instead these tests will provide valuable information as to the types and levels of stresses that could be employed to design an accelerated test to assess life characteristics. A good HALT profile would quickly reveal failure modes that will occur during the life of the product under normal operating conditions. HALT supports a robust design approach.

The basis of a quantitative accelerated life test is the model or relationship that quantifies the accelerated life to the actual life. The following bullets identify the most popular life-stress relationships used with quantitative accelerated life tests.

- The most commonly used life-stress relationship for accelerated life testing is the Arrhenius life-stress model, which is based on the Arrhenius reaction rate equation, $R(T) = Ae^{-\frac{E_A}{KT}}$, where R is the speed of the reaction, A is an unknown non-thermal constant, EA is the activation energy (eV), K is Boltzman's constant (8.617385 x 10^{-5} eV K^{-1}), and T is the absolute temperature (Kelvin).
- When thermal stress (temperature) is the acceleration variable the Eyring model is utilized. The Eyring relationship is also useful for other stress variables, such as humidity. The Eyring relationship is expressed as: $L(V) = \frac{1}{V}e^{-\left(A-\frac{B}{V}\right)}$ where L represents quantifiable life measure (i.e., mean life, characteristic life, median life, etc.), V represents the stress level (temperature values in absolute value, i.e., degrees Kelvin or degrees Rankine), A and B are model parameters that need to be determined.
- The inverse power law is often utilized when non-thermal accelerated stresses are considered for the accelerated life test. The inverse power law is expresses as: $L(V) = \frac{1}{KV^{\eta}}$ where L is quantifiable life measure, V is stress level, K and η are to-be-determined model parameters.

- The temperature-humidity relationship is a variation of Eyring model and has been developed to predict the life at use conditions when the accelerating stresses of temperature and humidity are combined in a test. This relationship is given by, $L(V,U) = Ae^{-\frac{\phi}{V}+\frac{b}{U}}$ where U is the relative humidity (decimal or percentage), V is temperature (in absolute units), ϕ, b (activation energy of humidity) and A are all to-be-determined parameters.
- Another combinatorial model that is utilized is the temperature-non-thermal model, which is used when temperature and a second non-thermal stress (i.e., voltage) are the accelerated stresses of a test. The temperature-non-thermal relationship is the result of a combination of the Arrhenius and inverse power law models and can be expressed as: $L(U,V) = \frac{C}{U^{\eta} e^{-\frac{B}{V}}}$ where U is the non-thermal stress (i.e., voltage, vibration, etc.), V is the temperature (in absolute units), B, C, η are parameters to be determined.

It is important to note that some accelerated life test techniques are appropriate at the part level, whereas others can be used for higher levels of assembly. For additional information on the advantages, disadvantages, and limitations of the various accelerated testing techniques refer to the following sources.

- **Accelerated Test: Statistical Models, Test Plans, and Data Analysis**, Wayne Nelson, John Wiley & Sons, New York, NY, 1990.
- **Accelerated Reliability Testing Utilizing Design of Experiments**, RL-TR-93-249, Rome Laboratory, 1993.
- **Understanding Accelerated Life-Testing Analysis**, Pantelis Vassiliou, 2001 Proceedings of Annual Reliability and Maintainability Symposium.

4.5.2.17 Life Data Analysis

Life data consists of in-house test data (from reliability tests) and field data (from repair centers, field repair personnel, returned units, customer surveys, etc.). The in-house data is a good immediate source of reliability information as it is obtained under controlled conditions, which allow the engineer to get the desired information without the "noise" associated with some types of field data. Unfortunately, in-house data is often expensive to obtain and limited in quantity, which can provide test results that cannot be replicated in the field. Field data is usually not as controlled as in-house data and the data obtained is often focused on collecting information other than the reliability of the product.

In typical life data analysis the goal is to determine a life distribution that describes the times-to-failure (TTF) of a product. The life data analysis is conducted with the aid of statistical distributions, which enable the analyst to determine the use level probability density function, or pdf, of the TTF. The appropriate pdf for the TTF can be determined using the times-to-failure/suspension data with an underlying statistical distribution, such as the following distributions.

- The Weibull distribution is a general-purpose reliability distribution that is very flexible as it can take different shapes and approximate other statistical distributions (i.e., shape parameter or slope, β, of 1 represents exponential distribution), which contribute to its extensive popularity. The Weibull distribution is predominantly used when analyzing life data for non-repairable system.
- The exponential distribution is commonly associated with components or systems that exhibit a constant failure rate.
- The lognormal distribution is used for general reliability analysis, cycles to failure due to fatigue, materials strengths, and loading variables in probabilistic design. A system that adheres to the lognormal distribution will possess data which when the natural logarithm of the TTFs are modeled they will be normally distributed.
- The normal distribution is also used for general reliability analysis like the lognormal distribution. The normal distribution is also a good approximation for TTFs of simple electronic and mechanical components, equipment, or systems.
- The mixed Weibull distribution is used when components or systems exhibit multiple failure modes. The mixed Weibull distribution will yield the global picture of the life of a product by mixing different Weibull distributions for different stages of the product's life.
- A less utilized life data model is the generalized gamma distribution, which has the ability to mimic the attributes of other distributions such as the Weibull or lognormal based on the values of the distribution's parameters.
- The Inverse Gaussian distribution has been found to be a useful model for those situations whenever early failures or occurrences dominate the lifetime distribution. The Inverse Gaussian distribution has become popular because there is less difficulty in justifying its use in a purely physical basis, it addresses a wider class of failure time distributions, and the small sample statistical properties and inference procedures are well developed and often parallel those of the normal distribution.

After the pdf is obtained from the life data analysis, all other applicable reliability metrics can be easily determined. Other reliability metrics that the analyst may determine include: percentage failing under warranty, risk assessment, design comparison, and wearout period.

The problem of censored data is often encountered when performing life data analyses. The data are censored (also know as suspended or truncated data) when a sample observation is discontinued before an event of interest (i.e., failure, death of the who sample) occurs. This situation occurs frequently as a fact of life and statisticians have found ways to deal with it successfully.

Censoring mechanisms can be classified, based on the status of the entity observed at the time we start and finish the observation starts or finishes or on whether the experiment is stopped at the time of an "event of interest" (e.g., failure or death) or not. Censoring can occur at either extreme (beginning or end) of the observation period. That is, the entity in question may have already started or may have not yet finished operation, when the observation begins or ends. For example, in Figure 4.12, Lines "a" and "b" show an entity that has been operating for an unknown period of time, before the observation starts. This is called "left-censoring." The "X" symbols in Figure 4.12 and Figure 4-13 represent failures in time when we finish monitoring the

entities. Similarly, an entity that we have been monitoring since the beginning of an experiment can disappear and we are no longer able to monitor it (as shown in Figure 4.12, Line "b"). This other type of truncation scheme is collectively known as right censoring and is represented by a right arrow. A more complex example is presented in Figure 4.12, Line "d." Here, both the beginning and end of the entity "life" are unknown, and we can only monitor it for some part of its "life span." Finally, we may stop monitoring all the entities at some arbitrary time T, because the experiment is over (as in Figure 4-12, lines "c" and "a"). These schemes are known as time censoring, time-truncation, or suspension in time. Censoring that is not event-motivated is known as Type I censoring.

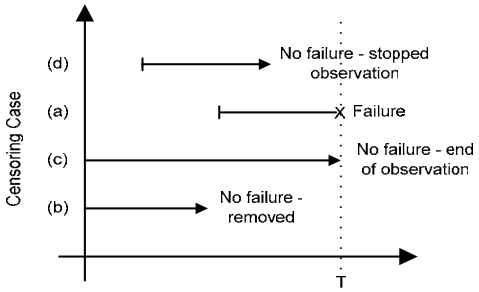


FIGURE 4-12: Type I (Time) Censoring

On the other hand, we may elect to observe a sample of "n" entities until some event of interest occurs, such as the i^{th} failure or death (denoted X_i). At this time, we will stop observing the sample (Figure 4-13, dashed line). This situation is often referred to as "failure or event truncation" and is collectively known as Type II censoring

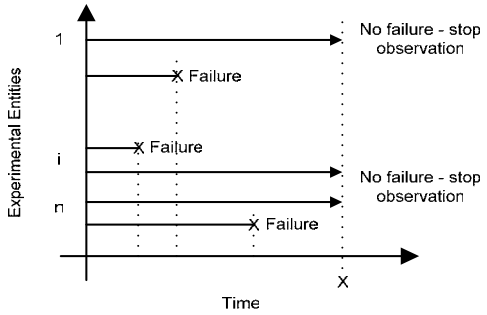


FIGURE 4-13: Type II (Failure) Censoring

In either censoring, Type I or II, the number of failures or "events" of interest, observed during the experiment, is denoted as "k" (out of the possible "n" events of all entities on trial). If the distribution of the "lives" of the entities is known, or if the probability "p" of occurrence of an event in the period of time T of observation of these entities, can be calculated, then we may be able to model the underlying statistical process. The modeling problem is approached differently if these failures are (or are not) replaced at the time they occur. The modeling also becomes much more difficult if the distribution of the entity "lives" is not Exponential (i.e., have a time-dependent hazard function). The Exponential, Weibull, and Lognormal distributions have all

proven effective in analyzing censored data, for additional information see the **Reliability and Life Testing Handbook** written by Kececioglu.

Nonparametric analysis allows the user to analyze data without assuming an underlying distribution, which can have certain advantages and disadvantages. The ability to analyze data without assuming an underlying distribution avoids the pitfalls associated with making incorrect assumptions about the distribution, but the confidence bounds associated with nonparametric analysis are usually much wider than those associated with parametric analysis and predictions outside the range of the observations are not possible with nonparametric analysis. There are several methods for conducting nonparametric analysis, including the Kaplan-Meier, simple actuarial, and standard actuarial methods. There are methods available to determine confidence bounds to the results of these nonparametric analysis techniques as well. The basis of nonparametric life data analysis is the empirical cumulative distribution function or CDF.

The Kaplan-Meier estimator or product limit estimator can be used to calculate value for nonparametric reliability for data sets with multiple failures and suspensions. The simple actuarial method is an easy-to-use form of nonparametric data analysis that can be used for multiply censored data arranged in intervals. The standard actuarial model is a variation of the simple actuarial method that involves adjusting the value for the number of operating units in an interval. The Kaplan-Meier and simple actuarial methods assume that the suspensions occur in a time period or interval at the end of that interval after the failures have occurred. The standard actuarial method assumes that the suspensions occur in the middle of the interval, which has the effect of reducing the number of available units in the interval by half of the suspensions in that same interval. Confidence bounds for nonparametric reliability estimates can be calculated in a manner similar to that of parametric confidence bounds, although determining an estimation of the variance is often difficult.

For additional information on life data analysis refer to **Applied Life Data Analysis**, by Wayne Nelson, which was originally published in 1982 by John Wiley & Sons.

4.5.2.18 Component Testing

The level of development for the components selected within a system can affect test plan development. If a system utilizes components in which their behavior is well established and the system is not subjecting the components to functional or physical stresses beyond their known limits of operation testing at the system level is acceptable, but if components with little historical data are selected component testing may be required. In this case, component testing forms an important part of the development process as the components are tested over a wide range of conditions to ensure satisfactory performance is achieved at conditions other than nominal. By achieving satisfactory performance of components at these non-nominal conditions it ensures that similar performance is likely when the components are integrated into the larger system.

A weakness of component testing is that it is often difficult to realistically simulate system environments, including parametric input and variation to the component. The extremely high reliability required of a single component requires a large number of tests to be conducted to

demonstrate component reliability. Therefore, component testing is often better suited for improving reliability by ensuring that the components that demonstrate optimum performance are selected for the system instead of quantifying the absolute value of the component's reliability.

If sufficient component testing is not conducted and system testing is commenced prematurely several risks will be present. Most notably component failures will occur, which will make tracking the system reliability difficult. Another potential risk is that the more often components fail the more often the system has to be re-started, which often presents conditions that are far more severe than those experienced at steady-state operation.

Component test plans should address several or all of the following types of tests to determine any component design limitations, behavior characteristics, and failure modes.

- Time or Life Testing: Tests enable estimations or demonstrations of numerical reliability to be conducted, but also can be used to identify the part in a component or component in a system that failed, mode(s) of failure, and mechanism (how and why) of failure. Time-to-failure testing by actually generating failure and then combining results with failure analysis helps to identify the when, which, how and why of the failure.
- Event Testing: Testing, which is analogous to time-to-failure testing, is primarily used when the starting and stopping operations are more destructive than the mere accumulation of time. The important parameter in this form of testing becomes mean number of cycles to failure.
- Peripheral Testing: Also known as overstress testing is very valuable in reliability assurance, but the test must be conducted carefully to ensure that test results remain conclusive (i.e., proving that a device fails at high stress levels is not meaningful, but defining the stress level that produces the critical stress is meaningful). Accelerated life testing which is presented in Section 4.5.2.16 provides additional information.
- Environmental Testing: Testing represents a survey of the reaction of the item to a broad spectrum of environments to show confidence in design beyond its ambient conditions (subsequent sections will present greater detail, i.e., ESS or HASS).

4.5.2.19 Analysis of Repairable Systems

Reliability is the probability that failure will not occur in the period of interest when more than one failure can occur for an item because it can be repaired after it has failed. For repairable systems, the distribution of times to first failures becomes far less important than the failure rate or rate of occurrence of failures (ROCOF) for the system. Repairable system reliability can also be characterized by MTBF, but only under the particular condition of a constant failure rate. When analyzing repairable systems, availability is a concern as well since repairs take time. Availability is the product of the failure rate and maintenance time (where maintenance is corrective or preventive). Therefore, the relationship between reliability and maintainability must be well understood for repairable systems as well as how each can affect availability.

A repairable system can be defined as an assembly of parts in which the parts are replaced when they fail. The system may be comprised of both repairable and non-repairable parts, therefore

focus is usually directed at the pattern of successive failures and whether the failed part will be replaced or repaired. The analysts first must consider a system comprised of only parts that are replaced on failure (i.e., most electronic systems), before examining the parts that are repaired (i.e., adjusted, lubricated, tightened, etc.) as the corrective action in response to failure. The system's reliability can be analyzed through the event series analysis methodology assuming that replacement (repair) times are negligible and the time to failure of any part is independent of any repair actions.

The failures occurring in repairable systems are an example of a series of discrete events, which is also referred to as recurrent event data or data from a stochastic point process. The Poisson process is often utilized when performing an analysis of such recurrent event data. The Homogeneous Poisson Process (HPP) can be used to describe the situation in which events occur randomly and at a constant average rate. HPP is a stationary point process in which the distribution of the number of events in a fixed length interval does not vary, regardless of when (where) the interval is sampled. An essential condition of any HPP is that the probabilities of events occurring in any period are independent of what has previously occurred (this assumption is known as "independent increments"). The times between failure of an HPP are a sequence of independent and identical exponentially distributed random variables. The Non-Homogeneous Poisson Process (NHPP) may also be used to model the reliability of repairable systems. The difference between the HPP and NHPP is that the rate of occurrence (intensity of events) varies with time for the NHPP rather than being a constant like the HPP. For the NHPP, not only are the points not exponentially distributed, but also they are not independent samples from any other single distribution. Therefore, statistical techniques that are based on the assumption that the data is independent and identically distributed are not valid to an NHPP.

For complex repairable systems the failure rate will tend to a constant value after most items have been replaced at least once. A constant failure rate (CFR) is indicative of externally induced failures, as in the constant hazard rate situation for non-repairable systems. A CFR is also typical for complex systems subject to repair and overhaul due to the different items of the repairable system exhibiting different patterns of failure with time and items have different "ages" since repair or replacement. Repairable systems can follow a decreasing failure rate (DFR) phenomenon when progressive repair (defective items fail early and are replaced by good items) improves reliability. An increasing failure rate (IFR) phenomenon is possible for repairable systems when wearout failure modes begin to dominate within the system. If times to failure for items are independently and identically exponentially distributed (IID exponential) the system will have a CFR equal to the sum of the reciprocals of the item's mean times to failure. This assumption of IID exponential for repairable systems can be deceptive therefore, it is important to note that:

- The overwhelming failure modes of systems are wearout-related (i.e., failure probabilities increase with time).
- Times to failure for items within a repairable system may not always be independent as the failure or repair of one item may affect the reliability of another item.
- The "good-as-new" theory to the renewal process introduced by item maintenance may not be valid as repairs may be imperfect or may introduce other defects, which lead to the failure of other items.

- Preventive maintenance (i.e., adjustment, lubrication, etc.) does not adhere to "good-as-new" theory as it extends the item's life, but it is not true renewal process.
- If spares have a decreasing failure rate in comparison to the items they replace it will increase the probability of successive failures.
- The ability to learn through experience results in the improvement of diagnostic abilities (i.e., fix effectiveness) for maintenance personnel. On the other hand, a loss or change to maintenance personnel can lead to reduced diagnostic ability and more reported failures.
- There is not always a link between item failures that leads to system failure.
- On-off cycling, various modes of operation, various operating environments, or different maintenance practices will generally have a more significant effect than operating times on generating stresses that will induce failures.
- The ability to capture objective failure data is rare as reported failures are often subjective to the individual reporting the failure. Operators or maintainers may tolerate a "problem" in some conditions, but might report the "problem" as a failure in other conditions. The perception of failure is conditioned by past experience, whether the failure is subject to a warranty, etc.
- Scheduled maintenance or planned overhaul will affect the probability of failure within a system. Systems generally exhibit higher failure rates after overhaul due to induced failures of items that may not have failed without the disturbance of overhaul. Undergoing a post-overhaul test period may mitigate these failures prior to returning the system to service.
- Spares are often not from the same population as the original items and therefore, may be better or worse in quality/reliability.
- Items operating within their specified limits can still lead to system failures as the combined tolerance of the items may cause the system to fail.
- Many reported failures are not the result of an item failing, but instead other related events such as intermittent connections, improper use, replacement of "suspect" parts, etc. are the cause of the reported failures.
- Not all items within a system operate to the overall system cycle.

For additional information on the reliability of repairable systems refer to **Repairable Systems Reliability**, by Ascher and Feingold, or **Recurrent Events Data Analysis for Product Repairs, Disease Recurrence, and Other Applications**, by Nelson.

4.5.2.20 Commercial-Off-The-Shelf (COTS) Assessment

The use of commercial-off-the-shelf (COTS) products and non-developmental items (NDI) within a military acquisition program has reliability and maintainability considerations.

COTS products may be developed with different assumptions about use-environment, maintenance venue availability or required reliability performance than regular defense equipment, therefore the item may not be properly designed for the environment and support concept that it will be subjected to by the military.

Evaluating COTS reliability is conducted differently than when evaluating the reliability of products developed specifically for the military. The lack of detailed engineering and

manufacturing data for COTS products is partially to blame, but the other primary reason is more obvious. A product under development or specifically developed for the military will have the government involved in the design process and testing as well as being active in evaluating reliability based on test results during design reviews. Table 4-3 describes the reliability activities for new development and for COTS in five areas of concern to the reliability practitioner.

Evaluating the reliability of any product in development can be done in one of four ways: using empirical models, using deterministic models, by similarity modeling, and from test or field data. Empirical models are primarily used to predict the frequency with which electronic equipment fails during any part of the equipment's useful life. Deterministic models or physics-of-failure models for reliability prediction are utilized for mechanical stress analysis to ensure that the product is designed to be sufficiently durable over its life. The similarity modeling estimates the reliability of a new product based on the reliability of its predecessor if the previous product and new product are sufficiently similar. The use of actual performance data from test or field operation enables reliability predictions to be refined and "measurements" to be taken.

TABLE 4-3: Comparison of Reliability Activities for New Development and for COTS

Area of Activity	Description of Activity	
	New Development*	**COTS****
Determine Activity	Develop requirements based on user needs and technology being used. Estimate achievable level of reliability.	Limited to verifying manufacturer claims and determining effect of military environment on reliability.
Understand the Design	Perform FMEA, FTA, and other analyses for entire design. Conduct design reviews. Develop derating criteria. Conduct development testing.	Limited to integration and design of any external items needed to allow the COTS to function.
Parts Selection	Analyze design to determine correct parts application for robust design. Identify needed screening.	At the mercy of the COTS manufacturer.
Validate the Design	Conduct extensive development testing that addresses all aspects of the design. Identify design deficiencies and take corrective action. Establish achieved levels of reliability.	Limited to what is needed to verify manufacturer claims and to validate integration or external item design.
Manufacturing	Design manufacturing process to retain inherent RAM. Implement statistical process control and develop good supplier relationships.	Limited to determining types of processes and process controls as well as developing good supplier relationships.

* Activities conducted by contractor under contract to Government. Government participation can vary, but the Government always has access to data, analyses, and design reviews.
** Activities conducted by contractor under contract to Government or by the Government.

There are several tools available to help the RAM practitioner perform COTS assessments. One well-known tool, COTS Assessment and Selection Tool, was developed through collaboration between Lockheed Martin Federal Systems and Virginia Tech. The SELECT Model was developed for the Air Force Research Laboratory Information Directorate through a contract with IIT Research Institute (now called Alion Science and Technology Corporation). SELECT (Selection of Equipment to Leverage Commercial Technology) leveraged the results of previous studies and the extensive databases of the Reliability Analysis Center into a PC-based software

tool that could quantify COTS equipment reliability and risk factors associated with the military environment. Other sources of information on COTS equipment include:

- Commercial Item Military Market Research (CMMR) Information Center, which is a DoD information center for market research data.
- Navy Product and Technology Surveillance (PATS), which is a subset of CMMR, that specializes in information related to computer electronics utilized in Navy applications.
- The US Navy also supports the Computer Open Systems Implementation Program (COSIP), which is an engineering process for identifying, evaluating, and documenting commercial and open-system computer resources for potential use within Naval combat systems.

4.5.2.21 Reliability Centered Maintenance (RCM)

RCM is a logical, structured framework for determining the optimum mix of applicable and effective maintenance activities needed to sustain the desired level of operational reliability of systems and equipment while ensuring their safe and economical operation and support. RCM is focused on optimizing readiness, availability, and sustainment through effective and economical maintenance.

Prior to the development of the RCM methodology, it was widely believed that everything had a "right" time for some form of preventive maintenance, usually replacement or overhaul. A widespread belief among many maintenance personnel was that by replacing parts of a product or overhauling the product (or reparable portions thereof), that the frequency of failures during operation could be reduced.

Despite this commonly accepted view, the results seemed to tell a different story. In many instances, preventive maintenance seemed to have no beneficial effects. Indeed, in many cases, preventive maintenance actually made things worse by providing more opportunity for maintenance-induced failures.

The RCM approach provides a logical way of determining if preventive maintenance makes sense for a given item and, if so, selecting the appropriate type of preventive maintenance. The approach is based on the following precepts:

- The objective of maintenance is to preserve an item's function(s). RCM seeks to preserve a desired level of system or equipment functionality.
- RCM focuses on the end system. The RCM process focuses throughout the life cycle on the end system, from design through disposal. It seeks to preserve end system functionality, not to prevent all failures.
- Reliability is the basis for decisions. The failure characteristics of the item in question must be understood to determine the efficacy of preventive maintenance. RCM is not overly concerned with simple "failure rate;" it seeks to know the conditional probability of failure at specific ages (the probability that failure will occur in each given operating age bracket).

- RCM is driven first by safety and then economics. Safety must always be preserved. When safety (or a similarly critical consideration) is not an issue, preventive maintenance must be justified on economic grounds.
- RCM acknowledges design limitations. Maintenance cannot improve an item's inherent reliability – it is dictated by design. Maintenance, at best, can sustain the design level of reliability over the life of an item.
- RCM is a continuous process. The difference between the perceived and actual design life and failure characteristics is addressed through age (or life) exploration.

The RCM process for the System Development and Demonstration phase is illustrated in Figure 4-14. Chapter 6 will discuss how the RCM process must be reviewed during the Operations and Support phase of the system's life cycle to ensure that field data supports the initial maintenance program developed during Step 2.

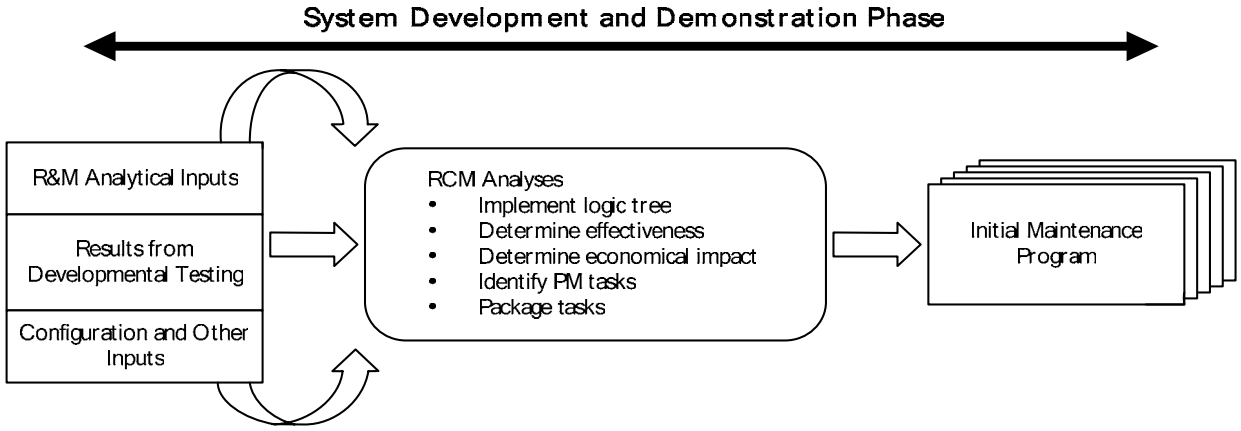


FIGURE 4-14: The RCM Process in the System Development and Demonstration Phase

Maintenance expenditures throughout a product's lifecycle often exceed the purchase price. Careful planning of scheduled preventive maintenance through RCM can greatly reduce the total cost of ownership. Dedicated application of the following steps of an RCM analysis can potentially save money.

Step 1: Design for Maintainability
- Facilitate required inspections with fewest tools possible.
- Match component failure rate to preventive maintenance schedule.
- Provide indicators of failure (gauges, alarms, wear indicators).
- Reduce risk of maintenance actions that may induce more failures (captive fasteners, built-in-test (BIT), etc.).

Step 2: Perform Functional Failure Mode Analysis
- FMEA (determines how a system can fail, see section 4.5.2.9).
- Fault Tree Analysis (discussed in section 4.5.2.10).
- Determine consequences of failure (safety, operational, economic, or hidden).

Step 3: Categorize the Failure Distributions

- Perform Weibull Life Data Analysis on parts (see section 4.5.2.17). Determine β (shape) and η (scale or characteristic life) parameters.
- If applicable, determine when wear out begins.
- Determine effectiveness of rework/rebuild actions (failure distribution before and after rework/rebuild).

Step 4: Determine Maintenance Tasks Intervals

- Maintenance task types in order of preference:
  - On-condition (inspection, measurement, observation, non-destructive testing) for parts more prone to failure (potential failure),
  - Rework/rebuild (restoration to "like new" condition),
  - Discard (remove and replace with new component/assembly), and
  - Failure identification (inspect for an undetected failure).
- Be conservative when necessary data is unavailable. Annotate these cases for later data collection efforts.
- Tasks should be both applicable and effective in order to be considered as part of an RCM program, criteria for both are identified in Table 4-4.

TABLE 4-4: Task Applicability and Effectiveness Criteria

Task Type	Applicability Criteria	Effectiveness Criteria
On-Condition	• Reduced failure resistance can be detected (potential failure) • Consistent time between potential failure and functional failure	• Task reduces failure to an acceptable level • Cost of scheduled preventive maintenance is less expensive than corrective maintenance and the cost of failure without preventive maintenance
Rework/Rebuild	• Components/assemblies exhibit a distinct wear out period ($\beta > 1$) • Most components/assemblies survive to this time • On-condition task not applicable and effective	• Task reduces failure to an acceptable level • Cost of scheduled preventive maintenance is less expensive than corrective maintenance and the cost of failure without preventive maintenance • Rework/rebuild will restore item to like new condition and failure resistance
Discard	• Components/assemblies exhibit a distinct wear out period ($\beta > 1$) • Most components/assemblies survive to this time • On-condition task or rework task not applicable and effective	• Task reduces risk of failure to an acceptable level • Cost of scheduled preventive maintenance is less expensive than corrective maintenance and the cost of failure without preventive maintenance
Failure Identification	• Failure is not evident to operators of equipment • Failure results in increased risk of failure to other components • On-condition task, rework task or discard task not applicable or effective	• Task reduces risk of multiple failures to an acceptable level • Cost of scheduled preventive maintenance is less expensive than corrective maintenance and the cost of failure without preventive maintenance

Step 5: Package All Tasks into an Implementable Plan

- Group tasks with similar intervals to a common interval assignment.
- Compromise (lengthen/shorten) intervals of tasks designed to prevent less serious failures to coincide with intervals of tasks designed to prevent safety or great economic consequence failures.

Step 6: Optimize Results with Data Collection Efforts

- Perform trend analysis to verify that your equipment is not degrading with the implemented preventive maintenance schedule.
- Utilize information from the data collection, analysis, and corrective action system (DCACAS) to analyze assumptions made in initial preventive maintenance schedule development.
- Adjust tasks and/or intervals based on data collected to optimize availability and expenditures.

Step 7: Analyze Results for Potential Corrective Action

- All tasks and intervals are based on economic grounds.
- Redesign is a consideration for any item whose failure modes cannot be reduced to an acceptable level with preventive maintenance.
- Redesign is mandatory for failure modes that cause safety consequences and cannot be reduced to an acceptable level with a preventive maintenance task or combination of tasks.

The histogram shown in Figure 4-15 represents an optimal preventive maintenance point for a representative RCM analysis. The optimal preventive maintenance point identified in Figure 4-15 is based on the percentage of components failed at various times to failure, in this case the PM point is chosen prior to the times to failure in which a majority of the component population will experience a failure. The optimal PM point is often based on some interval in which a specified percentage of the component population will have experienced a failure (i.e., the B10 life of bearings represents the point in which 10% of bearing population will fail). Before implementation of a preventive maintenance task and associated task interval, an economic justification should be performed. The cost of performing the preventive maintenance should be less than the cost of running to failure.

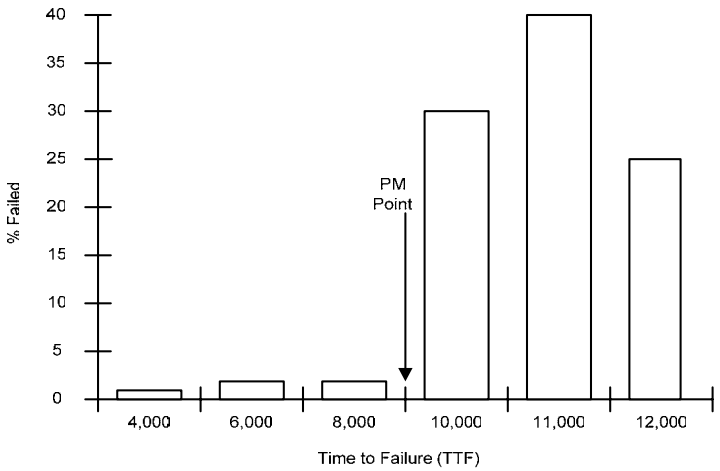


FIGURE 4-15: Determination of Optimum Preventive Maintenance Point

4.5.2.22 Condition Based Maintenance (CBM)

In an effort to reduce the total ownership costs, while simultaneously improving performance and reliability, many organizations have turned to condition-based maintenance (CBM) programs. CBM, when applied correctly, is compatible with and supports other maintenance optimization technologies like RCM. CBM is based on the premise that an optimal decision (maintenance point) will be one that maximizes the utility of the expected results (in terms of increased product output, decreased maintenance costs, etc.) given the costs (both short term and long term) of implementing the decision. CBM focuses on monitoring and managing equipment and system health. CBM can be planned during the System Development and Demonstration phase of the system's life cycle based on legacy systems, assemblies, or components. The planned CBM activities based on the legacy information should be verified during testing, but may not be fully proven until the system is deployed and exposed to its "real-world" conditions.

Condition monitoring, or continuous inspection, is the basis of CBM. Condition monitoring is the ongoing surveillance of the operation of a system or process to ensure specified performance and to detect abnormalities that may indicate an impending failure or of a failure that has already occurred. Therefore, condition monitoring enables corrective maintenance to be performed when an "out-of-specification" condition exists or preventive maintenance when early system deterioration occurs and a scheduled component replacement, adjustment, or calibration is desired.

CBM is ideal when it is not possible to accurately anticipate and predict the expected wear out trends and characteristics of a product or process with age. CBM is also effective when the criticality of a failure warrants the continuous monitoring of a particular product function or component, or process parameter. Different types of condition monitoring techniques and sensing apparatus exist and can be tailored to fit the nature, characteristics, and functionality of the parameter being observed.

There are numerous condition monitoring and non-destructive testing techniques available; the following bullets identify some of the more popular techniques.

- Visual Inspection Techniques: Visual inspection is one of the oldest and most utilized testing and condition monitoring techniques, but over the years some of the hurdles (i.e., personnel access, noise levels, light conditions, etc.) historically faced by visual inspection have been neutralized with the aid of new technologies (i.e., fiber optics, video cameras, etc.). Visual inspection is still limited to surface conditions as only surface defects and anomalies can be detected with this technique, but even more restrictive is the subjective nature of visual inspection as two inspectors can arrive at completely different conclusions.
- Optical Inspection Techniques: Optical inspection can be utilized to detect equipment part and component surface defects and inconsistencies, but requires far greater skill level than visual inspection to apply.
- Radiographic Monitoring Techniques: These techniques can be classified into two groups, static radiography and dynamic radiography. Both techniques generate a two-dimensional image that depicts the grade passage of X rays or gamma rays through equipment being monitored or inspected. Static radiography is used to analyze stationary objects, whereas dynamic radiography concentrates on moving components within

equipment. Either technique provides an effective way to detect internal cracks, bubbles, imperfections, non-homogeneities, and material composition inconsistencies. Obviously the biggest disadvantage to this technique is the cost associated with the radiography equipment and advanced training needed to perform it.

- Neutron Analysis Techniques: This technique determines equipment part material or fluid constituents as well as the individual quantities of these constituents. Therefore, this technique is highly effective in determining whether a process or product is within the required parameters with respect to material composition. The technique is accomplished by irradiating a fluid sample or piece part as each constituting material will have a different resulting radioactivity, which is first analyzed to identify the constituents and then estimate their percentage(s). Once again, this technique is costly, but with the exposure to radioactivity it can also be hazardous to personnel.
- Ultrasonic Monitoring Techniques: Both internal and external defects in a component or equipment part can be detected using ultrasonic monitoring. Ultrasonic waves are bombarded against the surface of an equipment piece part and these waves travel through the material of the component and are reflected back for analysis of material conditions. Ultrasonic monitoring equipment is significantly less expensive than radiographic monitoring equipment, but irregularly shaped objects and objects with a complex surface geometry are tedious, at best, to analyze.
- Acoustic Emission Technology: Acoustic emission captures the telltale noise (sound waves) created by material transformation due to cracks, tears and fissures, corrosion, etc. Acoustic emission not only captures these sound waves, but also can isolate the number and location of them. The technique is valuable in detecting "live" material transformations in which applied stress, progressive wear out, environmental degradation, or chemical exposure is currently affecting the product. Acoustic emission often needs to be combined with ultrasonic or radiographic techniques for a complete analysis as this technique alone can not determine the magnitude of the crack or other material transformation.
- Vibration Analysis Techniques: The underlying principle behind this technique is that the vibration characteristics of a component without a defect are different than the vibration characteristics of a similar component with a defect. The sensitivity of the technique to "pick up" very small fissures or cracks makes it popular for detecting component material transformation resulting from stressful conditions, environmental and chemical degradation, age or even dormant inconsistencies internal to a component relative to homogeneities. The skill level of personnel performing this technique must be high and set up time is often lengthy since experiments must be performed on defect-free components first.
- Lubricant Analysis Techniques: The objectives of equipment lubrication include decreased friction between moving parts, reduced heat generation, and inhibition of moving parts' wear out characteristics. The lubricating oil often "washes" away any loose or worn-out particles as well. Therefore, analysis of the oil can provide insight into the inner working of the overall equipment. Although wear out is always expected, progressive wear out trends may be estimated, potential failure preempted, contaminations detected, and any undue wearing out immediately detected and subsequently prevented by carefully analyzing this washed-out oil. Analysis of the lubricating oil may involve chemical spectroscopy, physical particle sizing and counting,

and ferrography (involves measurement and projection of progressive machine wear). Lubricant analysis techniques can be supplanted with the judicious use of advanced, small-pore filters as the filters can continuously capture the washed-out particles for a more efficient lubricant analysis.

- Magnetic Flux Leakage Techniques: Magnetic flux leakage is performed by first magnetizing the surface of the equipment or component being studied so that future deviations caused by surface discontinuities in the magnetic flux generated are detected, recorded, and analyzed. This technique is best suited for application when the surface of the object or component being analyzed has a simple and smooth geometry with limited sharp edges. Only ferromagnetic materials can be tested using this technique.
- Temperature Analysis Techniques: This approach is applicable when condition monitoring involves detecting any undue temperature deviations (e.g., a failure renders a cooling system valve inoperable resulting in high operation temperatures, which, in turn, may cause other potentially undesirable effects such as thermal viscosity breakdown, leaking gaskets, and engine seizure). Various tools enable temperature analysis to be effectively implemented including contact temperature sensors (thermocouples, thermometers, thermopiles, etc.) as well as infrared imaging. Infrared imaging can be used to detect and isolate "hot spots" as well as analyze circuits and detect breaks, shorts, and "cold spots." Temperature analysis equipment is very expensive though so it is difficult to warrant such analysis with some programs.
- Eddy Current Testing Techniques: Eddy currents are electric currents created whenever a metallic material is introduced into an electromagnetic field and relative movement between the two exists. The phase and magnitude of the eddy currents is affected by the presence of any material discontinuities such as bubbles, cracks, tears, or pores. Eddy current testing is highly sensitive and can be used to detect extremely minute defects, but it still remains relatively inexpensive. Obviously only electrically conductive and ferromagnetic materials may be inspected and monitored with this technique.
- Leak Detection Techniques: Also known as bubble testing, sonic or acoustic leak detection, and spectrometry depending on the type of approach utilized. Bubble testing coats the object surface with a solution that forms bubbles in the event of gases leaking out through the surface. Sonic and acoustic leak detection is based on the principle that sound waves are generated when fluids flow through a crack, pore, or orifice. These sound waves are accompanied by a certain amount of turbulence and/or cavitation, which can be "listened for" with the help of highly sensitive sonic receivers. The characteristics of the sound generated are not only a factor of the fluid, but the size of the leakage as well. Spectrometry involves introducing tracer gases into the fluid and then tracking these gases for potential tears or cracks in the equipment. The cost associated with the leak detection techniques depends on the level of sensitivity desired in the results.

