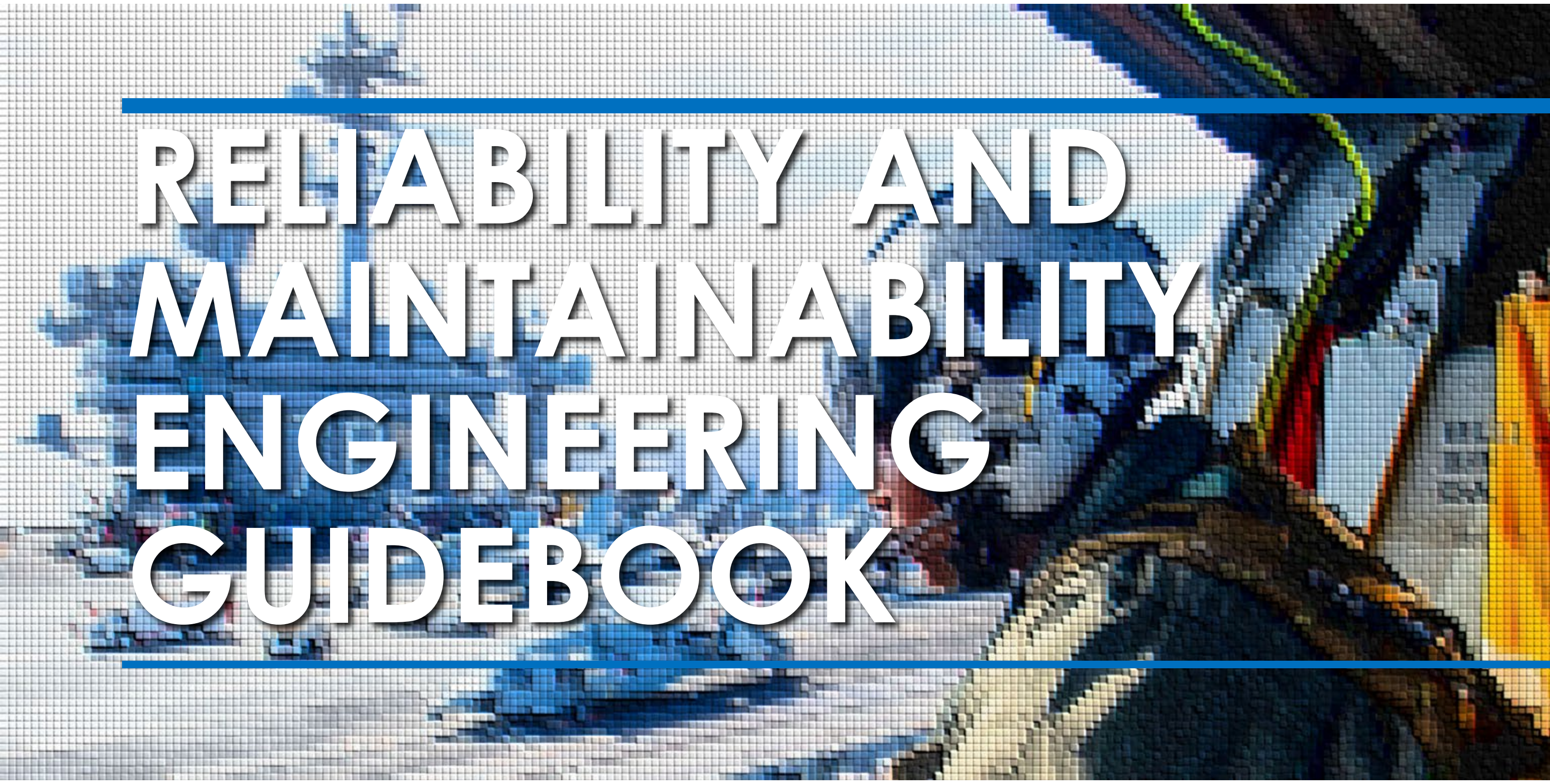
SECRETARY OF THE NAVY



RELIABILITY AND MAINTAINABILITY ENGINEERING GUIDEBOOK

JUNE 2022

Jennifer Glenn | DASN(RDT&E)
Paul Dube | NAVSEA
Karen Bain | NAVAIR
David Brooks | NAVWAR
James Howell | MCSC

This page intentionally left blank.

SECRETARY OF THE NAVY

RELIABILITY AND MAINTAINABILITY ENGINEERING GUIDEBOOK

JUNE 2022

Jennifer Glenn | DASN(RDT&E)
Paul Dube | NAVSEA
Karen Bain | NAVAIR
David Brooks | NAVWAR
James Howell | MCSC

NOTES TO THE PROGRAM MANAGERS

The Assistant Secretary of the Navy for Research, Development and Acquisition (ASN(RDA)) considers Reliability and Maintainability Engineering (R&ME) a Naval priority. In addition to ensuring readiness, the Government Accountability Office (GAO) reported that Operational and Support (O&S) costs are driven by the system's R&M qualities and account for approximately 80% of a system's Life Cycle Cost (LCC). Rigorous R&ME activities provide increased awareness of reliability problems early, and can avoid prohibitive sustainment costs to the Navy.

Early and upfront consideration and integration of R&ME by design is the only path to success. It cannot be added in at the end. Throughout the Government, its field activities, and contractors, there are reliability engineers. Seek them out and insert them into the process early and often throughout the acquisition process.

Familiarize yourself with this guidebook and properly appreciate and implement R&ME, especially the Design Phase essentials.

- Treat R&M as performance parameters from day one.
- Recognize that R&M performance drives O&S cost, LCC, and maintenance burden.
- R&ME by design delivers more results, more efficiently than later reliability growth efforts.

To align with best practices of successful commercial companies in R&ME, Program Managers must:

1. Leverage reliability engineers early and often throughout acquisition.
    a. Employ a Government lead R&ME systems engineer to work under the program's Chief Engineer or Lead Systems Engineer who has the knowledge, skills, and abilities to prepare an adequate approach for R&ME activities which includes and is fully integrated with design, test and evaluation, and sustainment.
2. Emphasize reliability with their suppliers.
    a. The PM must include in the contract and in the process for source selection, clearly defined and measurable R&M requirements and engineering activities as required by Section 2443 of Title 10, United States Code (U.S.C.) [Ref 2]. The PMs of major defense acquisition programs (MDAPs) and Major Systems must provide justification in the acquisition strategy for not including R&M requirements and other engineering activities in Technology Maturation and Risk Reduction (TMRR), Engineering and Manufacturing Development (EMD), or production solicitations or contracts.

3. Employ reliability engineering activities to improve a system's design throughout development.
    a. Including a small subset as follows: reliability predictions, physics of failure, failure mode and effects and criticality analysis (FMECA), fault tree analysis (FTA), design of experiments (DOEs), Failure Reporting, Analysis, and Corrective Action System (FRACAS), failure definitions and scoring criteria (FD/SC), accelerated life testing, and reliability growth curves (RGCs).
    b. Ensure R&ME activities are fully integrated with systems engineering, test & evaluation, product support, safety, configuration management, manufacturing, quality, and autonomy.

This guidebook is structured to provide life cycle information on how to conduct an R&ME program. A balance among capability, availability, reliability, and maintainability provides systems to the warfighter at the most optimized O&S cost to ensure our Fleet's readiness to support its mission and promote national security. More information on these activities can be found later in this guidebook. All Navy and Marine Corps acquisition and sustainment programs should implement this guidebook.

Key References:

GAO report, "Defense Acquisitions: Senior Leaders Should Emphasize Key Practices to Improve Weapon System Reliability" (GAO-20-151) [Ref 1].

Section 2443 of Title 10, United States Code (U.S.C.) [Ref 2].

GAO report, "Navy Shipbuilding: Increasing Focus on Sustainment Early in the Acquisition Process Could Save Billions" (GAO-20-2) [Ref 3].

Secretary of the Navy Instruction (SECNAVINST) 5000.2 [Ref 4].

EXECUTIVE SUMMARY

This guidebook discusses a wide range of Reliability and Maintainability Engineering (R&ME) roles, tasks, and opportunities in support of the Secretary of the Navy Instruction (SECNAVINST) 5000.2 series. Initially, the R&ME role was to validate requirements (ensure they are based in physics), translate user requirements (i.e., Sustainment Key Performance Parameters (KPPs), Key System Attributes (KSAs) through analysis, block diagrams, modeling, and predictions into well-defined contractual requirements. R&ME tasks and opportunities will evolve, as part of the systems engineering and logistics team, to include supporting analysis of alternatives, Failure Reporting, Analysis, and Corrective Action System (FRACAS)-based measurement, assessment, and improvement of system attributes. Reliability demonstration testing can be time consuming and resource intensive and needs to be planned from the outset of the program.

Fortunately, the guidebook's framework provides a synergistic opportunity for R&ME to identify and avoid a range of known R&ME issues. Related issues are discussed to give R&ME a proactive ability to avoid, rather than repeat and fix, experience-based issues. Today system's effectiveness requires the system to be reliable, dependable, and capable. This means reliability needs to be understood as a performance parameter and hence a design criteria starting with our Science and Technology (S&T) investments and progressing throughout a program's life. While reliability growth will play an important role in the program, a focus up front needs to be on deterministic design criteria. This document is laid out in eight chapters with four enclosures described below:

- **Chapter 1** provides background and importance for this handbook.
- **Chapter 2** contains general information about reliability and maintainability.
- **Chapter 3** discusses reliability and maintainability in the acquisition process.
- **Chapter 4** discusses requirements development and management to include understanding user needs and translating them into actionable requirements, and also the key role of the Operational Mode Summary / Mission Profile (OMS/MP).
- **Chapter 5** discusses JCIDS warfighter requirements and their relationship to achieving reliable systems.
- **Chapter 6** provides considerations on the relationship between software and system reliability.
- **Chapter 7** previews a DON R&ME checklist/scorecard currently under development which will help assess R&ME program health.
- **Appendix A** provides a list of references and resource documents.
- **Appendix B** provides a glossary of R&ME terms and acronym definitions.

R&ME includes identifying, analyzing, and affecting design to improve life cycle performance. The range of effort includes requirements analysis and allocation, developing appropriate contract language, Fault Tree Analyses (FTAs), Failure Modes and Effects Criticality Analysis (FMECA), parts selection, stress analysis, de-rating, physics of failure analysis, Test and Evaluation (T&E), parts selection, and FRACAS to realistically achieve desired fielded system R&M attributes. Recognize that piece-part predictions can provide for a sound relative assessment across differing contractor designs; however, they cannot be expected to accurately depict field performance. It is the engineering design features that will control or enable achievement of reliable, sustainable, and affordable capabilities.

All of this can be summed up in a simple statement: **Reliability and maintainability are operational capabilities and, hence design criteria.**

R&ME focuses the contractor on design-controllable elements. These include system reliability, system architecture (including redundancy), and system maintainability through *design for reliability* and *design for maintainability* activities. (Note: Neither *Operational Availability* (A_o) nor *Mean Logistics Delay Time* are design controllable values).

TABLE OF CONTENTS

FIGURES AND TABLES

1 | BACKGROUND AND IMPORTANCE

In the 70s through early 90s, the Department of Defense (DOD) saw significant improvement in weapon system Reliability and Availability. This focus was lost during the 90s and institutional knowledge/expertise were further lost in acquisition reform resulting in a decrease in system Reliability, Maintainability, and Availability. **Figure 1** traces the relative health of the Navy reliability program beginning in 1963 and projecting into the future, with **Table 1** providing a more detailed description of the events that led to these fluctuations.

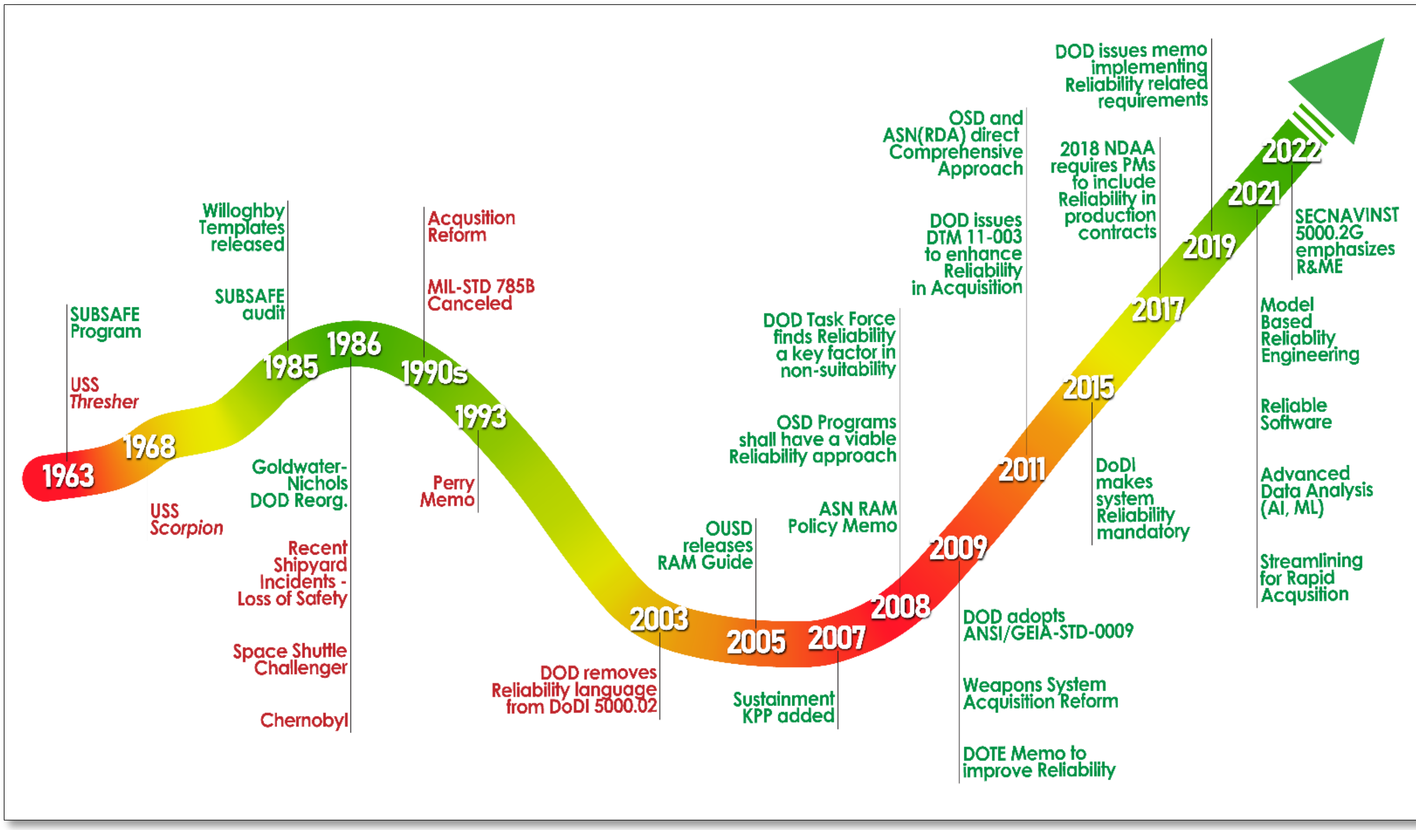


Figure 1: DOD Reliability Health

Table 1: Selected Laws and DOD Reliability-related efforts over time

1963	▪ USS *Thresher* nuclear submarine crew and vessel lost in deep dive ▪ Submarine Safety Program (SUBSAFE) started
1968	▪ USS *Scorpion* nuclear submarine crew and vessel lost
1985	▪ Willoughby Templates released ▪ SUBSAFE Audit
1986	▪ Change of Authority (Goldwater-Nichols, DOD Reorganization) Redirect PEOs ▪ Recent Shipyard Incidents Loss of Safety ▪ Space Shuttle Challenger mishap ▪ Chernobyl mishap
1990s	▪ Congress passes various acquisition reforms in the National Defense Authorization Act (NDAA) for fiscal years 1996-99 ▪ DOD cancels Military Standard 785B for reliability and reduces total number of reliability test and evaluation personnel
1993	▪ Perry Memo removes comprehensive approach and replaces with best commercial practices
2003	▪ DOD removes reliability language from DOD Instruction (DoDI) 5000.02
2005	▪ Office of the Secretary of Defense Reliability, Availability, and Maintainability guide is released
2007	▪ DOD adds sustainment Key Performance Parameters (KPPs), containing the reliability Key System Attributes (KSAs), to the Joint Capability Integration and Development System (JCIDS) process
2008	▪ Defense Science Board Task Force issues a report assessing the causal factors for DOD programs previously evaluated as not operationally suitable. Task Force finds poor reliability to be a key factor. ▪ OSD programs are directed to have a viable RAM strategy that includes a reliability growth program as an integral part of design and development ▪ ASN Memo on Reliability, Availability and Maintainability (RAM) policy
2009	▪ DOD adopts American National Standards Institute/Government Electronics and Information Technology Association standards (ANSI/GEIA-STD 0009) ▪ Congress passes the Weapons System Acquisition Reform Act to improve organization and procedures of DOD for the acquisition of major weapons systems. The act included provisions related to key requirements, including reliability requirements, for major acquisition programs. ▪ Director, Operational Test and Evaluation issues memorandum outlining steps to improve system reliability

2011	▪ DOD issues Directive-Type Memorandum 11-003 to enhance reliability in the acquisition process ▪ New Approach: OSD and ASN(RDA) direct that programs shall have a comprehensive approach, which includes MIL-STDs 470, 781, 785, and 1629
2015	▪ Update to DoDI 5000.02 to make systems reliability mandatory in planning stages for DOD weapons systems
2017	▪ Congress passes NDAA for fiscal year 2018 requiring program managers to include certain reliability requirements in weapons system engineering and manufacturing development, as well as production contracts
2019	▪ DOD issues memorandum implementing NDAA for fiscal year 2018 reliability-related requirements for development and production contracts
2021	▪ The DOD digital transformation expected to increase reach and effectiveness of reliability and maintainability engineering using model-based approaches, advanced data analytics, and stronger focus on reliable software
2022	▪ SECNAVINST 5000.2G updated to include more emphasis on R&ME to address concerns from the GAO 20-151 report

The Government Accountability Office (GAO) reported numerous DOD reliability problems, most recently in its study entitled “Defense Acquisitions: Senior Leaders Should Emphasize Key Practices to Improve Weapon System Reliability” (GAO 20-151) [Ref 1]. The DON suffers for this lack of emphasis on reliability and maintainability engineering during the operation and sustainment phases of the life cycle. A separate GAO report (GAO-20-2) [Ref 3] found that over the past 10 years Navy ships have required more effort to sustain than planned, in part because the sustainment requirements do not provide key information on how reliable and maintainable mission–critical systems should be. DOD guidance advises acquisition programs to plan for and design reliability and maintainability into the weapon system early in the acquisition effort.

THE FUTURE OF R&M ENGINEERING

The Under Secretary of Defense for Research and Engineering's (USD (R&E)) Reliability and Maintainability Engineering Working Group has established a collaboration space for Government, industry, and academia to come together to discuss and shape the R&ME landscape. This group, named the DOD R&ME Roundtable, meets at least twice annually to discuss R&ME issues and identify opportunities to advance the reach and benefit of the domain. Engineering is currently undergoing a quantum shift as the DOD adopts a Digital Engineering posture per the "DOD Digital Engineering Strategy" [Ref 5] and the DON adopts its Digital Engineering posture per the "U.S. Navy and Marine Corps Digital Systems Engineering Transformation Strategy" [Ref 6]. In response to this DOD strategy, the DOD R&ME Roundtable has established the following focus areas with each representing a key intersection point between R&ME and Digital Engineering.

Implement Digital Engineering into Reliability and Maintainability

Develops guidance for implementing a digital engineering ecosystem that uses model-based techniques to conduct R&M engineering activities that allow the collaboration needed to efficiently and cost-effectively improve design, sustainment, and mission effectiveness.

Goals of this effort include:

- Educate and train R&M engineers on the application of Model Based Engineering (MBE)
- Move from current static analysis to dynamic analysis and leverage interfaces to authoritative 3D engineering models (sources of truth) for components and systems
- Allow efficient and continuous engagement of R&M engineers with designers to increase design influence
- Decrease design cycle times
- Apply MBE to R&M models to best support weapon systems during the Operations and Support phase

Deliverables from this effort include:

- R&M MBE Use Cases (e.g., how engineering models are used in R&M engineering analyses)
- Pilot opportunities in MBE
- Guidance with lessons learned and best practices

- Guidance on model and data exchange between R&M engineering and other engineering models (data centricity)

Deliver Reliable Software

Develops R&ME guidance (and associated contract language) for defining, estimating, analyzing, testing, or verifying expected occurrences of software failures (that would occur) in an operational (field) environment.

Goals of this effort include:

- Define acceptable metrics to measure to and evaluate (define how software related failures impact current R&M system metrics and establish guidance for failure definition and scoring criteria (FD/SC) development)
- Effectively implement R&M into software development programs by emphasizing the use of DevSecOps as a key for reliable software. This includes development and also methods of gathering operational software performance metrics to identify, characterize, and address or correct software failures through continuous integration/continuous delivery (CI/CD) updates.
- Enhance programs' ability to contract for reliable software and effectively evaluate the risks of contractor's proposal to achieve reliable software
- Differentiate roles and responsibilities for reliability, software, security, and operations
- Explore the concept of architecting software using design patterns that incorporate reliability concepts to build software that is more failure resistant and fault tolerant
- Reduce the occurrence or impact of software failures during operation

Deliverables from this effort include:

- Contract language and guidance on implementation (including tailoring) for delivering reliable software
- Guidance for specifying, developing, and assessing reliable software
- Guidance for evaluating proposals for reliable software
- Standard R&M engineering guidance for Software failure definition, prediction, testing, and modeling

Reliability Estimates versus Observed Performance

Develops guidance that explains why there is a difference between reliability estimates and the observed values, what is impacted, and how the estimates should be interpreted and correctly applied throughout the life cycle. A second objective is to provide guidance on understanding the risks associated with various reliability prediction methods and if incorrect reliability values are used in operations and support (O&S) cost estimates.

Goals of this effort include:

- Educate and train R&M engineers on understanding the difference between predicted and observed reliability values during Developmental Test and Evaluation (DT&E), Operational Test and Evaluation (OT&E), and fielding
- Assess the adequacy of the feasibility (use of legacy and similar system field data) and trade-off (O&S cost versus R&M) sections of the RAM-C Outline Training, and update if needed
- Develop a blended approach that uses the best available data to predict reliability while also identifying failure modes needing elimination or mitigation during the design phase
- Explore modern data analysis techniques incorporating machine learning (ML) and artificial intelligence (AI)
- Implement life cycle Reliability Block Diagrams (RBDs)

Deliverables from this effort include:

- Use-Cases to identify the purpose, collection method (includes cleansing the data), and analysis of R&M data in each life cycle phase
- Training briefing with supplemental white papers (includes ensuring common metrics and requirements across (throughout) the life cycle)
- Assessment of the RAM-C Outline Training and update if needed
- Guidance using field data as a method to develop original (early upfront) reliability estimates
- Contract language and guidance for maintaining life cycle RBDs

DESIGN FACTORS VERSUS SUPPORT FACTORS

Generally speaking, programs endeavor to develop systems that are: Reliable (fail less), Available (mission ready), Maintainable (easier to repair), and Affordable (less costly to operate). However, the interplay between these factors is often misunderstood. Reliability and maintainability are design-controllable factors which means they are established in the design process. Once a system has been designed the only way to make a system more reliable or maintainable (given the same operating environment) is by changing the design. Maintenance and spare parts are product support factors that, when paired with a design (and all other product support factors), establish the system's availability to perform the mission. Product Support Analysis is not part of R&ME; however, Product Support Analyses establish product support strategies (such as parts sparing) and are greatly dependent on the system's R&M factors.

From a program perspective, R&ME should be considered an effort to expose hidden risks. Each R&ME analysis furthers the understanding of technical risk and enriches the program's understanding of the technical issues that must be addressed to meet the warfighter's needs. The reliability and maintainability of a system are established during the design process, either actively or passively.

- A passive R&ME approach allows designs to take form that may or may not be sufficient to meet R&ME requirements during testing. Passive approaches often culminate in systems not meeting requirements during late developmental tests or operational tests. Unfortunately, by this point in development, only extreme cost and schedule mitigation actions can improve the R&ME factors in the design. The standard and undesired (but expected) strategy at this point is to implement product support mitigations such as increasing spare parts, developing special tools, increasing manpower, developing special training, increasing maintenance periodicity, etc. Or worse, the program may simply find relief by relaxing the R&ME requirement to the level achieved during testing.
- Actively addressing R&M is accomplished by evaluating the system using specialized R&ME analyses. Each R&ME analysis forms a vignette of the overall picture of the system's ability to achieve its mission in an operational environment at a specific operational tempo. These analyses each build on the next and inform subsequent R&ME and product support analyses. This iterative approach is the basis for establishing a comprehensive R&M program tailored to the appropriate size and complexity that will achieve the system requirements needed for mission readiness.

Design analyses implemented in accordance with approved R&ME program plans ensure system designs are capable of acceptable R&M performance. The Government must actively monitor the activities during in-process reviews and at established formal systems engineering design reviews. Results of these activities are also used as a basis for review of R&ME requirements in specifications and drawings and system support factors.

An effective reliability program consists of engineering activities including: R&ME allocations, block diagrams and predictions; failure definitions and scoring criteria; failure mode, effects and criticality analysis; maintainability and built-in test demonstrations; reliability growth testing at the system and subsystem level; and a failure reporting and corrective action system maintained through design, development, production, and sustainment.

Product Support Strategy Impact to Operational Availability

While the acquisition process requires the development of system maintenance strategies in support of the required Operational Availability (A_o) associated with the Sustainment Key Performance Parameter, it is the engineering design features that will control or enable achievement of a reliable, sustainable, mission ready, and affordable capability. Reliability can significantly influence a weapon system's operating and support costs, which we have previously reported account for approximately 70 percent of a weapon system's total life-cycle cost (see **Figure 2**). DOD has previously reported that deficiencies in DOD weapon systems—such as high failure rates and an inability to make significant improvements in reliability—have historically limited program performance and increased operating and support costs.[1] A system's reliability and maintainability are major determinants of its life cycle cost. Increased R&M can significantly reduce the O&S costs of sustaining the system over its life in the field.

Figure 2: Acquisition Costs vs. O&S Costs

[1] GAO 20-151, "Defense Acquisitions: Senior Leaders Should Emphasize Key Practices to Improve Weapon System Reliability," Report to the Committee on Armed Services, U.S. Senate, January 2020. [Ref 1]

Consequently, early action is key, as indicated in the JCIDS, with a directed focus on R&ME to improve readiness of future Joint Forces.

Close coordination between engineering and product support during the design phase will maximize system Reliability and Maintainability. The Systems Engineering Plan (SEP) needs to ensure the product support strategy is executable through a disciplined approach to ensure that R&ME metrics are achievable. The product support strategy relies on the design teams' approach to meeting R&ME metrics to be successful. Therefore, the product support activities must align with and support the design if the system is to achieve its full reliability and maintainability potential during operation. Sustainment planning relies on R&ME data and system design information to fully address the support planning elements. However, benefits of coordinating the efforts of engineering and product support are not limited to increased product support capability. The engineering effort also benefits from close coordination by having a more complete understanding of how the system will be supported. Having a better understanding of the support approach and its limitations during the design process provides an opportunity to apply engineering solutions to address supportability issues. The opportunity to address these supportability issues during design is easily overlooked because engineering efforts are focused on achieving the technical requirements derived from the Capability Development Document (CDD). It is vital that design engineers understand the product support strategy and how their design choices will impact the future maintenance burden of the system. The need for maintenance is the prime driver of the logistics footprint and has a substantial impact on A_o.

A_o represents the percentage of time the system is operationally mission ready. A_o is driven by the reliability and maintainability of the system, combined with its product support structure. Achieving the required levels of A_o is a matter of establishing the logistics elements needed to address the R&M factors of the system. The logistics footprint is the overall size, complexity, and cost of the logistics solution that is needed to achieve the required A_o given the system's reliability and maintainability. A smaller logistics footprint is most favorable and can best be achieved when engineers make design decisions that reduces this footprint.

HOW DO COMPANIES DO R&ME WELL?

The GAO researched how companies do R&ME well and reported their findings in GAO-20-151 [Ref 1]. The GAO found that in the commercial sector, companies proactively address reliability from the beginning of the development process. In these companies, engineers strive to identify reliability issues at the component and sub-system level early in the development process to avoid expensive rework after producing an entire system. They identified the following key practices in the commercial sector:

- Leveraging reliability engineers early and often
- Establishing realistic reliability requirements—for example, not expecting a product to operate twice as long as its predecessor before failing
- Emphasizing reliability with their suppliers
- Employing reliability engineering activities to improve a system's design throughout development

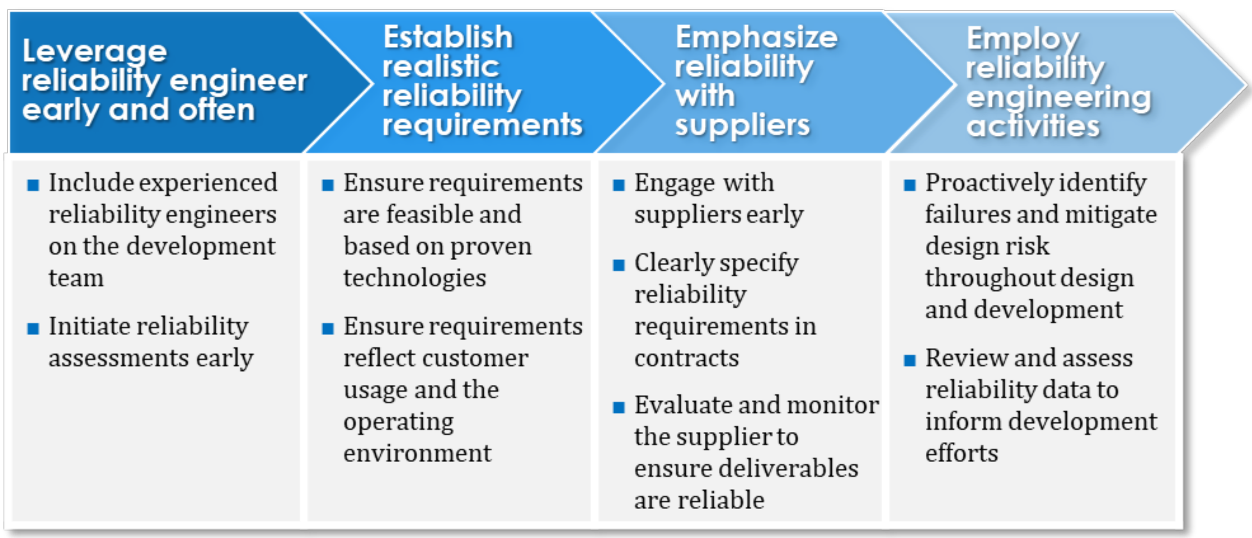


Figure 3: Reliability Engineering Activities Associated with Key Reliability Practices

Leverage Reliability Engineers Early and Often

Commercial companies include experienced reliability engineers as part of their development teams. These reliability engineers implement reliability tools and methods that integrate statistics, physics, and engineering principles to help develop a reliable product. Companies that do R&ME well understand the importance of initiating assessments early in the development life cycle when there is the greatest opportunity to influence product design.