4.5.2.23 Maintenance/Maintainability Demonstration and Evaluation

The basic objectives of designing for maintainability are to meet the operational readiness requirements for the product and to reduce support costs. An engineer committed to these objectives will continually challenge the design to uncover weaknesses and potential maintenance problems. The objective is to design in maintainability and if this objective is not met then corrective actions will have to be incorporated into the design later in the equipment's

life cycle at a significant expense. The primary emphasis of the maintainability program is to identify and correct maintainability problems early in the design process when correction simply requires changing drawings.

Maintainability is defined as the measure of the ability of an item to be retained in or restored to a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair.

Testing related to maintainability can be grouped into five basic areas: functional, performance, verification, demonstration, and evaluation.

1. Functional: Verify that a product or product function (i.e., on-condition monitoring or built-in test (BIT)) is operating as intended. Functional testing usually involves applying a known stimulus or set of stimulus to the test item and comparing the item response to a known response or set of responses.
2. Performance: Confirm that the level of performance that the product functions at meets the specified requirements. BIT and diagnostic tests are specialized types of performance testing for maintainability that is conducted.
3. Verification: Continually performed throughout product development to determine the accuracy of and update the analytical data obtained from engineering analysis. Verification is typically performed prior to any planned demonstration or evaluation test to provide assurances that the maintainability of the product can be achieved and demonstrated. Test data should be collected and used to verify the maintainability analyses and requirements.
4. Demonstration: A formal process conducted by the product developer and the end customer to determine whether specific maintainability requirements that have been specified have been achieved. Demonstration testing will require a formal test plan be developed that will use defined methods of analysis to determine compliance.
5. Evaluation: For all levels of maintenance and product design, evaluation testing determines the impact of the operational as well as maintenance and support environments on the maintainability parameters of the product. Evaluation testing should be performed for defined maintenance tasks in the product's actual use environments.

Maintainability analyses provide a means of:

- Determining how well the design is progressing toward meeting the maintainability requirements.
- Evaluating the impact of important design decisions, such as the type of fasteners used, design of support equipment, location of access panels, etc.

Maintainability analyses include, but are not limited to: equipment downtime analysis, maintainability design evaluation, FMEA, testability analysis, and human factors analysis. Equipment downtime analysis is used to evaluate the expected time that a piece of equipment is not available due to maintenance or a supply backlog. Maintainability design evaluation is the process of analyzing the maintenance implications of a proposed or evolving design and providing feedback to the designer in a timely manner. The maintainability design evaluation

process utilizes a set of standards consisting of a preliminary "use study," maintenance concept, qualitative and quantitative maintainability requirements as well as lessons learned. The FMEA as discussed previously is a reliability analysis and design tool, but in this case it is being used to establish the necessary maintainability design characteristics based on potential failure modes and their effects on subsystems, equipment, and product operation. The testability analysis determines fault detection percentages and the fault isolation effectiveness of designed tests. There are several modeling tools available to conduct the testability analysis; however, test effectiveness and model accuracy are the responsibility of the test designer. Human factors analysis helps achieve one of the most basic maintainability requirements as it ensures that the system be easily maintained by human personnel. The human factors analysis is performed to identify problems related to the interaction between maintenance personnel and the design model in performing each maintenance task. Past human factors analyses were time consuming as they required the construction of expensive physical mock-ups, but nowadays there are a variety of modern, animated, computer-aided-design (CAD) tools and new virtual reality techniques available that have proven to be effective and efficient.

For additional information on maintenance/maintainability, refer to MIL-HDBK-470A, **Designing and Developing Maintainable Products and Systems, Volume I and Volume II**, MIL-HDBK-472, **Maintainability Prediction**, and the **Maintainability Toolkit** prepared by the Reliability Analysis Center.

4.5.2.24 Analysis Demonstration and Test of Testability/Diagnostics

Requirements for system/subsystem diagnostics have traditionally taken the form of quantitative testability figures of merit. Although the quantitative method of specifying requirements remains appropriate, it does not sufficiently address the need to ensure that adequate and cost-effective diagnostic capabilities are present. The system developer should go beyond the quantitative method to identify to lower level design engineers the specifics as to how their equipment will fit into the overall demonstration/test strategy for the system.

Each level of repair must address the following functions of prognostics/diagnostics:

- Fault Detection: A process that discovers the existence of faults.
- Fault Isolation: Where a fault is known to exist, a process that identifies one or more replaceable units where the fault(s) may have occurred.
- False Alarms: An indication of a fault where no fault exists, such as operator error or built-in test (BIT) design deficiency.

Prognostics/diagnostics requirements are often expressed in the form of fractions such as:

- Fraction of Faults Detected (FFD): Quantity of faults detected by BIT or external test equipment divided by the quantity of faults detected by all detection means (including manual).
  - System and Equipment Level: FFD is usually weighted by the measured or predicted failure rates of the faults or replaceable units.

  - Microcircuit Level: FFD is called fault coverage or fault detection coverage, and all faults are weighted equally. In the fault-tolerant design community, "fault coverage" almost invariably refers to fault recovery coverage. This is usually expressed as the conditional probability that, given a fault has occurred and has been detected, the system will recover.
- Fault Isolation Resolution (FIR): Probability that any detected fault can be isolated by BIT or external test equipment ETE to an ambiguity group of size "x" or less (typically specified for several values of "x").
- False Alarm Rate (FAR): The frequency of occurrence of false alarms.

The overall demonstration/test strategy for the system often determines what type of demonstration or testing is employed at the lower levels of design for prognostics/diagnostics. The ability to perform the prognostics/diagnostics is based on the extent that the system developer has specified the following elements of the demonstration/test strategy to suppliers/subcontractors:

- Interfaces: Includes all test system interfaces to be utilized throughout the system hierarchy.
- Test Data Sharing: Identification of data to be passed from one system level to another.
- Data Deliverables: Sufficient data about internal test structures within supplier's equipment must be available to the test program set (TPS) developer.

The scope of prognostics/diagnostics for a system or subsystem can be broken into four parts: embedded, external, manual, and the TPS. The embedded portion of prognostics/diagnostics is defined as any portion of the system's prognostic/diagnostic capability that is a critical part of the prime system. The external portion includes the prognostic/diagnostic capability that is not embedded within the system or subsystem (primarily automatic test equipment or ATE). Manual prognostics/diagnostics includes testing that requires the use of technical manuals, troubleshooting procedures, and general-purpose test equipment (i.e., voltmeter) by a maintenance technician. The TPS is the portion of the prognostic/diagnostic capability that is comprised of the complete collection of data and hardware to test a specific unit-under-test on a specific ATE. The TPS consists of test vector sets (for a digital unit-under-test), test application programs (software that executes on ATE and applies vectors under necessary conditions), text fixtures and ATE configuration files, and documentation.

System prognostic/diagnostic requirements should be developed as an outgrowth of the user's needs and expectations. For military systems, the user is predefined, and their needs for the system are well documented. Commercial system development poses much greater risks and challenges. Extensive market research is often the only way to determine the user needs and expectations for the system. Once this is complete, the diagnostic requirement trade-offs involving reliability, maintainability, logistics, weight, power requirements, and allowable system interruption must be made. Realistically achievable fault detection and isolation capability is significantly different for various products depending on the percentage of non-digital electronics and the reliance on COTS equipment. A minimum requirement for commercial contracts should be end-to-end go/no-go fault detection either on-line or operator initiated. Typical values for testability at lower levels of assembly are shown in Table 4-5.

TABLE 4-5: Typical Testability Values

Parameter		% Capability	Repair Level
Fault Detection (all means)		80-90	Field Service
		100	Shop
		100	Factory
Fault Detection:	BIT & ETE	75-85	Field Service
	BIT & ETE	90-95	Shop
	BIT & ETE	95-100	Factory
Fault Isolation Resolution:	Three or fewer major units	90-95	Field Service
	One major unit	90-95	Shop
	Five or fewer circuit cards	100	Factory
	One circuit card	75-85	Shop

Notes:
ETE – External Test Equipment
BIT – Built-in Test
Major Unit – Power supply, amplifier assembly, etc.
Circuit Card – Replaceable electronic board with components attached.

The most important factor for designing prognostics/diagnostics into a system or subsystem is early planning to maximize the advantages of these tools and minimize any negative impacts such as increased design costs, higher hardware overhead, and increased failure rate. Designers and managers must remember that the effectiveness of the diagnostic capability, and the cost of development, is greatly influenced by the amount of testability that has been designed into the system. A lack of test points available to external test equipment, for example, may adversely affect the ability to isolate failures to smaller ambiguity group sizes. The result is higher costs to locate the failure to a single replaceable item.

The RAM Assessment section (4.5.2.4) introduced the problem with complex systems where development of the diagnostics software lags the operational software. The RAM assessment process has to include the functional reliability of the BIT and ID software. One approach used by some developers is fault insertion testing at subsystem and system levels to assess and validate fault detection and isolation logic algorithms. These are called "Initial BIT Assessments." At the vendor level, these IBA's effectively develop the functionality of the BIT software. At the integrated system level, they assess and develop the functionality of the Integrated Diagnostic software design. Both approaches are required through both the detailed specification and contract, and are a major section of the RAMPP for developing the overall maintainability of the platform.

Additional information on testability/prognostics/diagnostics can be found in

- Rome Laboratory's RL-TR-91-180, **Analysis and Demonstration of Diagnostic Performance in Modern Electronic Systems**,
- Air Force Guide Specification 87256 **Integrated Diagnostics**,
- MIL-STD-1309D, **Definitions of terms for Testing, Measurement, and Diagnostics**,
- Navy Technical Brief, **Built-in-Test Design and Optimization Guidelines,** TB# ABM1001-01, and
- The Reliability Analysis Center's **Maintainability Toolkit**.

4.5.2.25 Man-in-the-Loop Testing

Testing of human performance as part of the overall system is essential and should be an integral part of the engineering and development test program.

The objective of human-oriented or man-in-the-loop testing is to ensure that the technical and operational requirements can be met. A more general objective is to influence the system or process design in a manner that yields improved human performance and reliability. In particular, the objectives of the man-in-the-loop testing are to:

- Verify that personnel can safely perform tasks to time and accuracy standards without excessive workload.
- Verify that the facilities and system or process configuration support human use.
- Determine adequacy of human performance as a component of system or process performance.
- Determine the effects of environments and use scenarios on human performance in operation and maintenance.

The emphasis of man-in-the-loop testing activities changes as the system or process proceeds through the development process. Early in the development of the system or process, the developer and user identify the critical safety, ergonomic, and human performance-related issues and criteria to be used in both developmental and operational testing. Later in the development process, the emphasis shifts to evaluating the adequacy of the user-system interfaces.

It is possible to integrate aspects of man-in-the-loop testing with reliability and maintainability testing. What is normally a hardware-software reliability test would have its scope and its facilities expanded to account for participation by human test subjects. Similar monitoring can be used in maintainability testing. In both reliability testing with humans and maintainability testing, the facilities should resemble the actual operational facilities very closely.

The selection of humans to be used in testing (i.e., test subjects) can influence the results of the testing greatly. The guiding principle that should be used in selecting humans to be used in testing is that, "Testing should use 'typical users' to operate and maintain the system or process under conditions that simulate the actual use conditions."

"Typical users" are those selected from the population that will be associated with the system or process. In selecting these test subjects, one should consider the following factors:

- Demographic: age, aptitude level (ASVAB), educational level, gender, skill type and level, specialized training and experience
- Anthropomorphic: standing height, sitting eye height, weight and hand reach
- Physiological: color vision, dominant hand and eye, and strength

The preferred approach to testing, of course, is a physical test of the actual system or process in a physical and psychological environment that closely resembles the operational environment and with personnel who are representative of the user population. However, when physical testing is

not possible, one may resort to the use of computer modeling, simulations (preferably on-line interactive simulations), or engineering analyses.

On-line interactive simulation involves the use of real-time computer program simulations and actual test participant operators. Like other simulations, on-line interactive programs can be used to evaluate the application of specific procedures and equipment to specific operations. The time to use on-line simulation generally is before the construction of the actual hardware and the software. The following guidelines apply to the use of this form of simulation:

- Construct an accurate representation of the desired portion of the proposed system.
- Ensure that critical variables in the proposed system are duplicated properly in the simulation.
- Provide test participant consoles that are substantially similar to the system consoles being simulated.
- Preparation of test participant operator procedures that are substantially similar to the expected operational procedures.
- Construct the operator controls to resemble those planned for the actual system or process.

4.5.2.26 Sparing Models Assessment Methods

A common industrial practice that is used to reduce production downtime is to maintain an inventory of spare parts for the production equipment. Although theoretically the management of the spare parts inventory is straightforward the process can often be rather intricate in practice. The premise of maximizing production while minimizing the spare parts inventory costs is simple, but modeling this becomes complex as the production process, equipment type, failure mode and failure effect must all be accounted for. Therefore, a sparing model may be based on a discrete simulation of the production process, the reliability models associated with the equipment, and the logistics duration (specifically repair time and acquisition time). Historical data should be used to validate the model's accuracy.

The analysis of sparing levels has become more accurate and advanced as early attempts at determining the quantity of spares were based on a fixed percentage (5% to 10%) of the total units in operation, whereas current analyses utilize the Poisson probability distribution. The Poisson distribution defines the number of changes (failures) in a specified interval (time) when the average number of changes is small. The use of the Poisson distribution yields sparing levels that better fit the demand, which means spares are available (and not excessively) when they are needed with a limited footprint to storage space and invested capital.

The successful application of a sparing model will determine optimal initial support values for the product as well as incorporating changes from experience data that will further improve support while minimizing support costs as the product matures throughout its life cycle. A sparing model must have the following two basic elements:

1. Identify the minimum number of spares required at each point in the supply chain to achieve the objectives and requirements of the product.

2. Develop a plan for the logical flow of spares from the manufacturer or repair facility to the end user as well as the path that repairable parts will be returned.

The Multiple Spares Prioritization and Availability to Resource Evaluation (M-SPARE) Model was developed for the NASA Space Station Freedom by Logistics Management Institute. The Secretary of Defense's effort in 1985 to adopt a weapons management system that set inventory levels based on readiness and cost has developed into a weapons system management concept referred to as Readiness Based Sparing (RBS). The Army's Selective Stockage for Availability Multi-Echelon Model (SESAME) and the Naval Sea System Command's (NAVSEA) model named TIGER (see Section 4.5.2.27) compute supply support requirements based on the RBS concepts.

4.5.2.27 Specific Models (i.e., ACIM/TIGER)

There are several models that have been developed over the years to support the efforts of analysts as they examine the reliability, availability, and maintainability of products. Two such models are the Availability Centered Inventory Model (ACIM) and TIGER, which both were developed by the US Navy.

ACIM is a unique software tool that provides the analyst the capability to optimize a spare parts inventory. The primary objective of the ACIM software is to quantify the spare parts inventory in a manner that will minimize equipment downtime while awaiting parts. ACIM strives to maximize operational availability (A_o) for the equipment as well as better understand the complex relationship between reliability, maintainability, and supportability characteristics when the equipment is still being designed. ACIM will identify a spare parts inventory that will satisfy both a required A_o for the equipment at the lowest cost, and maximize A_o at a fixed cost.

ACIM is the only "sparing to availability" model currently approved for use on US Navy systems as it has proven itself time and time again in its ability to effectively improve A_o for several systems in the US Navy fleet. The central algorithm of ACIM is the Availability Centered Inventory Rule (ACIR), which has proven to be versatile as it has been implemented for spares optimization for equipment types in a multitude of business applications.

TIGER uses stochastic simulation (Monte Carlo type) to mathematically estimate reliability and availability for a complex system. The reliability block diagrams that are created by the TIGER software for a complex system can be readily translated into compact input coding. Apart from the standard reliability and availability figures of merit, TIGER provides quantified and ranked lists of reliability and availability critical equipment. TIGER uses "event driven" simulation techniques consisting of five distinct events:

- Equipment failure (up to down)
- Equipment repair (down to up)
- Change of operational equipment configuration requirements within the mission
- Beginning of mission
- End of mission

The equipment failure and equipment repair times are derived utilizing the simulation techniques of TIGER, whereas the change of operational equipment configuration, beginning of mission, and end of mission times are supplied as input data.

4.5.2.28 Parts Obsolescence and Diminishing Manufacturing Sources

The parts used in a system are purchased to specifications designed to ensure their reliability, and from suppliers who can produce parts with the desired RAM metrics. However, it often becomes unprofitable for a part supplier to continue production of a particular product line. When this happens, continued production of products using the parts and replacement of failed parts may require the use of parts with lesser reliability, resulting in degradation in the inherent reliability of the products using them. In extreme cases, replacement parts at reasonable cost may not be available. Attention to parts obsolescence helps avoid such problems. Another factor that has increased awareness in parts obsolescence and diminishing manufacturing sources is the move by the military to increase its use of non-developmental items (NDI), which includes commercial-off-the-shelf (COTS) items, in new and modified designs. It is imperative that manufacturers develop a strategy to cope with diminishing sources of parts, components, materials and/or suppliers resulting from unilateral supplier decisions, technology advancements, or shakeouts in a competitive marketplace.

By considering parts obsolescence as part of the overall system life cycle planning, it is possible to avoid the significant trouble and expense entailed in searching for replacement parts. The need for a replacement part that is no longer available on the market can be satisfied relatively cheaply and quickly when solutions to obsolescence are in place, or it can be addressed by time consuming and expensive crisis management actions when the unavailability of the part comes as a surprise.

Determining when components or materials will become obsolete or when the number of suppliers has reached a critical level requires a manufacturer to have in-depth knowledge of as well as a close working relationship with its supplier base. The ability to do so effectively allows both industry and the government to assess the impact of obsolescence on their systems and plan for the future. As product and system lifetimes are extended, and as new technology cycles get shorter, component/materials obsolescence and diminishing manufacturing sources become greater problems.

Parts management starts in the Concept Refinement phase with a preferred parts list (PPL), which provides a description of parts designers may use. No other parts should be allowed, except when it is impossible to meet a performance/RAM requirement with the parts of the PPL. The PPL should be updated before each application to a new product development. This update should consider the obsolescence of all parts listed. Parts that are likely to become difficult to obtain should be removed from the list. This action should be followed by the determination of an appropriate action to ensure that products currently using the part can continue to be supported.

Preferred parts lists should be reviewed periodically and individual parts listed should be re-evaluated at any sign of obsolescence (manufacturers discontinuing a production line,

introduction of newer technology with significant advantages, feedback from buyers reporting difficulty with spare parts purchases, etc.).

The explosive advance of technology has resulted in component parts that are smaller, lighter, cheaper, more capable and more reliable. One bad effect of this is that every technological advance reduces the market for older parts, which ultimately go out of production. As a result, it may become impractical to obtain replacement parts for failed components of a product in use. Attention to parts obsolescence is meant to lessen the impact of diminishing parts availability.

There are many possible remedies to part obsolescence problems when they are identified early. The options decline as time passes, some are:

- Lifetime (or Life of Type) buy: When it is reasonable to assume the availability of a part will soon decrease, a good strategy might be to purchase enough spares to last the expected lifetime of the product. This assumes that there will be no degradation of parts in storage.
- Substitution: If a newer part can be purchased with the same form, fit and function of the obsolete part, it can be directly substituted. The impact of the part substitution on inherent product RAM should still be assessed, however to ensure reliable performance.
- Redesign: To avoid the need for an obsolete part, a redesign of the product to eliminate it can be performed. This should be done at the lowest possible level of assembly (i.e., a board rather than an assembly of boards, an assembly rather than a module of many assemblies, etc.). The new design can then be retrofitted to the product when the obsolete part fails. If the new design has other benefits (i.e., faster speed, more memory, etc.), it may be desirable to retrofit the product before the part fails, as a performance upgrade. The effect of the redesign on inherent product RAM should still be evaluated to avoid the potential of no longer meeting the customer's RAM needs.

Component and supplier obsolescence management needs to be a basic part of a company's design, manufacturing and operating procedures. These best commercial practices should be implemented throughout all phases of the acquisition process, and should be product independent. Implementation of the component/supplier obsolescence management program prior to the start of the System Development and Demonstration phase of the system's life cycle can help ensure long-term reliable operation of the product or system, and the continuation of efficient maintenance and repair support.

4.5.2.29 Bayesian Techniques

All relevant information from tests and field use of related systems, developmental tests, early operational tests, and training and contractor testing should be examined for possible use in both the design and evaluation of operational tests. Given the importance of the decision on whether to proceed to full-rate production, state-of-the-art statistical methods for combining information should be used, when appropriate, to make tests and their associated evaluations as cost-efficient as possible.

Bayesian techniques provide a framework for combining such relevant information. In the Bayesian approach, the model consists of two parts: the likelihood function and the prior distribution. The likelihood function is typically constructed from the sampling distribution of the data, which describes the probability of observing the data before the experiment is performed. Once we perform the experiment and observe its data, we can consider the sampling distribution as a function of the unknown parameters. This function (or any function proportional to it) is called the likelihood function.

In Bayesian analysis, the unknown parameters in the likelihood function are treated as random, and a probability density function describes the uncertainty about them. This probability density function is the prior distribution for the parameters. In Bayesian analysis, the likelihood function and the prior distribution are the basis for parameter estimation, inference, and test design. Great care must be taken in the specification of the likelihood function and the prior distribution, as the results will be affected by these choices.

One major philosophical difference from classical frequency-based methods is the notion of probability that is considered. Classical methods are rooted in the well-known relative frequency notion of probability defined as the limiting relative frequency of an event in a repeated series of identical trials. In contrast to this notion, the cornerstone of Bayesian methods is the notion of subjective probability. Bayesian methods consider probability to be a subjective assessment of the state-of-knowledge (also called degree-of-belief) about reliability parameters of interest, given all the available evidence.

As a direct consequence of the use of subjective probability, Bayesian methods permit the incorporation and use of information beyond that contained in the test data. Whether the reliability analyst does or does not have test data available, he or she will often have other relevant information about the value of the unknown reliability parameters. Such relevant information is an extremely useful and powerful component in the Bayesian approach, and the parameter estimates will then reflect this knowledge. This relevant information is often derived from combinations of such sources as physics-based computer codes, engineering, developmental, and qualification test results, generic industry-wide reliability data, modeling and simulation, past experience with similar systems, and the subjective judgment of experienced personnel.

Different individuals and organizations may specify different prior distributions based upon either different information or differences in how they quantify the information. Different prior distributions lead to different inferences. Little justification is all too often given in a Bayesian analysis for the prior distribution selected. Because the prior distribution is based on degree of belief does not remove the analyst's responsibility to adequately defend the basis for its selection. Otherwise, the resulting inferences can often be criticized on the basis that the prior distribution has been "chosen" with bias to give "self-serving" results that do not reflect the actual uncertainty in the parameter. This is frequently a major criticism of Bayesian inferences. Sensitivity analysis can examine the relative strength of the priors and demonstrate the differences in results based on different prior specifications.

The prior distribution describes the analyst's state of knowledge about the parameter's value prior to obtaining the sample data. If this distribution summarizes information from various sources, it is called an informative prior; if it tries to capture ignorance or invariance, it is called a non-informative prior. After the test data have been obtained, the uncertainty associated with the parameter is fully expressed by the posterior distribution, which is calculated via Bayes' Theorem. Mathematically, Bayes' Theorem has the following form:

$$p(\theta \mid \underline{x}) = \frac{l(\underline{x};\theta)\pi(\theta)}{f(\underline{x})}$$

Where $\underline{x}$ denotes the test data, $p(\theta|\underline{x})$ is the posterior distribution for the parameter θ, $\pi(\theta)$ is the prior distribution for θ, $l(\underline{x}; \theta)$ is the likelihood function, and $f(\underline{x})$ is a normalizing constant. The posterior distribution serves naturally as the prior distribution for subsequent experimentation as additional data is collected.

The use of such deductive reasoning is straightforward and has intuitive appeal. Consequently, Bayesian reliability methods are easy to follow and the corresponding estimates are easy to interpret. Because of the Bayesian differences in reasoning and interpretation of probability, there are several related positive features of Bayesian reliability methods.

In most cases, for large sample sizes of test data, the difference between Bayesian and classical inferences will be insignificant. However, when test data are scarce, the differences are often significant, and Bayesian interval estimates based on informative priors are often shorter than classical confidence intervals. If the prior distribution is essentially non-informative, then the Bayesian and classical estimates are often quite similar.

An important special case occurs in the case of a binomial or Poisson sampling model when no events have occurred. In this case, the classical maximum likelihood estimate of the binomial failure probability or Poisson failure rate is zero, which is usually overly optimistic. On the other hand, in both cases, the corresponding Bayesian point estimate is non-zero, which is clearly a more useful estimate. Of course, this estimate will depend on the information contained in the prior distribution.

Because Bayesian credible intervals are true probability statements about unknown parameters, they may be easily propagated through complex system models such as fault trees, event trees, and other logic models. Except in the simplest cases, it is difficult or impossible to propagate classical confidence intervals through such models.

Features and nuisances of real-world reliability problems, such as complex censoring, random hierarchical effects, etc., can easily be accommodated and modeled by Bayesian methods. Such considerations are often either difficult or impossible to consider when using frequentist-based methods.

In the past, the computations required to perform Bayesian analyses were quite difficult, and in more complicated models, were impossible. For many years, these difficulties prevented practitioners from applying Bayesian modeling techniques to real-world problems. Fortunately,

that situation changed in the late 1980s and early 1990s with the advent of Markov Chain Monte Carlo (MCMC) algorithms.

MCMC algorithms are a general class of computational methods designed to produce samples from posterior distributions. They are often easy to implement and, at least in principle, can be used to simulate from arbitrary, and possibly very high dimensional, posterior distributions. Since their introduction into widespread use in the 1990s, they have been successfully applied in literally thousands of Bayesian applications.

For additional information the following sources may be referenced:

- **Bayesian Reliability Analysis**, H. Martz and R. Waller, Wiley, 1982.
- **Handbook of Parameter Estimation for Probabilistic Risk Assessment (NUREG/CR-6823)**, C. L. Atwood, J. L. LaChance, H. F. Martz, D. J. Anderson, M. Englehardt, D. Whitehead, T. Wheeler, Nuclear Regulatory Commission, 2003.
- "Unity Values for Bayes Reliability Demonstration Testing," R. Parker, H. Martz, R. Prairie, W. Zimmer, **Recent Advances in Life-testing and Reliability**, pages 173-194, CRC, Boca Raton, FL, *1995.*

4.5.2.30 Fault Insertion Testing

Fault insertion testing, as the name alludes to, is the practice of inserting a known fault into a system and verifying that the diagnostic capability of the system recognizes the inserted fault. If faults are not recognized then corrective action will be required to improve the diagnostic capability of the system. Fault insertion testing is a valuable tool for verification of fault detection rate (FFD) and fault isolation rate (FIR) algorithms used in a system's BIT routine. However, for False Alarm rate (FAR), the most effective approach appears to be monitoring, recording and reporting the BIT data from operation of complex integrated systems over time. Then, when apparent false alarms are revealed, detailed engineering analysis of both hardware and software will determine the false alarm root cause, and result in redesign. Most false alarms are generally the result of improper BIT monitoring thresholds or timing, and as such, can be corrected by modification of the BIT software or platform computer routines. See Section 4.5.2.23, Maintenance/Maintainability Demonstration and Evaluation, and Section 4.5.2.24, Analysis, Demonstration and Test of Testability/Diagnostics, for additional information on these topics.

Fault Insertion Testing was also sometimes used to estimate and model software reliability. Known faults were inserted into the code, and the test teams success at identifying and removing these was used to model the number of theoretical remaining faults. Problems with this technique include the aspect that inserted faults were often easier to spot than existing faults, and the natural reticence of project staff from introducing faults into software.

4.5.2.31 Reliability Qualification Testing and Acceptance Testing

A reliability qualification test (RQT) is conducted under specified conditions, by or on behalf of the customer, using items representative of the approved production configuration, to determine

compliance with specified reliability requirements as a basis for product acceptance or production approval. An RQT is used to measure the reliability of a fixed design configuration. It has the benefit of holding the manufacturer accountable for future considerations based on the initial design process. Therefore, the RQT strongly encourages the manufacturer to seriously consider the ramifications of properly conducting other design related reliability tasks.

Reliability measures of equipment and systems are often necessary during development, production and in use. Reliability demonstration is often conducted to satisfy a development and production contract or to quantify reliability prior to a production release and ensure that requirements have been reached. Reliability measurements usually consist of either a sample of equipment subjected to a formal reliability test or a monitoring program during development and initial use that can quantify reliability. There are several standard methods of test and analysis that can be utilized for reliability demonstration to illustrate that requirements have been achieved.

MIL-HDBK-781 identifies details for popular test methods (including reliability growth) and environments. One type of testing outlined within MIL-HDBK-781 is probability ratio sequential testing (PRST). Results of the PRST are plotted with the failures on the y-axis and the test time (in multiples of specified mean time between failures, MTBF) on the x-axis. The test results (failures versus test time) create a "staircase," which determines when testing is completed. If the "staircase" passes beyond either the upper (reject line) or lower boundary (accept line), a decision is rendered and the test is stopped. The reject line defines the level at which the equipment will have failed to meet the test criteria, whereas the accept line denotes the level at which the equipment will achieve desired test criteria. The decision lines (reject and accept) are truncated to ensure that testing is completed in a reasonable maximum time. Refer to Figure 4-16 for an illustration of the PRST plan. An operating characteristic (OC) curve can be derived for any sequential test plan to show the probability of acceptance (or rejection) for different values of true MTBF. Similarly, the expected test time (time to reach an accept or reject decision) for any value of MTBF can be derived.

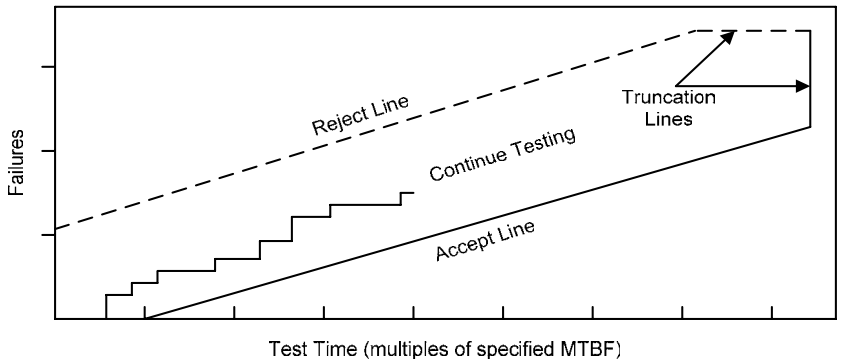


FIGURE 4-16: Typical PRST Plan

Sequential test plans generally have three outcomes that can occur as the desired reliability is demonstrated.

1. Conclude that reliability is satisfactory and terminate the test,

2. Conclude that reliability is unsatisfactory and terminate the test, or
3. Continue the testing process.

Although it is possible for a sequential test to require more test units than the equivalent fixed sample size test, generally a savings is realized, which is the primary motivation for sequential testing procedures.

Fixed duration (length) test plans are characterized by their discriminator ratio, total test time, and maximum allowable number of failures to accept demonstrated reliability. The underlying assumption of fixed duration test plans is that the item under test follows a distribution of times between failures that are exponential. The total test duration is set in advance with a fixed duration test plan. Fixed duration test plans can only terminate early through rejection (i.e., maximum allowable number of failures to accept is exceeded). The fixed duration test plans obviously differ from the PRST plans in that rejection is permitted only after a fixed number of failures have been observed.

MIL-HDBK-781 test plans are based on the assumption that a constant failure rate is applicable for the equipment being tested (i.e., fairly complex maintained electronic equipment after initial burn-in). The constant failure rate assumption means that MTBF will be the reliability index used for the MIL-HDBK-781 test plans. MIL-HDBK-781 offers numerous test plans that enable the analyst to determine which test plan fits the needs by balancing the statistical risks (producer's risk versus consumer's risk) involved and the minimum level of reliability acceptable.

Reliability demonstration testing to MIL-HDBK-781 is subject to limitations, which cause it to be a controversial method. The exponential distribution assumption of a constant failure rate is one fundamental limitation. However, it is also based on the implication that MTBF is an inherent parameter of a system and can be experimentally demonstrated. Reliability measurement is subject to the same fundamental constraint as reliability prediction (i.e., reliability is not an inherent physical property of a system, as is mass, electric current, etc.). Obtaining repeatable reliability measurements is highly unlikely between tests and often is not within the accepted statistical variability of such tests.

For equipment that operates only once or cyclically (such as pyrotechnic devices, missiles, fire warning systems, and switchgear), the sequential method of testing based on operating time may be inappropriate. MIL-STD-105, **Sampling Procedures and Tables for Inspection by Attributes**, and BS 6001 provide test plans based on success ratio for such items. MIL-HDBK-781 testing could be adapted for items that operate cyclically by using a baseline of mean cycles to failure or MTBF assuming a given cycling rate. For further information on determining the reliability of one-shot devices refer to Section 4.5.2.32.

4.5.2.32 One Shot Device Testing

A "one-shot" device is defined as a product, system, weapon, or equipment that can be used only once. After use, the device is destroyed or must undergo extensive rebuild. "One-shot" devices typically spend their life in dormant storage or standby readiness. The device may end its useful

life without ever being called upon to provide the function for which it was designed, limiting the availability of failure data during its life cycle.

Determining the reliability of a "one-shot" device poses a unique challenge to the manufacturers and users of these devices. Due to the destructive nature and costs of the testing, the current trend is to minimize testing. However, the expectations are for a high level of system reliability. Therefore, the test planner must have the knowledge necessary to determine the minimum sample size that must be tested to demonstrate a desired reliability of the population at some acceptable confidence level.

For "one-shot" devices, acceptance sampling is a statistical method used to predict the probability of success, or reliability, by estimating an attribute of the population through a sample. An attribute is an inherent characteristic that is evaluated in terms of whether or not the product performs as designed. Test results are measured by determining if the product was good or bad, passed or failed, etc. Non-conformance of the product characteristic is generally expressed as a proportion defective. Proportion defective is the number of failures that occurred in a sample size divided by the sample size.

Attribute sampling is based on the binomial distribution, which tests the hypothesis that a product has an acceptable defective rate at some acceptable level of risk. For "one-shot" devices, the object is to verify that the probability of success, when the device is called upon to function, is satisfactory at the desired confidence level.

The binomial distribution is based on "Bernoulli trials" (work of Jacob Bernoulli) in which each trial will result in only one of two possible outcomes (i.e., passed or failed). To use the binomial distribution to predict the probability of success for "one-shot" devices, the trials in the sample must meet the following conditions:

- Each trial must be independent. The outcome of one trial cannot influence the outcome of another trial.
- For each trial, there is only one of two possible outcomes.
- The number of trials in a sample must be fixed in advance and be a positive integer number.
- The probability of success must be the same for all trials.

4.5.2.33 Environmental Stress Screening (ESS)/Highly Accelerated Stress Screening (HASS)

As previously stated, the RAM activities of ESS and/or HASS should be planned during the System Development and Demonstration phase of the acquisition process and implemented during the Production and Deployment. Environmental stress screening (ESS) involves the removal of latent part and manufacturing process defects through application of environmental stimuli prior to fielding the equipment. Highly accelerated stress screens (HASS) use the highest possible stresses, frequently well above qualification test levels, to reduce the time required to conduct the screen. ESS and HASS implementation is addressed in Sections 5.5.5. and 5.5.6.

4.5.3 Technical Reviews

The RAM Program Plan and various RAM-related activities follow the systems engineering approach to systems acquisition. The technical reviews during Step 2: Design and Redesign for RAM will ensure that the Systems Engineering Plan is updated as the RAM Program Plan and RAM-related activities are completed. The technical reviews that occur during Step 2 include the System Functional Review, Preliminary Design Review, Critical Design Review, Test Readiness Review, and System Verification Review.

4.5.3.1 System Functional Review (SFR)

SFR ensures that the system under review can proceed into preliminary design. The SFR ensures that all system requirements and functional performance requirements derived from the Capability Development Document are defined and are consistent with cost, schedule, risk, and other system constraints. The SFR examines the functional baseline to verify that all required system performance is full decomposed and defined. The functional baseline decomposition and definition may then be used to define hardware and software requirements. SFR determines whether lower level RAM performance requirements are fully defined and consistent with mature system RAM requirements. The Program Manager should tailor the SFR to the technical scope and risk of the system and address the SFR within the Systems Engineering Plan. The SFR represents the last review before more technical design work commences to verify the credibility and feasibility of the system.

4.5.3.2 Preliminary Design Review (PDR)

The PDR is a multi-disciplined technical review to ensure that the system under review can proceed into detailed design as well as meet the stated performance requirements within the specified constraints. Generally, the PDR assesses the preliminary design as captured by in the allocated baseline (outlines performance specifications for each configuration item in the system at time of PDR) and verifies that each function in the functional baseline developed for the System Functional Review has been allocated to one or more system configuration items. Configuration items are defined as hardware or software elements, which include such items as airframes, avionics, weapons, crew systems, engines, trainers/training, etc. PDR assesses whether the preliminary RAM design will satisfy user requirements.

For complex systems the Program Manger may choose to conduct a PDR for each subsystem or configuration item with an overall system PDR to follow. The overall system PDR will determine whether the hardware, human, and software preliminary designs are complete and whether the Integrated Product Team is prepared to start detailed design and test procedure development. The Program Manager should tailor the PDR to the technical scope and risk of the system as well as ensuring that the PDR is addressed within the Systems Engineering Plan.

4.5.3.3 Critical Design Review (CDR)

The CDR focuses on assessing the system final design as captured in the product baseline (outlines performance specifications for each configuration item in the system at time of CDR). The CDR ensures that each product in the product baseline has been captured in the detailed design documentation. Product specifications (including production drawings) for hardware support the fabrication of configuration items, whereas software product specifications (e.g. Software Design Documents) allow the Computer Software Configuration Item to be coded.

Similar to the PDR, the CDR may be conducted for each subsystem or configuration item before leading to the overall system CDR. System CDR focuses on configuration item functional and physical interface design as well as overall system detail design requirements. CDR assesses whether the final RAM design will satisfy user requirements. At the conclusion of CDR the final detailed design of the hardware, human, and software will be complete and the Integrated Product Team is prepared to start system fabrication, demonstration, and test. The Systems Engineering Plan should once again be addressed at the conclusion of CDR.

4.5.3.4 Test Readiness Review (TRR)

The TRR assesses test objectives, test methods and procedures, scope of tests, and safety and confirms that required test resources have been properly identified and coordinated to support planned tests. The TRR verifies the traceability of planned tests to program requirements and user needs as well as determining the completeness of test procedures and their compliance with test plans and descriptions. The TRR will also assess the system under review for development maturity, cost/schedule effectiveness, and risk to determine readiness to proceed to formal testing. TRR assesses the ability of tests to confirm RAM requirements.

Test and evaluation is an integral part of the systems engineering approach to systems acquisition and should permeate the entire life cycle of an acquisition program. The Program Manager and Test and Evaluation Working-level Integrated Product Team should tailor any TRR to the specific acquisition phase, the specific planned tests, and the identified level of risk within the program. The scope of the TRR is directly related to the risk level associated with performing the planned tests and the importance of the test results to overall program success. The Program Manager is responsible for addressing the scope of the TRR(s) in the Systems Engineering Plan.