Commercial companies understand that reliability engineering activities can add value to decision-making by providing direction and feedback that helps development teams refine designs that lead to more reliable and cost-effective systems. They believe reliability engineers should be empowered to influence decisions, such as delaying overall project schedules or negotiating for more resources when necessary. In addition, management should provide sufficient resources and time dedicated specifically to improving reliability by discovering failures, implementing corrective actions, and verifying their effectiveness on outcomes. They understand that cost and schedule constraints can negatively influence reliability testing, which can limit development teams' ability to discover potential failures and improve designs through corrective actions.

These companies rely on developing experienced reliability engineers. Some of the top companies have a dedicated reliability engineering community that coaches members of the company's various product development teams. They focus on teaching development team members to ask the right questions at the right point in time with the right people in the room.

Establish Realistic Reliability Requirements Based on Proven Technology

Companies with the most reliable products emphasize that reliability requirements should be realistic, be based on proven technologies, and reflect customer usage in the operating environment. To determine feasibility of meeting a requirement, their reliability engineers recommend conducting comparative analysis with historical data and assessing risk due to new, unique, or challenging technology. Reliability Engineers in these companies seek justifications from programs for how reliability requirements were established to demonstrate they are within the realm of technological possibility.

If the reliability requirements are not technically feasible, it could have broad implications for the intended mission, life cycle costs, and other aspects of the system. These companies understand the importance of making informed trade-offs when considering requirements to reduce program risk or total ownership costs. Making trade-offs involving capability, reliability, and cost requirements requires having the right people involved in these trade-off decisions, and that they work with user representatives and reliability engineers to define their systems' reliability requirements.

Emphasize Reliability with Suppliers

Systems produced by commercial companies include parts or components produced by suppliers, and the reliability of those parts or components directly impacts the reliability of the overall system. Companies understand that vendor quality can affect a part's reliability, so it is critical that the reliability of vendors' parts be evaluated before being approved for use. Commercial companies engage with suppliers early, clearly specifying all requirements, while also evaluating and monitoring the supplier.

Engaging the supplier early in the process, often during concept development, and asking the supplier to demonstrate that it can meet the requirements is critical. This ensures that the supplier can meet quality standards and there is enough lead time and testing of components. Engineers at commercial companies work directly with the supplier and hold them responsible for meeting reliability requirements. This includes visiting their suppliers' testing facilities and evaluating their testing programs, focusing specifically on their failure analysis and reliability activities. Leading commercial companies use disciplined quality management practices to hold suppliers accountable for high quality parts through activities such as regular supplier audits and performance evaluations.

Successful companies understand that relying on an external supplier's quality assurances can be insufficient. Often, the product manager recommends in-house testing for critical components rather than relying on a supplier's testing that may not simulate real-world operating conditions. In-house testing is recommended to avoid discovering a failure after the product is brought to market. Post-sale failures result in dissatisfied customers, reputation damage, warranty claims and similar issues. In some cases, companies establish dedicated test facilities for vital, outsourced components provided by suppliers.

Employ Reliability Engineering Activities to Improve a System's Design Throughout Development

Companies often use reliability engineering activities such as a Failure Modes Effects and Criticality Analysis (FMECA) to identify potential product failures and their causes. They also use these activities to improve a system's design early and often throughout development to avoid surprises that lead to expensive rework or excessive repairs after integrating components and subsystems. Failures should be identified early, and that identification should be viewed as an opportunity to improve the design. The earlier changes are made to designs, the less costly they are to the program. It is expensive, time consuming, and risky to make changes late in development, as late changes jeopardize product reliability.

Successful companies understand the need to conduct reliability engineering activities iteratively until the design is optimized. They also avoid the common mistake of establishing a reliability plan but not actively utilizing it throughout development.

Reliability engineers use various reliability engineering activities described in this guidebook to increase system reliability, and generally refer to these activities as design for reliability tools. These tools can be tailored to meet the specific needs of a particular development project and can complement one another as well as increase reliability prior to any testing. These tools can help identify how long a part or component will work properly, how a part or component's failure will affect a system, and what actions are needed to correct failures.

2 | GENERAL

This document is intended to complement SECNAVINST 5000.2 [Ref 4] by providing guidance on the use of technical measures to produce Naval systems with desired Reliability and Maintainability characteristics that support both the warfighter mission at the cost the DON needs to maintain a fighting force into the future. It implements Naval policy detailing the need to address reliability as a performance parameter and, hence, design criteria. It provides a synopsis and timeline to implement a successful and effective Reliability and Maintainability program for Program Managers and R&ME practitioners.

DOD policy and guidance generally requires program managers to develop a Reliability, Availability, Maintainability – Cost (RAM-C) analysis that optimizes reliability, availability, and maintainability (RAM) within cost constraints. R&ME includes all activities that prescribe the designing, testing, and manufacturing processes that impact the system's RAM. The GAO has reported that O&S cost is driven by the system's RAM qualities and make up approximately 80% of a system's LCC. More importantly, R&M must be an integral part of the upfront design process. System stress and ease of maintenance are controlled through the design. A system's R&M factors significantly affect the performance and sustainment of the deployed system. This is the basis for SECNAVINST 5000.2, emphasizing and prioritizing rigorous and disciplined R&ME efforts early in the acquisition process.

Figure 4 shows three pillars of system effectiveness. Note that reliability and maintainability directly affect two of them. Generally, a design's R&M is be measured by reliability metrics such as Mean Time Between Failure (MTBF), or maintainability metrics such as Mean Time Between Repairs (MTBR); however, to affect these measures, R&ME must start early to ensure design rules and practices are adhered to throughout the development process.

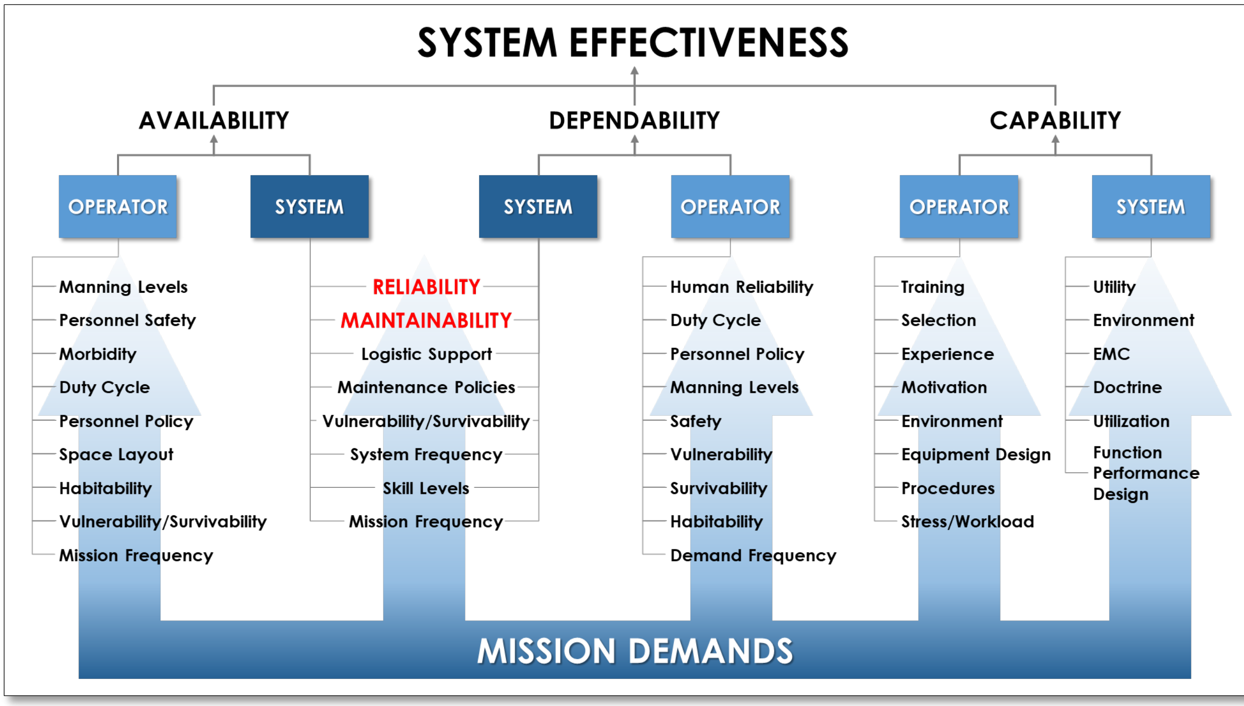


Figure 4: R&ME in System Effectiveness[2]

It is important that the Program Manager (PM) understands the importance and influences of these design factors early in a program or as a part of any block upgrade, tech refresh, or investment in supportability. The DON's direction is to address reliability as a performance parameter and, hence, a design criteria. To facilitate this, the PM is responsible for:

- Decomposing the Sustainment KPP and Reliability, Maintainability, and O&S cost either KSAs or additional performance attributes (APAs) into affordable and testable design requirements; and
- Developing sustainment requirements and resources for the design that will enable systems effectiveness (reliability, dependability, and capability).

This approach places the emphasis on design practices that correlate to fielded system performance. **Figure 5** highlights the importance of proper reliability by design criteria. Of the 14 programs listed, none met even half of their predicted reliability, proving that good design practices are the key. R&ME includes calculating, assessing, and improving the design to avoid deficiencies. The range of required effort includes stress analysis, de-rating, physics of failure analysis, T&E, and FRACAS to realistically achieve desired fielded system R&M attributes.

[2] Adapted from "Operational Availability Handbook: A Practical Guide for Military Systems, Sub-Systems and Equipment," Published by the Office of the Assistant Secretary of the Navy (Research, Development and Acquisition), NAVSO P-7001, May 2018 [Ref 7].

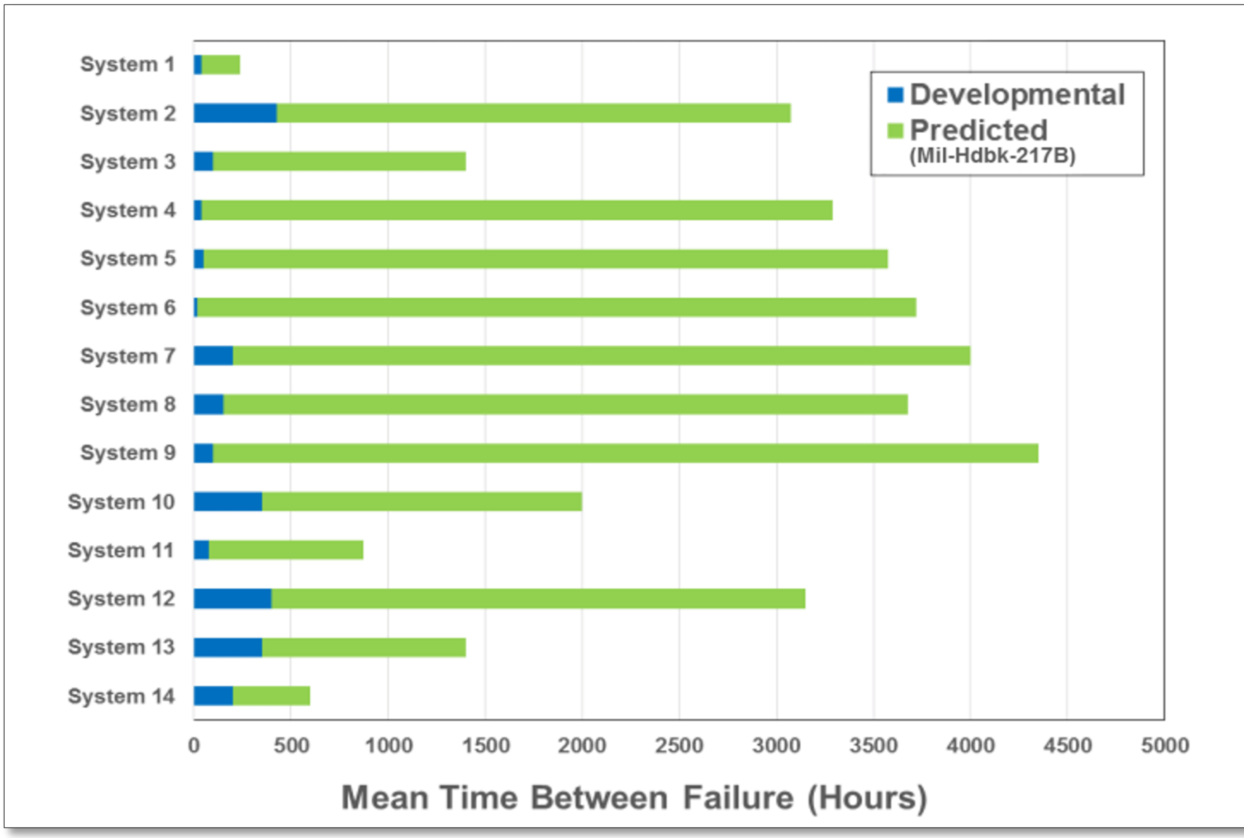


Figure 5: Developmental versus Predicted Reliability[3]

The National Academy of Sciences observed that 75% of programs do worse during Operational Testing (OT) than Developmental Testing (DT)[4]. This lack of correlation explains why reliability growth testing needs to be planned well into OT and fielding. Much of this is due to the relatively benign test environment verses actual OT conditions. While issues and correlation vary by program, from a DON standpoint it is clearly more cost effective to mandate reliability by design rules and, as necessary, growth testing throughout the life cycle.

A_o is a critical measure of mission readiness of fielded systems, however, its use as a metric is inappropriate early in the design process. This is because A_o is a combination of reliability (design controllable), maintainability (design controllable), and product support factors (not design controllable). Including an A_o requirement in the contract allows logistics planners to adjust spares quantities, in an attempt to decrease logistics delay times, to compensate for design deficiencies.

[3] National Research Council 2015. *Reliability Growth: Enhancing Defense System Reliability*. Washington, DC: The National Academies Press, page 112. https://doi.org/10.17226/18987 [Ref 8].
[4] *Reliability Growth: Enhancing Defense System Reliability* [Ref 8].

For the design of ships, NAVSEA places A_o into the contract specification requirements to define the ships readiness requirements to support each mission that the ship is designed to perform. This allows the ship design agent and the Government to define mission critical systems to support each mission area. The ship design agent must predict the Mean Time Between Failure (MTBF) and Mean Time To Repair (MTTR) for mission critical equipment and identify space and weight for spares necessary to ensure those systems can remain available throughout each deployment. With limited space onboard each ship for spares, the proper balance between reliability and maintainability is critical to ensure ship's readiness. The level of reliability needed of each system on a ship is dependent on the ability to repair or replace the items at sea and its criticality should the item fail during a mission. Designing for maintainability and provisioning of onboard spares are included for those items that are mission critical and can be easily repaired or replaced at sea, while mission critical items that are non-repairable or must be sufficiently reliable to ensure ships readiness throughout each deployment. Optimizing reliability and maintainability design controllable features are balanced with provisioning of spares to ensure ships readiness. This optimization is documented in the RAM-C Rationale Report.

Using Inherent Availability (A_i) instead of A_o in contract requirements may be a better choice because A_i does not include preventive maintenance or administrative and logistics delay times (ALDTs). Although preventive maintenance and ALDTs are relevant, they are not typically under the control (or at least full control) of the contractor and should therefore not be used to measure reliability or maintainability of the design. Once fielded, A_o will be the predominate measure of a system's readiness; however, A_i is more design centric and therefore better for evaluating the actual reliability and maintainability of a system. **Figure 6** compares A_o and A_i in their simplest forms and can be tailored to the Program's needs.