The level of specific risk will vary as a system proceeds from component level, to system level, to systems of systems level testing. Early component level test may not require the same level of review as the final system level tests. Sound judgment should dictate the scope of a specific test or series of tests. Readiness to convene a TRR is predicated on the Program Manager's and Test and Evaluation Working-level Integrated Product Team's determination that preliminary testing, functional testing, and pre-qualification testing results form a satisfactory basis for proceeding with a TRR and subsequent initiation of formal, system-level Developmental Test. An Operational Test Readiness Review (OTRR) will be conducted during Step 3 to ensure that Operational Testing may commence.

4.6 Output and Documentation

The documentation from Step 2: Design and Redesign for RAM is normally significant. Typically, the documentation is developed to perform the following major tasks:

- Manage the development process,
- Document the process undertaken,
- Document the results, and
- Produce contract deliverables.

This documentation would normally be customized to the program, project and contract requirement. The starting point for the tasks of Step 2 concentrates on how the user will challenge the system when in use. Any initial design should be evaluated with a formal documentation by a panel of experts who must comment on what is known and unknown about the RAM implications of each of the design choices. A model of the system's RAM metrics can be used to document the results. If the risks are unacceptable (i.e., too much unknown about a technology or a design), an alternative might be explored either alone or in parallel.

Documents should contain or refer to these evaluations and the documentation should reference the maintenance concept and the Integrated Logistic Support Concept. In other words, the documents should look at the whole system, including the interactions that the system will have with other systems.

A successful approach will have all the activities integrated together. There will be a RAM Program Plan, highlighting the relevance of each activity to achieving needed levels of RAM. The main points of the RAM Program Plan, especially at the system level, will be summarized in the Test and Evaluation Master Plan (TEMP). The RAM Program Plan will outline the whole process of maturing RAM.

The TEMP should provide the picture of how all the testing fits together and how the testing produces a system that can confirm not only the system's effectiveness at meeting the performance objectives for the capability, but the required reliability, availability, and maintainability as well.

Chapter 5 Produce Reliable and Maintainable Systems

5.1 Introduction

Once a system has been designed and developed, the next task in the acquisition life cycle is production, with the intent to produce reliable, available, and maintainable systems. The quality and fidelity of production cannot improve the inherent RAM of a system, but poor quality in manufacturing can reduce the system's inherent and fielded RAM performance. This chapter describes the third step of the four-step model, Produce Reliable and Maintainable Systems. The four steps are shown in Figure 5-1. In the Defense Acquisition process, the maturity of the system is demonstrated using Operational Test and Evaluation (OT&E), which is undertaken within Step 3.

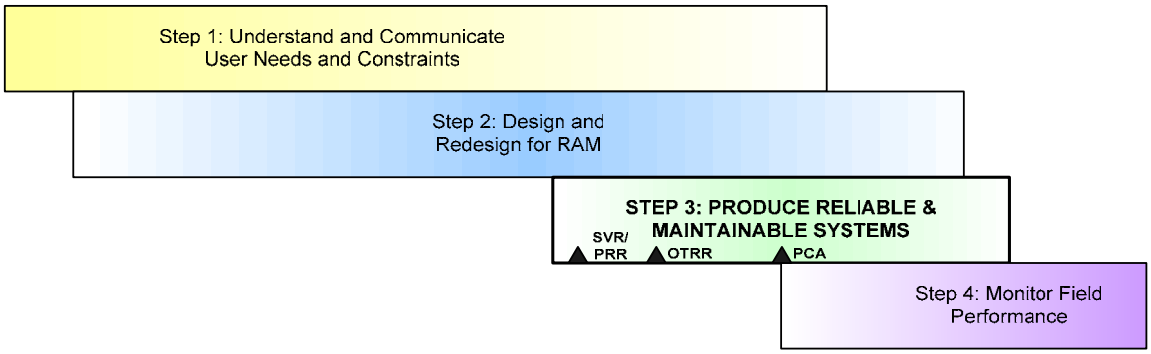


FIGURE 5-1: Produce Reliable and Maintainable Systems

5.2 Mission and Goals

As noted, the mission of Step 3: Produce Reliable and Maintainable Systems, is to reproduce with high fidelity the system that has been designed and developed. Manufacturing must be a controlled process that does not adversely affect the item with production defects. During this step the production organization implements production controls and continuous improvement processes to build production units, demonstrate acceptable performance of these units, and have them pass acceptance testing, without degrading the designed-in RAM levels of the system.

Acceptance requirements vary among programs based on a number of factors including risk, the total value of the program, technology domain, system type, number of production items, etc. Acceptance test requirements can range from comprehensive production acceptance testing of all produced articles up to type approval, followed by selected attribute testing. Testing issues range from verification of achievement of contractual specifications during Development Testing (DT), through Initial Operational Test and Evaluation (IOT&E) to confirm Low Rate Initial Production (LRIP) system performance and suitability for full-rate production, and then through Follow On Test and Evaluation (FOT&E) conducted on production items to determine the level of fielded performance.

RAM assurance activities during Step 3: Produce Reliable and Maintainable Systems can be summarized as:

- An emphasis towards process control, quality assurance, and environmental stress screening,
- Sample qualification tests,
- Configuration management and control,
- Supplier management, and
- Data collection activity (an extension of DCACAS initiated earlier, in development) to detect failures and maintenance anomalies as production items are delivered to operational units and enter the operational environment.

During Step 3, the following questions must be addressed before full-rate production can proceed in earnest:

- Do LRIP models of constituent elements (major units, assemblies, subcontract items, etc.) satisfy RAM and quality inspection and test requirements?
- What full-rate production RAM problems are revealed during LRIP model fabrication, testing, and manufacture?
- What specialized "burn-in," parts screening, or other special manufacturing process is required to meet production reliability/quality inspection and test criteria?
- How does the production rework and shrinkage rate for individual components, assemblies, units, etc., correlate with RAM of the production item as measured in factory acceptance tests?
- What impact do proposed engineering changes, manufacturing changes, BIT software changes, etc., have on RAM?
- Does pre-production model conform to specified reliability demonstration test requirements?
- What are failure modes of individual items failing reliability demonstration tests?
- Are procedures and processes in place for anticipating obsolescence and diminishing manufacturing sources and finding alternative ways of supplying the affected items?
- Are off equipment maintenance facilities, processes, hardware and software in development and refined sufficiently to support the system in an operational environment?

At the start of production, a large proportion of a system's total life cycle cost has often been determined by earlier actions and decisions.

Inherent RAM refers to the concept of a system's potential RAM performance. This inherent potential, rather than inherent performance, can only be achieved with well executed manufacturing and support programs. At each stage of development and deployment, adverse actions can reduce the level of RAM that will be achieved in service below the system potential. When manufacture and support programs are planned and executed well, the systems RAM potential can be achieved, but excellence in these steps cannot make the system better than this inherent level. The example in Figure 5-2 illustrates this point. The only way to achieve the inherent RAM is to manufacture and support it well. The only way to improve the inherent RAM of a system is to improve the design through design changes.

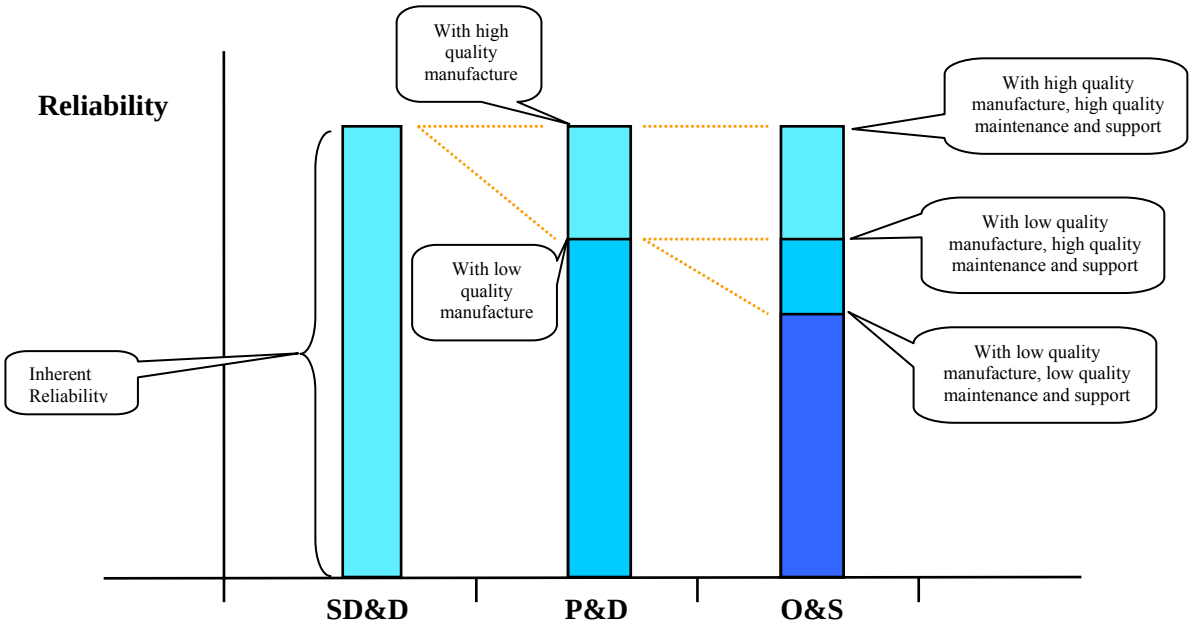


FIGURE 5-2: Achieving System Reliability During the System's Life Cycle

Some problems may only become apparent in the operational environment during OT&E. Problems identified may require redesign activity, using the techniques described in Chapter 4. Whenever possible, issues should be detected and mitigated early in deployment so that improvements can be incorporated as early as feasible in ongoing production.

5.3 People and Organizations

The people and organizations involved in Step 3, Produce Reliable and Maintainable Systems, are an evolution of the staff team identified in Chapter 4. As noted in Chapter 4, the design phase will normally be managed within a development contract. This contract will normally also include the production process, which may include responsibility for Low Rate Initial Production, Full-Rate Production, or both.

The Department of Defense Program Manager Office (PMO) that manages the System Development and Demonstration phase also manages the Production and Deployment phase of the system's life cycle. The responsibilities of the Program Manager, Lead Systems Engineer and team members include oversight of production and integration of deployment activity with the user. Although the PMO is normally supplemented with staff more experienced with production, it is desirable to continue some DT RAM staff capability to evaluate the RAM follow-on tasks such as LRIP equipment RAM, reliability growth and diagnostics maturation efforts, and overall supportability refinement.

As in the previous step, the contractor's organization will vary depending on contractual relationships, but generally the contractor's Program Manager would have continuing responsibility for achieving contractual requirements through production. Depending on the size and complexity of a project, positions and titles with elemental responsibility within a contractor organization will vary, but contractor staff relevant to production and the retention of RAM

capabilities could include the Production Manager, Quality Manager, and a RAM Engineering Manager. The development contractor will often assure the robustness of the production process with a multidisciplinary Integrated Product Team (IPT) including quality, production, and engineering and materials specialists. The use of Field Service Engineers, contractor representatives at user facilities, has proven to be a good means of communicating information from the user as the systems are deployed. This information may dictate the need for changes to the contractor's production process if deployed systems are not performing as expected or are not demonstrating their desired RAM (due to production related process errors).

Step 3 will normally cover various testing activities; hence, relevant staff also includes Project Office Test and Evaluation Manager, DT RAM engineering staff, independent government Operational Test and Evaluation (OT&E) staff, and OT&E authorities.

5.4 Supporting Information

5.4.1 Input Information

A large proportion of the design phase outputs are production phase inputs. The design phase activities of Step 2 should develop an item that is producible and suitable for production in Step 3. Documentation developed or refined in the previous phase and then in Step 3 includes the following:

- Design records
- Production documentation
- Product specifications
- Process specifications
- TEMP
- User requirements
- Preventive maintenance
- Diagnostic procedures

Contractual acceptance testing will rely on the specification and related performance requirements included in the contract. Development and Operational testing will utilize as the performance requirement those user requirements that were used to develop the contractual requirements.

5.4.2 Developed Information

The preliminary production processes and procedures developed in Step 2, Design and Redesign for RAM will be refined and developed in Step 3: Produce Reliable and Maintainable Systems. Although the baseline configuration of the production item is held under control, production can be a "learning" process and production refinements and efficiencies identified and introduced during Step 3. Clearly, any production changes that affect the form, fit, function and interface of the manufactured item necessitate formal configuration review procedures, typically an Engineering Change Proposal (ECP) or Software Change Review Board (SCRB) action.

5.5 Tools and Activities

Some of the tools and activities used in Step 3 are continuations or developments of those activities of previous steps, while some are new techniques that were not utilized in Step 1 or Step 2.

The emphasis of Step 3 shifts to process control, quality assurance, and environmental stress screening, which is also visible in the RAM activities expected during this phase. In addition, data collection from production articles deployed to operational units provides insight into how well production units are performing in the operational environment. Optional RAM activities during the Production and Deployment phase include a Failure Prevention and Review Board (examines DCACAS results to improve design by mitigating failure modes or indicated failures through prevention and root cause analysis to identify corrective actions), production reliability qualification/acceptance tests (see Section 5.5.8), lot acceptance testing (see Section 5.5.7). The RAM activities that are recommended for follow-up after initiation during the System Development and Demonstration phase include reliability growth testing, maintenance/maintainability demonstration & evaluation, and DCACAS. Required RAM activities include continued support of the DCACAS process and subcontractor controls as well as implementation of HASS/ESS to precipitate known failures prior to delivery. Technical reviews that are conducted during Step 3 include the Production Readiness Review (PRR), Operational Test and Readiness Review (OTRR), and Physical Configuration Audit (PCA).

5.5.1 Develop Production RAM Program Plan

The emphasis of the evolving RAM Program Plan (RAMPP) developed in earlier steps shifts from design and pre-build metrics to developing a RAMPP that will assure and verify that the required RAM characteristics are attained and retained through production. The production RAMPP uses process controls and quality assurance procedures that are vital for ensuring that contractual requirements are met and variability is minimized in the final product. The contractor should explicitly address the management aspects of its responsibilities, while the PMO should consider and document its responsibilities, concerning issues such as government furnished equipment (GFE) and its integration, as well as the coordination of government organizations, such as users and testers, for topics like data collection, etc.

5.5.2 Provide Contractual Incentives and Contractor Oversight

In circumstances when equipment with poor reliability reaches service and is outside warranty, the supplier or Original Equipment Manufacturer (OEM) may receive the unexpected benefit of extra work in continually repairing the item. This arrangement rewards the OEM in cases of poor reliability and eliminates their incentive for high reliability. Contracting for items should consider the effects of incentives and disincentives on contractor performance.

Users of equipment that can have high unreliability costs or risks have for some time imposed contractual conditions concerning reliability performance. Of course, every product warranty is a type of reliability contract, but contracts that stipulate specific incentives or penalties related to reliability achievement are increasing in popularity.

The most common form of reliability contract is one that ties an incentive or penalty to a reliability demonstration. The demonstration may be either a formal pre-acceptance test (see Section 5.5.8: PRAT as an example) or may be based on the user's experience, such as an in-service reliability demonstration. In either case, careful definition of what constitutes a relevant failure is imperative and a procedure for failure classification must be agreed upon between the contractor and the acquirer, such as the PMO. If the contract is based strictly on incentive payments, the user can often be the agreed-upon source of failure classification since there is no penalty if reliability objectives are not met. Straight incentive payments have advantages over incentive/penalty arrangements. It is vital that the reliability contract create a positive motivation, rather than a framework that can result in argument or litigation. Incentives are therefore more preferable when there is less conflict. Positive incentives above a base contract are easier to negotiate and hence more likely to be accepted as offered. Incentive payments can be structured to provide a substantial increase in profit for the contractor, whereas the user saves a small percentage of their overall savings due to the increased reliability. Receipt of an incentive fee has significant indirect advantages in terms of providing a morale booster and as a point worth quoting in future bid situations. A typical award fee structure is shown in Figure 5-3.

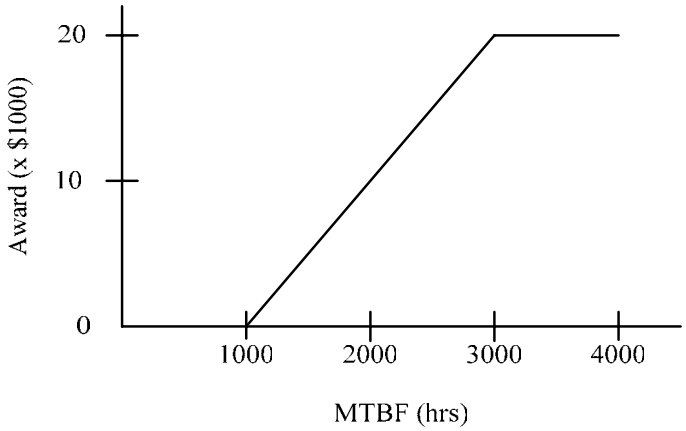


FIGURE 5-3: Reliability Incentive Structure

When planning incentive contracts it is necessary to ensure that other performance aspects are sufficiently well specified and covered by financial provisions such as incentives or guarantees (if appropriate). Tying the reliability incentive contracts to other performance aspects will minimize the possibility that the supplier will be motivated to achieve the reliability incentives at the expense of other system features. Incentive contracting requires careful planning so that the contractor's motivation is aligned with the user's requirements. The parameter values must provide a realistic challenge to the contractor, but at the same time the incentive fee must be high enough to make the challenge worth the effort for the contractor.

A type of reliability incentive contract first used in the 1960s that is increasing in popularity is a reliability improvement warranty (RIW). An RIW contract requires that the contractor conducts all repairs and provides all spares for a fixed period of time for a once-off fee. The contractor is then motivated to maximize their profit by ensuring the repair rate is minimized. Thus the user benefits from not only allowing the contractor to administer the supply and repair effort, but also

reaps the rewards of the reliability improvement to the system, which enables the user to focus their efforts on other areas of the acquisition process beside reliability. The following guidelines have been developed for RIW contracting.

- RIW contracts should only be applied to systems where there is not a high development risk and where the utilization will be reasonably stable and centralized. This allows both parties to the contract to agree upon likely reliability achievement.
- The contract fee must provide a good chance for the supplier to make a high profit and yet contain a reasonable risk element.
- Real difficulties can arise in administering RIW contracts in conjunction with conventional repair policies. For example, hardware subject to RIW needs special handling and marking to ensure that units are not opened or repaired by anyone other that the RIW contractor. Personnel involved with the repair and supply processes must be trained and procedures must be written to cover the operation of the RIW contract.
- The contractor must be given freedom to modify the system (at the contractor's expense) to improve its reliability. On the other hand, the user may wish to have some control over modifications since they may affect interchangeability or performance. The contract must specify the arrangements between the user and contractor in terms of notification, approval and incorporation of changes. One approach used is to give the contractor approval authority for Class II Engineering Change Proposals (ECPs), but the government should maintain approval for Class I ECPs. It is also recommended that a government activity, such as the Defense Contract Management Agency (DCMA), be required to concur in the classification of the change to ensure a Class I ECP is not inappropriately classified as a Class II ECP.
- The contract should clearly identify how the system will be operated and maintained if these factors can affect reliability.
- The system should be put into service immediately upon delivery to the user and failures should be reported promptly.

RIW contracts can be rewarding to all parties, but with any contract there are pitfalls to avoid. Therefore, careful planning, management and collaboration of all involved parties are essential to success. One caution is the area of processing suspected failed units where no failure is confirmed (i.e. the item is removed and returned to the contractor for a BIT reported and recorded failure where no failure can be confirmed. Often, the RIW contract addresses only failed (confirmed) units. Non-failed units are often processed at additional cost to the government. Systems with high BIT false alarms result in higher that predicted removal rates (based on failure rate) that result in more spare units needed to retain high weapons system availability. In these cases, the contractor should have to supply additional spare units at his cost so they will have incentive to eliminate or reduce the BIT false alarms as well as component reliability to maximize their profit.

5.5.3 Plan and Conduct Operational Test and Evaluation

Operational Test and Evaluation (OT&E) is conducted to confirm the operational effectiveness and suitability of systems using production or production-representative test articles and operationally representative personnel. OT&E is conducted under conditions and mission

scenarios, which are as operationally realistic as possible and practical. OT&E on Major Defense Acquisition Programs (MDAP) and major systems is normally planned, conducted, and evaluated by one or more of the Services' Operational Test Agencies (OTA). The OTAs assess RAM by conducting Operational Assessments (OA), operational tests before Initial Operational Test & Evaluation, IOT&E, and Follow-On Test and Evaluation (FOT&E). Title 10 USC Section 2399 establishes specific IOT&E requirements for defense acquisition programs. Many programs have OAs and operational tests before the IOT&E that stress the system in more realistic environments to learn about failure modes early. Sometimes OT personnel work with DT personnel during system development and demonstration to gain experience, share operational insights, and enhance learning.

The four OTAs are the Army Test and Evaluation Command (ATEC), the Navy Commander Operational Test and Evaluation Force (COMOPTEVFOR), the Marine Corps Operational Test and Evaluation Agency (MCOTEA), and the Air Force Operational Test and Evaluation Center (AFOTEC). The assigned OTA plans, conducts, and evaluates OT&E events. Planning for IOT&E begins in pre-acquisition. During the development of the user needs and constraints in Step 1, the T&E community (i.e., developmental and operational testers) develops the T&E Strategy that defines the Critical Operational Issues (COI), measures of effectiveness (MOE), and questions to be resolved in testing, the methodologies, and the quantity and types of test resources needed (test articles, data collection, targets, instrumentation, and operational and technical personnel). These considerations are refined as the user needs and constraints evolve in the ICD, CDD and CPD. Evaluation planning precedes test planning, the questions to be answered drive the number of test articles and kinds of test events needed to produce the data for evaluation. Test planning for commercial and non-developmental items recognizes commercial testing and experience, but nonetheless determines the appropriate testing to ensure operational effectiveness and suitability in the intended operational environment.

After the Milestone A decision, the OTA further refines the COIs and MOEs and includes them in the Test and Evaluation Master Plan (TEMP). The most revealing section of the TEMP is Part V that identifies the resources needed to complete the entire T&E program. If the needed resources are not listed in the TEMP, they may not be available later to support T&E. The Acquisition Milestone Decision Authority ensures that IOT&E entrance criteria are developed and documented in the TEMP. Before IOT&E begins, the Services each exercise their process to certify the system is ready for dedicated OT&E: review of DT&E results; assessment of the system's progress against critical technical parameters; analysis of identified technical risks to verify that those risks have been mitigated during DT; and review of IOT&E entrance criteria.

In terms of RAM objectives, test design identifies the R&M events, operating times, and conditions so as to learn about the system's characteristics and calculate operational measures with some degree of statistical confidence. Statistical techniques for assessing the reliability of repairable systems are presented in Appendix D. The IOT&E also assesses the prioritization and impact of upgrades, logistics supportability, life cycle factors (durability, spares, the logistics supply chain), and readiness for full-rate production and/or fielding.

The most frequent assertion about new systems, especially when they do not meet all requirements, is: "It is better than what we have now." The Program Manager and tester should

be able to provide data to support this claim through comparison testing or analyses based on historical operational and T&E data.

5.5.3.1 RAM in Developmental Testing (DT) versus Operational Testing (OT)

During DT, systems may not experience the same stresses, mission profiles, and other operationally relevant conditions found in the operational environment; and contractor maintenance specialists often perform the maintenance. In addition, sufficient numbers of flight hours and test events may not have been logged during DT in order to support accurate predictions of RAM. As a result, historical T&E results have shown that DT may provide overly optimistic assessments of RAM in comparison to OT.

A recent DOT&E study of the results of nearly one hundred developmental tests for various military systems over the last two decades has verified this concern (DT's optimistic assessment of RAM). The DOT&E study shows that for the 38 tests in which the same reliability metric was measured in DT and OT the reliability results were, on average, from 2 to 4 times higher during developmental testing than during operational testing. In some cases, reliability in DT was as much as 20 times higher than what was calculated for that system during OT.

The analysis is not complete but there are several possible explanations for the disparity: different ground rules during the two periods, different failure definitions and scoring criteria, different hardware and software configurations, different test times and test designs, different operator and maintainer skill levels, and others. Actions to close the gaps in each of these areas should make DT a better predictor of OT, provide earlier identification of failure modes, and facilitate earlier growth of RAM and diagnostics capability. The more robust and operationally representative the DT approach, the more effective it may be for identifying failure modes earlier. An advantage of earlier discovery is that more elements of the original design team may still be in place mitigate problems discovered in test.

5.5.3.2 Plan and Conduct Initial Operational Test and Evaluation (IOT&E)

The purpose of IOT&E is to determine if the system is operationally effective and suitable[27]; in other words, to determine if it meets the user's operational requirements (i.e., needs and constraints), before the full-rate production decision. In terms of the acquisition framework model, IOT&E is the major OT&E event in the Production and Deployment acquisition phase. In the four-step model for achieving RAM, however, IOT&E is an important and integral part of Step 3: Produce Reliable and Maintainable Systems. The system design is not suitable to begin full-rate production until the capability has been evaluated in the operational environment[28]. Dedicated IOT&E assesses reliability and maintainability against user's needs and constraints in

[27] The primary RAM component of operational effectiveness is mission reliability. The three components of RAM are each addressed in the definition of operational suitability: "the degree to which a system can be placed satisfactorily in field use with consideration given to availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, manpower supportability, logistics supportability, natural environmental effects and impacts, documentation, and training requirements (Defense Acquisition University Glossary).

[28] Although evaluating a system within its operational environment is desired prior to full-rate production some systems can not be operationally tested prior to full-rate production (e.g., a single dedicated satellite system that is operationally deployed once launched).

an operational environment and with operational personnel. New failure modes and maintenance shortfalls may be identified in this environment. As a result, Program Managers should anticipate the opportunities to discover and resolve problems during IOT&E and ensure sufficient resources are identified for appropriate data collection, analysis, and RAM improvements after IOT&E. This provides a late opportunity for achieving reliability growth, prior to locking in the full-rate production configuration. Continued participation by the PM's RAM team in IOT&E and FOT&E helps capitalize on opportunities for extended development.

5.5.3.3 Plan and Conduct Follow-On Test and Evaluation

Follow-On Test and Evaluation (FOT&E), in today's evolutionary acquisition environment is the continuation of OT&E after the full-rate production and/or fielding decision to ensure the system acquisition process is complete for that increment of capability. It answers specific questions about unresolved COIs and verifies the correction of deficiencies. Besides extending RAM data collection in the operational environment, FOT&E continues the development of new tactics, techniques and procedures. During all types of OT&E, typical users operate and maintain the system under conditions simulating combat stress and peacetime operations.

5.5.4 Participate in RAM-Related ECP and Diagnostic Software Reviews

An extremely important element of those responsible for ensuring that system requirements are met is to include RAM support and participation in interdisciplinary teams. The role of RAM in the review process is often a deciding factor for these teams. This is particularly true for engineering change proposal (ECP) reviews and Software Change Review Boards (SCRB). In order to make the most educated decisions, these review panels rely on participants to identify the impact of potential changes. Therefore, RAM practitioners must be prepared to provide a detailed RAM evaluation that includes an assessment of the potential impact of a proposed change on system performance as well as reliability, availability, maintainability and life cycle cost metrics. RAM assessments must account for all risks that may be presented by potential changes, therefore it is extremely important that these assessments have sufficient data to support a decision to either accept or reject proposed engineering changes. Table 5-1 illustrates a scorecard that could be utilized to select an appropriate ECP (assuming more than one proposal is available) based on RAM, cost of ECP, life cycle cost, manufacturing complexity, and risk.

TABLE 5-1: RAM-Related ECP Review Scorecard

ECP #	Reliability Impact[1]	Maintainability Impact[2]	Cost to Implement ECP ($)	Life Cycle Cost Impact[3]	Manufacturing Complexity[4]	Risk[5]
1						
2						
3						
…						
n						

[1] Measured in terms of ECP's affect on reliability measure (i.e., MTBF increases from 60 hours to 80 hours, etc.).
[2] Measured in terms of ECP's affect on maintainability measure (i.e., MTTR decreases from 1.5 hours to 1 hours, etc.).
[3] Measured in terms of ECP's affect on life cycle cost (i.e., life cycle cost associated with part reduced by 35%, etc.).
[4] Measured in terms of ECP's affect on the complexity to produce/manufacture item(s) affected by ECP (e.g., Increased, No Change, Decreased).
[5] Measured in terms of risk to implement ECP (e.g.., High, Medium, or Low).

5.5.5 Environmental Stress Screening

Environmental stress screening (ESS) was introduced in Section 4.5.2.33 and defined as the removal of latent part and manufacturing process defects through application of environmental stimuli prior to fielding the equipment. Random vibration and thermal cycling have proven to be the most effective screens for precipitating defects in electronic equipment. An equally important and inseparable aspect of the screening process is the item's electrical testing that is done as part of the screen, to detect and properly identify the defects that have been precipitated to failure. Several guidebooks have been developed to aid in setting effective ESS screening levels and to lend engineering and program management guidance for implementation. The following guidebooks can be referenced:

- **Environmental Stress Screening (ESS) of Electronic Equipment**, MIL-HDBK-344A, August 16, 1993.
- **Environmental Stress Screening (ESS) Process for Electronic Equipment**, MIL-HDBK-2164A, June 19, 1996.
- **Management and Technical Guidelines for the ESS Process**, Institute of Environmental Sciences and Technology, February 2000.
- **Environmental Stress Screening: Its Quantification, Optimization and Management**, Kececioglu, D. and Sun, F.B., Prentice-Hall Inc., 1995.

Contrary to popular belief, ESS does not increase the inherent reliability of a system. The inherent reliability of a system is driven primarily by the design, and ESS is one tool used to minimize the potential for adverse effects introduced by production. ESS is not a substitute to a sound RAMPP conducted during the System Development and Demonstration. There are three phases in the development of an ESS program:

- ESS Planning: Identify the equipment to be screened, develop quantitative goals for the ESS program, and describe initial screens.
- ESS Implementation: Identify the organizational elements that will be responsible for conducting the screening activity and the data collection, analysis and corrective action system (DCACAS) to be used for documenting failures.
- ESS Monitoring: Continuously monitor the screening process to ensure that it is both technically and financially effective.

Historically, two basic approaches have been utilized in the application of stress screens. In one approach, the customer explicitly specifies the screens and screening parameters to be used. In the second and preferred approach, the contractor develops a screening program that is tailored to the system.

The tailoring approach requires: (1) an estimate be made of the initial part and manufacturing type latent defects present in the equipment, (2) a determination of the maximum allowable latent defects present in the equipment after ESS, and (3) the development of screens that have a sufficient screening strength based on (1) and (2). A block diagram depicting this approach is found in Figure 5-4.

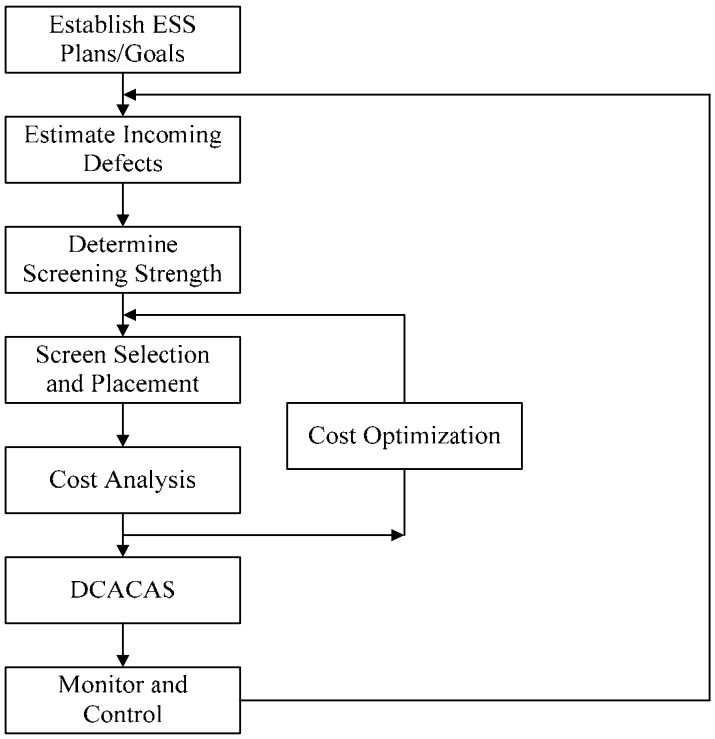


FIGURE 5-4: ESS Program Sequence of Events

To have an effective ESS program management must be committed to provide the time and resources needed to adequately support it. The roles of all participants must be clearly defined. Daily meetings are usually required when first implementing an ESS program, as the process of moving from paper concepts to physical tests can be daunting. The ESS program effectiveness should be monitored on a continuous basis. As the manufacturing process matures and potentially the number of manufacturing defects and workmanship errors decrease, the ESS program should be revised to ensure it remains effective at the assembly levels where it is being applied. A DCACAS forms the backbone of an effective ESS program as it provides the data needed to identify, track, and resolve deficiencies.

5.5.6 Highly Accelerated Stress Screens

As previously stated, highly accelerated stress screens (HASS) use the highest possible stresses, frequently well above qualification test levels, to reduce the time required to conduct the screen. HASS, therefore, cannot be used if highly accelerated life testing (HALT) has not been applied to the affected items during design. In such cases, "normal" environmental stress screening (ESS) should be used.

HASS is based on the principle that many stimuli exhibit an exponential acceleration for precipitating the flaws of a system. These stimuli enable the duration of the stress to be reduced (assuming the correct stress is applied), which in turn severely diminishes the screening equipment and manpower required.

HASS are performed for several reasons, which include: detecting and correcting design and process changes, reducing production time and cost, increasing out-of-box quality and field reliability, decreasing field service and warranty costs, and reducing infant mortality rates at system release. The screen of a HASS process must be developed based on any system limitations defined during HALT. The HALT results aid in the development of screens by seeding systems with defects to ensure screens detect the defects, determining the root cause of all observed failures, and initiating proof-of-screen process. HASS results need to be monitored throughout the life of the system.

5.5.7 Lot Acceptance Testing

In reliability assurance and the associated discipline of quality assurance, often the problem is to estimate a failure probability, mean number of failures, or other related quantity from test data. Moreover, the amount of test data is often quite restricted, since normally one cannot test large numbers of systems to failure. The number of destructive tests that may be performed is severely restricted both by cost and the completion time, which may be equal to the system design life or longer.

Probability estimation is a fundamental task of statistical inference, which may be stated as follows. Given a very large-perhaps infinite-population of items of identical design and manufacture, how does one estimate the failure probability by testing a sample of size N drawn from this large population?

Suppose we want to estimate the failure probability p of a system and also gain some idea of the precision of the estimate. Our experiment consists of testing N units for failure, with the assumption that the N units are drawn randomly from a much larger population. If there are n failures, the failure probability, may be estimated by:

$$\hat{p} = n/N$$

The caret indicates that $\hat{p}$ is a point estimate rather than a known true value.

Binomial sampling has long been associated with acceptance testing. Such sampling is carried out to provide an adequate degree of assurance to the buyer that no more than some specified fraction of a batch of products is defective. Central to the idea of acceptance sampling is that there is a unique pass-fail criterion.

A natural question that arises with acceptance testing is that if it is important that p be small why not inspect all of the units. Obviously the costs associated with this are the biggest detractor as in many cases it is simply too expensive to inspect every item of large-size batches of mass-produced items. More importantly, for a given budget, much better quality assurance is often achieved if the funds are expended on carrying out inspections, tests, or both on a randomly selected sample instead of carrying out more cursory tests on the entire batch.

When the tests focus on determining reliability metrics, the necessity for performing them on a sample become more apparent, for the tests may be destructive or at least damaging to the

sample units. If reliability is to be tested directly, each unit of the sample must be operated for a specified time to determine the fraction of failures. This time may be shortened by operating the sample units at higher stress levels, but in either case some sample units will be destroyed, and those that survive the test will have accumulated some degree of damage or wear, thus making them unsuitable for further use.

5.5.8 Production Reliability Assurance Testing

Production Reliability Assurance Testing (PRAT) is performed to ensure that the reliability of the hardware is not degraded as the result of changes in tooling, processes, workflow, design, parts quality, or any other variables affecting production. PRAT on production hardware is used to determine compliance to specified reliability requirements. PRAT is intended to simulate in-service evaluation of the delivered item or production lot. The testing must be operationally realistic and may be required to provide estimates of demonstrated reliability.

PRAT is usually based on sampling equipment from each lot produced as well as from all of the equipment produced. The test conditions (i.e., stress profile) applied during the test are normally determined by the customer and incorporated into the equipment specification. If the environmental stress types and levels are not specified by the customer or are not easily estimated from a similar application, the stress types and levels given in Table 5-2 should be applied. This table, taken from MIL-STD-781D, provides a summary of combined environmental test condition requirements applicable to the following categories of equipment:

- Category 1: Fixed ground equipment
- Category 2: Mobile ground vehicle equipment
- Category 3: Shipboard equipment (sheltered or unsheltered)
- Category 4: Jet aircraft equipment
- Category 5: Turbo-prop aircraft and helicopter equipment
- Category 6: Air-launched weapons and assembled external stores

TABLE 5-2: Environmental Stress Types and Levels

Parameter	Fixed Ground	Ground Vehicle	Shipboard		Fighter	Transport, bomber	Helicopter	Turbo-prop	Air-launched weapons, etc.
			Sheltered	Unsheltered					
Electrical stress									
Input voltage range	Nominal +5%-2%	Nominal ±10%	Nominal ±7%	Nominal ±7%	Nominal ±10%	±10%	±10%	±10%	±10%
Voltage cycle	1 per test cycle	1 per test cycle	1 per test cycle	1 per test cycle	1 per thermal cycle	1 per thermal cycle	1 per thermal cycle	1 per thermal cycle	1 per thermal cycle
Vibration stress									
Vibration type	Sine wave, single frequency	Swept-sine log sweep	Swept-sine continuous	Swept-sine continuous	Random	Random	Swept-sine log sweep	Swept-sine	Swept-sine and random
Amplitude[1]	-	-	-	-	-	-	-	-	-
Frequency range[2]	20-60 Hz	5-500 Hz	4-33 Hz	4-33 Hz	20-2000 Hz	20-2000 Hz	20-2000 Hz	20-2000 Hz	20-2000 Hz
Application	Minimum 20 minutes per equipment	Sweep 15 minutes per hour of operation	10 minutes (±2 minutes) per sweep	10 minutes (±2 minutes) per sweep	Continuous	Continuous	Sweep 15 minutes per hour of operation	12.5 minutes per sweep	See Note[3]
Thermal stress									
Storage temperature	-	-54°C to 85°C	-62°C to 71°C	-62°C to 71°C	-54°C to 71°C	-54°C to 71°C	-54°C to 71°C	-54°C to 71°C	-65°C to 71°C
Operating temperature	See Note[4]	-40°C to 55°C	0°C to 50°C (controlled)	-28°C to 65°C	-54°C to 95°C[5] -82°C to 95°C[6]	-54°C to 95°C[5] -82°C to 95°C[6]	-54°C to 95°C	-54°C to 95°C	-54°C to 114°C
Rate of change	-	5°C/min	5°C/min	5°C/min	5°C/min	5°C/min	5°C/min	5°C/min	5°C/min
Maximum rate of change	-	10°C/min	10°C/min	10°C/min	-	-	-	-	-
Duration (nominal)	-	-	-	-	3.5 hrs	3.5 hrs	3.5 hrs	3.5 hrs	3.5 hrs
Moisture stress									
Condensation	None	1 per test cycle	See Note[7]	1 per test cycle	1 per test cycle	1 per test cycle	1 per test cycle	1 per test cycle	1 per test cycle
Frost/Freeze	-	1 per test cycle	See Note[7]	1 per test cycle	1 per test cycle	1 per test cycle	1 per test cycle	1 per test cycle	1 per test cycle

[1] Refer to MIL-HDBK-781 and MIL-STD-810F for amplitude information regarding the vibration stress for the various equipment types.
[2] Frequency tolerance ±2% or ±0.5 Hz for frequencies below 25 Hz.
[3] Dependent on equipment used to transport stores, etc. Refer to MIL-STD-810F (Method 514.5) for additional information.
[4] 20 (heated and air conditioned); 40 (heated but not air conditioned); 60 (unoccupied tropical or semitropical).
[5] Condition applies for air-conditioned compartments.
[6] Condition applies for ram-cooled compartments.
[7] Sheltered equipment in a controlled environment shall be subject to condensation of moisture only if such conditions can occur during actual operational or standby conditions.

The test criteria should be carefully selected and tailored to avoid excessive cost or schedule impacts without significant reliability improvement. Accepted guidelines for planning and implementing PRAT include: "The statistical test plan must define the compliance (accept) criteria which limit the probability that the item tested, and the lot it represents, may have a true reliability less than the minimum acceptable reliability. These criteria should be tailored for cost and schedule efficiency. Because it is intended to simulate the item's operational environment and life profile, PRAT may require expensive test facilities; therefore, all-equipment production reliability acceptance (100% sampling) is not recommended. The sampling frequency may be reduced after a production run is well established; however, PRAT provides protection for the customer and motivation for the contractor's quality control program; thus it should not be discarded by a complete waiver of the PRAT requirement."

PRAT test plans should include the following consideration:

1. Tests to be conducted per MIL-HDBK-781
2. Reliability level (i.e., MTBF) to be demonstrated; the associated confidence level; and the relationship between demonstrated MTBF, confidence, test, and so on
3. Representative mission/environment profile
4. The number of test units, expected test time, calendar time factors, and scheduling of effort
5. The kinds of data to be gathered during the test
6. Definitions of failure (relevant, non-relevant)
7. Authorized replacement and adjustment actions
8. Logs/data forms to be maintained that record number of units on test, test time accumulated, failures, corrective actions, statistical decision factors, and accept/reject criteria

For additional information on PRAT refer to MIL-HDBK-781, **R&M-STD-R0030 Production Reliability Assurance Tests (PRAT)** from Naval Avionics Center (NAC), or Chapter 12 of **Reliability Engineering for Electronic Design** by Norman B. Fuqua.

5.5.9 Continuation of Growth/TAFT

The Reliability Growth method was introduced in Chapter 4 as a recommended RAM activity during Step 2: Design and Redesign for RAM. The monitoring of the reliability performance during Step 3 and the use of the growth analysis method provides an ongoing scrutiny and assurance of system RAM performance. Some programs have requirements that target ongoing growth during this and the subsequent step. As noted in Chapter 4, reliability growth can only be maintained through the monitoring of reliability performance, the analysis of failures, and the identification and removal of failure modes through engineering changes/modifications.

5.5.10 Continued Maintenance/Maintainability Demonstration and Evaluation

Chapter 4 presented the details of Maintenance/Maintainability Demonstration and Evaluation assessment methods that would normally be undertaken during Step 2 (depending on system needs, risk, etc.). Continuing this assessment during Step 3, or OT&E, may be necessary and

ensures that the maintainability of the system has not changed from the preliminary design to the production design.

Although a lot of effort is directed prior to the Production and Deployment phase of the system's life cycle at verifying the ability of the system to be maintainable to some specified level of demonstrated maintainability many maintenance related activities will continue while others begin to be implemented in response to deployment issues. The diagnostics software has obviously matured to the point that the system could be deployed, but until the system is deployed the diagnostics software will not undergo "real-world" testing. As "real-world" users operate the system they must begin to respond to false alarms and other ambiguities in the built-in test system as well as actual maintenance issues. These ambiguities and actual maintenance issues will require some level of maintenance to be performed so these are the first "real-world" maintainer activities on the system and problems are bound to be identified. Problems may manifest as revisions to the diagnostics software and/or repair manuals/documentation, whereas other maintenance problems may identify the need for system design changes due to accessibility, etc. It can be beneficial for DT RAM Team members to continue evaluation tasks throughout this phase based on their engineering experience with interpreting recorded data, recognizing and categorizing faulty indications, and communicating with the extended development team.

5.5.11 Continued RQT and Acceptance Testing

This assessment method also often begins during the System Development and Demonstration phase of the acquisition process (see Section 4.5.2.31). The RAM activities shift from qualifying the proposed design in SDD to ensuring that the manufacturing process is repeatable in producing acceptable systems during the Production and Deployment phase.

5.5.12 DCACAS

Refer to Section 4.5.2.7 for additional information on DCACAS, including the contents of this process, its setup, etc. The biggest change in the DCACAS process from Step 2 to Step 3 is where the input data is captured. Instead of developmental testing being the primary source of data, information can be captured from OT&E, initial deployment, and ongoing PRAT.

Test data can provide insight into how the system will behave when fielded, specifically operational test data. Test reports should be completed and tracked via a serially numbered test report with both successes and failures prepared upon occurrence. A comprehensive report should be initiated on a one-report-for-each-event basis (at a minimum this should be done for each failure, but these reports would be helpful for successes as well). Test event data recorded in the DCACAS should use a consistent method of identification as other event data to allow for accurate cross-referencing of incidents, and be stored on a readily available electronic database. Current aviation programs use on-board data recorders that include detailed data from the mission computers including platform attitude, altitude, date, time, event number, bureau or serial number, operating parameters of specific equipment like engines, generators, flight control actuators, etc. and all faults detected throughout the platform. They also record additional information such as the need for system servicing, life use indices, vibration analyses, operating

time used for scheduled maintenance, and platform and system level configuration control. This data can be processed to provide detailed mission and RAM information. Inclusion of these data within the DCACAS system throughout system ownership provides a rich opportunity for system management but also require a significant expansion of data storage requirements and software development for recording, analyzing and reporting relevant data. Many of these newly identified requirements are shared by the implementation of the Automated Maintenance Environment (AME) now deployed with complex USN and USAF aircraft.

The Failure Prevention and Review Board (FPRB) continues to address potential problem failure modes and actual problem failure modes as part of the DCACAS process during Step 3.

5.5.13 Quality and Quality Control Techniques

As indicated earlier, RAM assurance activities during production include an emphasis towards process control and quality assurance techniques. Given the coverage of these techniques in other documents and the limit of scope and emphasis of this guidebook, the following techniques will not be described further here:

- Statistical Process Control (SPC): The term used for the measurement and control of production variability.
- Process Capability: If a product has a parameter of interest, which has a tolerance or specification width, it is obviously important that the process variation is less than the tolerance. The ratio of the tolerance to the process variation is called the process capability.
- Run and Control Charts: Used to ensure that the process is under statistical control and to indicate when special causes of variation exist.
- Taguchi: Genichi Taguchi developed a framework for statistical design of experiments adapted to the particular requirements of engineering design. Taguchi suggested that the design process consists of three phases: system design, parameter design, and tolerance design.
- ISO 9000: Standard procedure published to provide a baseline for evaluating the quality assurance systems of companies.
- Continuous Improvement: Process of constantly seeking more efficient ways to produce products and services so that they continue to improve in value while making customer satisfaction a primary business goal.
- TQM: A philosophy of pursuing continuous improvement in every process through the integrated efforts of all members of the organization (marketing, engineering, production, and service).
- Quality Audit: An independent appraisal of all of the operations, processes, and management activities that can affect the quality of a product. In the United Kingdom BS 5750 is the controlling document, AQAP-1 describes the policy for NATO contracts, and ISO 9000 is the international standard.
- Six Sigma: Six Sigma is Motorola's nomenclature for the TQM process that can still be defined as the management system that directs the quality improvement philosophy and ensures its implementation in all aspects of the business.

These quality control techniques may be further pursued through the following referenced documents:

1. **Quality Toolkit**, Coppola, Anthony, Reliability Analysis Center, 2001.
2. **Practical Reliability Engineering**, Third Edition Revised, O'Connor, Patrick D.T., John Wiley & Sons, 1998.
3. **Introduction to Statistical Quality Control**, Third Edition, Montgomery, Douglas C., John Wiley & Sons, 1997.
4. **Statistical Problem Solving in Quality Engineering**, Kazmierski, Thomas J., McGraw-Hill Inc., 1995.
5. **Statistical Process Control**, Brown, Leonard A., Benham, David R., and Vicor W. Lowe Jr., Automotive Industry Action Group, 1995.

5.5.14 System Verification Review (SVR)

The SVR or Functional Configuration Audit determines whether the system under review can proceed into Low-Rate Initial Production and Full-Rate Production within cost, schedule, risk, and other system constraints. The SVR is often an audit trail for the system following the Critical Design Review. The SVR assesses the system final product, based on its production configuration, and determines if the system meets functional requirements, including RAM, (derived from the CDD and preliminary CPD) that are documented in the functional (SFR), allocated (PDR), and product (CDR) baselines. The SVR also establishes and verifies final product performance, which provides inputs to the CPD under development. The SVR is often conducted concurrently with the Production Readiness Review.

5.5.15 Production Readiness Review (PRR)

The PRR determines whether a design is ready for production and if the producer has accomplished adequate production planning to ensure designed-in RAM levels are not degraded. The PRR examines the risks associated with the design in terms of production or production preparations that might breach thresholds of schedule, performance, cost, or other established criteria. The PRR evaluates the full, production-configured system to determine if it correctly and completely implements all system requirements as well as verifying the traceability of final system requirements to the final production system.

The Integrated Product Team (IPT) participates in the PRR by reviewing the readiness of the manufacturing processes, the Quality Management System, and the production planning (i.e., facilities, tooling and test equipment capacity, personnel development and certification, process documentation, inventory management, supplier management, etc.). The PRR success is predicated on the determination of the IPT that the system requirements are satisfied in the final production configuration and that production capability warrants proceeding into Low-Rate Initial Production and Full-Rate Production.

PRRs should be conducted in an iterative fashion concurrently with other technical reviews such as the System Functional Review (SFR), Preliminary Design Review (PDR), and Critical Design Review (CDR) of Step 2. These preliminary PRRs identify and mitigate risks as the design

progresses with the "final" PRR occurring in conjunction with the System Verification Review (SVR) at the end of Step 2 as Step 3 commences in earnest.

5.5.16 Operational Test and Readiness Review (OTRR)

Program Managers often conduct another Test and Readiness Review (previously completed during Step 2) prior to Initial Operational Test and Evaluation (IOT&E) to ensure that the "production configuration" system can proceed into IOT&E with a high probability of successfully completing the operational testing. OTRR assesses the ability of operational tests to confirm RAM requirements. Successful performance during operational test generally indicates that the system is suitable and effective for service introduction as well as often the basis of the Full-Rate Production Decision. Prior to conducting the OTRR a thorough understanding of available system performance to meet the Capability Production Document is needed. The Service Acquisition Executive must identify materiel system readiness for IOT&E to conclude the OTRR.

5.5.17 Physical Configuration Audit (PCA)

At the time that the Full-Rate Production Decision is being made the PCA is conducted to examine the actual configuration of an item being produced. If the PCA is completed after the Full-Rate Production Decision it should be performed as soon as production systems are available. The PCA verifies that the related design documentation matches the item as specified in the contract as well as confirming that the manufacturing process, quality control system, measurement and test equipment, and training are adequately planned, tracked, and controlled in order to ensure that RAM is not degraded in the production process. The PCA validates many of the supporting processes used by the contractor in the production of the item and verifies other elements of the item that may have been impacted and/or redesigned since the SVR conducted at the conclusion of Step 2. Successful completion of the PCA is contingent upon the design and manufacturing documentation matching the item as specified in the contract.

5.6 Outputs and Documentation

There will be numerous outputs and documentation at the conclusion of the Production and Deployment phase of the system acquisition life cycle including:

- Production process management
- Acceptance test results
- Production contract deliverables

The outputs and documentation are often customized to the program, project, and/or contract requirements.

Chapter 6 Monitor Field Performance

6.1 Introduction

Once a system is successfully fielded, the focus of the RAM program changes to one of monitoring and sustaining. The fielded RAM performance has been achieved through the sustained effort of all of the previous steps. The user needs have been utilized to establish realistic RAM requirements as well as well understood use profiles and environments; design and redesign for RAM has been vigorously pursued within the systems engineering process; and quality production processes utilized with OT&E confirmation of the achievement of the user requirements.

Once a system is in routine use, degradation can occur as a result of many factors, such as changes in the intended operational environment or use profile; premature wearout of parts; mission and force application changes, etc. Degradation may be preventable and actionable if proper monitoring and trending of in-service performance is conducted and engineering resources are brought to bear on identified problems.

This chapter describes the process of monitoring field performance and, when warranted, taking action to sustain the inherent levels of RAM; these efforts comprise the fourth step of the four-step model. The four steps are shown in Figure 6-1 with Step 4: Monitor Field Experience highlighted for discussion in this chapter.

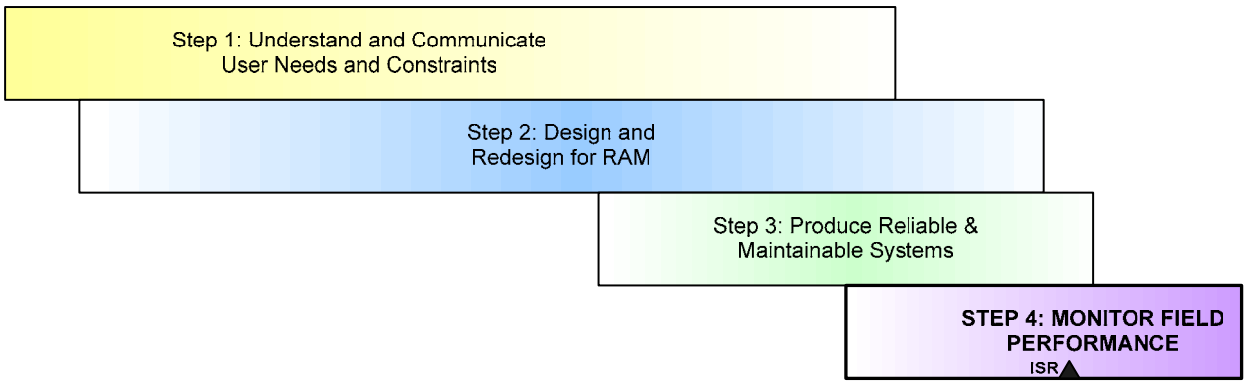


FIGURE 6-1: Monitor Field Experience

6.2 Missions and Goals

The nature and focus of the RAM activities change as the system moves through development, demonstration, and production into the Operations and Support (O&S) phase of its life cycle. The RAM activities in the prior phases focused on ensuring that the RAM requirements were met by "designing in" reliability and maintainability using sound design, analyses, and testing as well as maintaining that "designed in" RAM levels remain intact during manufacture. When the system was first deployed for Operational Test or initial fielding, RAM assessment focused on verifying that the "designed in" RAM had been achieved in the field and determining the cause and remedy of any shortfalls. Throughout the remainder of the system's operational life, assessment is focused on ensuring that fielded RAM performance is sustained.

During the O&S phase, the RAM activities seek to:

- Manage the RAM sustainment program,
- Identify RAM problems and prioritize those needing solutions,
- Identify opportunities for improving RAM, and
- Provide lessons learned to the Acquisition community.

6.2.1 Manage the RAM Sustainment Program

The purpose of the RAM Program Plan in the O&S Phase is to monitor system RAM performance, and to plan and implement actions that will, over the entire system life cycle, ensure that the product achieves its inherent design RAM potential, and that the RAM performance does not unknowingly degrade. These PMO management efforts ensure that the DoD will not incur a higher Life Cycle Cost or Total Ownership Cost than originally envisioned and that mission effectiveness is not compromised. Section 6.5 identifies several tasks that should be included in the RAM Program Plan during the O&S Phase related to RAM assessment.

The RAMPP needs planning and resourcing. Staff and systems will be needed to undertake in-service monitoring, develop and implement test and repair strategies, and support a comprehensive Data Collection, Analysis, and Corrective Action System (DCACAS).

6.2.2 Identify RAM Problems and Prioritize Solutions

RAM problems may arise from a number of sources and should be identified for management attention. If the performance is not monitored and analyzed, it is possible for performance degradation to be insidious and not readily perceived.

RAM problems could arise in service from situations such as:

1. Change of mission profile or other use change,
2. New environmental conditions,
3. Changes in maintenance or logistics philosophies,
4. Changes in the usage rates,
5. A poor lot of parts making it to the field,
6. Faulty workmanship in production or maintenance,
7. Unavailability of adequately trained support staff,
8. Unanticipated shipping or transportation stresses,
9. Prematurely discontinuing a planned reliability growth program,
10. Premature wear out of parts or sub-systems,
11. Installation of newly redesigned parts not available during previous phases, and
12. Integration of new systems/subsystems/units.

RAM program management should also consider parts obsolescence and spares availability throughout the life of the system. The solutions to logistics problems that are generated by through-life parts obsolescence and diminishing spares availability cannot necessarily be

identified up front, but the issue should be anticipated and managed. The most effective method of managing the issue of obsolescence is a comprehensive approach that begins with early phase activities such as part selection and application processes during the System Development and Demonstration phase of Step 2 through the Production and Deployment phase of Step 3 to the Operations and Support phase of Step 4. An ongoing program that monitors parts availability, authorizes technical substitution, considers subsystem technological upgrades and replacement is normally required. As major subsystems approach wear out, technological obsolescence, or become unsuitable for the required mission, the user may want to consider system modifications that employ new technologies that will potentially improve the performance of the existing product (i.e., product replacement) or extend its useful life (i.e., service life extension).

6.2.2.1 DCACAS

Data collection is the key to understanding RAM performance and enabling problems to be identified and prioritized. The DCACAS should have been planned in Step 2 and introduced and used by the design and manufacturing team to capture the information needed to identify and correct relevant product and process problems. The DCACAS is an important tool throughout the remainder of the system's life cycle. The DCACAS system needs to be flexible, given that it is typically developed during one phase and is then used across a number of subsequent phases. To operate effectively, it may be necessary to change the DCACAS substantially during different phases, but the tool needs to be managed and controlled. As responsibility for the system changes so do the data needs of management. The manufacturer's warranty program, where provided, is developed to meet contractual requirements and normally in parallel to Low Rate Initial Production (LRIP) production. During the Production and Deployment phase, techniques such as design of experiments (DOE) and statistical process control (SPC) can also be applied to control and improve manufacturing processes by reducing process variability. Ultimately, the In-Service Manager is interested in the RAM performance of the fielded systems; hence the type of data collected should correspond to these needs during the O&S phase.

The DCACAS and the maintenance concept must match. As current acquisition programs for complex digital weapons systems adopt different kinds of maintenance concepts, new data management challenges arise. When the prime contractor and the government enter into a contract with various vendors to provide all higher-level maintenance and repair on complex equipment rather than develop and support the capability in-house, the result is a maintenance philosophy where organizational level repair of a higher-level assembly is accomplished by removal and replacement of the suspected faulty unit, which is then sent directly to depot level or the vendor for repair. Without a government intermediate-level repair facility, there is no failure confirmation data for entry into DCACAS to match up with the equipment removal data, unless contractual provisions cover data reporting from the depot/vendor repair facility. Without that, the overall result is corruption of the RAM performance monitoring for those equipments under Organization-to-Depot (O to D) maintenance contracts.

With O to D, the government's production contract with the Prime Contractor should require continuation of vendor data in the DCACAS system identical to that RAM data philosophy developed for System Development and Demonstration phase of Step 2. Without vendor failure confirmation and repair data, RAM performance assessment is limited to only those systems where failure data is available through the normal maintenance data system.

The DCACAS is used for recording and analyzing data. The need to assess RAM metrics through the O&S Phase confirms the need to continue a DCACAS system. Typically, the services use some form of Computer Aided Maintenance Management (CAMM) tool, and the CAMM system is often used as the basis of data gathering for system failure and reliability data. The basic CAMM system may not have sufficient capability to provide the DCACAS needs. Customization of the CAMM system has become a popular means of bridging the gap between the needs of the maintenance management system (CAMM) and the needs of the DCACAS (as well as everything supported by the DCACAS). Decisions about how the DCACAS will evolve through the 4 key steps, how it will interface with the CAMM, and how data from all levels of maintenance (including O to D) will be collected and integrated are most effectively made starting with the system development and demonstration RAMPP.

The Failure Prevention and Review Board (FPRB) focuses on failure prevention and failure review by mitigating failure modes via corrective actions during the Operations and Support phase of the acquisition life cycle. Corrective action during Step 4 includes design modifications, which are based on the results of root cause analyses conducted on known failures, as well as failure prevention techniques that have been proven to be effective on the deployed system.

6.2.2.2 Other Prioritizing Issues

Some failures that occur during the O&S phase may be covered under warranty. Typically, there are contract-specific arrangements that will apply to failures, and the subsequent repairs. As illustrated in Figure 4-9, which shows the DCACAS process, the data associated with the warranty related failures should also be recorded within the normal DCACAS system.

In earlier acquisition phases, there is a significant emphasis on classifying failures for the purpose of assigning "responsibility." The classic problem is to identify how many failures are chargeable to the contractor to determine compliance with the contract requirements and the equipment to determine its suitability for acceptance. Once the item has been accepted and enters service, the emphasis normally shifts because all failures have logistics consequences and the operator is interested in having all failures recorded and addressed (note discussion of O to D failure data above). The issue concerning fault attribution is discussed further in Section 6.5.1.2, Fault Attribution and Classification.

6.2.3 Identify Opportunities for Improving RAM

It is highly likely that at some point in a system's lifetime, reliability and integrated diagnostics improvement modifications will be proposed and possibly become available. Some modifications may be simple and quick to incorporate. Each development option should be evaluated and, if agreement can be reached on how the embodiment will affect the existing system or process, then a rapid assessment, approval and deployment procedure should be available to incorporate such modifications into the equipments concerned. Liability for the installation of any reliability and diagnostics modifications and the interaction with the existing manufacturer's liabilities needs to be considered. Such modifications should be subject to agreed

validation methods and periods of performance. Such validation should be based on appropriate evidence available within the demonstration, but where project constraints apply, validation might be gained by an extension to the demonstration, based on a multiple of the previously observed mean time, or cycles or rounds, etc., between faults of the failure mode affected by the modification.

Alternatively, a limited demonstration on the immediately affected system could be considered using available test systems. The effectiveness of proposed modifications should be thoroughly demonstrated by testing on system integration benches, test-rigs, trials equipment, or by prototypes prior to being authorized for incorporation within equipment.

Identifying opportunities for RAM improvement is an extension of the process of finding RAM problems, but can be more challenging. Opportunities come from identifying potentially suitable changes and modeling the outcomes. The analysis of candidates requires insight and understanding of the cost of change implementation and the delta to the running cost and performance. Comprehensive analysis therefore requires sophisticated awareness of costs, which may not be easily provided in normal in-service management systems.

Fielded systems supported in different ways can produce different levels of average and peak availability performance and, hence, readiness outcomes. Alternatively, the same level of availability may be achievable using a different way of supporting the system that has a lower cost. Technology developments can also lead to the option of introducing replacement subsystems through authorized engineering changes that can lead to higher system RAM performance.

Modeling system performance and the consequence of changes provides RAM practitioners with the capability to evaluate opportunities for RAM improvements on a consistent basis. Classically, Return on Investment (ROI) is used to consider the cost effectiveness of changes.

6.2.4 Provide Lessons Learned to the Acquisition and Capability Development Community

Activities conducted prior to and during systems acquisition require accurate knowledge of in-service RAM performance. When concepts are developed and refined, the performance of the existing in-service systems is the basis for identifying shortfalls in capabilities, projecting existing and future needs that have yet to be met, and then calibrating these with achievable and desired levels of performance.

Development performance may not equate to fielded performance. RAM performance is affected by a number of aspects, including the use profile, the use environment, and the support environment. The effect of transitioning from the development environment to the operational environment should be analyzed so that these effects can continue to be understood and correctly accounted for in subsequent programs.

The acquisition community should utilize DCACAS, quantitative RAM data and the lessons learned from previous programs to ensure that attainable RAM metrics are set for future systems.

A DCACAS contains not only failure information, but records the equally important success data. A good source of lessons learned is the technical reports generated during different phases of system development testing. In the case of Naval Aviation, technical reports and technical papers are generated that include test results, conclusions and recommendations. Generally the recommendations include a compendium of lessons learned. Another source of lessons learned is the Knowledge Management System (KMS) developed by the Naval Air Systems Command.

Lessons learned should encompass the qualitative information from all personnel and organizations associated with the program, including procurers, designers, manufacturers, operators, maintainers, spare parts suppliers, etc. The "voice of the customer" is important in ensuring that a design achieves the requirements for a new system, and the many people that use, operate or support a system may not have their voice heard in the process of requirements development. The lessons learned activity provides an opportunity for problems identified during contracting, development, demonstration, production, deployment, operations, and maintenance to be identified and addressed in the current program and avoided in future programs.

In addition to a systematic data collection process, a system procurement, development, and production log is recommended. The log should capture requirements difficulties (in both the assigning and measuring requirements processes), scheduling hassles, design change processes, testing concerns and problems, manufacturing process records, and shipping/handling concerns. This data can be coordinated at a later time to failure events obtained from the DCACAS process to determine the significance of systems engineering modifications and lessons learned. The log could be used to correlate (benchmark) program activities with their end result in terms of RAM to determine what activities are most beneficial.

It is a good practice to routinely update the lessons learned database at each stage of the program and before key personnel depart. Otherwise, information which should captured in the lessons learned database might be lost because of the turnover of personnel common in many programs.

6.3 People and Organizations

The Program Manager is responsible for the total life cycle system management. This includes all activities from design and development through sustainment and disposal.

As products are delivered and utilized in-service, development contractor responsibilities decrease, and those of the in-service organizations increase. Defense personnel, civilian contractors, or a combination, depending on the program, can undertake in-service operations and support. Contractor personnel staff responsibilities and requirements are normally dictated by the relevant contract. The use of Field Service Engineers often diminishes during the Operations and Support phase, but the Field Service Engineers are still a good means of connecting field performance by the user to the developer/contractor to effectively mitigate concerns as they are identified during the Operations and Support phase.

The In-Service Manager generally has the support of a professional engineering team, led by an engineering manager. The engineering manager provides various engineering services, including

RAM support. There may a designated system or RAM engineering manager, or this may fall within the engineering manager general tasking.

The Engineering Manager normally takes over chairmanship of the Failure Prevention and Review Board (FPRB), as the FPRB's focus changes from development to in-service.

The RAM Engineering Manager is responsible for routine review of failures in the DCACAS system and conducts specialist reliability, availability and maintainability studies as designated by the FPRB.

The In-Service Manager also normally has logistics responsibilities for the system. The reliability and data analysis function from within engineering would also support spares and logistics initiatives, modeling, and analysis.

6.4 Supporting Information

The data developed during the Pre-Systems Acquisition and Systems Acquisition phases should be available to support transition of the system into the O&S phase to aid in-service management and engineering. This data includes: type record, user requirements statement with rationale, configuration data, Failure Mode and Effects Analysis, Fault Tree Analysis, Reliability Centered Maintenance Analysis, DCACAS system, RAM Rationale, RAM Case, and test results.

6.5 Tools and Activities

Tools and activities utilized to assess system RAM performance and to assure RAM during the O&S phase include the following:

- Data Collection, Analysis and Corrective Action System (DCACAS)
- Failure Modes and Effects Analysis (FMEA)
- Reliability Growth Testing Analysis Methodology
- Life Data Analysis
- Field Assessment and System Trending
- Continued ID/BIT Maturation
- Repair Strategy
- Reliability Centered Maintenance
- Condition Based Maintenance
- Parts Obsolescence and Diminishing Manufacturing Sources

The depth to which these tools and activities are applied should reflect the nature, complexity and cost of the system, and the strategic circumstances.

During Step 4: Monitor Field Performance, a single technical review is conducted: the In-Service Review (ISR). The purpose is to ensure that the system meets the users operational needs and the risks are well understood and managed.

6.5.1 Data Collection, Analysis, and Corrective Action System (DCACAS)

As discussed in Chapter 4, a data collection, analysis, and corrective action system (DCACAS) is the backbone of RAM assurance. It provides the data needed to monitor system performance and, if necessary, identify deficiencies for correction to ensure that RAM performance levels meet user needs and constraints. Figure 6-1 shows the operation of a DCACAS system.

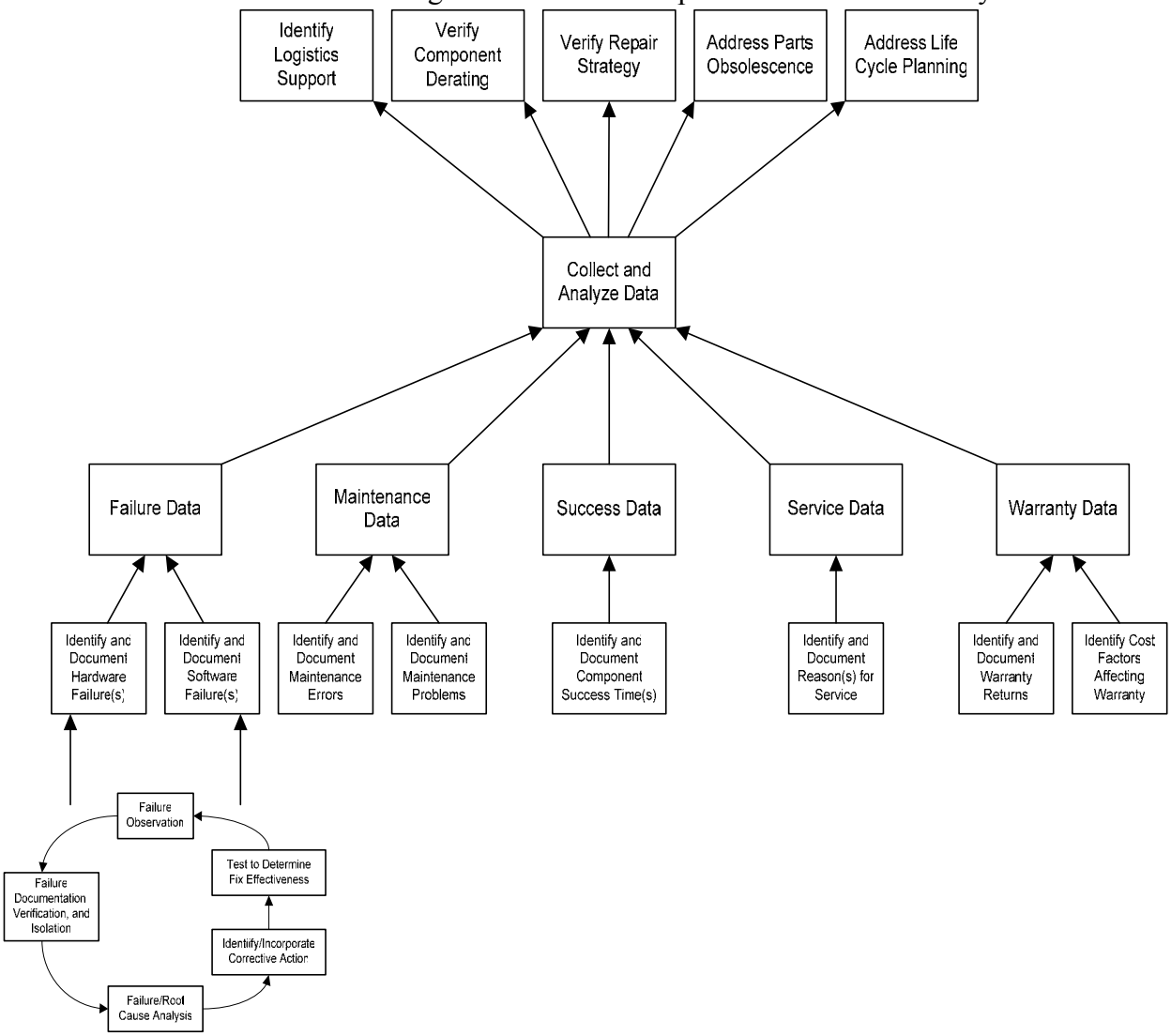


FIGURE 6-1: DCACAS Process

6.5.1.1 The DCACAS Design

In the O&S phase, the DCACAS relies on field reports for failure data, often from maintenance staff, as the system encounters the real world operating and support conditions. The use records, including mission type, hours, duty cycle, etc. are typically available from other data recording systems, depending on the system and circumstances. Ideally the relevant Service DCACAS system will provide a suitable, cohesive, and integrated system. At times, a customized data system or data mining system will need to be developed for the particular application. In the case of current aircraft weapon systems that use the Automated Maintenance Environment

(AME) (Section 5.5.12), there is a particular challenge associated with fielding a full-functioning AME capability with weapons system deployment. Many of the AME related functions may not be available for refinement during system Development and Demonstration because they are unique to the platform being supported. As a result, a useful form for the O&S phase may not appear until after initial deployment and opportunities for rapid maturation of RAM may be delayed or lost. Maintenance managers and personnel may be able to use work-arounds, however the best solution may be in finding ways to develop AME capability to match the deployment timeline.

Routine maintenance management is normally undertaken using a CAMM system, and the CAMM system is often used as the basis of data gathering for system failure and reliability data. Often a base CAMM system will not have sufficient capability to provide a program's DCACAS needs without significant customization.

The DCACAS system for the O&S phase is designed to achieve its requirements. Its purposes need to be understood, the system users identified and their needs understood. Data needs to be input, and the system should aid and enable analysis. Double entry of use and failure data is a waste of resources; hence automated information sharing between operational, maintenance and DCACAS systems is the most desirable situation.

A well-designed and instituted DCACAS can provide the necessary information for the timely identification and correction of design errors, part or process problems, support problems or workmanship defects. All of these deficiencies preclude the achievement of the inherent design RAM potential, with its consequential cost impact. The DCACAS should be in use throughout the system's life cycle.

The DCACAS database is important in establishing the significance (or lack thereof) of a failure. For example, the failure of a capacitor in a reliability growth test becomes more important if the database shows similar failures in incoming inspection of the part and in the environmental tests performed. A pattern of failures shows that there is a systematic reliability problem that will preclude achievement of the inherent RAM metrics unless it is corrected. The DCACAS database should document:

- Initial event reports,
- Diagnostic indications,
- Mission being performed,
- Date and time of failure,
- Part number and serial number of failed item,
- Technician that assessed the failure,
- Failure symptom(s),
- Circumstances of interest (i.e., occurred immediately after power outage), and
- The environment the item was being subjected to at the time of failure.

The failure documentation should be augmented with the verification of failure at the product level, and verification that the suspect part did indeed fail. In the case of O to D concepts,

contractual provisions should establish an efficient process for making that information available.

Once the failure is isolated, the DCACAS database and failure analysis can be used to determine its root cause, then formulate, implement and verify appropriate corrective action. Physics-of-failure, which was discussed in Chapter 4, is a popular failure analysis tool.

Failure and false alarm analyses can be performed to various degrees, and may require some cooperation from the Original Equipment Manufacturer (OEM). The most critical failures and false alarms (i.e., those that threaten the user's safety, cause mission aborts, occur most often, or are most expensive to repair) should receive the most in-depth analysis, perhaps including X-rays, scanning electron beam probing, etc., which typically requires specialized equipment. Where the in-service authority does not operate a suitable failure analysis laboratory, independent laboratories can be utilized. False alarm analyses may require the continuing support of the RAM integrated diagnostics development team, including software development personnel and facilities.

6.5.1.2 Fault Attribution and Classification

The inability of a system to perform any function in the hands of a system user is a failure. When a true failure is detected, it needs to be repaired. In addition to repair, failures should be managed and analyzed. Failure modes should be considered with regard to their impact on operations, cost and safety, and to confirm the original design considerations remain valid. Failure modes that are borne out in the field may continue to be tolerated, but also should be considered for removal through a change of design of the item (modification), or a change of use or maintenance procedures.

In modern complex systems, the operator rarely observes functional degradation. System BIT and the platform's ID programs provide this failure detection function. Experience has shown that where ID maturation tasks are not sufficient, too many failure indications turn out to be false in deployment and operation. It is important that the ID system undergo necessary maturation efforts to minimize the adverse impact that false alarms have on system availability, supportability and total ownership cost.

For the purposes of analysis, true hardware faults may be attributed based on the cause of the failure, typically assigned as design, manufacture, maintenance, human error, etc. For example, a failure that arises as a direct result of material selection would be classed as a design failure, while a failure caused by contamination during manufacturing might be classed as a manufacturing failure. For false alarms, most root causes are usually attributed to improper BIT thresholds, timing, or logic; most are correctable by system or platform mission computer software. Many are very difficult to eliminate because of their frequency of occurrence. This classification system provides a simple sorting aid for management of issues. The purpose of assigning a cause should be to ensure that solutions address the real reason that the failure indication is occurring.

During development or acceptance activities, the attribution of a fault may have involved acceptance consequences. In-service attribution issues can have an effect on warranty. Defining attribution for faults can be an area of concern or contention. It is extremely important to carefully consider all potential events and to specify unambiguous criteria for each failure attribution class. The definitions in the original contractual specifications should act as the starting point for classifying all faults observed. No divergence from these definitions and parameters should be made unless a procedure for modifying the definitions has been agreed.

The use of the terminology of "faults," "failures," "defects," and "incidents" needs to be carefully considered and clearly defined. Incidents may not always lead to a fault or defect, as in the case of BIT false alarms. "Minor" failures such as filament replacements and screw replacements may need to be defined as either counting or not counting towards the overall level of RAM depending on operational and logistics impact. Referring to the original RAM Rationale document definitions and the specification requirement (modified for operational RAM considerations) will ensure that consistency is maintained. If any agreements were made between the contractor and the PMO (user) during development that affected the categorization of failures or faults they must be documented for their effects on the DCACAS process.

Failures that are rectified by adjustment also need to be adequately addressed. When these faults are caused by design issues (such as the positioning of micro-switches) they should be attributed as such; similarly where a poor manufacturing process or initial setting has caused the need for further adjustments, then these problems should be correctly attributed. Where equipment removals are attributable to false BIT indications, the cost of subsequent repair actions should be properly accommodated in subcontractor repair contracts. In cases where in-service repair or maintenance activity induced the problem that requires later adjustment, these should be identified correctly, and recognized as not caused by equipment malfunction. However, if the need for repair is a result of errors in documentation provided to the user by the contractor the incidents should be counted against the equipment until the documentation faults are corrected. Failures caused by human error in operation or maintenance are generally not attributable against the equipment[29]. However, if the same human error persists then consideration needs to be given as to whether the fault should be attributable in particular circumstances and whether redesign is warranted. Full records of how each fault was attributed need to be maintained to support trending analysis.