MEASURE	EQUATION	REFLECTS
Inherent Availability	$A_i = \frac{MTBF}{MTBF + MTTR}$	The level of R&M achieved in design and the fidelity of the manufacturing processes
Operational Availability	$A_o = \frac{MTBM}{MTBM + MDT}$	The level of R&M achieved in design, the fidelity of the manufacturing processes, maintenance policy, in-theater assets, order/ship times, etc.

Where:
- **MTBF** is the mean time between "hard" failures
- **MTTR** is the mean time to repair as a function of design
- **MTBM** is the mean time between maintenance, all corrective and preventive maintenance
- **MDT** is the mean downtime, which includes the actual time to perform maintenance and accounts for any delays in getting the needed personnel or parts, number of spares on hand, etc.

Figure 6: Comparison of A_o and A_i

Figure 7 shows that life cycle cost is comprised of system acquisition cost and operation and support costs. Of note, many fielded systems exist 30 or more years before disposal. The system acquisition cost ranges between 20-40% of the life cycle cost, while operation and support cost ranges between 60-80% of the life cycle cost.

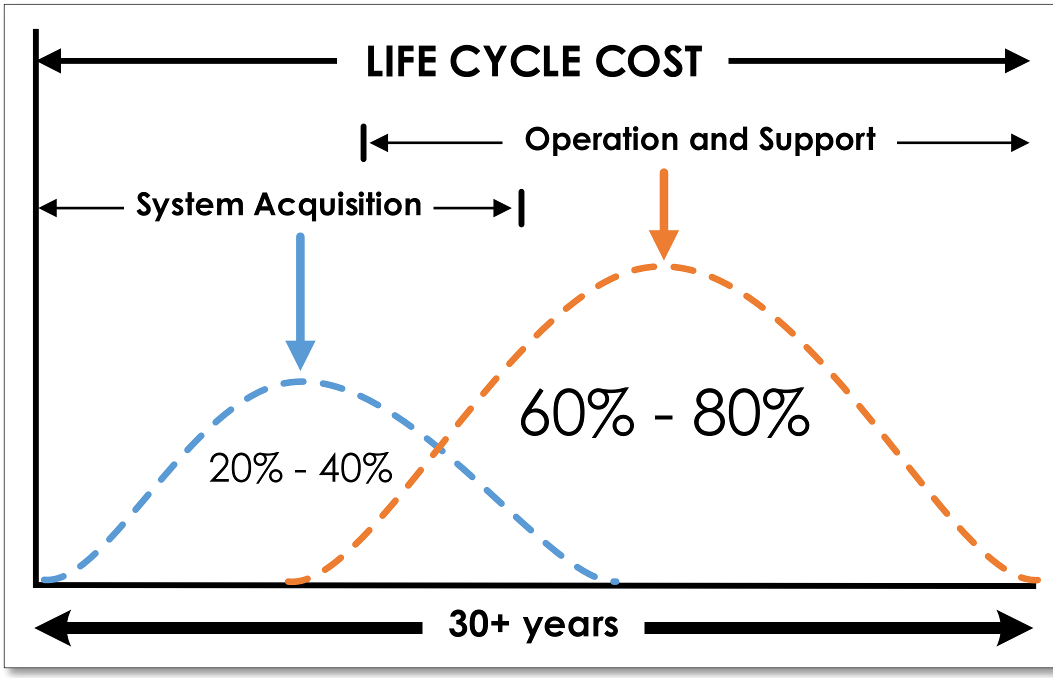


Figure 7: Life Cycle Cost Distribution[5]

In addition, **Figure 8** shows the relationship of cost committed to cost expended across the defense acquisition phases. It is important to point out that by MS B, about 70% of the life cycle cost is committed while less than 10% of the life cycle cost is expended. By Full Rate Production Decision, about 90% of the life cycle cost is committed, while about 20% of the life cycle cost is expended. So, acquisition decisions (and associated decision artifacts including requirements and contracts) have a significant impact on committing a significant portion of the life cycle costs. Thus, it is important that the requirements and contract deliverables are well thought out in support of these major program decisions.

[5] Adapted from Dallosta, Patrick M and Simcik, Thomas A. "Designing for Supportability: Driving Reliability, Availability, and Maintainability In...While Driving Costs Out." *Defense AT&L: Product Support Issue*, March-April 2012, page 35. [Ref 9]

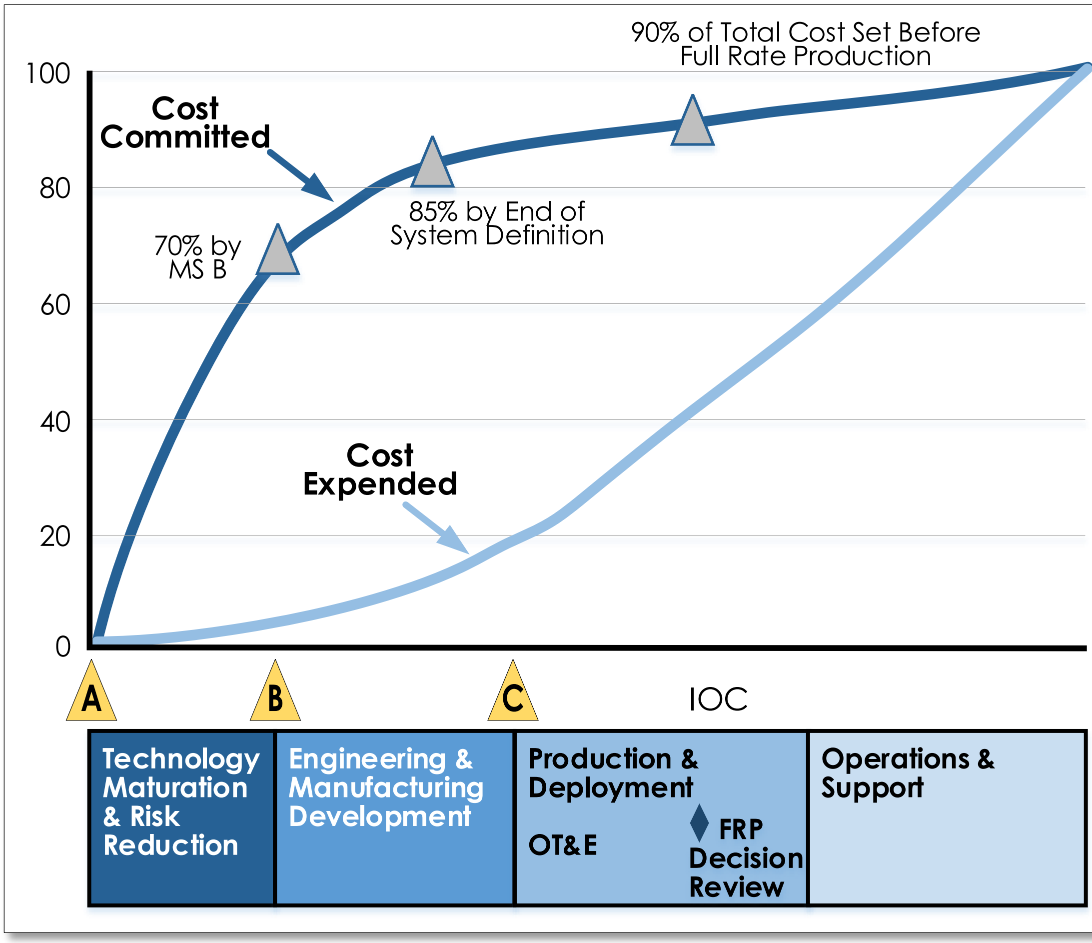


Figure 8: Cost Committed vs. Cost Expended Curves[6]

Optimizing system reliability and maintainability, through the RAM-C Rationale Report, will minimize the program's O&S cost through the reduction in spares and sound maintenance activities required to restore lost functions.

STANDARD METRICS

This section presents typical reliability, maintainability, and Built-in-Test (BIT) metrics, as shown in **Table 2** on the following pages. These are examples of metrics that are typically used on programs. Every metric will not apply. The R&M engineer will need to determine the appropriate metrics for the program based on the goals and intent of the respective metrics. For the reliability metrics, it should be noted, that "time" must be expressed in mission-relevant units of measure (e.g., hours, rounds, cycles, miles, events, etc.). It does not need to tie exclusively to "clock time."

[6] Adapted from Dallosta, Patrick M and Simcik, Thomas A., page 37. [Ref 9]

Table 2: Typical Reliability, Maintainability, and Built-in-Test (BIT) Metrics

RELIABILITY	
R_M (Note 1)	**Mission Reliability:** The measure of the ability of an item to perform its required function for the duration of a specified mission profile, defined as the probability that the system will not fail to complete the mission, considering all possible redundant modes of operation. *(Per JCIDS 2021; Figure B-23 - Recommended Sustainment Metrics)* $$R_M = \frac{Operating\ Hours}{Mission\ Failures}$$
R_L (Note 1)	**Logistics Reliability:** The measure of the ability of an item to operate without placing a demand on the logistics support structure for repair or adjustment, including all failures to the system and maintenance demand as a result of system operations. Logistics Reliability is a fundamental component of an O&S cost as well as Materiel Availability. *(Per JCIDS 2021, Figure B-23 - Recommended Sustainment Metrics)* The JCIDS definition for Logistics Reliability is a demand-based definition, not a failure-based definition. From an engineering perspective, logistics reliability measures the ability of an item to operate within its specified limits, for a particular measurement period under stated conditions. The failure of a redundant component that does not affect mission completion is a logistics failure, but not a mission failure. $$R_L = \frac{Operating\ Hours}{Logistics\ Demands}$$ Demand versus failure: If an end item (aircraft, ship, etc.) has multiple instances of the same component, the demand is calculated at the end-item by taking the end item's operating hours and dividing it by the number of demands. The component's reliability would be calculated by multiplying the end item's operating hours by the number of instances of the component and then dividing it by the number of failures. For example, if an aircraft has four engines, 100 flight hours, and five failures: Aircraft Mean Flight Hours Between Demand = 100 flight hours / five failures = 20 hours Engine Mean Flight Hours Between Failures = (100 flight Hours x 4 engines) / five failures = 80 hours

MTBF (Note 2)	**Mean Time Between Failure:** 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. This is a measure of Logistics Reliability because it considers all failures and any failure will generate a corresponding logistics action to rectify; however, not all failures will affect the operation of the system. $$MTBF = \frac{Total\ System\ Time}{Total\ Quantity\ of\ System\ Failures}$$
MTBOMF (Notes 3, 4)	**Mean Time Between Operational Mission Failure:** A measure of Mission Reliability. An OMF is a hardware failure or software fault that prevents the system from performing one or more mission essential functions ***during mission operation***. Mission Essential Functions (MEFs) are the minimum operational tasks that the system must be capable of performing to accomplish the assigned mission. This parameter also includes failures that are generally attributed to human errors during operation and maintenance that cause failures. $$MTBOMF = \frac{Total\ System\ Operating\ Time}{Total\ Quantity\ of\ Operational\ Mission\ Failures}$$
MTBCF / MTBEFF (Notes 3, 4)	**Mean Time Between Critical Failure / Mean Time Between Essential Function Failure:** A reliability measure of a system's mission capability. A Critical Failure (CF) / Essential function failure (EFF) is a hardware failure or software fault that prevents the system from performing one or more mission essential functions. Any failure that prevents the system from being Fully Mission Capable (FMC), regardless of the time when it occurs, is designated a CF / EFF. $$MTBCF = \frac{Total\ System\ Operating\ Time}{Total\ Quantity\ of\ Critical\ Failures\ or\ Essential\ Function\ Failures}$$
MTTF (Note 2)	**Mean Time To Failure:** A basic measure of reliability for non-repairable systems. The total system time divided by the total number of failures within the population during the specified measurement interval under stated conditions. $$MTTF = \frac{Total\ System\ Time}{Total\ Number\ of\ Failures}$$

MTBM (Note 5)	**Mean Time Between Maintenance:** A measure of the reliability with consideration of the maintenance policy. MTBM is the average time between performance of all maintenance actions required to keep the system operating. Can be focused on corrective maintenance (CM), preventive maintenance (PM), or both. Can be associated with one or more levels of maintenance (organizational, intermediate, and depot). $$MTBM = \frac{Total\ System\ Time}{Total\ Number\ of\ required\ maint.actions}$$
MAINTAINABILITY	
MTTR/ MCMT (Notes 3, 4, and 6)	**Mean Time To Repair (Hardware), Mean Time to Recover or Restore (Software) / Mean Corrective Maintenance Time:** Mean Time To Repair, also referred to as Mean Corrective Maintenance Time, is a basic measure of maintainability. MTTR / MCMT measures the average time required to bring a system from a failed state to an operational state. It is strictly design dependent, as it does not include logistics or administrative delay times. The sum of the corrective maintenance time (clock hours) divided by the total number of corrective maintenance actions. The corrective maintenance time includes fault isolation, access, removal, replacement, and checkout. This alone is not a good measure of maintenance burden as it does not consider the frequency of corrective maintenance, nor the man-hours expended. Each "Mean Time Between" reliability parameter will have an associated MTTR / MCMT. For example, MCMTOMF is mean time required to perform corrective maintenance for operational mission failures associated with the MTBOMF reliability metric. $$MTTR_{(HW/SW)} = \frac{\Sigma\ Corrective\ Maintenance\ Times}{Total\ Number\ of\ Maintenance\ Actions}$$ For additional details concerning classification of Marine Corps maintenance actions, see Note 4.
$MAXTTR_{\#\#\%}$ (Note 2)	**Maximum Time to Repair:** The maximum repair time associated with some percentage of all possible system repair actions. For example, $MAXTTR_{90\%}$ requires 90% of all maintenance actions are completed within the required time. Creates a limitation on the overall time required for performing on-equipment maintenance. Combining this with MTTR further defines the maintenance burden. MAXTTR is useful in special cases where the system has a tolerable Down Time. An absolute maximum would be ideal but is impractical because some failures will inevitably require exceptionally long repair times.

MMH/OH MR (Notes 3, 4)	**Mean Man Hours per Operating Hour or Maintenance Ratio:** Measures the maintenance burden associated with manning levels. A measure of the ratio of total maintenance man-hours required to maintain the system to system operating time. This metric can be focused on corrective maintenance (CM), preventive maintenance (PM), or both and can be associated with one or more levels of maintenance (organizational, intermediate, and depot). Used to develop trade-off comparisons between different maintenance policies. $$MR = MMH/OH = \frac{Total\ Maintenance\ Manhours\ to\ accomplish\ maintenance}{Total\ system\ operating\ time}$$
M_{PMT} (Note 2)	**Mean Preventive Maintenance Time:** A basic measure of preventative maintenance. Measures the average time required to perform preventive maintenance. Preventive Maintenance (PM) is defined as systematic inspection, detection, and correction of incipient failures either before they occur or before they develop into major defects. Adjustment, lubrication, and scheduled checks are included in the definition of preventive maintenance. Preventive Maintenance that inhibits the accomplishment of a MEF causes the system to be unavailable. $$M_{PMT} = \frac{\Sigma\ Preventative\ Maintenance\ Times\ for\ each\ PM\ Action}{Total\ Number\ of\ PM\ Actions}$$ For examples of preventive maintenance actions that are categorized as MEFs, see Note 4.
MRT (Note 2)	**Mean Reboot Time:** A software "maintainability" metric. MRT measures the elapsed time required to reboot software following the occurrence of a software fault regardless of severity. MRT includes only the time required to reboot the system physically, and not the time required for restoring all processes, functions, files, and databases to a tactically useful state. Calculated as: $$MRT = \frac{Total\ Elapsed\ Time\ to\ Reboot\ the\ System\ Software}{Total\ Number\ of\ Software\ Reboots}$$
ALDT (Note 4)	Administrative and Logistics Delay Time is the time spent waiting for parts, administrative processing, maintenance personnel, or transportation per specified period. During ALDT, active maintenance is not being performed on the downed piece of equipment.