The RAM Engineering Manager routinely reviews the failures recorded in the DCACAS. The manager should identify issues and raise them for consideration by the Failure Prevention and Review Board.

The FPRB should consider the recommendations of the RAM Engineering Manager and identify which failures may need further investigation or further actions, which may come in the form of modifications for operational or safety reasons. The effects of such modifications on the system

[29] Although human errors during operation and maintenance that cause failures are generally not attributable, but this should not be interpreted to imply that human error and/or maintenance faults are not attributable against the system during operational testing. During operational testing these failures are still attributable as Operational Mission Failures (OMFs) and should be considered when determining mean time between operational mission failures (MTBOMF).

need to be considered and methods agreed upon to attribute any effects, good or bad, in the overall results. The consequential effects of such modifications also need to be considered.

6.5.1.3 Failure Trending

Failure and false alarm trending is part of the routine analysis of failure indications. Ideally this capability should be available within the DCACAS system or easily applied to an export of the DCACAS data. If this has not been developed, it may require staff tasking to accomplish. Failure and false alarm trending involves applying continuous plotting and monitoring of relevant RAM performance characteristics. When any performance characteristic falls outside the designated level of normal variation, the system should automatically flag the items for further investigation by the RAM Engineering Manager.

Automated capabilities to investigate, mine and graphically display RAM data support a comprehensive analysis capability. For example, in addition to trending a fleet (e.g., F-15C), attention could be given to trending between the same system used at various operating locations (e.g., F-15C aircraft operated out of Kadena versus Langley or Ramstein) to determine if geographical factors or local operations and maintenance are affecting RAM performance.

Other automated features that aid the analyst are the identification of RAM bad actors, "lemons," pre-determined system drift, high failure rate items, low availability items, high cost of maintenance items, etc. Classically, trending is carried out at the system and major subsystem level, although some critical, high-value assemblies may also be tracked.

When a negative trend is detected, more detailed data collection and analysis may be necessary to determine the cause. In some cases, special teams are sent to the field to learn what is causing RAM problems.

More detailed discussion of analytical methods for RAM performance monitoring and system trending is provided in Appendix D.

6.5.1.4 Fleet Management

"Lead the Fleet" is a management technique for detecting and resolving problems associated with durability and wearout. For some system types, the In-Service Manager can monitor life related issues by managing life consumption and designating fleet leaders. When there is flexibility to which systems within the fleet that can be tasked, the designated systems are subjected to the high use tasking. These items experience aging associated with cycles of use and allow high life issues to be identified and fixes developed before the entire fleet is affected. Life management is routinely undertaken to manage the major scheduled maintenance load for high complexity assets such as aircraft or ships and maintain a suitable stagger for the scheduled maintenance organization.

For software intensive systems, similar approaches are often taken for major software changes. Often, because the software is hardware configuration dependent, selected users will receive a

particular new software configuration for limited use and evaluation prior to fleet wide dissemination.

6.5.2 Failure Modes and Effects Analysis

As discussed in Chapter 4, a failure modes and effects analysis (FMEA) considers the effects of individual failure modes of every part or function in a designated system. The FMEA may be suitable to aid failure analysis, to identify the root cause, implement corrective action, failure modeling, engineering change development, and BIT/BITE development. The data collected during the FMEA process should be available to the In-Service Manager during the O&S Phase.

The FMEA may also act in its traditional role as a design aid when considering modifications or upgrades to a product or process. FMEAs performed during the original design help establish inherent RAM metrics for the product. Revised FMEAs (when available) should be used to analyze proposed design changes. Design changes should not adversely affect the system's RAM, therefore potential failure modes and causes associated with the design changes should be thoroughly analyzed.

6.5.3 Reliability Growth Testing/Test-Analyze-Fix-Test

The methodology of Reliability Growth Testing (RGT) analysis can also be utilized to monitor the RAM performance of in-service equipment even in cases without growth. This method (Section 4.5.2.15) monitors improvements in reliability while deficiencies are being identified and fixed. The analysis methodology can provide an estimate of the current system reliability.

RGT is also suitable as a developmental technique to assess the impact of design changes and corrective actions on the reliability growth rate of the product.

6.5.4 Life Data Analysis

Life data analysis, originally discussed in Chapter 4, allows reliability practitioners to use system life data to determine the probability and capability of parts, components, and system to perform their required functions for desired periods of time without failure within their specified environment. In the Operations and Support phase, life data analysis takes on the role of supporting overhaul decisions, defining new maintenance philosophies or intervals (i.e., reliability-centered maintenance), and risk mitigation (i.e., safety or cost concerns).

Typically, problems are identified through trending of the DCACAS data (including data from platform data recorders) and user complaints. The analyst investigates the problem using root cause analysis and lab testing and then characterizes the part using Weibull or life data analysis. Additional uses of Weibull Life Data Analysis and its results are described in Section 6.5.7 Reliability Centered Maintenance. For some systems, field generated platform data recorder information is sent to major processing activities for storage, and further dissemination to interested parties (such as the engine contractor) to determine trending and perform detailed failure analysis.

6.5.5 Field Assessment and System Trending

As the system passes between the life cycle phases the manner in which RAM is assessed changes. Reliability predictions are the source of RAM assessments during the System Development and Demonstration phase, then in the Production and Deployment phase RAM metrics are verified using test results to ensure the inherent RAM has not degraded. Finally, in the Operations and Support phase the field RAM assessment is accomplished using the information captured within the DCACAS from deployed systems. Of particular note during the O&S phase, as more and more systems are fielded RAM metrics will be examined at the fleet level instead of a system-by-system assessment. Some of the more commonly utilized RAM metrics for the field assessments include:

- Failure Rate (λ): The total number of failures within an item population, divided by the total time expended by that population, during a particular measurement interval under stated conditions.
- Mean-Time-Between-Failure (MTBF): A basic measure of reliability for repairable items. The average time during which all parts of the item perform within their specified limits, during a particular measurement period under stated conditions.
- Mean-Time-Between-Maintenance (MTBM): A basic measure of reliability for repairable fielded systems. The average time between all system maintenance actions. Maintenance actions may be undertaken for repair or preventive purposes.
- Maintenance Labor Hours per Hour or per Cycle, per Action or per time period (e.g. MLH/FH for Flying Hour); a labor hour factor based on operating or calendar time, maintenance actions, or operating cycles.
- Mean Time Between Removal (MTBR): The average time between all removals of items for any reason, including corrective or preventive maintenance, and to facilitate other maintenance (e.g., gain access to a failed item).
- Mean-Time-To-Failure (MTTF): A basic measure of reliability for non-repairable systems. Average failure-free operating time, during a particular measurement period under stated conditions.
- Mean-Time-To-Repair (MTTR): A basic measure of maintainability. The sum of corrective maintenance times divided by the total number of repairs of the item. The average time it takes to fully repair a failed system. Typically includes fault isolation, removal, and replacement of failed item(s) and checkout. (Also called mean corrective maintenance time, M_{ct}.)
- Mean-Downtime (M_{dt}): The average time a system is unavailable for use due to a failure. Time includes the actual repair time plus all delay time associated with a repairman arriving with the appropriate replacement parts.
- Operational Availability (A_o): The basic measure for "real-world" availability, as this term quantifies the degree to which an item is in an operable state at any time. A_o includes maintenance downtime caused by preventive or scheduled maintenance as well as logistic delay times.
- Operational Readiness: Probability that the system is either available at the beginning of the mission or can be brought to operationally ready state by the beginning of the mission within a prescribed period of time.

- Mean Time between False Alarms: The basic measure for BIT on equipment that has experienced a detected fault where subsequent maintenance fails to confirm the fault. The average time between detected faults where no fault is found. Usually given as operating time or Flight Hours between false alarm.
- Fault Detection Rate: The number of detected failures divided by the total number of failures, both detected and not detected. Usually given as a percent.
- Fault Isolation Rate: The number of detected failures unambiguously isolated to the repairable assembly (preferably one) divided by the total number of detected failures. Usually given as a percent.
- False Alarm Rate: A measure of false failure indications divided by the total number of indicated failures, both true (verified) failures and false (unverified) failure indications. Note: this measure is no longer used for Naval aviation systems.

Statistical models and techniques are used to evaluate system RAM (for individual systems as well as a fleet level). Automated tools and aids allow analysts to apply techniques to system performance data.[30] The mathematics of this consideration is relatively complex therefore the analysis methodology is reviewed in Appendix D.

6.5.6 Repair Strategy

Repair Strategy is formulated during demonstration and development (Section 4.5.2.3) and evolves as more is learned about evolving system RAM. This continues during operations and support. When a product fails it is desirable to restore it to operation in a fast and economical manner. But it is also important that the repair activity does not degrade the inherent RAM of the product. To achieve these ends, it is necessary to formulate and adapt the appropriate repair strategy. As systems are deployed, there is usually a need to review the repair strategy. Inevitably, no matter how well the original repair strategy accounted for the expected needs of the deployed system, changes will be warranted due to unexpected needs or conditions encountered during the Operations and Support phase. The need for repair strategy modifications may come from maintainer feedback, design changes due to modification or upgrade, safety concerns associated with performing repair(s), etc. The DCACAS provides an analytical basis for identifying and prioritizing refinements. The data from on-board recorders and used in the AME environment also supports fine-tuning the repair strategy in response to system performance over the operational portion of the life cycle.

6.5.7 Reliability Centered Maintenance (RCM)

The RCM process was first discussed in Chapter 4 since it is implemented during System Development and Demonstration (SDD). However, it should also be reviewed during the Operations and Support phase. The predicted reliability that was the basis for the RCM planned

[30] The *NIST/SEMATECH e-Handbook of Statistical Methods*, Chapter 8, Reliability, provides an excellent overview, and the automated tools, to assess reliability, choose a statistical model, plot reliability data, test reliability model assumptions, plan data collection for an assessment test, and analyze the data. It is available on line at http://www.itl.nist.gov/div898/handbook/. A CD containing the same information and analysis tools is available, upon request from NIST at no charge. The e-Handbook is NIST Handbook 151. Dataplot™ is NIST Handbook 148.

during SDD should be compared to the field reliability data captured on the deployed systems (via DCACAS).

As previously stated, RCM is a logical, structured framework for determining the optimum mix of applicable and effective maintenance activities needed to sustain the desired level of operational reliability of systems and equipment while ensuring their safe and economical operation and support. RCM is focused on optimizing readiness, availability, and sustainment through effective and economical maintenance.

The RCM process is illustrated in Figure 6-2. Figure 6.2 shows both the RCM process that was completed as part of Step 2 during SDD and the RCM activities conducted during O&S.

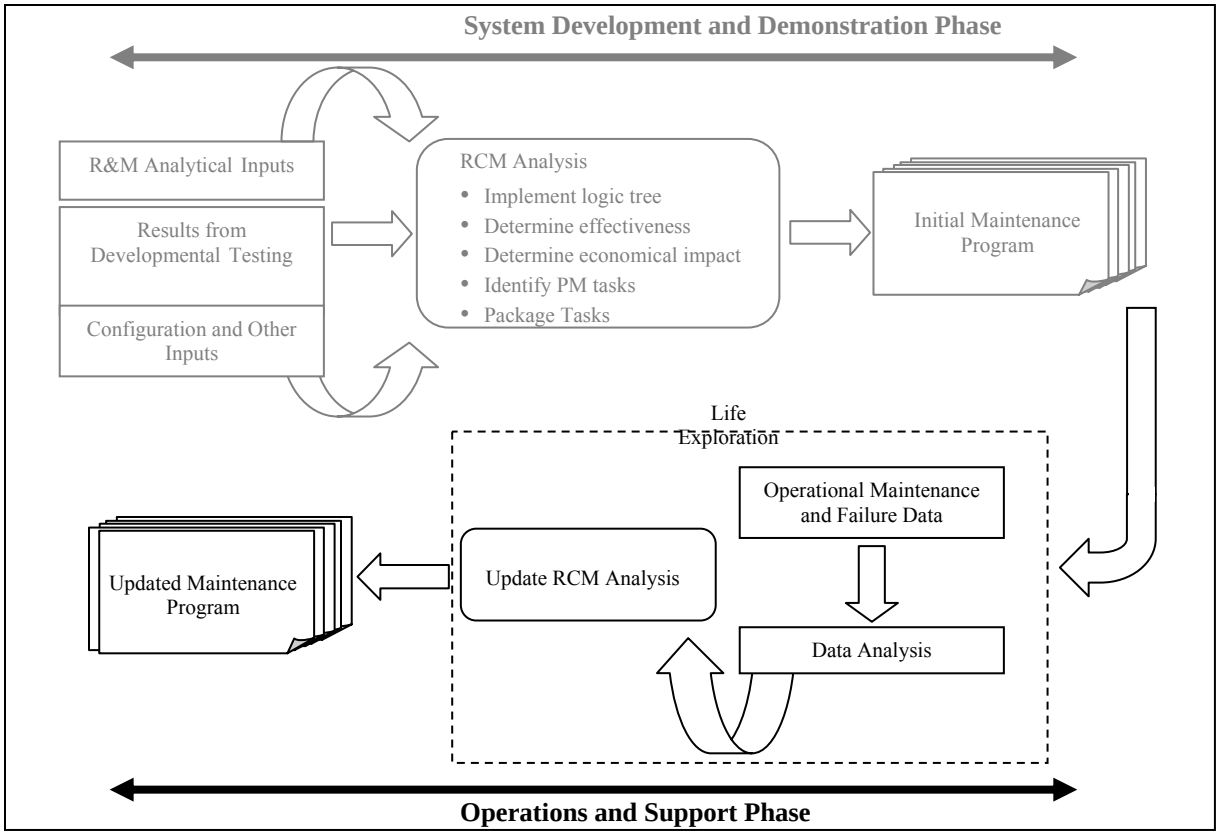


FIGURE 6-2: The RCM Process Continues Throughout the Life Cycle of a System[31]

Maintenance expenditures throughout a system's life cycle often exceed the purchase price. Careful planning of scheduled preventive maintenance through RCM can greatly reduce the total cost of ownership. Re-applying the following seven steps during the Operations and Support

[31] Figure 4-14 concentrated on RCM activities conducted during SDD. In Figure 6-2, completed activities from SDD are shown as muted. SDD RCM results are evaluated during O&S RCM analyses (highlighted) and the maintenance program is updated as appropriate.

phase of the system's life cycle will re-address the ability of the original RCM plans to save money through carefully planned preventive maintenance.

1. Design for Maintainability
2. Perform Functional Failure Mode Analysis
3. Categorize the Failure Distributions
4. Determine Maintenance Tasks Intervals
5. Package All Tasks into an Implementable Plan
6. Optimize Results with Data Collection Efforts
7. Analyze Results for Potential Corrective Action

As always before any preventive maintenance task and its associated task interval is implemented, an economic justification should be performed. The cost of performing the preventive maintenance should be less than the cost of running to failure.

6.5.8 Condition-Based Maintenance (CBM)

As outlined in Chapter 4, many organizations (in an effort to reduce the total ownership costs while simultaneously improving performance and reliability) have turned to condition-based maintenance (CBM) programs. CBM programs are based on the premise that an optimal decision (maintenance point) maximizes the utility of the expected results (in terms of increased product output, decreased maintenance costs, etc.) given the costs (both short term and long term) of implementing the decision. CBM focuses on monitoring and managing equipment and system health.

CBM is ideal when it is not possible to accurately anticipate and predict the expected wear out trends and characteristics of a product or process with age. CBM is also effective when the criticality of a failure warrants the continuous monitoring of a particular product function or component, or process parameter. During Step 4: Monitor Field Performance, all previously planned (i.e., during SDD) CBM programs for the system are monitored to verify their ability to maximize the expected results versus the costs to implement the CBM program. If changes are warranted based on the data and information gathered in Step 4 then the existing CBM program should change accordingly. The changes to the CBM program may include revising the maintenance point for a previously identified item to implementing a new maintenance point for an item that had no prior CBM program specifications.

Different types of condition monitoring techniques and sensing apparatus exist and can be tailored to fit the nature, characteristics, and functionality of the parameter being observed. The list of condition monitoring and non-destructive testing techniques available includes: visual inspection techniques, optical inspection techniques, radiographic monitoring techniques, neutron analysis techniques, ultrasonic monitoring techniques, acoustic emission technology, vibration analysis techniques, lubricant analysis techniques, magnetic flux leakage techniques, temperature analysis techniques, eddy current testing techniques, leak detection techniques, and engine performance parameter monitoring and analysis techniques.

6.5.9 Parts Obsolescence and Diminishing Manufacturing Sources

Most systems will encounter a problem with parts obsolescence or diminishing manufacturing sources during their lifetime as previously discussed in Chapter 4. The most likely phase of the system's life cycle in which these problems will be realized is the Operations and Support phase. Therefore, Step 4: Monitor Field Performance must also track issues related to parts obsolescence and diminishing manufacturing sources. It is imperative that manufacturers (in this case manufacturers represents the spares supplier(s)) develop a strategy to cope with diminishing sources of parts, components, materials and/or suppliers resulting from unilateral supplier decisions, technology advancements, or shakeouts in a competitive marketplace.

By considering parts obsolescence as part of the overall system life cycle planning, it is possible to avoid the significant trouble and expense entailed in searching for replacement parts. Although the need for a replacement part that is no longer available on the market can be satisfied relatively cheaply and quickly when solutions to obsolescence are in place if the unavailability of the part comes as a surprise it will require time consuming and expensive crisis management actions. Unfortunately, the consequences of poorly planning for the system's life cycle in terms of parts obsolescence and diminishing manufacturing sources is rarely realized until the system is deployed.

Preferred parts lists should be reviewed periodically and individual parts listed should be re-evaluated at any sign of obsolescence (manufacturers discontinuing a production line, introduction of newer technology with significant advantages, feedback from buyers reporting difficulty with spare parts purchases, etc.).

There are many possible remedies to part obsolescence problems when they are identified early. Although the options decline as time passes, the remedies to parts obsolescence include lifetime buys, parts substitution, and/or redesign.

Component and supplier obsolescence management needs to be a basic part of a company's design, manufacturing and operating procedures. These best commercial practices should be implemented throughout all phases of the acquisition process, and should be product independent.

6.5.10 In-Service Review (ISR)

The ISR is intended to characterize the in-service technical and operational health of the deployed system. The ISR provides an assessment of risk, readiness, technical status, and trends in a measurable form. These assessments substantiate in-service support budget priorities. ISR objectives can be achieved by consistently applying sound programmatic, systems engineering, and logistics management plans, processes, and sub-tier in-service stakeholder reviews. Support groups may include the System Safety Working Group and the Integrated Logistics Management Team. The effective use of available government and commercial data sources will support the ISR. In-service safety and readiness issues are prioritized to form an integrated picture of in-service health, operational system risk, system readiness, and future in-service support requirements. The ISR provides an assessment of the achieved levels of in-service RAM, in the

context of user needs expressed in the RAM Rationale and earlier assessments of RAM documented in the RAM Case. An analysis of the effectiveness of achieving RAM levels results in a lessons learned opportunity for Operations and Acquisition professionals to use in future capability and system acquisitions.

6.6 Outputs and Documentation

Use of a structured and controlled data acquisition process provides the necessary information to perform trend analyses on the behavior of the subject equipment/system and to support root cause analyses of failure situations. Application of RAM tools and techniques is extremely data-dependent and the root of: (1) oversight/insight into program or system behavior, (2) validation decisions made earlier during the System Development and Demonstration phase, and (3) the identification of modifications/actions needed to sustain the program. For example, if reliability centered maintenance (RCM) were used during design, operations will provide the opportunity to validate or revise the maintenance decisions (redesign, condition monitoring, or run to failure) that were made during the System Development and Demonstration phase. For the purpose of capturing lessons learned that can be utilized on future programs, even one-shot item operation provides the capability to explore what did and did not go well. The most essential ingredient that will help guarantee the success of any operational RAM program is management's continuing commitment and support.

All RAM analysis activities are dependent on the available RAM data. It is important to consider the desired outputs of the RAM analysis at the start of the RAM program, so that a data collection system can be designed to capture the necessary inputs.

Proposals and Contracts

The Defense Federal Acquisition Regulation Supplement (DFARS) requires system acquisition managers to address reliability, availability, and maintainability (RAM) planning:

DFARS PART 207 - ACQUISITION PLANNING

From DFARS 207.105(b)(13)(ii) discuss the mission profile, reliability, and maintainability (R&M) program plan, R&M predictions, redundancy, qualified parts lists, parts and material qualification, R&M requirements imposed on vendors, failure analysis, corrective action and feedback, and R&M design reviews and trade-off studies.

The contract. Both the contractor and the government have responsibility to ensure that the contract clearly specifies (either as a requirement or goal, depending on the phase of the program), the level of RAM to be delivered, stated in the units most appropriate to the system, and the full RAM rationale. For example, operating hours might be the best measure of life for an engine, miles traveled for a truck, cycles for a starter. The contractor should be required to carry out the activities described in the Statement of Work and the proposal to achieve the required levels of RAM. The contract should identify those aspects of the system that are critical, assumptions, the operating and support concepts under which the system will be used, and all other factors that could influence RAM performance in the field.

Evaluating the proposal. In the proposal, the contractor should show a clear understanding of the overall needs of the customer. These needs include what the system is required to do, operational performance parameters (including RAM), how the system will be used and where, operating and support concepts, constraints, and so forth. Based on this understanding, the contractor should address in the proposal the topics shown in Table A-1.

TABLE A-1: Addressing RAM in Contractor Proposals

Describe:

- The activities that will be used for ensuring requisite RAM will be achieved. For each activity, describe the objective, rationale for selection, method of implementation, methods of assessing results, and any associated documentation.
- How RAM activities will be integrated into the product and manufacturing design processes.
- How the results of RAM activities will be used to support other activities, such as logistics planning, safety analyses, etc.
- The definition of failure.

Explicitly show a clear understanding of:

- The importance of designing for RAM and the relationship of RAM to other system performance characteristics.
- RAM design techniques, methodology, and concepts.
- The importance of integrating RAM activities into the overall systems engineering process.

Show an appreciation for the importance of:

- Thoroughly understanding the RAM aspects of design (e.g., failure mechanisms, accessibility, etc).
- Validating the design and manufacturing processes.
- Ensuring proper parts application.
- Addressing all portions of the product including those provided by suppliers and vendors.
- Evaluate the achieved reliability throughout development.
- Determining feasibility of requirements.
- Data rights to failure data, maintainability data and diagnostics performance and the technical data to analyze RAM (such as interface control documents or drawings (ICDs))
- Software documentation for operations support and maintenance
- Contractor Logistics Support for spares and to sustain a level of operational readiness at a fixed price.
- Application DoD requirements for Unique Identifiers (UID)

An example reliability specification template is provided on the next few pages along with a sample statement of work.

RELIABILITY SPECIFICATION TEMPLATE

1. The following levels of reliability are required.
2. Product Reliability

2.1 Failure Free Operation. The product shall provide _____ years (or other time period) of failure free performance verified by demonstrating to a __% level of confidence that the _____ year success probability is greater than _____.

2.2 Usage Profile. The product shall perform its intended function at a duty cycle of __% over the __ year required failure free operating period.

2.3 Life-Limited Items. The product shall contain no life-limited components requiring replacement during the failure free operation period. (if there are life limited items, these should be listed here with recommended replacement schedules)

2.4 Transportation and Storage. The product will be designed so that its reliability will not be reduced due to the effects of being shipped by land, sea, or air, or by periods of storage up to __ years (or other time period).

2.5 Maintenance. Reliability must be satisfied without any maintenance action for single usage hardware. For reuse products, maintenance shall not exceed __% of product cost over the required failure free operating period.

2.6 Operational Environment. The product will be designed so that its reliability specifications will be met under the following environmental conditions:

2.6.1 Temperature. (state minimum and maximum temperatures)

2.6.2 Vibration/shock. (state expected frequency and/or g-force acceleration)

2.6.3 Humidity. (state % relative humidity and/or range, if applicable)

2.6.4 Pressure. (state maximum pressure)

2.6.5 Others. (as appropriate)

2.7 Failure Definition. The product shall be considered failed when it can no longer achieve the following functions to the specified performance levels: (Author should list all relevant performance characteristics and the levels at which the product operation is considered unacceptable. Only clear, unequivocal terms should be used.)

3. Reliability Demonstration. The supplier shall delineate the test(s) that will be performed to verify whether the specified requirement has been met. The element of reliability specification should answer the following questions:

3.1 How the equipment/system will be tested: Specify test conditions such as:

- Environmental conditions
- Test measures
- Length of test(s)
- Equipment operating conditions
- Accept/reject criteria
- Test reporting requirements
- Etc.

3.2 Who will perform the tests? Specify appropriate department organization or outside vendor responsible for conducting the test(s).

3.3 When the tests will be performed? Specify life cycle phase (development, production, field operation)

3.4 Where the tests will be performed? Specify the location of in-house testing laboratory or vendor's facility.

When responding to the RFP, the contractor must consider the following issues:

- What design approaches and analyses tools will help achieve the required levels of contractual RAM?
- How can the contractual RAM requirements be addressed simultaneously with all other performance requirements to produce the best overall product?
- How can the achievable contractual RAM be assessed? How can progress toward meeting the required levels of contractual RAM be measured? How can the achieved levels be demonstrated or determined?

RFP responses should be evaluated, in part, on the basis of a RAM Program Plan as follows.

Understanding. The plan should show a clear understanding of:

- Importance of designing in RAM.
- RAM techniques, methodology, and concepts.
- Importance of integrating RAM activities into the overall systems engineering process.

Approach

Management. The plan should identify:

- Who is responsible for RAM and their experience and qualifications.
- The number of RAM personnel assigned to the program, the experience level of the RAM personnel, and the number of labor hours allocated to RAM activities.
- How RAM personnel fit in the organizational framework of the program.
- An effective means of communication and sharing of information among RAM engineers and analysts, design engineers, manufacturing engineers, and higher management.
- The contractor's system for controlling the RAM of items from subcontractors and vendors.
- How the contractor implements concurrent engineering practices and integrates RAM into the overall engineering and manufacturing effort.

Design. The plan should explain:

- If and how design standards; guidelines; and criteria such as part derating, thermal design, modular construction, Environmental Stress Screening (ESS), and testability will be used.
- The contractor's system for tracking failures and the actions taken to correct (i.e., eliminate or reduce the effect of) the failures.
- If and how a parts control program will be implemented and the approval procedures for nonstandard parts.
- If and how tradeoff studies will be used for critical design areas.
- The time-phasing of RAM activities in relation to key program milestones.
- Any areas of RAM risk.

- If and how software reliability will be addressed.

Analysis/Test. The plan should identify and describe:

- Methods of analysis and math models to be used.
- RAM modeling, prediction, and allocation procedures.
- The time phasing and dependencies of the RAM and other testing in relation to the overall program schedule.
- The time available for the test type required (such as maximum time for sequential test) and how that time was determined.
- How the ESS program (if one is planned) is consistent with the requirements in terms of methodology and scheduling.
- If the contractor will predict the RAM (in whatever parameters are specified) prior to the start of testing.
- How the contractor will monitor the level of RAM through the development.
- The resources (test chambers, special equipment, etc.) needed to perform all required testing, how they were determined, and their availability.
- How the results of all testing will be used to evaluate RAM and identify RAM problems.

Compliance

Design. The plan should include:

- Justification (models, preliminary estimates, data sources, etc.) to back up the claims of meeting RAM requirements.
- Evidence of compliance with required military specifications and standards, when required, and good engineering practices for RAM.
- Each equipment environmental limitation specified.
- If derating will be used and, if so, the methods of verifying derating requirements.

Analysis/Test. The plan shall indicate:

- An explicit commitment to perform all RAM analyses cited in the RAMPP or required by contract.
- An explicit commitment to perform all RAM testing and screening cited in the RAMPP or required by contract.
- That the contractor complies with all product-level RAM test requirements and that the contractor will demonstrate the RAM figures of merit by test using any specified accept/reject criteria or by analysis.
- That the contractor uses the failure definitions in the specification (if none are provided in the specification, then definitions commonly accepted within the engineering community should be used).
- If and how the contractor will perform verification testing, the type of verification testing planned, and the specific purpose of the testing.

Data. The plan should show an explicit commitment to deliver all required RAM data items in the format specified.

Finally, the government must:

- Review proposals and select a winner.
- Consider the winning proposal from all perspectives (including RAM) for inadequacies and apply risk mitigation techniques.
- Negotiate inclusion of any additional required RAM activities.

Software Reliability

State of the art weapon systems (ground vehicles, ships, aircraft, C4ISR[32] systems) and business systems depend on complex software. Modern hardware systems of all kinds contain electronic subsystems and components for which software provides functionality and flexibility. According to a 2000 Defense Science Board report, in the last 40 years, functionality provided by software for aircraft has increased from about 10 percent in the early 1960s for the F-4 to 80 percent for the F/A-22. "The reasons for this are simple: performance requirements for weapon systems have become increasingly demanding, and breakthroughs in software capability have led to a greater reliance on software to provide more capability when hardware limitations are reached."

Software reliability is defined by the Institute of Electrical and Electronics Engineers (IEEE), much like hardware reliability, as "the probability that software will not cause a system failure for a specified time under specified conditions." But hardware and software reliability differ in important ways. Hardware failures are generally a result of a combination of a physical fault and a physical or chemical degradation that progresses over time often as a result of stress, shock or other environmental or operating conditions. Software failures are generally caused by inherent faults that were present all along and are discovered during operation when a particular path, system state, or loading is experienced. Since software failures are physically different from hardware failures, software failures are often called errors or anomalies, since they generally result from an architectural, logical, or coding error, rather than a physical failure.

Software reliability events have degrees of criticality like hardware. If the computer locks up and takes two minutes to restart, it may be unimportant and just a simple annoyance. If the problem recurs frequently, the severity of the impact increases. If it occurs just before target launch or just after an enemy missile locks onto your vehicle, it can be catastrophic. A mission reliability failure, whether caused by hardware, software, or their interaction, is still a mission failure.

Software reliability metrics are similar to hardware metrics for a repairable system. The statistical data is usually a series of times of failures or other events. These data are used during software development to measure time between events, analyze the improvement resulting from removing errors and making decisions about when to release or update a software product version. Metrics are also used to assess software or system maturity (or stability). For example on the F/A-22 development program, the term mean time between avionics anomaly (MTBAA) was used to assess the stability of the avionics subsystems of the aircraft. The program had to meet a requirement that the test aircraft demonstrate a MTBAA of 5 hours before proceeding into operational testing.

A robust system engineering process is fundamental to effective system design, including the systems analysis, allocation of functions to hardware/software, development, integration and test. The highest payoff efforts for reliability and maintainability for both hardware and software is in the front-end design.

[32] C4ISR is an acronym for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.

Repair actions to fix the design of hardware and software are generally less than 100 percent effective. Repairs to correct software reliability problems have a similar potential to induce new problems when the fixes are implemented.

The following lessons are taken from previous acquisition programs.

Understand and document user needs and constraints. Generally the definition of user needs and constraints will not specifically address needs broken out to the level of software. Whatever software implementation is developed in the system will have to be sensitive and responsive to the user needs and constraints.

Design and Redesign for RAM. Over the past decade, more weapon system functionality is allocated to software. Current statistics are not available, but a 1999 analysis indicated that 85 percent of software intensive projects finished over time or budget; half of projects doubled original cost estimates; projects slipped an average of 36 months; and one-third of projects were canceled. Software reliability is a product of robust software design.

Good identification of software requirements in the systems engineering process is essential. If not, software developers can find themselves chasing a moving requirements target or the requirements change after development. Several studies have shown the requirements process is the biggest reason for software failures.

Designers should address software in system reliability design and analysis activities. A system's software must be modeled in its Reliability Block Diagram, otherwise we are assuming it will never fail (MIL-HDBK-338). Further, if a system includes software, then the failure modes and effects analysis (FMEA) should recognize software as a possible failure point. To neglect the software is to assume it will be error-free.

Use commercial best practices. In 2004, the General Accounting Office reviewed the application of software best practices in commercial use and identified three practices used by successful companies. They then examined use of such practices on five DoD weapon system programs. Two programs that used the commercial best practices were successful while three programs did not use them and were not successful. The three best practices are to 1) focus attention on the software development environment, 2) have disciplined development processes, and 3) use metrics methodically to ensure that software is developed within cost, schedule and performance targets. In general the successful companies "employ a spiral development process that sets realistic development goals and ensures those goals are met before the next phase of development begins. In each development spiral, the companies...use a four-stage process, separated by rigorous reviews. Those stages include determining requirements; establishing a stable design; manufacturing code; and testing to validate that the software meets requirements."

DoD program managers should follow the wisdom gained from other defense acquisition experience. The Defense Acquisition Guidebook's Section 4.4.4 Software states that the Program Manager should base software systems development on robust systems engineering principles. It specifically highlights a key contractual activity for success -- selecting contractors

with domain experience in developing comparable software systems; with successful past performance; and with a mature software development capability and process. In addition, it recommends the Program Manager adopt the life cycle view by:

- Preparing for life-cycle software support or maintenance by developing or acquiring the necessary documentation, host systems, test beds, and computer-aided software engineering tools consistent with planned support concepts, and
- Preparing for life-cycle software support or maintenance by planning for transition of fielded software to the support/maintenance activity.

This forward looking recommendation recognizes that changing user needs will inevitably occur over the life of a system as the mission requirements and the environment evolve to meet new challenges.

Software testing should be ranked as a top concern and addressed at the start of a program. The Software Program Managers Network's Little Book of Testing identifies that:

- A poor testing program can cause mission failure, can significantly impact operational performance and reliability, and can double or triple field support and maintenance costs.
- A good testing program is a major program cost. Complex programs can spend more than half their total program effort on T&E activities. To make testing effective you have to take the time up front to plan and organize it properly.
- A good testing program will help significantly as you define your early requirements and design work. That help is critical to getting the project started right, and it can have a major influence on overall project success.
- A good testing program forces you to deal with problems as the work is done, and when the cost of rework and fixes is much lower.
- A good testing program cannot totally make up for a poor software project, but it does help prevent many ills and will let you know you are in trouble early.

Configuration control provides significant challenges to the effective test and evaluation of software. Statistics, Testing and Defense Acquisition: New Approaches and Methodological Improvements (also referred to as STDA) is the source of this observation. Test planning (for software development, system development testing, and operational testing) must take into account the "facts of life" situation with respect to software stability and configuration control. In the case of most avionics programs, the software is still unstable late in the DT phase and often well into OT. A case study from STDA describes a similar problem; the system they reviewed was a COTS evolutionary procurement of a large command and control system. The system experienced a number of problems during test. As a result of frequent failures, the goal of having the system run for the planned (reasonable) number of hours without failure was changed. The large number of components for the system (40) created the potential for interaction problems each time one was upgraded, since it would result in 40 different product enhancements and release cycles. With little configuration control, the systems tested in OT&E were materially different from systems being fielded.

The following is taken from the Defense Acquisition University (DAU) reliability and maintainability course (LOG 203) concerning software reliability and maintainability.

Software reliability and maintainability is defined as, "The probability of failure-free operation of a software component or system in a specified environment for a specified time"

Ten guidelines for increasing software R&M are:

1. Good identification/requirements: Often the software developers are changing a moving requirements target, or the requirements change after development. Several studies have shown the requirements process is the biggest reason for software failures.
2. Modular design: By keeping the lines of code for a particular function packaged together, there is less chance of making a software error, and less difficulty in trouble-shooting one that might occur.
3. Use of high order languages (HOL): HOLs like C++ and Ada are more English-like than assembler language or machine language. Hence, software developers are less likely to make a mistake writing in HOLs.
4. Re-usable software (like pre-packaged, debugged software packages): Like buying a car with a proven engine, re-usable software has less of the "unknown" quality.
5. Use of a single language: Use a single language, if possible, because it does not require translating, converting, or otherwise communicating among several languages, which can be a possible source of error.
6. Fault tolerance: This is the ability to withstand a fault without having an operational failure. It may be achieved by active or inactive redundancy.
7. FMEA: If a system includes software, then the FMEA should recognize software as a possible failure point. To neglect the software is to assume it will be error-free.
8. Review and verification via second team: This allows a second independent team to look at the software before it is released.
9. Functional test-debugging the software: Software can be checked on a simulator before it is released. This can save time and money, while missions and safety are not jeopardized.
10. Good documentation: Good documentation will make it easier to trouble-shoot or upgrade software.

Guideline 6: Fault Tolerance is one of the most important aspects of any RAM Program Plan and is no different for software, therefore it is examined more closely in the subsequent paragraphs. Two techniques for increasing Fault Tolerance are given:

1. N-Version Programming (see Figure B-1), in which:

    - Several versions of the same software (written by different teams or organizations) are running independently at the same time, and
    - Decision algorithm decides which output(s) to use.

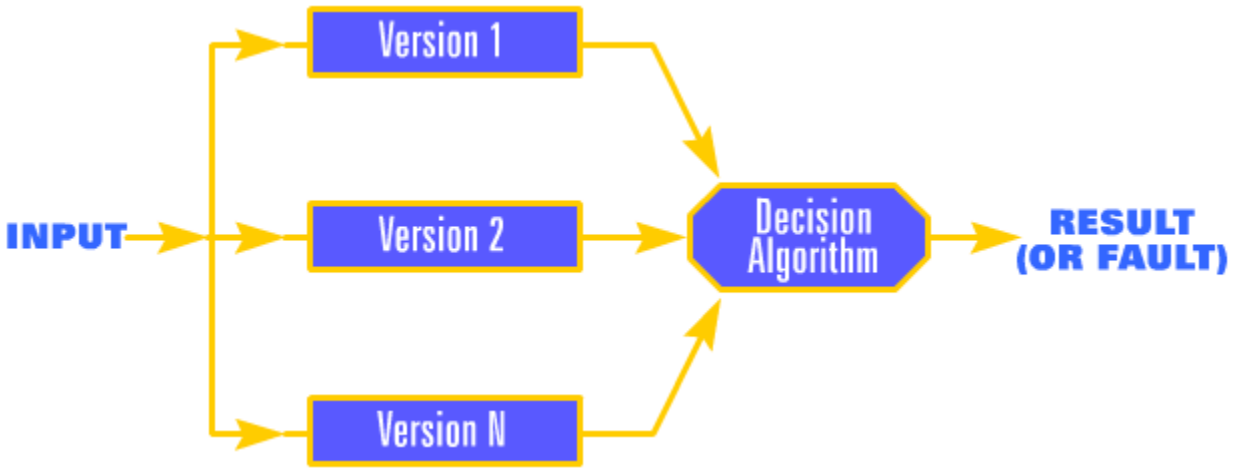


FIGURE B-1: N-Version Programming Fault Tolerance

It is analogous to active redundancy for hardware. It may NOT protect against common errors.

2. Block Recovery Programming Technique (shown in Figure B-2), in which:

   - Independent primary and alternate versions of the same program [or 'Block'] are written, and
   - If primary program fails acceptance test, the alternate program is executed.

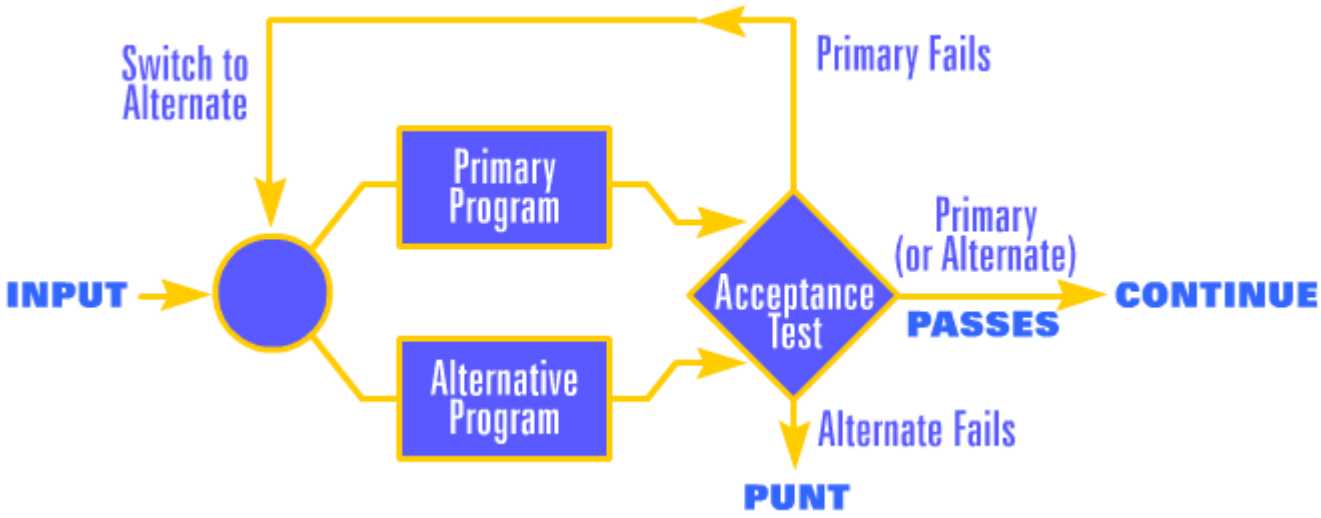


FIGURE B-2: Block Recovery Programming Technique Fault Tolerance

It is analogous to passive redundancy for hardware.

Reliability Growth Management

C.1 Reliability Maturation Metrics for Failure Mode Coverage and Fix Effectiveness

Although having a measure of the achieved mission reliability as the Technology Development (TD) phase progresses would be useful, it may be particularly difficult to do in a statistically meaningful fashion. The various test events may be focused on different performance aspects of the prototypes. In particular, the "operational profile" would not be typically followed. However, to the extent that the TD test events and supplemental analysis provide adequate potential failure mode coverage and effective corrective actions (termed fixes) are implemented, or at least formulated and approved for implementation in the System Development and Demonstration (SDD) units, progress is being made (although it may not be quantifiably measurable as mission reliability). This suggests that to monitor such progress, it would be useful to formulate and track metrics that capture such features of the reliability effort. One such coverage metric could be based on fault trees developed for each of the identified potential system aborts. For example, for a given potential failure that causes system abort, one would first identify each major assembly or minimal set of assemblies that could cause the system abort. Next program management should identify at least the dominant failure mechanisms and associated failure sites that would trigger a malfunction in the assembly or in the assemblies associated with the minimal set that give rise to the system abort failure. Going through this process for each potential system abort failure demands a good understanding of the intended missions, the kinds of assembly failures that prevent the mission from being accomplished, and the potential dominant failure mechanisms and failure sites one needs to guard against to preclude the loss of the mission. Having a good understanding of the preceding is crucial to achieving a successful reliability growth program. Once this process is completed, the basis for a meaningful coverage metric will be in place.

One useful formulation for a coverage metric can be based on the information that describes the ways in which a system abort can occur. In particular suppose all the minimal cut sets for each type of system abort failure (the undesirable end event) have been identified by the fault tree process discussed above such that the elements of these cut sets are failure modes that occur independently from one another. If all the failure modes in a cut set occur during a mission then the mission is lost (i.e., a system abort failure is triggered). The set is minimal in the sense that all the failure modes must occur to trigger the system abort. Thus the number of elements in a minimal cut set (called the order of the minimal cut set) is a measure of redundancy. For example, suppose the minimal cut set of smallest order for a given type of system abort failure is of order two. Then the system is designed such that at least two independently triggered failure modes must occur to cause the system abort failure. Most of the minimal cut sets usually consist of only one failure mode. However there may be many minimal cut sets associated with a given type of system abort failure. The coverage metric would simply be a ratio of the number of minimal cut sets (associated with any of the system abort types of failure) addressed adequately by test or analysis to date divided by the total number of minimal cut sets for the current fault tree. Such a ratio could be tracked for the entire system or separately for each major assembly and high risk assembly interface. The tracking would be done on a calendar basis. A test event or analysis, where necessary, would be deemed adequate for a minimal cut set if the event or analysis was of sufficient scope to either (1) provide a high assurance that none of the failure

modes in the cut set would be triggered during a mission or (2) provide information that would allow implementation of effective corrective actions to mitigate all the failure modes associated with the minimal cut set (and thus preserve the intended degree of design redundancy for cut sets of order two or higher). Hopefully the numerator will be increasing steadily with respect to calendar time. Note however, the denominator should change as well. The system and assembly fault trees should be refined as the system concept and design is matured. Analogous coverage metrics could be formulated and tracked for larger classes of failures that include the system abort failures, such as the class of all failures that induce a logistics burden.

As mentioned earlier, achieving good progress with respect to failure mode coverage is only part of the story. To realize the potential improvement in reliability that such coverage progress allows, effective corrective actions must be implemented to address the failure modes that actually surfaced during the test events as well as failure modes deemed likely to occur with an unacceptable probability, based on the test events and analysis. Thus metrics that capture progress with respect to root cause analyses, Failure Prevention and Review Board (FPRB) approval, and physical implementation should be formulated and tracked. Such metrics could include the calendar time between the event (either test or analysis) that establishes the perceived need for corrective action to one or more of the failure modes associated with a minimal cut set addressed by the event and: 1) the completion of the root cause analysis; 2) the approval of the proposed corrective action plan by the FPRB; and 3) the actual physical implementation of the corrective actions to the target population of test units. These metrics provide a measure of the timeliness of the corrective action process. Metrics that capture the effectiveness of the implemented corrective actions are also of importance. One such metric would be the number of failures attributed to a corrected failure mode that occur on all the test units that receive the corrective action divided by the total test time accumulated on the units since the fix was implemented. This ratio is the number of repeat failures per unit time for the corrected failure mode. Such a ratio could be computed for each corrected mode for which the modified test units have collectively accumulated at least a specified minimum amount of time. Using these ratios for each such corrective failure mode one could then construct a histogram of the failure mode repeat rates. For an effective corrective action program most of these measured repeat failure rates should be zero. Note that a repeat failure rate of zero does not imply the fix drove the true but unknown mode failure rate to zero. For example, if the rate of occurrence of failures due to the mode was 0.0001 before the fix and 0.00001 after the fix, the fraction reduction in the mode failure rate is (0.0001 - 0.00001) / 0.0001 which equals 0.90 (termed the fix effectiveness factor or FEF). Thus even though the fix is not perfect (i.e., the FEF is not 1.0) the probability of seeing a repeat failure on corrected test units that collectively accumulate 5000 test hours is only 0.049. On the other hand, the occurrence of one or more repeat failures in the 5000 hours would be an indication that the fix needs to be reconsidered. If the amount of time accumulated on units and number of failures attributed to a failure mode prior to the corrective action implementation is also available then an estimate of the mode FEF can be made by estimating the mode failure rate before and after the fix, say λ_b and λ_a respectively. Then the estimate would be $(\lambda_b - \lambda_a)/\lambda_b$. Although this is a statistically valid estimate of the mode FEF it is frequently a poor estimate in the sense that whenever λ_a equals zero the estimated FEF is 1.0, indicating a perfect fix. In such cases it would be better to place a lower statistical confidence bound on the FEF, which is easily done by standard methods. One could also utilize a Bayesian approach by constructing a prior on the mode FEF and updating it with the test information. The

mean or median of the posterior distribution could then serve as the mode FEF assessment. A histogram of the mode FEF assessments, along with the arithmetic average of the assessments, for those modes for which assessments can be made, would serve as a useful progress indicator. In the above discussion it is assumed that the fixes are tactical fixes, also referred to as long-term fixes. Many times during a test program short-term fixes are incorporated that allow testing to continue in a timely fashion. These non-tactical fixes are often highly effective with regard to preventing repeat failures for the duration of a test event. Sometimes the "fix" may simply be not to exercise certain system functionalities in the test to avoid known problems. This may especially occur with regard to exercising software. Thus it is important to only utilize information that pertains to the tactical fixes to calculate the FEF metrics.

The above failure mode coverage and corrective action metrics were discussed in connection with the TD phase. However, they are equally meaningful indicators of reliability maturation progress in the subsequent SDD phase. Note the discussed metrics are model independent.

C.2 Reliability Growth Tracking

The most widely used reliability growth models provide assessments when the failure modes corrected are uncovered during the testing. The choice of the correct model to use is highly dependent on the management strategy for incorporating corrective actions in the system. In the test-fix-test strategy problem modes are found during testing and corrective actions for these problems are incorporated during the test. For the test-find-test strategy problem modes are found during testing but all corrective actions for these problems are delayed and incorporated after the completion of the test. A common approach is a combination of these two approaches, referred to as test-fix-find-test. This is the practical situation where some corrective actions are incorporated during the test and some corrective actions are delayed until the end of the test. In order to properly manage a reliability growth program it is vital that realistic and valid reliability assessments be made. The correct model and approach depend on the corrective action strategy: test-fix-test, test-find-test, or test-fix-find-test. In practice corrective actions may be delayed for a number of reasons. For example, it may not be possible to stop the testing for corrective actions or a corrective action to solve a particular problem may take considerable time.

One can also attempt to apply a reliability growth model to the typically more structured SDD test data to statistically track reliability growth. The most promising type of test events for such tracking within SDD are when the system is being operated in a manner similar to the "operational profile." Under such circumstances a simple growth model such as the power law model discussed in MIL-HDBK-189 may be suitable. This is the AMSAA (Crow) power law model discussed for test-fix-test data in more detail later in this appendix (refer to IEC International Standard 61164 as well as Crow's 1975 and 1986 Annual Reliability and Maintainability Symposium (RAMS) papers). Such a model utilizes the cumulative times to failure as measured from the start of a test event. Using these individual failure times, the length of the test and the number of failures that occur one can apply statistically derived formulas to perform a model goodness-of-fit test and estimate model parameters of interest. There are also statistical techniques that can deal with interval data (i.e., when only the amount of test time and number of failures per calendar period are known). The power law model is based on an empirical observation, originally made by Duane. Letting $N(t)$ denote the number of failures by

time *t*, Duane observed that the logarithm of the average cumulative number of failures observed by test time *t* (i.e., *N(t)/t*) versus the logarithm of the cumulative test time tends to exhibit a linear relationship. Taking the inverse logarithm of both sides of this linear equation yields the power law, namely

$$N(t) = \lambda t^{\beta} \tag{1}$$

where $\lambda > 0$ and $\beta > 0$. The negative value of the slope associated with the linear relationship is termed the growth rate and is denoted by α. The value β is defined to be $1-\alpha$. The derivative of (1) with respect to *t* represents the rate of occurrence of failures, termed the failure intensity. The reciprocal is the instantaneous mean time between failures (*MTBF*) at time *t*, denoted by *MTBF(t)*. Thus

$$MTBF(t) = \left(\lambda\beta\, t^{\beta-1}\right)^{-1} \tag{2}$$

Note growth occurs for $\beta < 1$, that is, for $\alpha > 0$.

Statistical procedures are available (e.g., MIL-HDBK-189) to estimate the growth rate and the *MTBF* at any time *t* during the test. Statistical confidence interval procedures are also available for these parameters. All the statistical procedures are based on assuming the number of failures by time *t* is a Poisson process with mean value function *E(N(t))* given by

$$E\big(N(t)\big) = \lambda t^{\beta} \tag{3}$$

Thus for statistical analysis the form of the deterministic Duane relationship in (1) is utilized but *N(t)* is given a stochastic interpretation. In particular, *N(t)* is considered a Poisson random variable with mean λt^{β}. The Poisson process assumption implies that the number of failures that occur in disjoint time intervals are independent Poisson random variables, and the probability that more than one failure occurs in an interval $[t, t+\Delta t]$ is of order Δt. The last condition simply states that the ratio of the probability that more than one failure occurs in the interval to Δt goes to zero as Δt goes to zero. Practically speaking, this last condition says that for a Poisson process, multiple failures do not occur at the same time. Collectively, the conditions imply that a Poisson process should only be assumed for the independently occurring primary failures and should not include the induced secondary failures.

The Duane postulate for reliability growth during test-fix-test development testing states that the instantaneous system *MTBF* at cumulative test time *t* is $M(t) = \left[\lambda\beta t^{\beta-1}\right]^{-1}$, where $\lambda > 0$ and $\beta > 0$ are parameters.

Dr. Larry Crow in his 1974 SIAM paper modeled the Duane postulate stochastically as a Non-Homogeneous Poisson Process (NHPP) with intensity

$$r(t) = \lambda\beta t^{\beta-1} \tag{4}$$

thus allowing for statistical procedures based on this process for reliability growth analyses. This model is applicable to test-fix-test data. Estimation procedures, confidence intervals, etc. are given in MIL-HDBK-189, IEC International Standard 61164, and Dr. Crow's 1975 RAMS paper.

The parameter λ is referred to as the scale parameter and β is the shape parameter. For $\beta = 1$, there is no reliability growth, when $\beta < 1$, there is a positive reliability growth (i.e., the system reliability is improving due to corrective actions), and for $\beta > 1$, there is negative reliability growth.

During the testing failures occur which are caused by the corresponding failure modes. A repair restores the system to an operating status, but the reliability has not been improved. A fix or corrective action is aimed at improving the reliability of the failure mode to reduce its rate of occurrence. Management makes a decision to either continue to repair a failure mode (no corrective action) or to implement a fix. It may take time to implement a corrective action so the failure mode may be repaired one or more times before a corrective action is incorporated into the system. The test-fix-test strategy is to incorporate all corrective action into the system during the testing.

During testing the actual failure times may be known. In some practical applications only the number of failures over intervals of time may be known and available for analysis. This situation is called "grouped data," which is covered in the subsequent paragraphs.

Test-Fix-Test Data

Suppose a development test program begins at time 0 and is conducted until time *T* and stopped. Corrective actions for all problem failure modes surfaced are incorporated into the system during the test. This is commonly referred to as a test-fix-test corrective action management strategy. A widely used model for analyzing test-fix-test data is the AMSAA (Crow) power law model given, which is discussed in MIL-HDBK-189, AMSAA TR-652, Crow's 1974 Society for Industrial and Applied Mathematics (SIAM) paper, IEC International Standard 61164, and Crow's 1975 RAMS paper. For this model, let *N* be the total number of failures recorded and let $0<X_1 < X_2 < \ldots X_N < T$ denote the known *N* successive failure times on a cumulative time scale. Assume that the AMSAA (Crow) NHPP assumption applies to this set of data. Under the AMSAA (Crow) basic model the maximum likelihood estimates (MLEs) for λ and β (numerator of MLE for β adjusted from *N* to *N-1* to obtain unbiased estimate) are

$$\hat{\lambda} = \frac{N}{T^{\hat{\beta}}}, \quad \hat{\beta} = \frac{N-1}{\sum_{i=1}^{N} \ln\left(\frac{T}{X_i}\right)} \tag{5}$$

Under the AMSAA (Crow) basic model the achieved or demonstrated failure intensity at time *T*, the end of the test, is given by *r(T)*. The achieved failure intensity is denoted by

$$\lambda_{CA} = r(T) \tag{6}$$

The achieved or demonstrated *MTBF* at time *T* is given by $M(T) = \frac{1}{r(T)}$.

It is important to note that the AMSAA (Crow) test-fix test model does not assume that all failures in the data set receive a corrective action. Based on the management strategy some failures may receive a corrective action and some may not. This topic of management strategy is further discussed in the upcoming paragraphs.

The grouped data version of the AMSAA (Crow) model addresses the test-fix-test situation where the actual failure times may not be known. In this case the total test period is partitioned into *K* intervals and the number of failures in each interval is known. It is not required that the intervals be of the same length.

Let the length of the qth interval be L_q , $q = 1,\ldots,K$. Also, let $T_1 = L_1$, $T_2 = L_1 + L_2$, …, etc, be the accumulated time through the qth interval. Let N_q be the total number of failures in the qth interval. See Table C.2-1.

Table C.2-1: Grouped Data for Test-Fix-Test

Interval	# of Failures	Length	Accumulated Time
1	N_1	L_1	T_1
2	N_2	L_2	T_2
q	N_q	L_q	TS_q
K	N_K	L_K	T_K

For the test-fix-test grouped data case the AMSAA (Crow) model failure intensity is estimated by

$$\hat{r}(T) = \hat{\lambda}\hat{\beta}T^{\hat{\beta}-1} \tag{7}$$

Where the values $\hat{\lambda}$ and $\hat{\beta}$ satisfy

$$\sum_{q=1}^{K} NI_q \left[\frac{\left\{ [S_q]^{\hat{\beta}} \ln[S_q] - [S_{q-1}]^{\hat{\beta}} \ln[S_{q-1}] \right\}}{[S_q]^{\hat{\beta}} - [S_{q-1}]^{\hat{\beta}}} \right] \tag{8}$$

$$\hat{\lambda} = \frac{N}{T^{\hat{\beta}}} \tag{9}$$

and where *N* is the total number of failures. The achieved or demonstrated *MTBF* is estimated by

$$\hat{M} = [\hat{r}(T)]^{-1} \tag{10}$$

Discrete reliability growth models apply to systems, such as missiles, which are used one time. When the systems are operated the resulting outcome for each trial is either success or failure. These systems are often called "one-shot" systems. The model considered in this section is the discrete version of the AMSAA (Crow) model.

The AMSAA Discrete Reliability Growth Model developed by Dr. Crow in 1983 applies to one-shot systems and assumes that reliability growth takes place on a configuration by configuration basis. That is, for configuration 1 of the system under development N_1 copies are made and tested. The number of failures in the N_1 trials is denoted by M_1. Based on these failures corrective actions are introduced into the system and the updated design is configuration 2. For configuration 2 N_2 copies are made and tested. The number of failures observed for configuration 2 is M_2. This process is continued for K configurations and based on the data it is desired to estimate the reliability of the K^{th} configuration. The reliability of configuration K represents the current reliability of the system.

Let T_i be the cumulative number of trials through the i^{th} configuration, $i = 1,\ldots,K$. That is $T_1 = N_1$, $T_2 = N_1 + N2$, etc. For the Discrete Model the failure probability for the i^{th} configuration is given by

$$f_i = \frac{\lambda T_i^{\beta} - \lambda T_{i-1}^{\beta}}{N_i} \tag{11}$$

Where $i = 1,\ldots,K$. The reliability for the i^{th} configuration is given by $R_i = 1 - f_i$, where $i = 1,\ldots,K$.

Based on the success-failure data for the K configurations the estimates of the parameters of the model are given by $\hat{\lambda}$ and $\hat{\beta}$ that satisfy the following equations:

$$\sum_{i=1}^{K} H_i S_i = 0$$

$$\sum_{i=1}^{K} U_i S_i = 0$$

Where,

$$H_i = \left[T_i^{\hat{\beta}} \ln T_i - T_{i-1}^{\hat{\beta}} \ln T_{i-1} \right] \tag{12}$$

$$U_i = \left[T_i^{\hat{\beta}} - T_{i-1}^{\hat{\beta}} \right] \tag{13}$$

$$S_i = \left[\frac{M_i}{\hat{\lambda} T_i^{\hat{\beta}} - \hat{\lambda} T_{i-1}^{\beta}} - \frac{N_i - M_i}{N_i - \hat{\lambda} T_i^{\hat{\beta}} + \hat{\lambda} T_{i-1}^{\beta}} \right] \tag{14}$$

Before using a statistical model, such as the power law model, one should decide whether the model is in reasonable agreement with the failure pattern exhibited by the data. This should be done graphically as well as statistically. Graphically, a plot of the model estimate of the expected number of failures as a function of test time may be compared to the observed cumulative number of failures. Also, the logarithm of the average cumulative number of observed failures can be plotted against the logarithm of the test time to see whether the data exhibit an approximately linear relationship between these quantities. Any logarithmic base can be used, (i.e., base 10 or base e logarithms can be utilized). The Cramer-von Mises statistical test, which is discussed in MIL-HDBK-189, Crow's 1974 SIAM paper, and IEC International Standard 61164, can be applied to test the null hypothesis that the power law mean value function fits the data. If the graphical and statistical goodness-of-fit checks do not provide strong evidence against the model and there are no non-statistical considerations that argue against using the model to represent the growth pattern exhibited by the data, then one can make the non-statistical decision to analyze the data based on the model representation and associated statistical techniques.

A statistical growth model that only utilizes two or three parameter values cannot hope to capture all the features of the actual growth pattern. The best that can generally be expected is that such a growth model reasonably reflects the overall trend of the realized growth pattern. Adding more than three parameters to a growth model could degrade the usefulness of the model due to the lack of sufficient failure data to estimate the additional parameters. This is especially true if the estimated model quantities of interest are not sensitive to the additional parameters. In general, the underlying causes of growth at the system level do not readily lend themselves to an analytical formulation with parameters that can be estimated from the data. In those cases where the statistical model provides a reasonable representation of the overall growth pattern one can use the model to statistically confirm that growth is occurring and to obtain an estimate for the *MTBF* at the end of a test phase based on the data within the test phase. For the power law model, one can also obtain point and interval estimates of the growth rate α (refer to MIL-HDBK-189).

Even when a model fits the data, one has to be careful about the interpretation of the model parameter estimates. For example, if one applies the power law model to a data set to which it fits one may obtain a positive value of α, e.g., 0.25. This would be a reasonable value to expect for a tracked vehicle based on past data. However, one has to ascertain whether the measured growth rate reflects the implementation of tactical corrective actions or is merely a reflection of the fact that effective short-term fixes have been implemented. Also, if an estimated growth rate is larger or smaller than expected that could be due to a change in the test conditions or in the set of exercises being tested over the test phase. For example, suppose for an artillery system mostly high zone rounds are being fired towards the end of the test phase, while a mixture of lower zone rounds are fired during the rest of the test phase. Then the estimated growth rate would tend to be smaller than it would be if a mixture were maintained throughout the test phase. This is due to the fact that the rate of failed rounds is typically larger for the high zone rounds. The opposite

effect tends to occur if a more demanding environment or set of exercises is undergone towards the beginning of the test phase. The estimate of *MTBF* must be viewed with care as well for the same reason. Even when the conditions within a test phase are reasonably homogeneous, one must exercise caution in what the estimated *MTBF* represents. Unless adjusted, the estimated *MTBF* simply reflects the failure data generated under the test scenarios and conditions experienced in the test phase. Often the test scenarios and conditions in a developmental test phase preclude or significantly reduce certain sets of potential tactical failure modes from occurring. To the extent this occurs, the estimated *MTBF* does not reflect the full extent of the system's potential unreliability when exposed to the tactical conditions. Thus, for example, the reported *MTBF* at the end of the developmental test phase is often significantly higher than the measured *MTBF* during the following IOT&E. This can occur due to the fact that the set of potential operational failure modes associated with the IOT&E is typically significantly precluded from occurring during the developmental test phase. This discrepancy can be partially addressed by conducting some limited user tests (LUTs) during the DT and noting the different types of failure modes that result. To the extent that these modes are addressed by effective fixes prior to the IOT&E and that the failure mode coverage for the potential operational failure modes provided by the LUTs is adequate, the discrepancy between the *MTBF* estimate based on the DT non-LUT data and the measured *MTBF* in the IOT&E should be diminished. One can also attempt to adjust the DT estimate of *MTBF* based on how many operational failures per DT failure have been experienced for a given type of weapon system during past operational tests or LUTs.

It has been stated that due to the additional potential operational failure modes that an unadjusted *MTBF* estimate based on the DT potential failure modes is a poor predictor of the realized *MTBF* in operational testing or in the field. However, this is only partially the case. A low *MTBF* estimate based on the DT data has been a good predictor of failure in a follow-on operational test. A February 2002 study was conducted by the RAM Directorate of the Army Test and Evaluation Command[33], which covers Army systems that under went both DT and OT testing in the timeframe from 1996 through October 2001. The study indicates that of the systems that met their reliability requirement in the DT as a point estimate, 68% succeeded in the follow-on OT. The remaining systems that failed to meet their reliability requirement in the DT as a point estimate experienced only an 18% success rate in the following OT. Such results indicate several things: 1) program management needs to plan opportunities in DT to surface the potential failure modes associated with the operational test/field environment; and 2) if a system fails to meet its reliability requirement even as a point estimate in the DT, then the system should be deemed not ready to undergo the IOT&E.

C.3 Reliability Projection

In addition to utilizing a statistical tracking model over the DT or portion of the DT test phase, one may wish to use a reliability growth projection model. A projection applies to test-find-test and test-fix-find-test management strategies. In both cases some corrective actions for the surfaced problem failure mode are incorporated at the end of the test as delayed fixes. The objective of the projection is to estimate the impact on reliability of the delayed corrective actions.

[33] "Reliability Performance Today," Army Test and Evaluation Command Briefing, February 2002.

Test-Fix-Test Data

Suppose a system is tested for time T. During the testing problem failure modes are identified, but all corrected actions are delayed and incorporated at the end of the test phase. This is test-find-test. These delayed corrective actions are usually incorporated as a group and the result is generally a distinct jump in the system reliability. A projection model estimates this jump in reliability due to the delayed fixes. This is called a "projection." These models do not simply extrapolate the tracking curve beyond the current test phase, although such an extrapolation is frequently referred to as a reliability projection. This type of reliability projection through extrapolation implicitly assumes that the conditions of test do not change and that the level of activities that promote growth essentially remain constant (i.e., the growth rate, α, remains the same). One situation for which such extrapolation is inappropriate is when a significant group of fixes to failure modes that occurred in the test phase are to be implemented at the conclusion of the test phase. Reliability projection models have been developed to assess the impact on reliability due to such delayed fixes (refer to AMSAA TR-357, AMSAA TR-652, IEC International Standard 61164, Crow's 1983 and 2004 RAMS papers, and Corcoran, Weingarten, and Zehna's July 1964 article in Management Science). These methods assume there exist k potential failure modes at the start of the test phase where k is assumed large compared to the number of modes that occur over the test phase. Currently the most widely used models assume k is generally unknown prior to and at the conclusion of the test phase. It is important to note that the failure modes include more than potential design problems. They also include potential failure modes due to quality problems, maintenance procedures and operational problems. These models also split the types of failure modes into two categories, the B-modes and the A-modes. The number k pertains to the number of potential B-modes. A failure mode is referred to as a B-mode if it will be addressed by a corrective action if it is surfaced during the test phase. All other modes are termed A-modes. Examples of typical A-modes would be those associated with COTS or GFE. All the potential failure modes are assumed to occur independently, have an exponential time to occurrence (or geometric number of trials to occurrence for the discrete case), and cause system failure upon occurrence.

Often the distinction between A- and B-modes is not clear-cut. A mode could initially be classified as an A-mode simply because the failure mechanism is currently not well enough understood to formulate a corrective action. Alternately, the mode could be viewed as an A-mode due to current budgetary constraints. However, the classification of such modes could change, for example, due to additional reoccurrences of the mode. Such reoccurrences could shed more light on the underlying root cause of the mode. Also, such repeats might increase the urgency to address the mode in order to meet the reliability requirement. If too many modes are inherently ambiguous with respect to classification, conceptual and estimation problems can ensue. However, current methods that use this classification are based on underlying theory that relies on this conceptual distinction.

In the following we shall consider only the continuous case for constant initial mode failure rates where test duration is typically measured in time or miles. For discussion purposes we shall use time as a measure of test duration. For the simple case where all fixes are delayed, the estimate of the unknown initial B-mode failure rate for mode i can be taken to be N_i/T where N_i denotes the number of failures attributed to B-modes that occur during the test phase of length T. The

system failure intensity after implementation of the delayed corrective actions can be viewed as the realization of a random value whose value depends on the random set of B-mode failures that occur in the test phase. AMSAA TR-357 as well as Crow's RAMS 1983 paper proposed an approximation to the expected value of this random value, which can be expressed as

$$\rho(T) = \lambda_A + \sum_{i=1}^{k} (1 - d_i)\lambda_i + \mu_d h(T) \tag{15}$$

In this expression λ_A denotes the assumed constant A-mode failure rate, λ_i denotes the initial B-mode failure rate for mode *i*, μ_d is the assumed common mean of all the fix effectiveness factors when considered as random variables for the k B-modes, and d_i denotes the realized value of the achieved FEF for mode *i* if mode *i* is surfaced. The function *h(T)* represents the rate of occurrence of new B-modes at the end of the test phase. The assessment of the realized value for the system failure intensity after implementation of the delayed fixes is taken to be the assessment of the expected failure intensity given in AMSAA TR-357 and Crow's RAMS 1983 paper. The reciprocal of the assessment of $\rho(T)$ is utilized as the assessment of the realized *MTBF* after the delayed fixes have been implemented. In the AMSAA (Crow) projection model outlined in AMSAA TR-357, AMSAA TR-652, IEC International Standard 61164, and Crow's 1983 RAMS paper the number of surfaced distinct B-modes during the interval [0,t], denoted by *M(t)*, is assumed to be a Poisson process with mean value function

$$E(M(t)) = \lambda_c t^{\beta_c} \quad \text{for } t > 0, \tag{16}$$

where the constants λ_c and β_c are positive. These constants are subscripted by c to emphasize they should not be equated to the corresponding constants for the tracking model from MIL-HDBK-189. The constants in (16) are estimated from the B-mode first occurrence times. Note the rate of occurrence of new B-modes at time *t* is just the derivative of *E(M(T))* and is geometrically the slope of the graph of *E(M(T))*. Thus, in particular, for the AMSAA (Crow) projection model,

$$h(t) = \lambda_c \beta_c t^{\beta_c - 1} \tag{17}$$

represents the rate of occurrence of new B-modes at time t. For the usual case of a decreasing rate of occurrence of new B-modes, one has $0 < \beta_c < 1$.

The details of the estimation procedure can be found in AMSAA TR-357, AMSAA TR-652, and Crow's 1983 RAMS paper. Here we shall simply point out several things to keep in mind when applying such a model. First note that the estimation procedure for λ_i mentioned above is only valid when all the fixes are delayed to the end of the test phase. This ensures that λ_i is constant over the test phase. If this is not the case alternate projection models and/or estimation procedures must be utilized. Thus one should graphically and statistically investigate whether all fixes have been delayed. This would imply that $\rho(t)$ is constant during the test phase. Occasionally, a developer will assert that all the fixes will be implemented at the end of the test phase. At times such a statement merely implies that the long-range fixes will not be

implemented until the test's conclusion. However, even in such cases it is not unusual that expedient short term fixes are applied during the test period to allow completion of the test without undue interference from known problems. As mentioned earlier, sometimes the "fix" is simply to attempt to avoid exercising portions of the system functionality with known problems. In such instances projection methodology that depends on the λ_i remaining constant during the test phase should not be used. Examples for projection methods that do not require all the fixes to be delayed can be found in AMSAA TR-652 and Crow's 2004 RAMS paper. Another potential application problem is the lack of uniform testing conditions during the test phase. This can greatly influence the pattern of B-mode first occurrence times and thus seriously distort any attempted projection. In particular, the projection models that have been alluded to in the references should not be applied to data from a series of different types of stress tests that take place within a test phase. Also, although there are no hard and fast rules, one needs to surface enough distinct B-modes to allow *h(T)* to be statistically estimated. This implies that there must be enough B-modes so that the graph of the cumulative number of B-modes versus the test time appears regular enough and in conformance with the projection model's assumed mean value function that parameters of this function can be statistically estimated. In fact one should visually compare the plot of the cumulative number of observed B-modes verses test time to the statistically fitted curve of the estimated expected number of B-modes verses test time. Such a visual comparison can help determine if the assumed mean value function for the expected number of B-modes as a function of test time captures the observed trend. There are also statistical tests for the null hypothesis that *E(M(T))* is the mean value function based on the fact that for any time truncated Poisson process, conditioned on the number of observed B-modes *m* over the time period [0,*T*], the cumulative times of B-mode first occurrences are order statistics of a random sample drawn from the distribution given by

$$F(t) = E(M(t))/E(M(T)) \quad \text{for} \quad 0 \le t \le T \tag{18}$$

The Cramer-von Mises test can be used to test the null hypothesis that the first *m* order statistics given by the B-mode first occurrence times are from the distribution (18) for *E(M(T))* given by (16). Thus this provides a test of the null hypothesis that the assumed Poisson process has a mean value function given by the power law.

Another mean value function for the expected number of B-modes that is used in the AMSAA Maturity Projection Model (AMPM) given in AMSAA TR-652 for the case when not all fixes need be delayed is given by:

$$E(M(t)) = (\lambda_B / \beta)\ln(1 + \beta t) \tag{19}$$

In (19) β is a positive constant and λ_B denotes the initial failure rate due to all the B-failure modes. The constant β in (19) is not the β of the power law tracking model discussed earlier. Statistical tests for this mean value function can be based on the B-mode first occurrence times conditional on *m* as indicated above. As for the power law, the distribution function given by (18) for the mean value function in (19) only depends on one nuisance parameter, namely β. However, unlike for the power law mean value function, this distribution is not transformable to a location-scale distribution. Thus β will remain as a nuisance parameter in any of the empirical distribution function (EDF) goodness-of-fit statistics presented in **Goodness-of-Fit Techniques**[2].

Thus the null hypothesis must specify a value for β. Specifically, the null hypothesis is that the mean value function is given by (19) for a specified value of β. One can use any of the empirical distribution function (EDF) tests[34], which include the well-known Kolmogorov supremum statistic to test this null hypothesis. This hypothesis is tested by applying the EDF statistic to the null hypothesis that, conditioned on *m*, the *m* B-mode first occurrence times are from the distribution given in (18) for the mean value function in (19) with β equal to the specified value. Typically the specified value is set equal to a point estimate of β. Unfortunately, if β is specified in such a data dependent way, the resulting EDF significance levels are not exact. Thus they should only be viewed as informal plausibility indicators for such a specified β. Alternately, one can utilize a Chi-Squared Goodness-of-Fit test (for which an estimated value of β can be used).

One advantage of the mean value function in (19) is that it does not have a singularity at zero. This allows estimation of the initial B-mode failure rate based on the B-mode first occurrence times via maximum likelihood estimation. One can then proceed to estimate the projected failure rate by utilizing the formula given in AMSAA TR-652:

$$\rho(t) = \lambda_A + (1 - \mu_d)(\lambda_B - h(t)) + h(t) \tag{20}$$

The assessment of μ_d is taken to be the arithmetic average of the assessed FEFs associated with the surfaced B-modes. Thus, μ_d is only as subjective as the assessments of the individual FEFs. For the case where all the fixes are delayed, one can assess the individual λ_i and apply the assessed individual FEFs to mitigate the estimated λ_i. Such use of individual FEFs could conceivably improve the accuracy of the MTBF projection, provided the assessed mode FEFs are close to the true values. However, the use of an average FEF could provide a more robust MTBF projection. A simulation study is necessary to adequately address these conjectures. The average FEF approach is especially useful for conducting sensitivity analyses with respect to the assessed failure mode FEFs.

Note (20) expresses the expected failure intensity once all the fixes have been implemented to the B-modes surfaced by test time $t \geq T$. This expected rate of occurrence is the sum of three terms. The first term λ_A is simply the assumed constant failure rate due to all the A failure modes. This is estimated by N_A/T where N_A denotes the number of A-mode failures that occur during [0, *T*]. The rate of occurrence of B-modes at time *t*, denoted by *h(t)* can also be shown to represent the expected rate of occurrence of failures due to the B-modes that have not been surfaced by *t*. Thus λ_B-*h(t)* is the expected rate of occurrence of failures due to the B-modes that have been surfaced by *t*. If these surfaced failure modes are fixed with an average FEF of μ_d then after mitigation, the expected residual rate of occurrence of failures due to these surfaced B-modes can be approximated by $(1-\mu_d)(\lambda_B - h(t))$. The final contribution to $\rho(t)$ is the rate of occurrence of failures due to the unsurfaced B-modes which is *h(t)*. The arithmetic average of the individual mode FEFs for the surfaced B-modes can be utilized as an assessment of μ_d. For the case in which all the fixes are delayed, one can simply estimate λ_B by N_B/T where N_B denotes the number of B-mode failures that occur over the test interval [0, *T*]. However, if not all the fixes are delayed then one should not use this estimate since at least some B-modes are being

[34] **Goodness-of-Fit Techniques**, D'Agostino, Ralph B. and Stephens, Michael A., Marcel Dekker, Inc., 1986.

fixed during the test. Instead, one can utilize a maximum likelihood estimate of λ_B based on the number of surfaced B-modes, denoted by *m*, and the B-mode first occurrence times (refer to AMSAA TR-652 for further information). To consider estimation of *h(t)* recall that *h(t)* is the derivative of *E(M(T))*. Thus for *E(M(T))* given by (19) one has

$$h(t) = \lambda_B / (1 + \beta t) \tag{21}$$

Along with λ_B, the parameter β can be estimated by the method of maximum likelihood based on *m* and the B-mode first occurrence times per AMSAA TR-652.

The rate of occurrence of new B-modes can provide a useful maturity metric. In particular, if at the end of a developmental test phase the estimated rate of occurrence of new B-modes is high relative to the reliability requirement, expressed as a failure rate, then no matter how effective the implemented fixes are the residual failure rate due to *h(T)* and λ_A may preclude meeting the requirement in a subsequent IOT&E. Thus prior to entering the IOT&E one should attempt to ensure that the sum of the rate of occurrence of new B-modes plus λ_A is suitably small.

The projection models discussed above assume that the corrective actions do not introduce additional failure modes. Under this assumption the rate of occurrence of new B-modes should be a decreasing function of test time. Since these models also assume that there is a large but finite number of potential B-modes at the start of the test period, one has that *h(t)* must decrease to zero in the limit as *t* increases to infinity. The resulting limiting value of $\rho(t)$ is called the growth potential failure rate, ρ_{GP}. Its reciprocal is termed the growth potential *MTBF*, $MTBF_{GP}$. Taking the limit of the expression in (15) with *T* replaced by *t* as *t* increases one obtains

$$\rho_{GP} = \lambda_A + \sum_{i=1}^{k} (1 - d_i)\lambda_i \tag{22}$$

From (9) one can obtain an alternate expression for ρ_{GP} in terms of the average FEF:

$$\rho_{GP} = \lambda_A + (1 - \mu_d)\lambda_B \tag{23}$$

If the reliability requirement *MTBF* is at or above the assessed reciprocal of (22) or (23) then this may indicate high risk. In such an instance one needs to address a higher fraction of the initial failure rate with corrective actions (the λ_B portion) or increase the effectiveness of the corrective actions.