BUILT-IN-TEST/HEALTH MONITORING	
P_{CFD} (Note 3)	**Probability of Correct Fault Detection:** A maintainability measure for the effectiveness of Built-in-Test (BIT). The measure of BIT's capability to detect failures/faults correctly. $$P_{CFD} = \frac{Number\ of\ Failures/Faults\ Correctly\ Detected\ by\ BIT}{Total\ Number\ of\ Actual\ System\ Failures/Faults}$$
P_{CFI} (Note 3)	**Probability of Corrective Fault Isolation:** A maintainability measure for the effectiveness of Built-in-Test (BIT). The measure of BIT's capability to isolate the failure/fault correctly to a specified replaceable assembly. $$P_{CFI} = \frac{Number\ of\ Failures/Faults\ Correctly\ Isolated\ by\ BIT}{Number\ of\ Failures/Faults\ Correctly\ Detected\ by\ BIT}$$
P_{BFA} (Note 3)	**Probability of BIT False Alarm (BFA):** A maintainability measure for the effectiveness of Built-in-Test (BIT). A BFA indicates a failure, where upon investigation, it is found the failure cannot be confirmed. The ratio of incorrectly indicated failures compared to all indicated failures. This includes: • Intermittent indications that clear, when the fault logs are reset or are reinitialized by subsequent BIT cycles (may be automatic BIT or on demand BIT); • Indications, which do not require maintenance actions and are set because of poor SW and/or HW design; and/or • Indications, which cannot be confirmed by organizational maintenance personnel, when the suspected faulty Line Replaceable Unit (LRU) is found to perform satisfactorily at higher levels of maintenance. One problem with the P_{BFA} formula, a simple ratio, is if only a few BIT indications are encountered during test, and many are BFAs, the probability of these can be very high. For that reason, P_{BFA} should be used with other BIT measures to determine if the system BIT is effective. $$P_{BFA} = \frac{Number\ of\ Incorrect\ BIT\ Fault\ Indications}{Total\ Number\ of\ BIT\ Fault\ Indications}$$
BFA*h* (Note 3)	**BIT False Alarms per hour:** A maintainability measure for the effectiveness of Built-in-Test (BIT). A BFA indicates a failure, where upon investigation, it is found the failure cannot be confirmed. The number of incorrect BIT failure/fault indications of failures that occurred per hour of operating time. Calculated as: $$BFAh = \frac{Number\ of\ Incorrect\ BIT\ Failure/Fault\ Indications}{Total\ System\ Operating\ Time}$$

MTBBFA (Note 3)	**Mean Time Between BIT False Alarms:** A maintainability measure for the effectiveness of Built-in-Test (BIT). A BFA indicates a failure, where upon investigation, it is found the failure cannot be confirmed. The number of system operating hours divided by the number of incorrect BIT failure/fault indications. Inverse of *BFAh.* Calculated as: $$MTBBFA = \frac{Total\ System\ Operating\ Time}{Number\ of\ Incorrect\ BIT\ Failure/Fault\ Indications}$$ Often a more meaningful measure of BFAs in that it is easier to relate to the operational situation. The data behaves similarly to MTBOMF data and can have a confidence interval.

Sourced by:

Note 1: *CJCSI 5123.01I, "Charter of the Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration and Development System (JCIDS)," 30 October 2021 [Ref 10]*

Note 2: *Reliability Information Analysis Center, "System Reliability Toolkit: A Practical Guide for Understanding and Implementing a Program for System Reliability," 15 December 2005. [Ref 11]*

Note 3: *Commander Operational Test and Evaluation Force, "Operational Suitability Evaluation Handbook," 26 March 2019 [Ref 12].*

Note 4: *Marine Corps Operational Test and Evaluation Activity (MCOTEA), "Operational Test & Evaluation Manual," Third Edition, 22 February 2013. [Ref 13]*

Note 5: *MIL-STD-721C, "Definitions of Terms for Reliability and Maintainability," 12 June 1981. [Ref 14]*

Note 6: *ISO/IEC 25023:2016, "Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of system and software product quality," 15 June 2016. [Ref 15]*

3 | R&ME IN THE ACQUISITION PROCESS

POLICY

The reliability and maintenance engineering policy for the Department of Defense has been established in Title 10 US Code (USC) 2443, "Sustainment Factors in Weapon System Design" (26 August 2021) [Ref 2]; DoDI 5000.88, "Engineering of Defense Systems" (18 November 2020) [Ref 16]; DoDI 5000.91, "Product Support Management for the Adaptive Acquisition Framework" (4 November 2021) [Ref 17]; SECNAVINST 5000.2G, "Department of the Navy Implementation of the Defense Acquisition System and the Adaptive Acquisition Framework" (8 April 2022) [Ref 4], and the DON "Gate 7 Sustainment Reviews" Policy Memo (27 September 2021) [Ref 18].

10 USC 2443

Title 10 USC 2443 "Sustainment Factors in Weapon System Design" states in part:

- The Secretary of Defense shall ensure that the defense acquisition system gives ample emphasis to sustainment factors.
- The requirements process shall ensure that R&M attributes are included in the Sustainment KPP.
- Solicitation and Award of Contracts shall:
  - Include clearly defined and measurable R&M requirements for engineering activities in solicitations of a covered contract.
  - Document the justification for exceptions if R&M requirements or activities are not included in solicitations.
  - Ensure that sustainment factors are emphasized in the process for source selection and encourage use of objective R&M criteria in the evaluation.
- Contract Performance shall:
  - Ensure the use of best practices for responding to positive or negative performance of a contractor in meeting sustainment requirements.
  - Be authorized to include provisions for incentive fees and penalties.
  - Base determinations on data collection and measurement methods in the covered contract.
  - Notify the congressional defense committees upon entering contracts that includes incentive fees or penalties.

DoDI 5000.88

DoDI 5000.88 “Engineering of Defense Systems” includes in part:

- For all defense acquisition programs, the Lead Systems Engineer (LSE)*, working for the PM, will integrate R&ME engineering as an integral part of the overall engineering process and the digital representation of the system being developed.

The LSE will plan and execute a comprehensive R&M program using an appropriate strategy consisting of engineering activities, products, and digital artifacts, including:

1. R&M allocations, block diagrams, and predictions.
2. Failure definitions and scoring criteria.
3. Failure mode, effects, and criticality analysis.
4. Maintainability and built-in-test demonstrations.
5. Reliability testing at the system and subsystem level.
6. A failure reporting, analysis, and corrective action system maintained through design, development, test, production, and sustainment.

** Note: The LSE equivalent in SYSCOMs includes SDM/SIM (NAVSEA) and APM-E (MARCOR, NAVWAR and NAVAIR).*

DoDI 5000.91

DoDI 5000.91 “Product Support Management for the Adaptive Acquisition Framework” contains references to the JCIDS Sustainment KPPs, KSAs, and Additional Performance Attributes. It also states the following regarding the RAM-C Rationale Report:

- The product support manager (PSM) will work with systems engineers and users to develop the RAM-C Rationale Report to ensure supportability, maintenance, and training are incorporated into the design through early user assessments and to incorporate user feedback into supportability planning. This collaboration will ensure sustainment thresholds are valid and feasible. More detail on the RAM-C Rationale Report may be found within relevant engineering instructions (e.g., DoDI 5000.88 [Ref 16]) and in the JCIDS Manual [Ref 10] (Annex D, Appendix G, Enclosure B, paragraph 2.5.1).

SECNAVINST 5000.2G

SECNAVINST 5000.2G provides additional Navy guidance regarding R&ME implementation in the acquisition process and requires:

For all Adaptive Acquisition Framework (AAF) programs other than provision of Services, the PM will implement a comprehensive R&ME program. The R&ME program will include Government and contractor efforts that address reliability, maintainability, diagnostics, Health Management (HM) specifications, and other engineering tasks and activities necessary to resolve operational requirements, design requirements, and Government and contractor R&ME activities. For acquisition category (ACAT) I and II programs, the PM shall ensure that solicitations and resulting contracts include R&ME factors and requirements. The Government R&ME program shall be documented in an R&ME Program Plan that shall be approved by the Systems Command (SYSCOM) R&ME Tech Authority or subject matter expert (SME).

a. For urgent capability, major capability acquisition (MCA), or middle tier of acquisition (MTA) programs, R&ME programs will consist minimally of the following:

(1) Warfighter requirements, including an availability Key Performance Parameter (KPP), Reliability, Operations and Support Cost Key System Attributes (KSA), and the Reliability, Availability, Maintainability – Cost (RAM-C) Rationale Report.

(2) A Concept of Operations (CONOPS) / Operational Mode Summary / Mission Profile (OMS/MP).

(3) Allocation of KPPs and KSAs to contract specifications for reliability, maintainability, diagnostics, and HM, which supports a portion allocated to Government risk.

(4) Failure Definitions and Scoring Criteria (FD/SC) for both warfighter and contractor specification requirements. There will only be one set of warfighter requirement FD/SC utilized by engineering, DT&E and OT&E.

(5) Government and contractor R&ME program plans documenting personnel, planning and activities, and reliability and HM growth strategies.

(6) Failure Modes Effects and Criticality Analysis commencing early in the design process to impact design.

(7) Reliability and maintainability allocations, block diagrams, and predictions.

(8) Testability analyses, including HM functionality and design description documents.

(9) Failure Reporting, Analysis, and Corrective Action System (FRACAS) maintained through design, development, production, and sustainment.

(10) Maintainability considerations, including design for maintainability, reliability-centered maintenance planning, integrated diagnostics (fault detection, fault isolation, and false alarm), access and removal analysis, and maintainability demonstrations.

b. The Government R&ME program will be conducted under the direction of the program's SYSCOM Chief Engineer (Program CHENG) or other Technical Authority (TA), as designated. The R&ME systems engineer will operate under the purview of the Program CHENG, Ship Design Manager or System Integration Manager.

c. Each SYSCOM CHENG or designee will designate an R&ME manager responsible for SYSCOM R&ME policy, standards, guidance, oversight and implementation for their designated platforms, environments, and Command structure.

d. Software-only programs will use Availability and Restore Time parameters, measures and maturity metrics. Software quality should be assessed during development to predict software reliability cost when fielded. Programs that are primarily software can be treated as software programs; however, acquisition of the limited hardware components will include R&ME requirements, activities and technical specifications, as appropriate.

e. Programs will maintain a R&M associated risks and risk mitigations list, including deviations from the R&M Program Plan. Future impacts such as, cost, availability, and mission effectiveness should be primary factors considered in risk acceptance. Internal control oversight of R&M risk acceptance will be conducted during Systems Engineering Technical Reviews (SETRs), Technical Review Boards (TRBs), independent logistics assessments (ILAs), independent technical review assessments (ITRAs), and Gate Reviews as appropriate.

DON Gate 7 Sustainment Reviews Policy Memo

Sustainment Reviews will be conducted as the Gate 7 in the DON's "Two-Pass, Seven Gate Review" process. Prior to the review, programs will re-validate the sustainment Business Case Analysis and Product Support Strategy, and support development of the Independent Cost Estimate (ICE). The required content for the Sustainment Review is provided below. Programs will update their Life Cycle Sustainment Plans (LCSPs) following the Gate 7 review, as required. Sustainment reviews will be conducted every five years after the initial Gate 7 Sustainment Review (SR).

The DON intends to utilize the appropriate Systems Command's cost estimating organizations, working with the program offices, to conduct the required O&S ICE in coordination with Director, Cost Analysis and Program Evaluation and in accordance with DOD and DON cost policies and procedures. The ICE will include all costs for the remainder of the program's life cycle. Results of the ICE, including any critical cost growth, will be reported in the SR. The DON will provide mitigation plans, or certification, for critical cost growth annually to Congress.

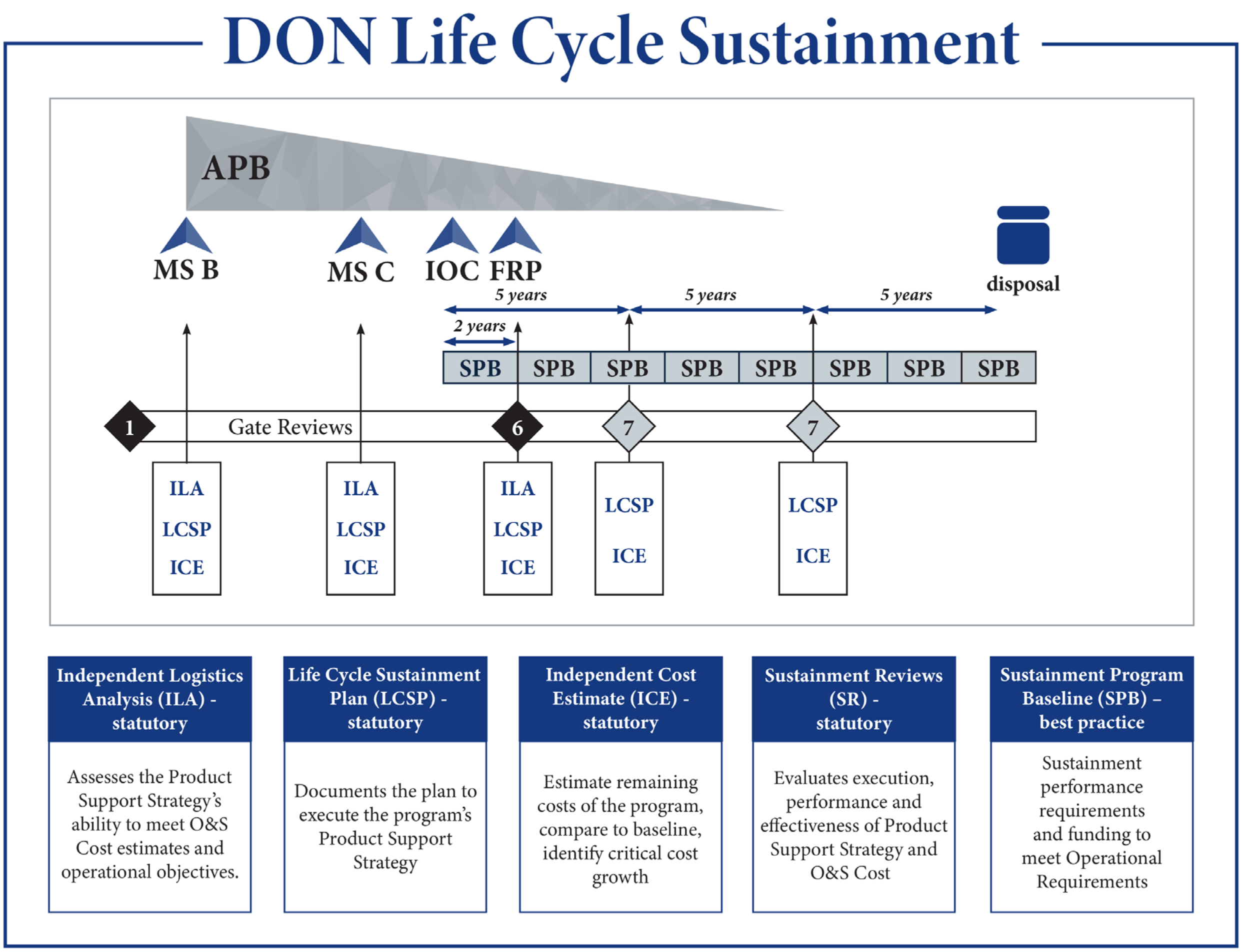


Figure 9: DON Life Cycle Sustainment

DON SUSTAINMENT REVIEW/GATE 7 REQUIREMENTS:

1. Overarching sustainment strategy summary, assessment of LCSP execution, identify any proposed changes from previous versions.
2. Sustainment schedule with milestones, including anticipated retirement date.
3. Product Support BCA revalidation summary.
4. Results of the ICE of O&S cost for remainder of the program; compare to baseline costs and identify any critical cost growth per 10 US Code (USC) 2441 [Ref 2].

5. Comparison of actual costs to funds budgeted and appropriated in the previous five years. If funding shortfalls exist, provide implications on weapon system availability.
6. Comparison between assumed and achieved system reliabilities.
7. Performance to approved SPB requirements (if applicable).
8. Analysis of the most cost-effective source of repairs and maintenance.
9. Evaluation of costs of consumables and depot-level repairables.
10. Evaluation of costs of information technology, networks, computer hardware, and software maintenance and upgrades.
11. Assessment of actual fuel efficiencies compared to projected fuel efficiencies, if applicable.
12. Comparison of actual manpower requirements to previous estimates.
13. Analysis of whether accurate and complete data is reported in cost systems of the military department concerned. If deficiencies exist, a plan to update the data and ensure accurate and complete data will be submitted in the future.
14. Information regarding any decision to restructure the LCSP for a covered system, or any other action that will lead to critical O&S cost growth, if applicable.

GUIDANCE

Related guidance documents with specific reference to R&ME include: DOD R&ME Management Body of Knowledge (DOD RM BoK) [Ref 19]; USD (R&E) Systems Engineering Guidebook (Feb 2022) [Ref 20]; Reliability, Availability, Maintainability, and Cost (RAM-C) Rationale Report Outline Guidance (Feb 2017) [Ref 21]; Engineering of Defense Systems Guidebook (Feb 2022) [Ref 22]; Systems Engineering Plan (SEP) Outline (v. 4.0, Sep 2021) [Ref 23]; Life Cycle Sustainment Plan (LCSP) v2.0 (Jan 2017) [Ref 24]; and Test and Evaluation Master Plan (TEMP) Guidebook v. 3.1 (Jan 2017) [Ref 25].

The DOD RM BoK presents the procedures that program managers, project engineers, and R&M engineers should use for implementing and executing R&M programs. It provides very detailed descriptions and guidance for each associated task and life cycle phase. The USD (R&E) Systems Engineering Guidebook provides systems engineering guidance and recommended best practices for defense acquisition programs. The RAM-C Rationale Report, the SEP Outline, LCSP Annotated Outline, and the TEMP assist in the preparation of the respective documents. These guidance documents described are examples of planning documents that span the life cycle of the program and therefore appear as activities during different acquisition phases.

Results of R&M engineering activities are essential for programmatic decision and control functions. The R&ME design methods and procedures are not new, but the challenge occurs in the management of these methods and procedures to achieve reliable and maintainable systems. Effective management control of the R&ME program, using the policies and guidance set forth by DOD, DON, and the Naval SYSCOMs will ensure timely performance of the necessary activities to achieve the requirements and the development of adequate data to judge the acceptability of R&ME achievement at major milestones.

Naval SYSCOM R&ME Guidance

Naval SYSCOMs provide R&ME guidance for implementing the DOD and DON policy for their platforms and operating environments. Other SYSCOM guidance consists of:

- **NAVSEA:**
  - T9070-BS-DPC-010_076-1 Reliability and Maintainability Engineering Manual, 21 Feb 2017 [Ref 26]
- **NAVAIR**
  - Most of the NAVAIR R&ME guidance comes in the form of Standard Work Packages (SWP) including:
    - Validate and Translate R, M, and BIT Requirements for Joint Capabilities Documents
    - Develop and Implement a Reliability, Maintainability, and Integrated Diagnostics Program
    - Perform Reliability, Maintainability & BIT Design Analyses
    - Perform R&M Pre-installation Design Verification Tests
    - R&M/IHMS Test and Evaluation Management
    - Reliability Control Board: Reliability and Maintainability Analysis Process
    - Reliability Growth Planning, Tracking and Projection During Developmental and Operational Testing
    - Reliability, Availability, Maintainability, and Cost (RAM-C) Analysis and Report Development Cross Domain SWP
    - Systems Engineering Plan: Reliability and Maintainability Inputs
    - SETR Event Process: R&M Preparation and Attendance
    - SETR Event R&M Risk Assessment Process

Acquisition Life Cycle

This section and **Table 3** identify R&ME activities in each phase of the system life cycle regardless of acquisition pathway (For more detailed information about the adaptive acquisition framework and acquisition pathways, see AAF.dau.edu [Ref 27]). R&ME should be included in programs early to ensure R&M requirements are realistic and achievable, and to provide early influence into the design. They also provide data to assist PMs in making sound R&ME decisions at critical "in-process" review points and major transitional milestones in the defense acquisition life cycle. The R&ME activities are applicable for all MCA new-start programs. For all other acquisition pathways, the PM assisted by the R&M engineer, can tailor the tasks and activities to fit the product development timelines. All tailoring should evaluate risks associated with the exclusion of a task or activity while allowing for creativity and innovation. Regardless of the acquisition pathway, the R&ME design and development impact on product performance and support are important to ensure system readiness and achievement of the Sustainment KPP.

Table 3 outlines MCA tailoring guidelines based on the program phase and type of equipment being acquired. This table identifies the engineering activities identified in DoDI 5000.88 [Ref 16], DoDI 5000.91 [Ref 17], and SECNAVINST 5000.2G [Ref 4], as well as specific tasks and activities that support the overall R&ME program. Checkmarks indicate tailoring is required to address the equipment type and unique requirements of the system. The table identifies when an update is recommended and should be tailored to the program's needs. The tasks and activities presented in **Table 3** are in concert with the DOD RM BoK [Ref 19], which provides very detailed descriptions and guidance for each associated task and life cycle phase. For more details of the procedures, criteria, and data, refer to DOD RM BoK [Ref 19].

Table 3: MCA R&M Engineering Activities

R&ME Tasks and Activities	DoDI 5000.88	DoDI 5000.91	SECNAVINST 5000.2G	MCA Program Phase: MS A	TMRR	EMD	P&D	O&S	Equipment Type: New Design/ Major Change	Modified	NDI/COTS/GOTS
Reliability and Maintainability Program Plan	●		●	Initial	Update	Update	Update	Update	✓	✓	✓
Mission Profile Definition: Review and Summarize the OMS/MP			●	Initial	Update	Update	Update	Update	✓	✓	✓
Perform R&M Requirements Validation			●	Initial	Update	Update	Update	Update	✓	✓	✓
Subcontractor Requirements: Translate JCIDS R&M values into design and contract requirements			●	Initial	Update	Update	Update	Update	✓	✓	✓
Review the Acquisition Strategy				Initial	Update	Update	Update		✓	✓	✓
Provide or Update R&M Input to SEP	●			Initial	Update	Update	Update		✓	✓	✓
Prepare or Update RAM-C Report	●	●		Initial	Update	Update	Update		✓	✓	✓
Provide or Update R&M Input to Test and Evaluation Master Plan (TEMP)				Initial	Update	Update	Update		✓	✓	✓
Provide or Update the Performance Specification				Initial	Update	Update	Update		✓	✓	✓
Provide or Update R&M Inputs into the Statement of Work (SOW)				Initial Phase based	Initial Phase based	Initial Phase based	Initial Phase based	Initial Phase based	✓	✓	✓
Parts Derating Guideline and Stress Analysis				Prelim	Initial	Update			✓	✓	
Evaluate GFE/COTS				Initial	Update	Update	Update		✓	✓	✓
Prepare or Update allocations of R&M requirements	●		●	Prelim	Initial	Update	Update		✓	✓	✓
Prepare or Update R&M Block Diagrams	●			Prelim	Initial	Update	Update	Update	✓	✓	✓
Predict R&M to estimate feasibility	●			Initial	Update	Update	Update	Update	✓	✓	✓
Prepare or Update failure definitions and scoring criteria (FD/SC)	●		●	Initial	Update	Update	Update	Update	✓	✓	✓
Perform or Update FMECA	●		●		Initial	Update	Update	Update	✓	✓	✓
Reliability Critical Items					Initial	Update	Update	Update	✓	✓	✓
FRACAS	●		●		Plan	Implement	Execute	Execute	✓	✓	✓
Provide R&ME Design Support					Execute	Execute			✓	✓	
Perform Design Trade-off Studies				Execute	Execute	Execute	Execute	Execute	✓	✓	✓
Conduct Growth and Design Verification Tests					Plan	Execute	Execute	Execute	✓		
Perform Subsystem Tests	●				Plan	Execute	Execute		✓		
Perform System Tests	●				Plan	Execute	Execute		✓	✓	✓
Production Planning							Initial	Update	✓	✓	✓
Fleet R&M Data Analysis								Execute	✓	✓	✓
Engineering Change Proposals							Execute	Execute	✓	✓	✓
Life Cycle Sustainment Plan		●	●		Initial	Update	Update	Update	✓	✓	✓
Integrated Logistics Assessment		●	●		Initial	Update	Update	Update	✓	✓	✓

Prelim *– Preliminary draft of the artifact may not be needed for the phase.* ***Initial*** *– Artifact required in support of a specific decision point, potentially requires an update at a later date.* ***Update*** *– Maintenance of the document to account for design maturation, strategy changes, contractual updates, design modifications, and lessons learned.* ***Plan*** *– Plan the test or activity.* ***Execute*** *– Conduct the task or activity*

A. RELIABILITY AND MAINTAINABILITY ENGINEERING PROGRAM PLAN

Each program, regardless of acquisition pathway, should formulate a comprehensive R&ME program to ensure the program's tasks and activities are properly scoped, resourced, and scheduled. Both the Navy and prime contractor's comprehensive R&ME plan should be documented in their respective life cycle R&ME Program Plans.

The Government R&ME Program Plan describes the Reliability (R), Maintainability (M), and Health Management (HM) engineering effort for the full life cycle of the program. Planning activities will typically commence with Materiel Solution Analysis (MSA) or TMRR and run through O&S. This plan establishes a properly constructed and tailored R&ME management approach to ensure that all elements of the R, M, and HM engineering efforts are uniformly implemented, properly conducted, evaluated, documented, reported, and integrated. This Government plan will serve as the master planning and control documentation for the R, M, and HM program.

The prime contractor's R&ME Program Plan describes how the program will be conducted, and the requirements, controls, monitoring and flow down provisions levied on subcontractors and vendors. It describes the R&ME, including HM, procedures, and tasks to be performed and their interrelationship with other system related tasks. The principal use is to provide a basis for review and evaluation of the contractor's R&ME program and for determining compliance to specified R&M requirements.

Government R&ME Program Plan

The Government R&ME Program Plan should be initiated early in the program life cycle (review with PM, LSE, PSM) and reviewed for program updates and changes. An appropriate Government R&ME Program Plan should address the following:

- Management
- Management Activities Description
- Management Activities Schedule
- Resources
- Problem and Risk Areas
- Acquisition Program Documents
- R&M Program Tailoring
- R&M Demonstration/Verification
- Surveillance
- Data Requirements
- R&M Specification
- Request for Proposal (RFP)

Contractor R&ME Program Plan

A Contractor R&ME Program Plan should be required in accordance with Data Item Description, DI-SESS-81613A [Ref 28], with delivery soon after contract award. The plan should be reviewed and updated periodically. Ensure the contractor's R&M Program Plan addresses the following:

- Program Management
- Activity Description
- Activity Schedule
- Failure Recording, Analysis, and Corrective Action System (FRACAS)
- Growth Planning and Procedures
- R&ME Data
- Test Plan
- R&ME Test Monitoring
- R&ME Collaboration

B. MISSION PROFILE DEFINITION: REVIEW AND SUMMARIZE THE OMS/MP

As per the JCIDS Manual, the OMS/MP is the Component-approved document that describes the operational tasks, events, duration, frequency, and environment in which the materiel solution is expected to perform each mission and each phase of a mission.

Adequate levels of reliability cannot be achieved without having a complete understanding and knowledge of the environments and stress levels to which a system will be exposed. Therefore, the OMS/MP is a key artifact for all programs regardless of acquisition pathway. The OMS/MP provides a profile of events, functions, and environmental conditions that a system is expected to encounter during operational use and in support of each mission that the system will be capable of performing.

The R&M engineer should summarize the OMS/MP and environment for the program. An accurate and thorough OMS/MP, based on the CONOPS or combat scenario deemed to be the most representative, is critical to ensuring the equipment meets the user's needs. Any special conditions of use that would affect the sustainment of the system should be identified.

C. PERFORM R&M OPERATIONAL REQUIREMENTS VALIDATION

The R&M engineer should review the system performance capabilities established in the draft Initial Capabilities Document (ICD)/CDD to ensure the R&M operational requirements are valid in that they support the war fighters' needs; are achievable within the program's cost, schedule, and trade space; and are supported by technology.

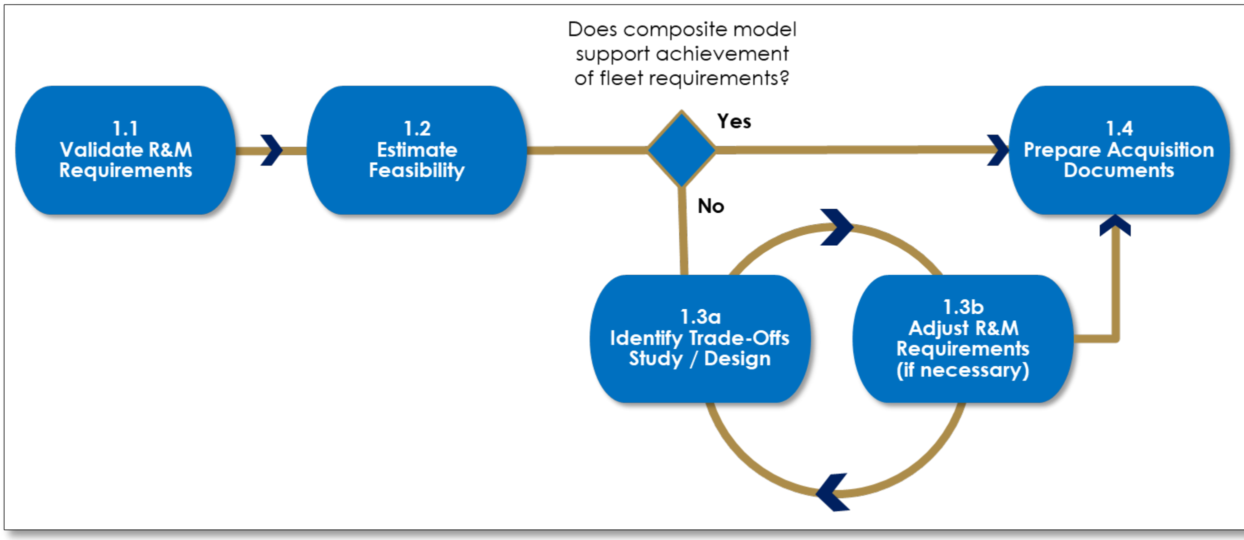


Figure 10: R&M Operational Requirements Validation Process

This analysis process is described in the following section of the DOD RM BoK [Ref 19]: "MSA Activity #4, R&M Requirement Analysis, System Engineering." As part of the validation, the R&M engineer does the following:

- **STEP 1.1:** The R&M engineer reviews the desired capabilities established in the draft CDD to refine (if necessary) the OMS/MP, operational sequence and maintenance concept. The R&M engineer should ensure the system boundaries, FD/SC, and mission time are defined and consistent with the program acquisition concepts of operation.
- **STEP 1.2:** The R&M engineer performs preliminary R&M analysis, feasibility and trade-off studies of the design concepts. This includes the development of a composite model for early planning and determining feasibility of the reliability, maintainability, and availability metrics.
- **STEP 1.3:** Based on results of the R&M analysis, the R&M engineer:
  - Recommends adjustment (if necessary) of the R&M thresholds.
  - Summarizes whether the sustainment parameters are valid and feasible.
  - Identifies any significant issues in OMS/MP, CONOPS, failure definitions or maintenance approaches.
  - Provides issues and recommendations to the requirements developers and other stakeholders.
  - Repeat above steps as necessary until requirements are determined to be feasible.
- **STEP 1.4:** Once the Operational requirements are considered valid, R&M engineer ensures the appropriate documents are updates.