The AMSAA (Crow) projection model (refer to AMSAA TR-357, AMSAA TR-652, IEC International Standard 61164, and Crow's 1983 RAMS paper) for test-find-test places all failure into two groups, A and B. Type A failure modes are all modes such that if seen during test no corrective action will be taken. This accounts for all modes for which management determines that it is not cost-effective to increase the reliability by a design change. Type B failure modes are all modes such that if seen during test a corrective action will be taken. This Type A and Type B determination helps define the reliability growth management strategy. The basic projection model assumes that the Type A failure modes has constant failure intensity λ_A, the i^{th}

Type B failure mode follows the exponential distribution with failure rate λ_i, and the initial failure intensity for Type B failure modes is λ_B. The total number of failures for the j[th] observed distinct Type B mode is denoted by N_j and the total number of Type B failures seen during the test is $N_B = \sum_{j=1}^{M} N_j$.

A fix effectiveness factor (FEF) d_j is the fraction decrease in λ_j after a corrective action has been made for the j[th] Type B mode. The failure rate for the i[th] Type B failure mode after a corrective action is $(1-d_j)\,\lambda_j$. In practice, for application of the projection model, the FEFs are assigned based on engineering assessments, test results, etc. Studies indicate that an average FEF, d, of about 0.70 is typical for a reliability growth program. Individual FEFs may vary.

For test-find-test the system failure intensity is constant, say, λ_S, during the testing and then jumps to a lower value due to the incorporation of corrective actions. The intensity at the end of the test T, before delayed corrective actions are introduced into the system, is the achieved intensity. The reciprocal of the intensity is the achieved *MTBF* M_S.

The achieved failure intensity $\hat{\lambda}_S$ can be determined by

$$\hat{\lambda}_S = \hat{\lambda}_A + \hat{\lambda}_B, \quad \hat{\lambda}_A = \frac{N_A}{T}, \quad \hat{\lambda}_B = \frac{N_B}{T} \tag{24}$$

The estimated AMSAA (Crow) projected failure intensity is presented in Crow's 1983 RAMS paper by

$$\hat{\lambda}_P = \hat{\lambda}_A + \sum_{j=1}^{M} \left(1 - d_j\right) \frac{N_j}{T} + \bar{d}\hat{h}(T) \tag{25}$$

which is often expressed with $\hat{\lambda}_A = \hat{\lambda}_S - \hat{\lambda}_B$ where $\bar{d} = \frac{\sum_{j=1}^{M} d_j}{M}$, is the average FEF, and

$$\hat{h}(T) = \hat{\lambda}\hat{\beta}T^{\hat{\beta}-1} \tag{26}$$

The estimated projected *MTBF* is

$$\hat{M}_p(T) = \left(\hat{\lambda}_p\right)^{-1} \tag{27}$$

The projection model $\hat{\lambda}$ and $\hat{\beta}$ for (26) use only the M first occurrence failure times of the seen and unique Type B failure modes (see AMSAA TR-357, AMSAA TR-652, IEC International Standard 61164, and Crow's 1983 RAMS paper). Also, it is noted that the AMSAA (Crow) projection model uses FEF input for the Type B individual failure modes.

Test-Fix-Find-Test Data

The Extended Reliability Growth Projection Model for test-fix-find-test was developed by Crow and presented at RAMS in 2004 to address the common and practical case where some corrective actions are incorporated during test and some corrective actions are delayed and incorporated at the end of the test.

This model extends the AMSAA (Crow) Basic Model for test-fix-test and the AMSAA (Crow) Projection Model for test-find-test. That is, these other two AMSAA (Crow) models are special cases of the Crow Extended Model.

In order to provide the assessment and management metric structure for corrective actions during and after a test, two types of B modes are defined. Type BC failure modes are corrected during test. Type BD failure modes are delayed to the end of the test. Type A failure modes, as before, are those failure modes that will not receive a corrective action. These classifications define the management strategy and can be changed. The AMSAA (Crow) basic test-fix-test model does not utilize the failure mode designation. The AMSAA (Crow) projection model for test-find-test data utilizes failure mode designation for the situation of A modes and BD modes only. The BC and BD failure mode designation is an important practical aspect of the Extended Model.

Note that in the failure mode designation BC modes are entirely different than BD modes. For example mode BC1 would be an entirely different failure mode from failure mode BD1 although both have a similar sub designation "1." The test-fix-find-test strategy will fix more failure modes than with the test-fix-test management strategy. During test the Type A and Type BD failure modes do not contribute to reliability growth. The corrective actions for the BC failure modes affect the increase in the system reliability during the test. After the incorporation of corrective actions for the Type BD failure modes at the end of the test, the reliability increases further, typically as a jump. Estimating this increased reliability with test-fix-find-test data is the objective of the Crow Extended Model.

For the Crow Extended Model the achieved *MTBF*, before delayed fixes due to BC corrective actions, should be exactly the same as the achieved failure intensity λ_{CA} for the AMSAA (Crow) Basic Model for test-fix-test data. To allow for BC failure modes in the Extended Model replace λ_S by λ_{CA} in (25) or,

$$\lambda_P = \lambda_{CA} - \lambda_B + \sum_{i=1}^{K}(1-d_i)\lambda_i + dh(T) \tag{28}$$

Also, let λ_{BD} be the constant failure intensity for the Type BD failure modes, and let $h(t|BD)$ be the first occurrence function for the Type BD failure modes (see equation (10)).

The Crow Extended Model projected failure intensity is

$$\lambda_{EM} = \lambda_{CA} - \lambda_{BD} + \sum_{i=1}^{K}(1-d_i)\lambda_i + dh(T|BD) \tag{29}$$

The Crow Extended Model projected *MTBF* is $M_{EM} = 1/\lambda_{EM}$. This is the *MTBF* after the incorporation of the delayed BD failure modes that we wish to estimate.

Under the Crow Extended Model the achieved failure intensity, before the incorporation of the delayed BD failure modes, is the first term λ_{CA}. The achieved *MTBF* at time *T* before the BD failure modes is $M_{CA} = [\lambda_{CA}]^{-1}$. That is, the achieved *MTBF* before delayed fixes for the Crow Extended Model is exactly the same as the achieved *MTBF* for the AMSAA (Crow) Basic Model for test-fix-test.

The estimate of the projected failure intensity for the Crow Extended Model is

$$\hat{\lambda}_{EM} = \hat{\lambda}_{CA} - \hat{\lambda}_{BD} + \sum_{j=1}^{M}(1-d_j)\frac{N_j}{T} + \bar{d}\hat{h}(T|BD) \tag{30}$$

If it is assumed that no corrective actions are incorporated into the system during the test (no BC failure modes), then this is equivalent to assuming that $\beta=1$ for λ_{CA} and λ_{CA} is estimated by $\hat{\lambda}_{CA} = \hat{\lambda}_A + \hat{\lambda}_B$ in equation (24). In general, the assumption of a constant failure intensity ($\beta=1$) can be assessed by a statistical test from the data. For details on estimation and application of the Extended Model refer to Crow's 2004 RAMS paper.

In using the Crow Extended Model it is important that the classification of a B-mode with respect to the BC and BD categories not be dependent on when the mode occurs during the test phase. In some testing programs, modes that occur in the early portion of the test phase tend to have fixes implemented during the test and are thus classified as BC, while those that occur later are not implemented until after the test phase and are thus classified BD. Under such conditions the pattern of BD first occurrence times will provide an inaccurate estimate of the failure rate due to the unobserved BD failure modes. This in turn would degrade the accuracy of the MTBF projection.

For the case where all fixes are delayed one can utilize the AMSAA (Crow) methodology discussed above. An alternate method that uses only individual mode FEFs is discussed in AMSAA TR-751 and in Ellner and Hall's RAMS Paper 2005. The method uses an estimation criterion utilized by Stein in **The Annals of Statistics** to estimate the vector of means for multinormal random variables. The criterion applied to estimating the vector of initial B-mode failure rates $(\lambda_1,...,\lambda_K)$ produces the estimated vector $(\tilde{\lambda}_1,...,\tilde{\lambda}_K)$ where $\tilde{\lambda}_i = \theta\hat{\lambda}_i + (1-\theta)\left\{\frac{1}{K}\sum_{i=1}^{K}\hat{\lambda}_i\right\}$ for i=1,…,K. In this expression $\hat{\lambda}_i = \frac{N_i}{T}$ and θ is chosen to be the value $\theta_S \in [0,1]$ that minimizes the expected sum of squared errors $\sum_{i=1}^{K}(\tilde{\lambda}_i - \lambda_i)^2$. The corresponding projected failure rate is estimated as:

$$\hat{\rho}(t) = \hat{\lambda}_A + \sum_{i\in obs(B)}(1-d_i^*)\tilde{\lambda}_i + \sum_{i\in \overline{obs}(B)}\tilde{\lambda}_i \tag{31}$$

where d_i^* is the assessment of the true value of FEF d_i. AMSAA TR-751 shows that

$$\theta_S = \frac{KVar(\lambda_i)}{KVar(\lambda_i) + \left(\frac{\lambda}{T}\right)\left(1 - \frac{1}{K}\right)} \tag{32}$$

where $Var(\lambda_i) = \frac{\sum_{i=1}^{K}(\lambda_i - \overline{\lambda})^2}{K}$, $\lambda = \sum_{i=1}^{K}\lambda_i$, and $\overline{\lambda} = \frac{\lambda}{K}$. Thus θ_S depends on the unknown values of K, λ, and the population variance of the λ_i, $Var(\lambda_i)$. Proceeding as for the AMSAA Maturity Projection Model (AMPM) in AMSAA TR-652, the λ_i are regarded as a realized random sample from a gamma distribution. Doing so, one can derive an MLE of θ_S, say $\hat{\theta}_{S,K}$, for finite K. The limit for the $\hat{\theta}_{S,K}$, $\lim_{K\to\infty}\hat{\theta}_{S,K}$ is then shown to equal $\hat{\theta}_{S,\infty} = \frac{\hat{\beta}_\infty}{1 + \hat{\beta}_\infty T}$. In this formula, $\hat{\beta}_\infty$ satisfies the equation $\left(\frac{N_B}{\hat{\beta}_\infty T}\right)\ln\left(1 + \hat{\beta}_\infty T\right) = m$, the number of observed B-modes. This yields a projected MTBF, $\hat{M}_{S,\infty}$, such that

$$\hat{M}_{S,\infty} = \frac{1}{\hat{\rho}_{S,\infty}(T)} \text{ for } \hat{\rho}_{S,\infty}(T) = \frac{N_A}{T} + \sum_{i\in obs(B)}\left(1 - d_i^*\right)\tilde{\lambda}_{i,\infty} + \sum_{i\in\overline{obs}(B)}\tilde{\lambda}_{i,\infty} \tag{33}$$

where $\sum_{i\in\overline{obs}(B)}\tilde{\lambda}_{i,\infty} = \left(1 - \hat{\theta}_{S,\infty}\right)\left(\frac{N_B}{T}\right)$, $\tilde{\lambda}_{i,\infty} = \hat{\theta}_{S,\infty}\left(\frac{N_i}{T}\right)$ for each $i \in obs$. In light of the above procedure, the derived projection is termed AMPM-Stein. Simulations conducted by the U.S. Army Materiel Systems Analysis Activity (AMSAA) to date indicate that the accuracy of the AMPM-Stein projection appears favorable compared to that of the international standard adopted by IEC and ANSI, even when the λ_i were randomly chosen from Weibull or lognormal parent populations. Thus, with regard to these three parent populations the results obtained in the simulation study were robust, even though the estimation procedure assumes that the parent population of the λ_i is a gamma distribution. Examples of these simulation results are given in AMSAA TR-751.

One can also apply the AMPM-Stein procedure to the case where failure modes are classified into inherent A-modes and non-inherent A-modes. The set of inherent A-modes, denoted by A_I, consists of those modes that are A-modes by necessity, not by choice. These modes would consist of all those A-modes that are not sufficiently understood to identify the number of failures N_i attributed to the mode. The non-inherent A-modes are comprised of all the B-modes together with those modes that are A-modes by choice (i.e. modes that have $d_i = 0$ by choice).

Let N_{A_I} denote the total of all the encountered failures during test that cannot be categorized by mode, i.e. those failures associated with unidentified inherent A-modes. The failure intensity projection given by the AMPM-Stein procedure is

$$\hat{\rho}_S(T) = \frac{N_{A_I}}{T} + \sum_{i \in obs} \left(1 - d_i^*\right)\widetilde{\lambda}_i + \sum_{i \in \overline{obs}} \widetilde{\lambda}_i \tag{34}$$

In the above, d_i^* is the assessment of the true FEF d_i, obs is the index set for all the observed failure modes that are not inherent A-modes, $\overline{obs}$ is the index set of all the non-inherent A-modes and B-modes that were not surfaced by T, and $\widetilde{\lambda}_i$ is the Stein estimate for λ_i. Using a corresponding definition for $\widetilde{\lambda}_i$ with inherent and non-inherent failure mode categories, one can show that

$$\sum_{i \in \overline{obs}} \widetilde{\lambda}_i = \left(1 - \frac{m^+}{K^+}\right)\left(1 - \theta_S\right)\left(\frac{N_B^+}{T}\right) \tag{35}$$

In this equation m^+ is the observed number of B-modes plus the non-inherent A-modes. Likewise N_B^+ is the number of failures due to B-modes and non-inherent A-modes. Also, K^+ denotes the number of B-modes plus the non-inherent A-modes. For finite K^+, the AMPM-Stein estimate, $\widetilde{\rho}_{S,K^+}(T)$, is given by

$$\hat{\rho}_{S,K^+}(T) = \frac{N_{A_I}}{T} + \sum_{i \in obs} \left(1 - d_i^*\right)\widetilde{\lambda}_{i,K^+} + \sum_{i \in \overline{obs}} \widetilde{\lambda}_{i,K^+} \tag{36}$$

For large K^+, i.e. as $K^+ \to \infty$, this yields

$$\hat{\rho}_{S,\infty}(T) = \frac{N_{A_I}}{T} + \sum_{i \in obs} \left(1 - d_i^*\right)\widetilde{\lambda}_{i,\infty} + \sum_{i \in \overline{obs}} \widetilde{\lambda}_{i,\infty} \tag{37}$$

where $\widetilde{\lambda}_{i,\infty} = \hat{\theta}_{S,\infty}\left(\frac{N_i}{T}\right)$ for $i \in obs$ and $\sum_{i \in \overline{obs}} \widetilde{\lambda}_{i,\infty} = \left(1 - \hat{\theta}_{S,\infty}\right)\left(\frac{N_B^+}{T}\right)$. In the above, $\hat{\theta}_{S,\infty} = \frac{\hat{\beta}_\infty T}{1 + \hat{\beta}_\infty T}$ where $\hat{\beta}_\infty$ satisfies the equation

$$\left(\frac{N_B^+}{\hat{\beta}_\infty T}\right)\ln\left(1 + \hat{\beta}_\infty T\right) = m^+ \tag{38}$$

It should be noted that the AMPM-Stein method that uses the A, B failure mode categories requires that at least one B mode have a repeat failure. The version of the AMPM-Stein method

that classifies failure modes into inherent A-modes and all other modes (non-inherent A modes plus b-modes) requires that at least one non-inherent A mode or B mode have a repeat failure.

C.4 Reliability Growth Planning

A reliability growth plan attempts to lay out a feasible growth path from a current estimate of reliability to a value of reliability sufficiently high at the end of the developmental test phase. This end value should ideally be high enough such that if this value were achieved just prior to entering the IOT&E then the system would have a reasonable probability of demonstrating its requirement during the IOT&E. If the threshold requirement goal is to be demonstrated with statistical confidence, say for example at the 0.80 confidence level, then the DT reliability goal should be set higher than the threshold requirement for two reasons: 1) the realized reliability in the IOT&E is typically lower than that attained during the DT as discussed earlier due to the potential operational failure modes and 2) the realized reliability value in the IOT&E needs to be sufficiently higher than the threshold for the system to have a reasonable probability of passing the IOT&E. For expensive systems with high user reliability requirements a statistical demonstration that relies only on data from the IOT&E may not be feasible. Additional supplemental data sources would need to be considered in such instances. However, as a minimum, the system reliability goal to be attained by the end of the DT should be set sufficiently high so that a system which attains this goal has a low probability of providing strong evidence during the IOT&E that the reliability requirement has not been met.

A crucial part of reliability growth planning involves ensuring that there will be adequate resources available to support the desired growth path. These resources include sufficient test time and units that are allocated to reliability testing, spare units for analyzing failure modes and formulating corrective actions, test and engineering personnel, and RAM testing facilities. Without such underlying resources the target curve will not be realized. Another factor necessary for a successful growth program, sometimes overlooked, is sufficient calendar time during the developmental program to analyze, gain failure prevention and review board (FPRB) approval and implement corrective actions. There may be periods of time throughout the DT during which it would be convenient to implement corrective actions into the test units. For example, refurbishment periods or periods where block updates of functionality are scheduled may be convenient for this purpose. Another consideration with respect to calendar time is how long is the expected calendar time from when the failure mode is discovered to when a fix can be implemented. This will vary from mode to mode but it can be useful to work with an expected value for planning purposes. Thus, for example, if fixes are to be implemented in refurbishment periods and experience indicates that it takes on average 3 months lead time before they can be implemented, the only modes that would be expected to be addressed during an upcoming period that begins on calendar date *C* would be modes that were discovered at least 3 months prior to *C*. A detailed planning curve should explicitly incorporate and display such time lags. One additional significant planning issue with regard to calendar time concerns the delivery schedule of the test units and availability of the test site, personnel, and facilities for RAM testing. When scoping out a reliability growth plan one must take into account the major milestones and any associated interim reliability goals. Of particular importance is the reliability goal at the end of the DT. Attaining this reliability goal could be put in jeopardy if the hardware/software delivery schedule and RAM test resource availability imply that the lion's share of the RAM test hours

will occur late in the DT. In such a case, sufficient RAM test hours may still be realized by the use of multiple test units. However, such a late surge in RAM testing would tend to produce a large number of failure modes over a short calendar period that would need to be addressed. In such an instance, there may not be sufficient calendar time and analysis resources to develop and implement corrective actions, let alone confirm the effectiveness of the fixes, prior to the end of DT. Such a situation could lead to entering the IOT&E with less than fully mature test units. This suggests that a useful risk management metric, based on the detailed growth plan, would be the expected cumulative number of RAM test hours that will be accomplished versus calendar time. RAM calendar milestones should also be displayed on the graphic. If the resulting profile is steeply rising toward the end of the DT then this might indicate the need to modify the planned growth program to mitigate the risk of not attaining the goal reliability during the DT.

The reliability planning curve may extend over all the test phases or just over one test phase. Typically a smooth growth curve is portrayed which represents the overall expected pattern of growth over the test phases. For ease of discussion we shall measure reliability by the *MTBF* metric and test duration by time. The smooth curve is termed the idealized growth curve and is usually specified by a simple mathematical formula that utilizes several parameters. One widely used form is based on the power law expression for the expected number of failures as a function of cumulative test time given by Equation (3). This form is used throughout MIL-HDBK-189. For planning purposes it is more convenient to express $E(N(t))$ in terms of the growth rate α and an initial *MTBF* value, say M_I. Using the form (3), the rate of occurrence of failures, called the failure intensity, is $\nu(t)$ where

$$\nu(t) = \frac{dE(N(t))}{dt} = \lambda\beta t^{\beta-1} \tag{39}$$

For growth one has $0<\beta<1$. Thus (39) has a singularity at $t=0$. Although all the statistical procedures developed for the power law are based on assuming $N(t)$ is a Poisson process with failure intensity $\nu(t)$ for $t>0$ this singularity causes difficulties with respect to planning. In particular, using (39) to portray growth for all $t>0$ suggests that the initial *MTBF* is zero. Thus for planning purposes one uses the power law to represent the idealized overall growth pattern only for values of test time t beyond an initial test phase of length t_1. For t in the initial test phase one either assumes that no growth is taking place and the constant *MTBF* over this period is M_I or that M_I represents an average *MTBF* over the initial test phase. By an average *MTBF* we mean that M_I equals the length of the initial test phase divided by the expected number of failures over the initial test phase. Thus for planning, assuming a constant *MTBF* in the initial test phase,

$$MTBF(t) = M_I \quad \text{for } 0 \le t \le t_I \text{ and } MTBF(t) = 1/\lambda\beta t^{\beta-1} \text{ for } t > t_I \tag{40}$$

In terms of the expected number of failures one has

$$E(N(t)) = \lambda_I t \text{ for } 0 \le t \le t_I \text{ and } E(N(t)) = \lambda t^{\beta} \text{ for } t > t_I \tag{41}$$

where $\lambda_I = M_I^{-1}$.

To make the expected number of failures a continuous function of test time one must have λ_I and t_I satisfy the equation

$$\lambda_I t_I = \lambda t_I^{\beta} \tag{42}$$

This yields

$$\lambda = t_I^{\alpha} / M_I \tag{43}$$

Finally, replacing λ in (40) one obtains

$$MTBF(t) = M_I \quad \text{for} \quad 0 \le t \le t_I \text{ and } MTBF(t) = \{M_I/(1-\alpha)\}(t/t_I)^{\alpha} \text{ for } t > t_I \tag{44}$$

The expressions in (44) are used for planning in MIL-HDBK-189.

Suppose one wishes to achieve a goal *MTBF* of M_G at a milestone by which T test hours have been planned where $T>t_I$. Thus one sets M_G equal to *MTBF(T)* given by (44). One can attempt to use the associated growth rate as a programmatic risk factor. In particular, based on similar systems, for specified T, M_G, t_I, and M_I does the corresponding growth rate α appear achievable? Note by (44) the value of α depends on the ratio T/t_I. The larger this ratio the smaller (and hence less challenging) the needed growth rate will be. This emphasizes the need for care in specifying t_I when applying the power law model for planning. One can always arrive at a reasonable looking growth rate by choosing t_I small enough, no mater what value is used for T. This feature of the power law model is due to the singularity of the failure intensity function at $t=0$. To avoid choosing t_I unduly small and consequently arriving at a growth rate that understates the programmatic risk, one should keep several things in mind. First note that the use of (44) to portray the general reliability growth trend implies that the *MTBF* is tending to increase for $t>t_I$. Thus t_I should be chosen large enough that the test, find, analyze, and fix process has commenced by the end of t_I. For this process to have commenced typically means that at least one B-mode has occurred in test by t_I and that implementation of fixes has begun by t_I. To analytically obtain a value of t_I by which the growth process could plausibly begin let the ratio λ_B/λ_I be denoted by *MS*, termed the management strategy. Thus *MS* is the fraction of the initial failure rate due to B-modes (i.e., modes to which fixes would be applied if surfaced during test). Let ρ denote the probability that a B-mode is surfaced by t_I. The value of t_I should be chosen so that this probability is sufficiently high. The relationship between ρ and t_I is given by

$$p = 1 - e^{-(MS)\lambda_I t_I} \tag{45}$$

For example, choosing ρ=0.95 yields a value of t_I of approximately $3(M_I/MS)$. See Crow's 1986 RAMS paper for additional information on this topic.

Besides the singularity at zero, the power law model has the property that the *MTBF* can grow without bound (i.e. the failure intensity goes to zero as *t* increases). This is only consistent with assuming all failure modes are B-modes and fixes are perfect. However neither of these conditions usually occur. Thus the power law is only appropriate to apply to a time period over which the power law failure intensity does not become unrealistically small. Care must be exercised in using the power law model for planning over a number of test phases that can collectively encompass a calendar period of many years. In such instances the planned cumulative test time on all the test units could be many thousands of hours. If the power law is applied over this entire period with constant growth rate α, the implied final *MTBF* may be unrealistically high even for reasonably chosen values of t_I and M_I, and a modest growth rate. Practically, this is simply a reflection of the fact that even a modest growth rate cannot be maintained forever. Eventually, technological and resource constraints come into play. Thus, the assumed log-log linear relationship between the *MTBF* and test time with slope α must eventually be untenable. This should be kept in mind when formulating an idealized curve based on the power law. Several reliability projection concepts, not explicitly part of the power law model, are useful in considering this issue. The growth potential, $MTBF_{GP}$, was discussed earlier with respect to projection. This was the theoretical value that would be reached if all B-modes were surfaced and corrected with the assumed or assessed FEFs. Assuming an average FEF μ_d, management strategy *MS*, and initial *MTBF* M_I one can express the growth potential *MTBF* as follows:

$$MTBF_{GP} = M_I / \left(1 - (MS)\mu_d\right) \tag{46}$$

If the final *MTBF* on the idealized growth curve is not below the *MTBF* growth potential for reasonable planning values of *MS* and μ_d then even if the growth rate α appears modest it might not be sustainable over the entire period over which the idealized power law model has been applied. In such a case one could consider applying separate power law idealized curves over the major test phases. Thus each subsequent test phase would have a higher initial *MTBF* than the previous test phase and probably a lower growth rate as the system matures. However, applying the power law with the new origin located at the beginning of the subsequent test phase implies (even with a lower growth rate) that the *MTBF* is initially growing much more rapidly than it grows towards the conclusion of the previous test phase. This is again due to the singularity of the power law at the origin. Thus portraying growth by using separate idealized curves governed by the power law over adjacent test phases implicitly assumes that a new set of potential "vital few" failure modes have been introduced in the subsequent test phase. This could be the case if new functionality has been added or if different test conditions prevail.

Besides checking the growth rate for reasonableness and whether the final *MTBF* is below a reasonable growth potential *MTBF*, there are other things to check. One is the ratio of the initial *MTBF* M_I to the goal or final *MTBF* M_G. Studies have determined that the achieved ratio is usually at least 0.15 where M_I is the estimated *MTBF* of an early engineering test unit in SDD and M_G is the estimated *MTBF* of a test unit at the conclusion of DT or during the subsequent IPT. Another item to consider is the implied expected number of failures over the test period over which the idealized curve is portrayed. This can be calculated by applying equations (44) and (42). Equivalently this expected number of failure can be calculated from the equation below

$$E\big(N(T)\big) = T/\big((1-\alpha)M_G\big) \tag{47}$$

In this equation T is the test length of the period and M_G is the goal *MTBF* to be attained at T. This equation allows calculation of the expected number of failures in the interval beyond t_I. This expected number of failures is simply $E(N(T))-E(N(t_I))$, where $E(N(t_I))=\lambda_I t_I$. At the risk of mixing models, one can also calculate the expected number of B-mode failures beyond t_I as the previous difference minus $\lambda_A(T-t_I)$, where $\lambda_A=(1-MS)\lambda_I$. If the expected number of B-mode failures, or the expected number of failures is small over this interval then the expected number of B-modes would be at least as small. Such small numbers over this interval would indicate that attempting to portray an idealized overall growth pattern over $[t_I, T]$ would add little value and could be misleading. The actual growth pattern under such circumstances would tend to be quite discrete.

More generally, if the reliability growth strategy is to substantially apply fixes only during a few convenient relatively short periods, then the resulting *MTBF* growth pattern would consist of a few steps. One would have a step corresponding to the initial *MTBF* and a few additional steps corresponding to the planned *MTBF* at the conclusion of each fix implementation period. Again, representing such a planned growth pattern by an idealized growth curve would be misleading. This would be especially true if the idealized curve portrayed a suitably high *MTBF* to enter a subsequent test event, such as the IOT&E, but the planned *MTBF*, based on the actual scheduled fix implementation periods, was significantly lower. Also, as discussed earlier, a realistic assessment of the average lag time from the discovery of a failure mode to when a fix is physically implemented into a test unit could result in the planned *MTBF* being substantially lower than the portrayed idealized *MTBF* at a milestone.

The idealized curve provides some useful programmatic risk measures that are independent of the fix implementation strategy. The growth rate for the idealized curve is an implicit function of the underlying values of *MS,* average FEF, and B-mode test profile and is indicative of how the *MTBF* would grow on a test time basis (i.e., as a function of accumulated test time only) due to these underlying factors if fixes are being implemented. By a B-mode test profile is meant the implicitly assumed underlying sequence of unknown initial B-mode failure rates, ordered from the highest failure rate. Note that a low realized growth rate could be due to the *MS* or average B-mode FEF being low or due to a fairly flat B-mode test profile, for example, one that consists of a large number of very small B-mode initial failure rates. Such modes take a long time to surface and, even when corrected with high FEFs, individually contribute little in reducing the system's failure intensity.

The idealized *MTBF* reached after t test hours can be interpreted as the reciprocal of what the expected failure intensity would be if fixes were implemented to all the B-modes surfaced in test by t (with $t>t_I$ for the power law). This interpretation suggests a flexible approach to constructing a detailed planning curve from an idealized curve based on the power law or based on the expression in (20) for the projected failure intensity. This later approach would avoid the singularity problem encountered with the power law at the origin. One could utilize (20) with any continuous decreasing function $h(t)$ such that $h(t)$ approaches zero as t increases and $h(0)$ is a finite positive number. The planning parameters would be the easily interpreted quantities μ_d

and *MS*. The function *h(t)* is a reflection of the test profile. In fact for *h(t)* given by (21), one can show that the fraction of *h(0)* that is contributed by the largest initial B-mode failure rates is a function of β/λ_B. Thus, high values of β lead to a rapidly diminishing *h(t)* in (21). Whether the power law or some other function of test time is used for the idealized curve, one approach to constructing the detailed test plan is as follows:

1. Specify the calendar periods over which corrective actions will be applied, for example refurbishment periods. Let the i'th calendar period be from S_i to E_i;
2. Assume the average calendar lag time from when a B-mode is surfaced to when it can be implemented is Δ;
3. Let t_i' denote the amount of test time accumulated on all the test units by S_i' (calendar date the precedes S_i by Δ).

Then plot $MTBF(t_i')$ from the end of period *i* to the end of period *i+1*, that is, over the calendar period from E_i to E_{i+1}. In the above $MTBF(t_i')$ is given by (40) for the power law model or by $\rho^{-1}(t_i')$ using (20) for the projection failure intensity. The first step is simply M_1 which extends from the calendar date at the start of the test period to the ending calendar date E_1 of the first fix implementation period. The milestones should also be depicted on the graphic of the detailed planning curve. Note the curve is presented on a calendar basis. This detailed planning curve is a reflection of the underlying smooth idealized curve, the assumed average fix lag time, and the planned implementation periods. Using the idealized curve one can calculate the expected number of failures (for the power law) or the expected number of B-modes (for the projection models) that are to be addressed in any fix implementation period. This can be used to judge the adequacy of the allotted calendar durations for the implementation periods. Most importantly, the positioning of the planned implementation periods relative to the reliability milestone goals can be assessed from the resulting *MTBF* curve.

It should be noted that the statistical assessment procedures for tracking and projection are only based on the failures and failure modes that are surfaced during the analyzed test period. Also the planning methodology to a large extent only explicitly takes into account reliability growth due to surfacing and fixing failure modes through reliability testing of the system. In practice, additional potential failure modes are considered through analysis and discovered by a variety of lower level tests. In fact analysis and accelerating testing of components and subassemblies are all important sources of knowledge about potential failure mechanisms and sites. Thus, such activities should be addressed in terms of resources and schedule in any reliability growth program. The realized initial planning *MTBF* values can be significantly enhanced by these activities if the resulting knowledge is used to implement corrective actions to potential failure modes prior to the planned reliability test period. Such on-going activity during a reliability test can be a significant part of the failure mode analysis effort and lead to more effective fixes to the B-modes surfaced during test.

Field Assessment and System Trending

Evaluating the RAM of systems begins with the realization that a sequential failure process exists for the system. This failure process is composed of many sequential random variables.

This system failure process is depicted in Figure D-1. A point process is characterized by observations in the form of point events occurring in a continuum such as time. Such processes arise in many fields of study such as economics, physics and system reliability. A point process can be defined by specifying:

- Description of each event and the measure of time (i.e., operating hours, rounds, cycles, etc.).
- The observed intervals between successive events denoted TBF_1, TBF_2, … TBF_N or the instants of occurrences of the events measured from the time origin denoted $TTSF_1$, $TTSF_2$, $TTSF_3$, … $TTSF_N$.

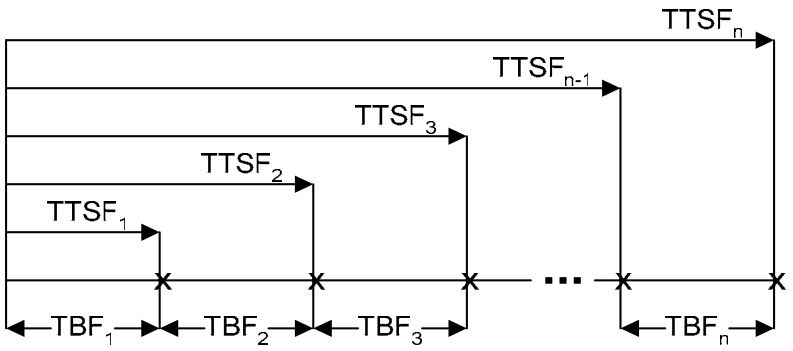


FIGURE D-1: Repairable System Failure Process.

The observed intervals between successive events (TBF_1, TBF_2, …) are termed inter-arrival times and the intervals to the occurrence of events measured from the time origin ($TTSF_1$, $TTSF_2$, …) are termed arrival times. The arrival times are obtained by forming the cumulative sums of the inter-arrival times or

$$TTSF_1 = TBF_1, TTSF_2 = TTSF_1 + TBF_2, TTSF_3 = TTSF_2 + TBF_3, ... TTSF_n = TTSF_{n-1} + TBF_n$$

where,

$TTSF_n$ = *is the arrival time of the* n^{th} *event*

Given that a system can be characterized by a point process, a major concern for the reliability analysis lies in describing this detailed pattern of occurrence. Of particular concern is whether a trend or some other systematic feature exists. For example, trends indicating that the inter-arrival times (TBF_i) are becoming smaller over a period of observation indicate that system performance is deteriorating. The modeling and analysis of point processes provides measures to quantify such systems.

Unlike part failure data, the chronological ordering of time-between-failure (TBF) data is extremely important for a repairable system. Therefore, disrupting or failing to track this ordering of failure events should be avoided. This can be illustrated in the following example, given the following three time-between-failure (TBF) values of: 10, 50, and 100. If the sequential order of these events is unknown, then a total of six different unique system processes can be created. The total number of unique system processes can be calculated using the equation for permutations:

$$p_r^n = \frac{n!}{(n-r)!}$$

where,

$n = total\ number\ of\ objects$

$r = number\ of\ objects\ selected\ out\ of\ the\ total\ number$

Substituting n = 3 and r = 3, the permutation equations above yields:

$$p_3^3 = \frac{3!}{(3-3)!} = \frac{6}{1} = 6$$

The six unique system processes, identified by their unique arrangements of inter-arrival values are as follows:

1. 10, 50, 100 (improving trend)
2. 10, 100, 50 (no trend established)
3. 50, 10, 100 (no trend established)
4. 50, 100, 10 (no trend established)
5. 100, 50, 10 (deteriorating trend)
6. 100, 10, 50 (no trend established)

If order statistics and distributions plotting techniques were incorrectly used to model each system process, *the same distribution parameters would be calculated* for all six of the systems. To evaluate one unique repairable system point process, order statistics and distribution plotting and fitting techniques obviously cannot be applied. If, on the other hand, a number of system failure processes are available, order statistics and distribution plotting techniques can be used to evaluate the distribution of time-to-first-failure (TTFF) of the repairable system. This also holds true for any other unique inter-arrival time (such as time between first and second failure). The appropriate system modeling tools will be presented and discussed in the following subsections.

D.1 Point Process Models

When modeling a single repairable system point process, the two most popular models that have been publicized are the:

- Homogeneous Poisson Process (HPP)

- Non-Homogeneous Poisson Process (NHPP)

The HPP model can be used to describe a process which is stationary and whose time-between-failures show no trends to increase or decrease as the system ages. This type of repairable system is characterized by a constant rate of occurrence of failure (ROCOF). This constant rate is also called the peril rate, ρ.

The NHPP model can be used to describe a process whose time-between-failures show trends to increase or decrease as the system ages. The NHPP is a good first approximation for a repairable system because it models a process characterized by a time dependent rate of occurrence of failure or $\rho(t)$.

The procedure for selecting which process model should be applied is provided in Figure D-2.

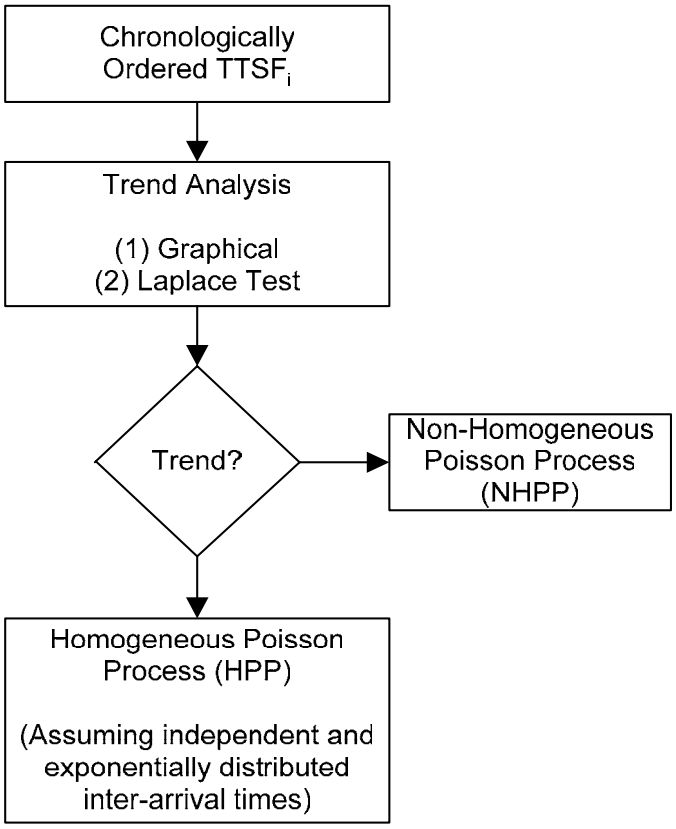


FIGURE D-2: Selecting the Appropriate Process Model.

Both process modeling and trend analysis procedures (HPP, NHPP) will be discussed in the following subsections.

D.2 Homogeneous Poisson Process (HPP)

The Homogeneous Poisson Process can be used to model a system failure process whose time-between-failures (TBF_i) are independent and identically exponentially distributed. The inter-arrival values of the point process (TBF_i) must exhibit no trend to increase or decrease as the system ages. Inter-arrival values possessing this characteristic are referred to as "random" inter-arrival values. A system that is neither improving nor deteriorating (i.e., constant rate of occurrence of failure) is generally a good candidate for the HPP model.

The Poisson Process is characterized by the number of failures in any interval from t_1 to t_2 having a Poisson distribution with mean $\rho(t_2 - t_1)$. The Poisson process can be characterized as:

$$P\{N(t_2) - N(t_1) = j\} = \frac{e^{-\rho(t_2 - t_1)}\{\rho(t_2 - t_1)\}^j}{j!},\ j \geq 0$$

where,

$N(t)$ represents the number of failures to time t and ρ is the constant rate of occurrence of failure. The Poisson distribution equation states the probability of having "j" failures in the interval t_1 to t_2 for a homogeneous Poisson process.