As the design matures, the R&M engineer should continue to update the requirements analysis and assess the risk associated with the R&ME performance. The DOD RM BoK contains detailed procedures for requirements analysis in each life cycle phase.

D. CONTRACTOR REQUIREMENTS

Once JCIDS warfighter requirements have been validated and assessed for feasibility, the R&M engineer should translate thresholds and objectives into contractual R&M design requirements. The translation accounts for differences between operational environments and acquisition developmental environments. These differences are not statistical variations or confidence intervals but are, in part, attributed to the fact that operational systems include more elements and potential failures in the operating environment than systems under contract evaluated in a developmental environment. This task should be completed regardless of the acquisition pathway.

Further info is located in **Chapter 4,** "Translating and Allocating KPP and KSA/APA Requirements into Contract Specifications."

E. REVIEW THE ACQUISITION STRATEGY

The Acquisition Strategy (AS) for each program should include a description of activities essential for verifying and achieving R&M requirements. The AS should also specify how sustainment KPP thresholds have been translated into R&M design and contract specifications. The AS is updated beginning with the MSA phase and should be updated in each phase of acquisition. The R&M engineer should review the acquisition strategy and subsequent updates for decision reviews.

F. PROVIDE OR UPDATE R&ME INPUT TO SEP

The SEP is a living technical planning document and blueprint for conduct, management, and control of the technical aspects of the Government's program from concept to disposal. The SEP defines methods for implementing all R&ME activities, technical staffing, and technical management within the overarching systems engineering process. Additionally, the SEP should reference the RAM-C Rationale Report and the Government R&ME Program Plan.

A SEP outline is provided in the Systems Engineering Plan (SEP) Outline [Ref 23].

G. PREPARE OR UPDATE RAM-C RATIONALE REPORT

Using the DOD RAM-C Rationale Report Outline guidance [Ref 21], programs should describe the sustainment parameters, maintenance concept feasibility, and trade-off analyses. During the Analysis of Alternatives (AoA), the report may be limited in scope due to unknowns at various stages of the program, but should articulate the life cycle sustainment requirements and concepts for each alternative. The RAM-C Rationale Report should provide a quantitative basis for reliability, availability, and maintainability requirements, as well as improve cost estimates and program planning. The tasks in **Table 3** (“Perform R&M Requirements Validation” and “Translate JCIDS R&M Values into Design and Contract Requirements”) will support the RAM-C analysis. RAM-C Rationale Reports are to be developed and attached to the SEP at Milestone A, RFP Release Decision Point, Milestone B, and Milestone C. The RAM-C analysis and the RAM-C Rationale Report are required for all urgent capability acquisition (UCA), MCA, or MTA programs. However, it is beneficial to create a RAM-C-like report for all acquisition programs to document the analyses behind the requirements for future reference.

The RAM-C Rationale Report Outline [Ref 21], as well as additional training and other resources, may be found at DAU’s R&M Engineering Community of Practice [Ref 29].

H. PROVIDE OR UPDATE R&M INPUT TO TEST AND EVALUATION MASTER PLAN (TEMP)

The TEMP documents the overall structure and objectives of the Test and Evaluation (T&E) program. It provides a framework within which to generate detailed T&E plans and document schedules and resource implications associated with the T&E program. The TEMP identifies necessary DT&E, OT&E, and Live Fire Test and Evaluation (LFT&E) activities. It relates program schedule, test management strategy and structure, and required resources to: Critical Operational Issues (COIs), Critical Technical Parameters (CTPs), objectives and thresholds documented in the Capability Development Document (CDD), evaluation criteria, and milestone decision points.

The TEMP should specify how R, M, and HM will be tested and evaluated during the associated acquisition and test phases. Beginning in MS B, the Reliability Growth Strategy and associated Reliability Growth Curves should be included in the TEMP. The TEMP should provide the picture of how all testing fits together and how testing produces a verification of not only the system’s effectiveness at meeting the performance objectives for the capability, but the required R, M, and HM as well. The TEMP should identify R, M, and HM testing and data requirements. Test limitations should be discussed, including impacts of limitations and potential mitigation.

The DOT&E TEMP Guidebook [Ref 25] can be found at: https://www.dote.osd.mil/Guidance/DOT-E-TEMP-Guidebook/.

I. PROVIDE OR UPDATE THE PERFORMANCE SPECIFICATION

The performance specification is the contractual design document stating requirements and associated verification methodology for a product. The requirements describe what the product should do, how it should perform, the environment in which it should operate, and interface and interchangeability characteristics. The requirements should not specify how the product should be designed or manufactured.

Performance specifications are governed by MIL-STD-961 titled "Defense and Program-Unique Specifications Format and Content." The current version, as of this publication, is MIL-STD-961E, with Change 4 dated 16 July 2020 [Ref 30].

The System Specification is a performance description addressing all system level functional and performance requirements. The System Specification makes up the "Functional Baseline" of the system under development.

The system requirements are stated in "Section 3" of the Specification.

The verification method for each requirement is stated in "Section 4" of the Specification.

The R&ME performance requirements should include the following:

- A quantitative statement of the reliability requirement as determined by translation of JCIDS war fighter requirements;
- A full description of the environment in which equipment/system will be stored, transported, operated, and maintained;
- Clear identification of "time" measurement (for example, operating hours, flight hours, cycles);
- A clear definition of what constitutes a failure/fault; and
- A description of verification methodologies.

MIL-HDBK-338B "Electronic Reliability Design Handbook," Section 6.2, "Reliability Specification" [Ref 31] provides further guidance and approaches to reliability specification.

Maintainability specification requirements should include:

- A quantitative statement of maintainability requirements as determined by translation of JCIDS war fighter requirements.
  - In addition to parameters such as Mean Time To Repair, Maximum Time To Repair, and direct maintenance man-hours per operating hours, maintainability also includes health management requirements such as, Built-In-Test fault detection, BIT fault isolation, BIT false alarms, and testability.
  - To properly specify maintainability, product maintenance concept must be understood and align with product life cycle sustainment strategy.
- A clear identification of repair tasks that are included in countable maintenance time. List the tasks and activities included in repair times, such as fault location and

isolation, equipment access (open doors and panels, etc.), equipment removal and replacement, and system closeout (close doors and panels, etc.). In addition, list tasks and activities that are not included, such as tool gathering and software loading.

- Clear definitions and equations for BIT and testability requirements.
- Qualitative design for maintainer requirements.
- Description of verification methodologies.

Reliability Information Analysis Center (RIAC)'s "Maintainability Toolkit" [Ref 32] provides further guidance and approaches for maintainability specification.

J. PROVIDE OR UPDATE R&ME INPUTS INTO THE STATEMENT OF WORK

The Statement of Work (SOW) contains the narrative of a project's work requirements. It defines product specific activities, deliverables, and timelines for suppliers providing the services to the Government. The SOW tasking and activities will vary based on the program's life cycle phase and type of product being developed. The SOW will also contain data item descriptions (DIDs) to address scope and format for data delivery. There will be multiple SOWs across the products life cycle. The R&ME engineer should ensure the appropriate tasks and activities are called out for each phase. The DOD RM BoK contains detailed descriptions of R&ME tasks and activities that should take place during each phase of the product life cycle. When tailoring tasks and activities required by the SOW, R&M engineer will need to tailor based on the risk of not completing tasks and program's acquisition pathway and timing. Often, the short-term risk may seem minimal, but long-term sustainment planning and execution risk will be much higher. For example, a program can save time and cost if a reliability development test is not required. However, this will result in delivery of a less mature (lower reliability) product, resulting in higher sustainment and maintenance costs.

The SOW tasks should be defined and scheduled so they are deemed as proactive tasks and analyses positively impacting the design vice reactive tasks and analyses that just document the design.

For more information, refer to MIL-HDBK-245E, "Preparation of Statement of Work (SOW)," 14 June 2021 [Ref 33].

K. PARTS DERATING GUIDELINE AND STRESS ANALYSIS

Parts derating is the reduction of electrical, thermal, and mechanical stresses applied to a part to decrease the degradation rate and prolong the expected life of the part. Derating may be considered the largest single contributor to reliability. The Contractor should establish, utilize, and maintain design derating for all types of parts and materials to provide for reliability operation at the maximum operating stress levels. These design deratings should be based on maximum rating for the parts and materials which, as limiting values, define electrical, mechanical, thermal, environmental and special sensitive criteria beyond which either initial performance or operations are impaired. All critical parameters must be addressed for each part or material subclass. Stress derating practice ranks with mission profiles as one of the most critical design factors associated with high reliability, low risk products.

L. EVALUATE GFE/COTS

The R&M engineer should review contractor's analysis of Government-Furnished Equipment (GFE)/ Commercial-off-the-Shelf (COTS) components' R&M attributes. Using GFE/COTS can enhance operational effectiveness and reduce costs as the development and supply system for these items are already established.

To fully investigate GFE/COTS options and make informed decisions, the acquiring activity should acquire design data, test results, and information on field performance and interface compatibility for specific GFE/COTS items identified in the contract.

GFE/COTS Data Required:

- Performance characteristics of GFE/COTS item(s) under consideration
- Physical and functional configuration as defined in applicable configuration documents and procurement specifications
- Observed (or predicted) failure rates, repair rates, and Built-in Test (BIT) performance derived from field or other approved data sources with associated environmental/operational use conditions
- Environmental performance problems related to GFE/COTS operating outside their qualification levels that will jeopardize R&M in the integrated system
- When called for under the contract, an analysis to diagnose problems, determine root causes, and provide recommended corrective actions

Review all GFE and COTS for R&M adequacy. The R&M attributes and failure mode characteristics of GFE/COTS should be compatible with requirements that would otherwise have been allocated to GFE items in the same application.

M. PREPARE OR UPDATE ALLOCATIONS OF R&M REQUIREMENTS

R&M allocation refers to the optimization process on the R&M attributes of all or some of the components of a given system in order to meet the target of overall system R&M attributes with minimum cost. One of the first steps in the allocation process is the construction of the system models. In a complex design, it is necessary to break down the overall requirement into separate requirements for the numerous items that make up the system.

The allocation process is approximate and usually results from a trade-off between the R&M of individual items. If the R&M of a specific item cannot be achieved at the current state of technology, then system design must be modified, and allocation reassigned. This procedure is repeated until one allocation is achieved that satisfies the system level requirement and results in items that can be designed.

Caution must be exercised in allocating system requirements when GFE or COTS items are part of the system. Often, the source data originally specified for such GFE or COTS items are used in lieu of the actual field data experienced in the Fleet. Use of original source data (i.e., specification or lab demonstrated values) can impact achievement of system requirements, development time and cost. If actual GFE or COTS source data is significantly worse than the original specification values, then allocation for Contractor items will be inadequate to satisfy system requirements. On the other hand, if GFE or COTS source data is significantly better than the specified value, then allocations for Contractor items will be higher than required and could cause an increase in development time and cost necessary to satisfying system requirements.

Regardless of the type of acquisition, R&M allocations must be constructed for all procured systems.

MIL-HDBK-338B [Ref 31], Section 6.3 “Reliability Apportionment/Allocation” provides extensive coverage of the R&M allocation process, including software and human elements.

N. PREPARE OR UPDATE R&M BLOCK DIAGRAMS

R&M block diagrams are graphical and mathematical models of elements of a system permitting the calculation of system R&M given attributes of the elements. The model reflects reliability performance structure including series, parallel, standby and other arrangements of system elements. R&M block diagrams enable creation of meaningful R&M allocations and predictions. It is convenient to create several block diagrams. The first would be a simple diagram showing first order breakdown of the system. Separate block diagrams are then constructed for each first order breakdown of the system. Level I & II diagrams represent first order breakdown of the system and usually are producible from information available in the system planning stage. These diagrams are considered adequate for making preliminary allocations and feasibility estimates. Level III & IV diagrams are produced as the design information becomes available to show specific configurations at the subsystem and unit levels. The level V diagrams represent the part level where stress analyses and failure mode studies are performed on individual parts within the system.

It is imperative to implement life cycle R&M block diagrams which can be updated as more accurate data becomes available. The R&M block diagrams are used to identify potential areas of poor R&M and where improvements can be made. This method can be used in both design and operational phases to identify poor reliability and provide targeted improvements.

MIL-HDBK-338B [Ref 31], Section 6.4, "Reliability Modeling and Predication" provides extensive coverage of R&M block diagrams and math models.

O. PREDICT R&M TO ESTIMATE FEASIBILITY

The role of R&M predictions during design are to provide an evaluation of the proposed design or for a comparison of alternative designs. It is the process of quantitatively assessing the system's R&M performance during its development. Predictions do not contribute to system R&M, rather they identify those components that need further evaluation. Predictions constitute decision criteria for selecting courses of action, which affect R&M performance.

Reliability Estimate Maturity Level

A reliability estimate maturity level (REML) is created as a mechanism to differentiate the relative understanding of the reliability data used in reliability predictions. REMLs are used to understand the relative confidence in a system's predicted reliability and to determine the importance of completing additional R&M analysis or reliability testing on equipment to understand the failure rate in applicable environments. REMLs are sometimes used to describe if a FMECA, reliability sensitivity analysis, derating analysis, or reliability testing must be performed to improve confidence in the reliability and projected failure rate of the equipment.

REMLs are used to describe the level of confidence in reliability predictions. REMLs describe the level of knowledge that we have in the accuracy and completeness of the failure rate data on specific equipment in the environment that it is intended to be used. A prediction may be followed by the percentage REML in each category (I –IV) as described below. REMLs are assigned during the design and development process to understand how the new design compares to what is known today regarding the equipment's reliability and should be included in the prediction analysis.

The following categories are used to assign REMLs when designing new systems and may be tailored to support the system under design:

- **I –** New technologies under development: Equipment or technologies that are currently under development or have no credible DOD field experience in similar applications. These have little to no fielded data; predictions are based solely on MIL-HDBK-217 [Ref 34] type predictions. These items or systems represent a high reliability application and prediction risk due to the lack of relevant data. Further reliability analysis and testing are recommended to mitigate the risk.

- **II –** Existing technologies used in different applications: Equipment or technologies that have limited to no relevant DOD/DON field data or data that does exist is from a different industry with remotely related use or environments (such as the auto industry). This may be equipment where only manufacturer's data is available, but it is not relevant to the Naval applications. These items could also be existing equipment that does not meet their reliability requirements and are considered candidates for a reliability improvement program. These items or systems represent a moderate-to-high reliability application and prediction risk due to the lack of relevant data. Further reliability analysis and testing are recommended to mitigate the risk.
- **III –** Existing technologies used in similar applications: Existing equipment that has been in use previously in similar applications (such as commercial marine applications, but not on Naval systems / commercial aircraft but not Naval aircraft), and there are abundant reliable sources of reliability and maintainability data available to support R&ME estimates. These may be commercial items or items that have been tested by the Government for which test results are available. These items or systems represent a low-to-moderate reliability application and prediction risk because they have been demonstrated in a similar application. Further reliability analysis and testing may be necessary to mitigate the risk.
- **IV –** Existing technologies used in identical applications: Existing equipment that are already fielded in similar Naval applications and have relevant field data that demonstrate a proven failure rate. The equipment may be standard DON issue items or COTS items with a proven failure rate in the same application that it is intended to be used. These items or systems represent a low reliability risk. Further reliability analysis and testing may not be necessary to mitigate the risk.