By setting $j = 0$, the probability of no failure in the interval t_1 to t_2 can be determined as:

$$P\{N(t_2) - N(t_1) = 0\} = e^{-\rho(t_2 - t_1)}$$

The previous equation represents the probability of survival, or reliability, in the interval t_1 to t_2 which can be represented as:

$$R(t_1, t_2) = e^{-\rho(t_2 - t_1)}$$

D.3 Non-Homogeneous Poisson Process (NHPP)

A functional form of time variant rate of occurrence of failure (ROCOF), ρ(t), for the NHPP is:

$$\rho(t) = \lambda\beta t^{\beta - 1}$$

where,

$\lambda > 0$

$\beta > 0$

$t \geq 0$

Given a system failure process which contains a trend, the ROCOF or $\rho(t)$, can be determined by maximum likelihood estimators of β and λ shown below, as identified in Crow's "Reliability Analysis for Complex Repairable Systems," 1974 SIAM paper.

$$\hat{\beta} = \frac{n}{\sum_{i=1}^{n-1} \ln \frac{TTSF_n}{TTSF_i}}$$

$$\hat{\lambda} = \frac{n}{TTSF_n^{\hat{\beta}}}$$

where,

$TTSF_i$ = *Arrival times as identified in Figure* $5-1$

n = *Total number of system failure events*

As an example, consider the system failure process illustrated in Figure D-3.

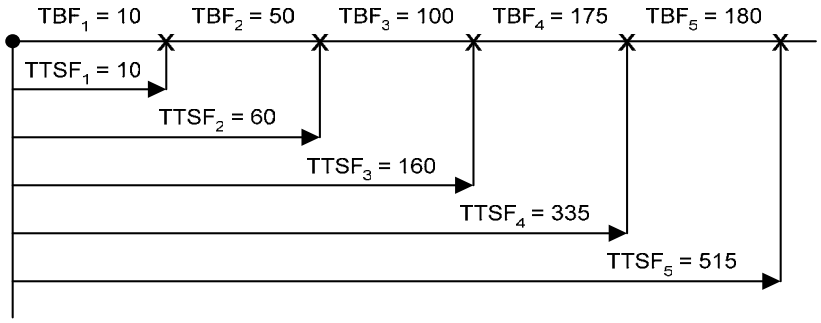


FIGURE D-3: Repairable System Failure Process, Example.

Using the above calculations we can determine the values of β and λ for this example.

$$\hat{\beta} = \frac{5}{\ln\frac{515}{10} + \ln\frac{515}{60} + \ln\frac{515}{160} + \ln\frac{515}{335}} = 0.65$$

$$\hat{\lambda} = \frac{5}{515^{0.65}} = \frac{5}{57.9} = 0.086$$

Substitution of β and λ into the NHPP equation yields:

$$\rho(t) = (0.086)(0.65)t^{0.65-1}$$

$$\rho(t) = 0.056t^{-0.35}$$

The expected number of failures in the interval zero to *t*, *V(t)*, is given by the following equation:

$$V(t) = \int \rho(t)dt$$

If we substitute the NHPP equation into this equation to determine the expected number of failures, *V(t)*, the following equation is the result:

$$V(t) = \hat{\lambda} t^{\hat{\beta}}$$

Substituting the values from our example this new equation can yield the expected number of failures before a time of 300 hours.

$$V(300) = (0.086)(300)^{0.65} = 3.5$$

This value of 3.5 failures corresponds with the expected number of failures before t = 300 hours for the system shown in Figure D-3.

D.4 Trend Analysis of System Failure Data

In this section we will present two procedures for evaluating if a trend exists in a system failure process. The two procedures for evaluating trends are:

- Graphical plot of cumulative failure versus cumulative operating time using linear scales
- Laplace test statistic

Each of these trend analysis procedures is easy to apply and interpret.

As indicated in Table D-1, the determination whether or not a trend (i.e., increasing or decreasing TBF_i) exists in essential in selecting the appropriate model for the process.

D.5 Plotting Cumulative Failures vs. Cumulative Operation Time

Let us now consider the two system failure processes defined in Table D-1.

TABLE D-1: System Failure Process Data.

Failure Order Number (i)	System A Arrival Times ($TTSF_i$)	System B Arrival Times ($TTSF_i$)
1	15	177
2	42	242
3	74	293
4	117	336
5	168	368
6	233	395
7	410	410

The data for System A was intentionally fabricated to represent an increasing trend in the time-between-failures (TBF_i), whereas the data for System B was intentionally fabricated to represent a decreasing trend in time-between-failures (TBF_i).

Both of these systems (A, B) can be evaluated by constructing a plot of cumulative failures versus cumulative test time on linear scales as shown in Figure D-4. The data from Table D-1 was used to generate each curve.

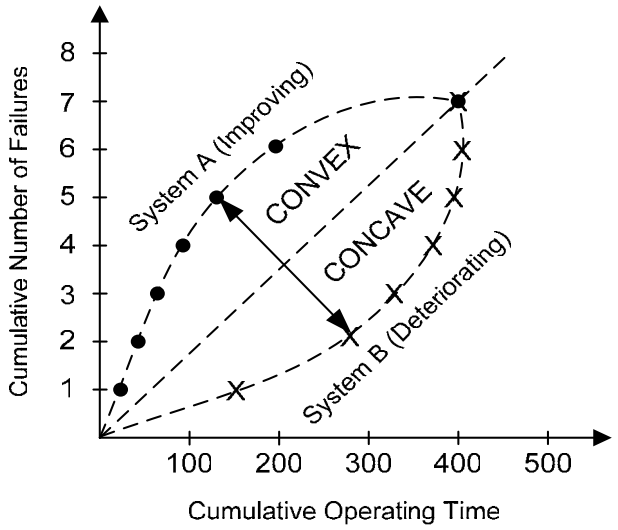


FIGURE D-4: Cumulative Failures vs. Cumulative Operating Time.

Using Figure D-4 as a visual reference, we can conclude that failure processes (such as System A) which exhibit a *convex* curve on a plot of cumulative failures versus cumulative operating time using linear scales represent improving systems (i.e., TBF_i are tending to increase). Failure processes (such as System B), which exhibit a *concave* curve on a plot of cumulative failures versus operating time, represent deteriorating systems (i.e., TBF_i are tending to decrease).

This graphical technique provides a simple but effective means to visually assess whether or not a trend exists in a system failure process and can be applied prior to modeling using the HPP or NHPP.

In addition to the previous comments on trending, we should make the point that a negative trend can result from premature wear out of a part, poor maintenance, inadequate repair strategies, etc. Also, determining the underlying causes of a negative trend can involve a lot of hard work, additional data collection, testing, etc.

D.6 Laplace Test Statistic

Pierce Simon Laplace (1749-1827) was one of the great mathematicians of the eighteenth century and was responsible for many of the statistical theorems which are still in use today – one being the central limit theorem and another being the much less known Laplace statistic. Here we adopt his principle to evaluate whether or not a trend is present for failure events of a system.

As with the graphical method discussed in the previous subsection, the Laplace test statistic can also be used to determine if sequential inter-arrival times (TBFi) are tending to increase, decrease or remain the same. The underlying probability model for the Laplace test is a NHPP having log-linear intensity function. (The test may be misleading if the underlying probability model for the Laplace test is not applicable.) The Laplace test statistic for a process with "*n*" failures is:

$$U = \frac{\left[\left(\sum_{i-1}^{n-1} TTSF_i\right)/(n-1)\right] - (TTSF_n/2)}{TTSF_n\sqrt{1/(12(n-1))}}$$

The conclusions which can be rendered based on the Laplace statistic, *U*, are:

1. *U* approximately equal to zero indicates the lack of trend.
2. *U* greater than zero indicates inter-arrival values (TBF_i) are tending to decrease (i.e., system deterioration).
3. *U* less than zero indicates inter-arrival values (TBF_i) are tending to increase (i.e., system improvement).

If we again utilize the system failure process definitions of Figure D-4 and calculate the Laplace statistic for System A then B:

System A:	*System B*:
$Given: n = 7$	$Given: n = 7$
$TTSF_n = 410$	$TTSF_n = 410$
$\sum_{i=1}^{n-1} TTSF_i = 646$	$\sum_{i=1}^{n-1} TTSF_i = 1811$

Calculate the Laplace statistic using the equation for a process of "*n*" failures in the following manner:

$$U_A = \frac{(646/6) - (410/2)}{410\sqrt{1/72}}$$

$$U_A = -2.01\ (System\ TBF_i\ tends\ to\ increase)$$

$$U_B = \frac{(1811/6) - (410/2)}{410\sqrt{1/72}}$$

$$U_B = +2.00\ (System\ TBF_i\ tends\ to\ decrease)$$

A

A_i	Inherent Availability
A_o	Operational Availability
ACIM	Availability Centered Inventory Model
ACIR	Availability Centered Inventory Rule
AEC	Army Evaluation Command
AIAG	Automotive Industry Action Group
ALDT	Administrative and Logistics Delay Time
ALT	Accelerated Life Testing
AME	Automated Maintenance Environment
AMPM	AMSAA Maturity Projection Model
AMSAA	Army Materiel Systems Analysis Activity
AoA	Analysis of Alternatives
ASR	Alternative System Review
ATE	Automatic Test Equipment
ATEC	Army Test and Evaluation Command

B

BIT	Built-in-test
BITE	Built-in-test equipment

C

C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAD	Computer-Aided Design
CAMM	Computer Aided Maintenance Management
CBM	Condition Based Maintenance
CDD	Capability Development Document
Cdf	Cumulative Distribution Function
CDR	Critical Design Review
CFR	Constant Failure Rate
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CMMR	Commercial Item Military Market Research
COI	Critical Operational Issues
COMOPTEVFOR	Commander Operational Test and Evaluation Force (Navy)
COSIP	Computer Open Systems Implementation Program
COTS	Commercial-Off-the-Shelf
CPD	Capability Production Document
CR	Concept Refinement (acquisition phase)
CSI	Critical Safety Items

D

DAB	Defense Acquisition Board
DAU	Defense Acquisition University
DCACAS	Data Collection, Analysis, and Corrective Action System
DCMA	Defense Contract Management Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DoD	Department of Defense
DOE	Design of Experiments
DOT&E	Director Operational Test and Evaluation
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities
DRR	Design Readiness Review
DT&E	Developmental Test and Evaluation
DT/OT	Development Test/Operational Test

E

ECP	Engineering Change Proposal
EDA	Exploratory Data Analysis
EDF	Empirical distribution function
EMI	Electromagnetic interference
ESS	Environmental Stress Screening
ETE	External test equipment

F

FAA	Functional area analysis
FAR	False Alarm Rate
FEA	Finite Element Analysis
FEF	Fix effectiveness factor
FFD	Fraction of Faults Detected
FIR	Fault Isolation Resolution
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FNA	Function Needs Analysis
FOC	Full Operational Capability
FOT	Follow on Operational Test
FOT&E	Follow on Operational Test and Evaluation
FPRB	Failure Prevention and Review Board
FRACAS	Failure Reporting, Analysis, and Corrective Action System
FRP	Full Rate Production
FRPDR	Full Rate Production Decision Review
FSA	Functional Solution Analysis
FTA	Fault Tree Analysis

G

GAO	General Accounting Office
GFE	Government Furnished Equipment
GFI	Government Furnished Information

H

HASS	Highly Accelerated Stress Screening
HALT	Highly Accelerated Life Testing
HOL	High order language, Higher order language
HPP	Homogeneous Poisson Process

I

IBR	Integrated Baseline Review
ICD	Initial Capabilities Document
ICD	Interface Control Document or Drawing
ID	Integrated Diagnostics
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IFR	Increasing failure rate
IID exponential	independently and identically exponentially distributed
IIT	Information Integration Technology
IOC	Initial Operational Capability
IOT&E	Initial Operational Test and Evaluation
IOT	Initial Operational Test
IPT	Integrated Product Team
ISO	International Standards Organization
ISP	Information Support Plan
ITR	Initial Technical Review

J

JCIDS	Joint Capabilities Integration and Development System
JROC	Joint Requirements Oversight Council

K

KPP	Key Performance Parameters

L

LFT&E	Live Fire Test and Evaluation
LRIP	Low Rate Initial Production
LUT	Limited User Test

M

$\overline{M}_{ct}$	Mean corrective maintenance time
M_{dt}	Mean Downtime
M_{Max}	Maximum time to repair, Maximum active corrective maintenance time
M-SPARE	Multiple Spares Prioritization and Availability to Resource Evaluation
MCMC	Markov Chain Monte Carlo
MDA	Milestone Decision Authority
MCOTEA	Marine Corps Operational Test and Evaluation Agency
MDAP	Major Defense Acquisition Program
MDT	Mean down time
MLE	Maximum likelihood estimate, maximum likelihood estimator
MOE	Measures of effectiveness
MR	Maintenance ratio
MS	Milestone
MTBAA	Mean time between avionics anomaly
MTBCF	Mean time between critical failure
MTBF	Mean time between failure
MTBM	Mean time between maintenance
MTBOMF	Mean time between operational mission failure
MTBR	Mean time between repair
MTB_	Mean time between (event) e.g., critical failure, maintenance action, etc.
MTTF	Mean time to failure
MTTR	Mean time to repair

N

NASA	National Aeronautics and Space Administration
NAVSEA	Naval Sea Systems Command
NDI	Non-Developmental Item
NHPP	Non-Homogeneous Poisson Process

O

OA	Operational Assessment
OC	Operating characteristic
OEM	Original Equipment Manufacture
OMF	Operational Mission Failure
OPEVAL	Operational Evaluation (Navy)
O&S	Operations and Support
OS	Operations and Support (acquisition phase)
O to D	Organizational to Depot (maintenance levels)
OT	Operational Test
OTA	Operational Test Agency
OT&E	Operational Test and Evaluation

OTRR	Operational Test Readiness Review

P

P&D	Production and Deployment (acquisition phase)
PATS	Product and Technology Surveillance (a subset of CMMR)
PCA	Physical Configuration Audit
Pdf	Probability density function
PDR	Preliminary Design Review
PEO	Program Executive Officer
PoF	Physics of Failure
PM	Preventive maintenance
PM	Program Manager
PMO	Program Management Office
PPL	Preferred Parts List
PRAT	Production Reliability Assurance Testing
PRST	Probability ratio sequential testing
PREDICT	Performance and Reliability Evaluation with Diverse Information Combination and Tracking
PRR	Production Readiness Review

Q

QA	Quality assurance

R

R&M	reliability and maintainability
RAC	Reliability Analysis Center
RAM	Reliability, availability, and maintainability
RAMS	Reliability and Maintainability Symposium
RAMPP	RAM Program Plan
RBD	Reliability Block Diagram
RBS	Readiness Based Sparing
RCM	Reliability-Centered Maintenance
RFP	Request for Proposal
RGT	Reliability Growth Testing
RIW	Reliability improvement warranty
ROCOF	Rate of occurrence of failures
RoI	Return on Investment
RQT	Reliability Quality Testing, Reliability Qualification Test

S

SAE	Service Acquisition Executive

SAE	Society of Automotive Engineers
SCRB	Software Change Review Board
SDD	System Development and Demonstration (acquisition phase)
SELECT	Selection of Equipment to Leverage Commercial Technology
SESAME	Selective Stockage for Availability Multi-Echelon Model
SEP	Systems Engineering Plan
SFR	System Functional Review
SIAM	Society for Industrial and Applied Mathematics
SPC	Statistical Process Control
SRR	System Requirements Review
STA	System Threat Assessment
SVR	System Verification Review

T

TA	Testability Analysis
TAFT	Test-Analyze-Fix-Test
TD	Technology Development (acquisition phase)
TDS	Technology Development Strategy
TECHEVAL	Technical Evaluation (Navy)
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TEP	Test and Evaluation Plan
TES	Test and Evaluation Strategy
TOC	Total Ownership Cost
TPS	Test program set
TQM	Total Quality Management
TRR	Test Readiness Review
TTF	Times-to-failure
TTFF	Time-to-first-failure

U

UID	unique identification
USC	United States Code
USDAT&L	Under Secretary of Defense Acquisition, Technology and Logistics

V

W

WCCA	Worst Case Circuit Analysis

X

Y

Z

Chapter 1 References

1. **Defense Acquisition System DoD Directive Number 5000.1**, Office of the Undersecretary of Defense, Washington, DC, May 12, 2003.
2. **Operation of the Defense Acquisition System DoD Instruction 5000.2**, Office of the Undersecretary of Defense, Washington, DC, May 12, 2003.
3. **Statistics, Testing, and Defense Acquisition: New Approaches and Methodological Improvements,** National Research Council, Michael Cohen, John Rolph, and Duane Steffey, Ed., National Academy Press, 1998.
4. **Reliability Issues for DoD Systems**, National Research Council, Francisco Samaniego and Michael Cohen, Ed., National Academy Press, 2002.
5. **BEST PRACTICES: Setting Requirements Differently Could Reduce Weapon Systems' Total Ownership Costs**, GAO final report, February 11, 2003; [GAO Code 120092/GAO-03-057]
6. **Independent Review of Reliability Analyses**, NASA Preferred Reliability Practices, PD-AP-1302, Jet Propulsion Laboratory, December 1998.
7. "Achieving High Reliability," Crow, L. H., The Journal of the Reliability Analysis Center, Fourth Quarter, 2000, 1-3.
8. "Reliability Performance Today," Army Test and Evaluation Command Briefing, February 2002.
9. "Making Reliability a Reality," AEC-AMSAA paper, Army Acquisition Logistics & Technology Magazine, March 2003,
10. "Five Key Ways to Improve Reliability," AEC-AMSAA paper, RAC Journal, 2Q 2003.

Chapter 2 References

1. **Defense Acquisition System DoD Directive Number 5000.1**, Office of the Undersecretary of Defense, Washington, DC, May 12, 2003.
2. **Operation of the Defense Acquisition System DoD Instruction 5000.2**, Office of the Undersecretary of Defense, Washington, DC, May 12, 2003.
3. **A Practical Guide to Statistical Analysis of Material Property Data**, Romeu, J. L. and C. Grethlein, AMPTIAC, 2000.
4. **Accelerated Testing; Statistical Models, Test Plans and Data Analysis**, W. Nelson, Wiley, 1990.
5. **An Introduction to Probability Theory and Mathematical Statistics**, Rohatgi, V. K., Wiley, NY, 1976.
6. **Automobile Industry Action Group FMEA Standard**, 1992.
7. **Designing Engineering Experiments**, C. Lipson, McGraw-Hill, 1973.
8. **Electronic Reliability Design Handbook**, MIL-HDBK-338B, October 1998.

9. **Failures Modes, Effects, and Criticality Analysis**, RAC, 1993.
10. **Fatigue of Materials**, S. Suresh, Cambridge University Press, 1998.
11. **Fault Tree Application Guide**, RAC, 1990.
12. **Fault Tree Handbook**, US Nuclear Regulatory Commission, NUREG-0492, January 1981.
13. **Handbook of Reliability Engineering and Management**, W.G. Ireson et al, McGraw-Hill, 1996.
14. **Handbook of Statistical Methods for Engineers and Scientists**, H.M. Wadsworth, McGraw-Hill, 1989.
15. **Independent Review of Reliability Analyses**, NASA Preferred Reliability Practices, PD-AP-1302, Jet Propulsion Laboratory, December 1998.
16. **Jet Propulsion Laboratory Reliability Analyses Handbook**, JPL-D-5703, July 1990.
17. **Mechanical Reliability**, A. D. S. Carter, John Wiley & Sons, 1986.
18. **Methods for Statistical Analysis of Reliability and Life Data**, Mann, N., R. Schafer and N. Singpurwalla, John Wiley, NY 1974.
19. **Procedures for Performing a Failure Mode, Effects and Criticality Analysis**, MIL-STD-1629 (canceled, but still useful reference).
20. **NIST/SEMATECH e-Handbook of Statistical Methods**, Chapter 8, Assessing Product Reliability, http://www.itl.nist.gov/div898/handbook/, 2004.
21. **Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program**, NASA-STD-8729.1, December 1998.
22. **Practical Reliability Engineering**, P. D. T. O'Connor, John Wiley & Sons, 1998.
23. **Probabilistic Mechanical Design**, Haugen, John Wiley & Sons, 1980.
24. **Probabilistic Reliability Engineering Approach**, M. L. Shooman, McGraw-Hill, 1968.
25. **Probability and Statistics for Engineers and Scientists**, Walpole and Myers, Prentice Hall, NJ, 1988.
26. **Product Reliability, Maintainability, and Supportability Handbook**, ARINC Research Corporation, Mike Pecht, Editor, 1995.
27. **Quality Engineering by Design**, Phadke, Prentice Hall, 1989.
28. **RCM II**, Moubray, Industrial Press, 1992.
29. **Reliability and Life Testing Handbook, Volumes 1 and 2**, D. Kececioglu, Prentice Hall, NJ, 1993.
30. **Reliability Centered Maintenance**, A. Smith, McGraw-Hill, 1993.
31. **Reliability Engineering Handbook**, D. Kececioglu, Prentice Hall, 1991.
32. **Reliability Fault Tree Analysis**, Society for Industrial & Applied Mathematics, 1975.

33. **Reliability in Engineering Design**, K. C. Kapur and L. R. Lamberson, John Wiley & Sons, 1977.
34. **Reliability Prediction – Mechanical Stress/Strength Interference (Non-Ferrous)**, Lipson C. et al, RADC-TR-68-403, 1968.
35. **Reliability Prediction, Mechanical Stress/Strength Interference**, Lipson, C. et al, RADC-TR-66-710, 1966.
36. **Reliability Toolkit: Commercial Practices Edition**, RAC, 1994.
37. **Statistical Methods for Reliability Data**, Meeker, William Q. and Luis A. Escobar, John Wiley & Sons, 1998.
38. **Systems Engineering and Analysis**, Blanchard, Benjamin S. and Wolter J. Fabrycky, Prentice Hall, January 1998.
39. **The New Weibull Handbook**, R. Abernathy, 1996.
40. **Designing and Assessing Supportability in DoD Weapon Systems: A Guide to Increased Reliability and Reduced Logistics Footprint**, Office of Secretary of Defense, February 12, 2003.

Chapter 3 References

1. **Systems Engineering Guidebook**, Martin, James N., CRC Press LLC, Boca Raton, FL, 1996.
2. **Systems Engineering Fundamentals**, Defense Acquisition University Press, Ft. Belvoir, VA, 2000.
3. **Systems Engineering: A Practical Approach to Systems Engineering Processes and Basic Capability Maturity (SYS2)**, Manary, Joel, Reliability Analysis Center, Rome, NY, 2004.
4. **Reliability Toolkit: Commercial Practices Edition**, Dudley, Bruce etc. al., Reliability Analysis Center, Rome, NY, 1994.
5. **Reliability Program Plan (RPP) Guidelines**, Yuhas, Stephen P., DA RAM Panel Validation Subgroup, 2001.
6. **User Requirements to System Specification Program**, Criscimagna, Ned, Clark, David, and Denson, William, Reliability Analysis Center, Rome, NY, 1994.
7. **RAM Rationale Report Handbook**, US Army Training and Doctrine Command (TRADOC) and US Army Material Command (AMC), Virginia, 1987.
8. **Defense Acquisition System DoD Directive Number 5000.1**, Office of the Undersecretary of Defense, Washington, DC, May 12, 2003.
9. **Operation of the Defense Acquisition System DoD Instruction 5000.2**, Office of the Undersecretary of Defense, Washington, DC, May 12, 2003.

10. **Defense Acquisition Guidebook Version 1.00** (formerly Interim Defense Acquisition Guidebook dated October 30, 2002 and DoD 5000.2-R, dated April 5, 2002), Office of the Undersecretary of Defense, Washington, DC, November 17, 2004.
11. **Operation of the Joint Capabilities Integration and Development System CJCSM 3170.01A**, Chairman of the Joint Chiefs of Staff Manual, March 12, 2004.
12. **Joint Capabilities Integration and Development System CJCSM 3170.01D**, Chairman of the Joint Chiefs of Staff Instruction, March 12, 2004.
13. **Jet Propulsion Laboratory Reliability Analyses Handbook**, JPL-D-5703, July 1990.
14. **Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program,** NASA-STD-8729.1, December 1998.
15. **Reliability and Maintainability (R&M) Assurance Guidance Part 3 R&M Case**, Ministry of Defence, Defence Standard 00-42, Issue 2, June 6, 2003.
16. **The R&M Case – A Reasoned, Auditable Argument Supporting the Contention that a System Satisfies its R&M Requirements**, Fuqua, Norman B., START 2004-2, Volume 11, Number 2, Reliability Analysis Center.
17. **Practical Reliability Engineering**, Third Edition Revised, O'Connor, Patrick D.T., John Wiley & Sons, 1998.
18. **Reliability and Maintainability (R&M) Part 4 (ARMP-4) Guidance for Writing NATO R&M Requirements Documents**, Ministry of Defence, Defence Standard 00-40, Issue 2, June 13, 2003.

Chapter 4 References

1. **Sampling Procedures and Tables for Life and Reliability Testing**, MIL-HDBK-H 108, 29 April 1960 (canceled but provides a good reference).
2. **Reliability Growth Management**, MIL-HDBK-189, 24 October 2000.
3. **Reliability Prediction of Electronic Equipment**, MIL-HDBK-217F, 28 February 1995.
4. **Reliability/Design Thermal Applications**, MIL-HDBK-251, 19 January 1978.
5. **Electrostatic Discharge Control Handbook for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)**, MIL-HDBK-263B, 31 July 1994.
6. **Electronic Reliability Design Handbook**, MIL-HDBK-338B, 1 October 1998.
7. **Environmental Stress Screening of Electronic Equipment**, MIL-HDBK-344A, 16 August 1993.
8. **Failure Rate Sampling Plans and Procedures**, MIL-STD-690C, 6 December 1999.
9. **Definitions of Terms for Reliability and Maintainability**, MIL-STD-721C, 5 December 1995 (canceled but provides a good reference).
10. **Reliability Modeling and Prediction**, MIL-STD-756B, 4 May 1998 (canceled but provides a good reference).

11. **Reliability Test Methods, Plans and Environments for Engineering Development, Qualification and Production**, MIL-HDBK-781A, 1 April 1996.
12. **Reliability Design Qualification and Procedure Acceptance Tests: Exponential/Distribution**, MIL-STD-781D, 8 October 1996 (canceled but provides a good reference).
13. **Reliability Program for Systems and Equipment, Development and Production**, MIL-STD-785B, 30 July 1998 (canceled but provides a good reference).
14. **Reliability Assurance Program for Electronic Parts Specifications**, MIL-STD-790F, 20 September 2002.
15. **Reliability Program Requirements for Space and Missile Systems**, MIL-STD-1543B, 4 May 1998 (canceled but provides a good reference).
16. **Procedures for Performing a Failure Modes, Effects, and Criticality Analysis**, MIL-STD-1629A, 4 August 1998 (canceled but provides a good reference).
17. **Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)**, MIL-STD-1686C, 25 October 1995.
18. **Failure Classification for Reliability Testing**, MIL-STD-2074, 8 August 1994 (canceled but provides a good reference).
19. **Failure Reporting, Analysis and Corrective Action System (FRACAS)**, MIL-STD-2155, 11 December 1995 (canceled but provides a good reference).
20. **Environment Stress Screening Process for Electronic Equipment**, MIL-STD-2164, 16 January 1996 (canceled but provides a good reference).
21. "Learning Curve Approach to Reliability Monitoring," Duane, James T., IEEE Transactions on Aerospace, volume 2, No. 2, 1964.
22. "Reliability Performance Today," Army Test and Evaluation Command Briefing, February 2002.
23. "Non-Operating Reliability," Carchia, Michael, Carnegie Mellon University, Spring 1999.
24. "Estimating Reliability after Corrective Action," Corcoran, Weingarten and Zehna, Management Science, volume 10, No. 4, July 1964.
25. **An Improved Methodology for Reliability Growth Projections**, AMSAA TR-357, Crow, Larry, June 1982.
26. **AMSAA Reliability Growth Guide**, AMSAA TR-652, Broemm, William J. and Ellner, Paul M. and Woodworth J., September 2000.
27. **Goodness-of-Fit Techniques**, D'Agostino, Ralph B. and Stephens, Michael A., Marcel Dekker, Inc., 1986.
28. **AMSAA Reliability Growth Data Study**, Interim Note R-184, Ellner, P. and Trapnell, B., January 1990.

29. "A Taxonomy of Reliability Growth Models," Logistics Spectrum, Jung, Won, Wasserman, Gary S. and Lamberson, Leonard R., Spring 1990.

30. "The Applicability of Markov Analysis Methods to Reliability, Maintainability, and Safety," Selected Topics in Assurance Related Technologies, Fuqua, Norman, Volume 10, No. 2, Reliability Analysis Center, 2003.

31. **Application of Markov Techniques**, IEC 61165, International Electrotechnical Commission, 1995.

32. **Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems**, IEC 61508, International Electrotechnical Commission, 2004.

33. **Reliability Toolkit: Commercial Practices Edition**, Dudley, Bruce et al. al., Reliability Analysis Center, Rome, NY, 1994.

34. **Practical Reliability Engineering**, Third Edition Revised, O'Connor, Patrick D.T., John Wiley & Sons, 1998.

35. **Reliability: Management, Methods, and Mathematics**, Lloyd, David K. and Lipow, Myron, American Society for Quality Control, 1984.

36. **Repairable Systems Reliability**, Ascher, Harold and Feingold, Harry, Marcel Dekker, Inc., 1984.

37. **Recurrent Events Data Analysis for Product Repairs, Disease Recurrences, and Other Applications**, Nelson, Wayne B., Society for Industrial and Applied Mathematics, 2003.

38. **Evaluating the Reliability of Commercial Off-the-Shelf (COTS) Items**, Criscimagna, Ned H., Reliability Analysis Center, August 1999.

39. "A Comparative Analysis of Reliability Prediction Techniques," McGowen, Douglas J., Army Material Command in Texarkana, TX, April 1975.

40. **Failure Modes, Effects and Criticality Analysis (FMECA)**, Rossi, Michael, Reliability Analysis Center, April 1993.

41. **Statistical Problem Solving in Quality Engineering**, Kazmiersi, Thomas J., McGraw-Hill, 1995.

42. "Sparing Analysis – A Multi-Use Planning Tool," Myrick, Al, Annual Reliability and Maintainability Symposium Proceedings, 1989.

43. **Accelerated Life Testing Reference**, ReliaSoft Publishing, 2001.

44. **Built-in-Test Design and Optimization Guidelines**, Office of the Assistant Secretary of the Navy (RDA), TB# ABM1001-01, October 2001.

45. **Maintainability Toolkit**, Criscimagna, Ned H., Reliability Analysis Center, 2000.

46. "Guided Missile Frigate Tiger Assessment," Lohmar, John W. and Mandel, David B., Annual Reliability and Maintainability Symposium Proceedings, 1981.

47. "ACIM: Availability Centered Inventory Model," Hall, Fred and Clark, Andy, Annual Reliability and Maintainability Symposium Proceedings, 1987.

48. "Analysis of "One-Shot" Devices," Selected Topics in Assurance Related Technologies, Sherwin, Edward, Volume 7, No. 4, Reliability Analysis Center, 2000.
49. "Censored Data," Selected Topics in Assurance Related Technologies, Romeu, Jorge, Volume 11, No. 3, Reliability Analysis Center, 2004.
50. "Environmental Stress Screening," Selected Topics in Assurance Related Technologies, Farrell, Jack, Volume 7, No. 3, Reliability Analysis Center, 2000.
51. "What HALT and HASS Can Do For Your Products," Hobbs, Gregg K., Evaluation Engineering, November 1997.
52. "Processes Which Will Greatly Improve Your Product Quality & Customer Satisfaction," McLean, Harry, 7th Annual SAE International RMS Workshop, 1995.

Chapter 5 References

1. **Reliability Toolkit: Commercial Practices Edition**, Dudley, Bruce et al. al., Reliability Analysis Center, Rome, NY, 1994.
2. **Practical Reliability Engineering**, Third Edition Revised, O'Connor, Patrick D.T., John Wiley & Sons, 1998.
3. **Maintainability Toolkit**, Criscimagna, Ned H., Reliability Analysis Center, 2000.
4. "Environmental Stress Screening," Selected Topics in Assurance Related Technologies, Farrell, Jack, Volume 7, No. 3, Reliability Analysis Center, 2000.
5. "What HALT and HASS Can Do For Your Products," Hobbs, Gregg K., Evaluation Engineering, November 1997.
6. "Processes Which Will Greatly Improve Your Product Quality & Customer Satisfaction," McLean, Harry, 7th Annual SAE International RMS Workshop, 1995.
7. **Production Reliability Assurance Tests (PRAT)**, R&M-STD-R0030, Sadlon, R.J., US Navy/Naval Avionics Center, 1988.
8. **Reliability Growth Management**, MIL-HDBK-189, 13 February 1981.
9. **R&M-STD-R0030 Production Reliability Assurance Tests (PRAT)** from Naval Avionics Center (NAC).
10. **Reliability Engineering for Electronic Design**, Fuqua, Norman B., Chapter 12, Marcel Decker, 1987.
11. **Reliability Design Qualification and Production Acceptance Tests: Exponential Distribution**, MIL-STD-781D, Cancelled 1996 (but still useful reference).
12. **Reliability Test Methods, Plans, and Environments for Engineering Development, Qualification, and Production**, MIL-HDBK-781, 1987.

Chapter 6 References

1. **Reliability Toolkit: Commercial Practices Edition**, Dudley, Bruce et al. al., Reliability Analysis Center, Rome, NY, 1994.
2. **Practical Reliability Engineering**, Third Edition Revised, O'Connor, Patrick D.T., John Wiley & Sons, 1998.
3. **Maintainability Toolkit**, Criscimagna, Ned H., Reliability Analysis Center, 2000.
4. **Failures Modes, Effects, and Criticality Analysis**, RAC, 1993.
5. **Methods for Statistical Analysis of Reliability and Life Data**, Mann, N., R. Schafer and N. Singpurwalla, John Wiley, NY 1974.
6. **Procedures for Performing a Failure Mode, Effects and Criticality Analysis**, MIL-STD-1629 (canceled, but still useful reference).
7. **RCM II**, Moubray, Industrial Press, 1992.
8. **Reliability and Life Testing Handbook, Volumes 1 and 2**, D. Kececioglu, Prentice Hall, NJ, 1993.
9. **Reliability Centered Maintenance**, A. Smith, McGraw-Hill, 1993.
10. **Reliability Growth Management**, MIL-HDBK-189, 13 February 1981.

Appendix A References

1. **Defense Federal Acquisition Regulation Supplement (DFARS)**, Office of the Undersecretary of Defense, Washington, DC.
2. **Reliability Toolkit: Commercial Practices Edition**, Dudley, Bruce et al. al., Reliability Analysis Center, Rome, NY, 1994.
3. **Electronic Reliability Design Handbook**, MIL-HDBK-338B, 1 October 1998.

Appendix B References

1. **Defense Acquisition Guidebook Version 1.00** (formerly Interim Defense Acquisition Guidebook dated October 30, 2002 and DoD 5000.2-R, dated April 5, 2002), Office of the Undersecretary of Defense, Washington, DC, November 17, 2004.
2. Stronger Management Practices Are Needed to Improve DoD's Software-Intensive Weapon Acquisitions, GAO-04-353. March 2004.
3. Innovations in Software Engineering for Defense Systems, National Academy of Sciences, http://www.nap.edu/books/0309089832/html/
4. DoD Logistics 203 Course, Software Reliability and Maintainability Module
5. Statistics Testing and Defense Acquisition: New Approaches and Methodological Improvements, Cohen, Michael L., John E. Rolph, and Duane L Steffey, Ed. National Academy Press, 1998. Chapter 8 Testing Software-Intensive Systems.
6. Electronic Reliability Design Handbook, Chapter 9
7. Meeker, William Q and Luis A. Escobar, Statistical Methods for Reliability Data, John Wiley and Sons, 1998.

8. Software Program Managers Network, The Condensed Guide to Software Acquisition Best Practices, June 1998. http://www.spmn.com
    a. Little Book of Testing Volume I Overview and Best Practices, June 1998.
    b. Little Book of Testing Volume II Implementation Techniques, June 1998.

Appendix C References

1. **Reliability Growth Management**, MIL-HDBK-189, 13 February 1981.
2. "Learning Curve Approach to Reliability Monitoring," Duane, James T., IEEE Transactions on Aerospace, volume 2, No. 2, 1964.
3. "Reliability Performance Today," Army Test and Evaluation Command Briefing, February 2002.
4. "Estimating Reliability after Corrective Action," Corcoran, Weingarten and Zehna, Management Science, volume 10, No. 4, July 1964.
5. **An Improved Methodology for Reliability Growth Projections**, AMSAA TR-357, Crow, Larry, June 1982.
6. **AMSAA Reliability Growth Guide**, AMSAA TR-652, Broemm, William J. and Ellner, Paul M. and Woodworth J., September 2000.
7. **Goodness-of-Fit Techniques**, D'Agostino, Ralph B. and Stephens, Michael A., Marcel Dekker, Inc., 1986.
8. "Reliability Analysis for Complex, Repairable Systems, in Reliability and Biometry," Crow, Larry H., Society for Industrial and Applied Mathematics, 1974.
9. **Reliability Growth-Statistical Test and Estimation Methods**, IEC International Standard 61164, International Electrotechnical Commission, 1995.
10. "Reliability Growth Projection from Delayed Fixes," Crow, Larry H., Annual Reliability and Maintainability Symposium Proceedings, 1983.
11. "On Tracking Reliability Growth," Crow, Larry H., Annual Reliability and Maintainability Symposium Proceedings, 1975.
12. "An Extended Reliability Growth Model for Managing and Assessing Corrective Actions," Crow, Larry H., Annual Reliability and Maintainability Symposium Proceedings, 2004.
13. "AMSAA Discrete Reliability Growth Model**,"** Crow, Larry H., Methodology Office Note 1-83, US Army Materiel Systems Analysis Activity, Aberdeen Proving Ground, MD, March 1983.
14. "On the Initial System Reliability," Crow, Larry H., Annual Reliability and Maintainability Symposium Proceedings, 1986.
15. **The AMSAA Maturity Projection Model based on Stein Estimation**, Ellner, Paul M. and Hall, J. Brian, AMSAA TR-751, July 2004.
16. "Estimation of the Mean of a Multivariate Normal Distribution," **The Annals of Statistics**, Stein, Charles M., Vol. 9, pp 1113-1151, 1981.
17. "AMSAA Maturity Projection Model Based on Stein Estimation," Ellner, Paul M. and Hall, J. Brian, Annual Reliability and Maintainability Symposium Proceedings, 2005.

Appendix D References

1. **Reliability Toolkit: Commercial Practices Edition**, Dudley, Bruce et al. al., Reliability Analysis Center, Rome, NY, 1994.
2. "Reliability Analysis for Complex Repairable Systems," Crow, Larry, Society for Industrial and Applied Mathematics, 1974.