Hardware Reliability Prediction

As per Cybersecurity and Information Systems Information Analysis Center (CSIAC)'s final technical presentation titled "Managing Life Modeling Knowledgebase for the Naval Air Systems Command" [Ref 35], hardware reliability prediction methods can be broken down into two basic categories: statistically based empirical methods and deterministically based physics-of-failure methods. Additionally, field data on predecessor systems is often used to predict reliability for new products. It is important to understand the reliability prediction methodology used, the strengths and weakness of each methodology, and the applicability to the program.

Statistically based empirical reliability prediction methods:

- Predict failure frequency caused by randomly occurring failures during any period of a system's useful life and
- Consider failures caused by manufacturing defects, component variabilities, and customer use variations.

The underlying assumption with use of empirical methods is that all life limiting failure mechanisms far exceed useful operating life of the system, leaving only latent manufacturing defects, component variability and manufacturing defects, component variability and misapplication to cause field failure. Examples include MIL-HDBK-217, MIL-HDBK-217Plus, and Telcordia, etc.

The R&ME practitioner needs to recognize that these statistically based "piece-part" predictions (especially such as MIL-HDBK-217 [Ref 34]) can provide for good relative assessment across differing contractor designs, but will not accurately depict field performance.

Physics-of-failure methods are used to:

- Predict when single specific failure mechanism will occur for an individual component due to wear out; and
- Analyze numerous potential failure mechanisms (e.g., electromigration, solder joint cracking, die bond adhesion, etc.) to evaluate the possibility of device wear out within useful life of the system.

The physics of failure process requires detailed knowledge of all device material characteristics, geometries, and applications which may be unavailable to system designers, or which may be proprietary.

Software Reliability Prediction

Software reliability is often referred to as software maturity. The IEEE 1633-2016 "Recommended Practice on Software Reliability" [Ref 36] defines software reliability in two ways:

- The probability that software will not cause the failure of a system for a specified time under specified conditions.
- The ability of a program to perform a required function under stated conditions for a stated period of time.

There are different models and methods for software reliability predictions. The IEEE 1633-2016 [Ref 36] defines the software reliability engineering (SRE) processes, prediction models, growth models, tools, and practices. The document identifies methods, equations, and criteria for quantitatively assessing the reliability of a software or firmware subsystem or product.

Refer to **Chapter 6** for more detail on software reliability.

System Reliability Predictions

System reliability predictions are obtained by determining the R&M of the lowest system level item and proceeding through intermediate levels, until an estimate of system performance is obtained. There are various formal prediction procedures and software-based tools based on theoretical and statistical concepts.

When reviewing or conducting design analysis predictions, it is important to understand the data sources (e.g., MIL-HDBK or like or similar system), ensure failure rates used are appropriate for the design and design environment, and note the associated risks of prediction methodology.

P. PREPARE OR UPDATE FAILURE DEFINITIONS AND SCORING CRITERIA

Multiple or ambiguous failure definitions and scoring criteria (FD/SCs) are a major cause of unsatisfactory ratings in operational test reports. Clear, unequivocal definitions of failures 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 clearly defined scoring criteria and a contractual framework acceptable to the program manager, T&E, and the contractor for the proper accounting of failures against the various operational and contractual R&M metrics. For the contractual R&M metrics, the contract should clearly state agreed failure definitions and specify any conditions under which faults are not the contractor's liability such as battle damage, operations outside agreed upon limits, and user negligence. For warfighter operational R&M metrics, FD/SCs are addressed in the TEMP or R&M T&E Charter or the Government R&ME Program Plan as agreed to by the Developmental Test and Operational Test activities. FD/SCs should be consistent for all systems installed on a platform or integrated together.

- The FD/SC is considered a living document, in that failure definitions may be refined as system design is matured. Changes to FD/SCs may result from an increased understanding of how the system executes mission functions and should not be used to change the requirement, severity, or timelines for meeting those functions. Instability in failure definitions leads to drastically varying reliability and maintainability measurements.
- The FD/SC should be agreed to by all parties involved. Disagreements must be elevated and resolved within the DON. The cognizant Operational Test Agency (OTA), Operational T&E Force (COTF), Marine Corps Operational T&E Agency (MCOTEA) action officer who chairs the Reliability and Maintainability Scoring Board

for the Operational Test and Evaluation and the program chief engineer, ship design manager (SDM) or systems integration manager (SIM) should assure that only one FD/SC is used.

- All time or cycle parameters used should be clearly defined. For example, time parameters must clarify or differentiate between flight hours versus operating hours, or operating hours versus power on or standby hours. Any terms specifically defined in the contract that are inconsistent with the FD/SC should be noted.
- Mission essential, mission critical, mission specific, system critical, safety critical and self-protection/defense functions are all critical parameters to be addressed in the FD/SC. The system operations necessary to maintain those functions should be identified, so failures and severity can be tied back to mission function.

Q. PERFORM OR UPDATE FMECA

FMECA is a systematic and proactive analysis conducted to identify and assess potential system failure modes on system performance. The FMECA can be used to rank potential failure modes based the severity and likelihood of failures. FMECA is typically a joint effort between design and R&M engineering. The results are used by design engineers to improve the design by addressing the most frequently occurring failure modes and failure modes having the most serious effects, particularly single points failure which directly result in mission failure or create unsafe conditions. FMECAs can also be used to determine how each failure is detected and whether the BIT and diagnostics need to be improved. Final FMECA results are also provided to logistics to develop test equipment requirements and maintenance planning basis. They are the starting point for Reliability Centered Maintenance analyses. System Safety uses the results of the FMECA for System Risk and Hazard Assessments.

There are several different types of FMECAs, including design, process, and software. Design FMECAs evaluate system design to identify failure modes. Process FMECAs evaluate manufacturing process to identify potential issues. Software FMECAs evaluate failure modes in software design and hardware software interface.

Design FMECAs can be conducted in a bottom-up or a top-down approach. In the more common bottom-up approach, each component's failure modes are considered individually. When all components are assessed the FMECA is complete. The top-down approach can be used in early design before the system architecture is defined. The top-down approach analyzes functions and how they may fail and effect system performance.

Many different Government and industry standards and guidelines address the FMECA process, elements, and typical ground rules and assumptions. MIL-STD-1629 [Ref 37], although cancelled, is one of the most used guides. The FMECA is not a one-time analysis but should be updated throughout the life of the system. It should be updated during test and sustainment to incorporate failure modes that were not foreseen, to update failure rates for each failure mode, and to ensure detection methodologies are accurate. These updates should be coordinated with Reliability Centered Maintenance (RCM), System Safety, and Logistics to ensure their planning efforts are updated as necessary.

For more information, refer to DI-SESS-81495B, "Failure Modes, Effects, and Criticality Analysis" [Ref 38] and DI-SESS-82495, "Model-Based Engineering Failure Modes, Effects, and Criticality Analysis Profile (SYSML Version)" [Ref 39].

Reliability Critical Items

Based on the FMECA, a reliability critical items analysis is performed to identify those components/subsystems that require exercise of special care and control because of usual or exceptional risk and to develop the special program controls necessary to mitigate risk. Through review of design and R&M analysis information, identify those items that for reasons of complexity, criticality, application of advanced state-of-the-art techniques, or other special R&M risk require special controls to mitigate risks. Develop those special controls and implement them in the conduct of the program. Those controls may include such things as special oversight over subcontracts, special testing, special design analyses, special attention to failure tracking, analysis, and corrective action development, and any number of things to assure achievement of R&M objectives and control risks.

For more information, refer to DI-SESS-80685A, "Reliability Critical Items List" [Ref 40].

FRACAS

A disciplined and aggressive closed loop FRACAS is an essential element in the early and sustained achievement of the R&ME required in military systems. It is the key requirement for a Reliability Growth Program. The essence of a closed loop FRACAS is that failures and faults of both hardware and software are formally reported, analysis is performed to the extent that the failure cause is understood, and positive corrective actions are identified, implemented, and verified to prevent further recurrence of the failure. The basis of FRACAS is further discussed and defined in MIL-HDBK-2155, "Failure Reporting, Analysis, and Corrective Action Taken" [Ref 41].

Additionally, DoDI 5000.88 [Ref 16] requires that each program implement a FRACAS, maintained through design, development, test, production, and sustainment.

For more information, refer to DI-SESS-81927, "Failure Analysis and Corrective Action Report (FACAR) (Navy)" [Ref 42].

R. PROVIDE R&ME DESIGN SUPPORT

Evaluate adequacy of the contractor's design analysis, critical area investigations, problem diagnosis, and corrective action. As part of its systems engineering function, the contractor should apply R&M engineering principles in each step of design. The contractor usually establishes these principles in its design guidelines and company policies on items such as design margins and parts derating. Evaluation of contractor effectiveness in achieving the desired level of R&ME design integration should determine the degree to which the contractor's design activity is receiving (and responding to) design guidance from the R&M engineering staff.

Evaluate contractor R&ME performance in the following areas:

- Worse Case Analysis
- Sneak Circuit Analysis
- Design Margin
- Failure and Repair Distributions
- Parts and Materials Application
- Design Dos and Don'ts
- Use of Redundancy
- Design Verification
- Statistical and Mathematical Data Sources
- Heat Dissipation
- Sensitivity Analysis
- Derating
- Protection Measures
- Stress versus Strength and Wear Out Analysis
- Parts Selection

For more information, refer to MIL-HDBK-338B [Ref 31].

S. PERFORM DESIGN TRADE-OFF STUDIES

The use of trade studies is another essential and critical element of a successful R&ME program that the R&M engineer needs to address. It must be remembered that the contractor's management, and to some extent, the Program Manager, are primarily concerned with their research and development (R&D) and production costs. From an R&ME standpoint, all trade studies must be based on total life cycle costs, not just R&D and production costs. Keep in mind that what may appear to be big nonrecurring costs, looking at just the R&D and production costs, are usually insignificant when compared to operation and maintenance costs to the Navy to support a less reliable piece of equipment for the next twenty years. Trade studies are used to evaluate techniques, methods, systems, concepts, and policies in terms of cost and effectiveness to optimize the design and development of a system during the acquisition process. They should result in a study of design, testing, and production alternatives culminating in a selection that best balances need against what is realistically achievable. They should also provide a method for concentrating on risk reduction areas such as design simplification, ease of factory and Fleet test, and compatibility with production processes. In addition, they need to provide a method for evaluating concepts representing new technology or new processes prior to the beginning of the system development and demonstration phases. The R&M engineer should make sure that all trade studies assess each design concept for its producibility. The contractor has a corporate design policy and process to ensure that design trade-off studies continue throughout the system development and demonstration phases. The contractor also has procedures that establish a specific schedule, identifies individuals responsible, and defines proper levels of reporting trade study results, and all trade studies identify the relative risks of all options associated with the use of new technology.

Some of the most common trade study types include:

- **General Trade Studies**
  - Identify and execute trade-offs among requirements, design, schedule, and cost.
  - Support decision needs of system engineering process.
  - Level of study commensurate with cost, schedule, performance, and risk impact.
- **Requirements Analysis Trade Studies**
  - Establish alternative performance and functional requirements.
  - Resolve conflicts between requirements.
- **Functional Analysis/Allocation Trade Studies**
  - Support functional analysis and allocation.
  - Determine preferred set of requirements for function interface.
  - Determine requirements for lower-level functions.
  - Evaluate alternative architectures.
- **Synthesis Trade Studies**
  - Establish system/critical item configurations.
  - Assist in selecting system concepts and design.
  - Select Hardware/software, make or by, examined proposal changes, etc.
- **System/Cost Effectiveness Analysis**
  - Develop measures of effectiveness hierarchy.
  - Identify critical measures of effectiveness as technical performance measures.

T. CONDUCT GROWTH AND DESIGN VERIFICATION TESTS

The Government and contractor's T&E activities begin to provide a source of in-process R&ME review data in the TMRR phase. The activities usually consist of design verification tests called for under the contract as appropriate to evaluate known critical technology areas, assess prototype characteristics in the proposed design. R&ME tests may be called for as a component of technology studies and other technology demonstrations during the TMRR phase.

Design verification and/or risk reduction tests should be performed whenever there is reasonable doubt as to the adequacy or validity of analytical results related to a critical (high-risk) area of design.

Perform Subsystem Tests

A typical contractor test program consists of several basic tests that have complementary objectives. Specific R&ME-led tests (e.g., HALT, Reliability Development Growth Test (RDGT), subsystem/equipment BIT assessments) generally fall under design verification tests. The broad objectives of these tests are to detect unforeseen failure modes for correction, verify or revise predicted failure rates, verify equipment BIT performance capabilities, and evaluate equipment conformance to specification requirements under specified conditions. These design development tests focus on R&ME improvements.

All failures during contractor subsystem tests, and later during production and deployment, should be recorded in the FRACAS. The contractor should flow FRACAS requirements to subcontractors and vendors to ensure failures are recorded, analyzed, and corrected. A regular failure review board should be held jointly with the contractor to review contractor failure analysis reports and evaluate the depth to which failure diagnosis has been probed for cause-and-effect relationships, and failure modes and mechanisms.

It is important to note that many times, these R&ME specific tests are cancelled due to test asset shortages, schedule constraints, or financial issues. **It is imperative that these tests be conducted.** All these subsystem level tests allow for early identification of design issues, which are much less expensive to repair during EMD than in production and sustainment. Additionally, if these tests are cancelled, the equipment R&ME design will be matured in the Fleet causing additional burden on the maintainers, increased costs, and decreased system availability. These risks should be captured by the contractor risk process and rolled up into the program risk assessment.

Perform System Test

System tests are used to determine acceptability of the design for release to production, for example, to verify the conformance to JCIDS and contractual specification requirements. The TEMP is the governing document. There are two types of system tests, Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E). In general, DT&E activities support data generation for independent evaluations. They also provide program engineers and decision-makers with information to measure progress, identify problems, characterize system capabilities and limitations, and manage technical and programmatic risks. PMs use DT&E activities to manage and reduce risks during development, verify that products are compliant with contractual and technical requirements, prepare for OT&E, and inform decision-makers throughout the program life cycle. DT&E results verify exit criteria to ensure adequate progress before investment commitments or initiation of phases of the program, and as the basis for contract incentives. During DT&E, the R&ME team reports on the program's progress to plan for reliability growth and assess R&M performance to the JCIDS and contractual requirements for use during milestone decisions.

It is imperative that the R&ME team collects all appropriate data to conduct analyses. During system testing, all maintenance tasks should be monitored to ensure technical publication adequacy and maintenance documentation accuracy. All data related to each maintenance action should be recorded for analysis against JCIDS and contractual requirements. This data will be recorded in the FRACAS/maintenance data collection system and reviewed and scored as part of the R&M Review Board (RMRB) or Joint Reliability and Maintainability Evaluation Team (JRMET). The FD/SC will be used to score the data and calculate metric values against appropriate specification requirements and CDD thresholds. The R&ME team should coordinate with OTAs to ensure that data collection, R&M monitoring, and FD/SC processes are compatible with processes of both OTAs and program offices to evaluate contractual and operational R&M performance and suitability characteristics.

System tests to demonstrate R&M and BIT include the maintainability demonstration, the system BIT demonstration, and the system R&M assessment:

- **Maintainability Demonstration** – This demonstration is used to assess maintainability critical areas, verify conformance of system installation with maintainability requirements and maintenance concept, and identify installation interface problems for correction and evaluate field installable software patches to demonstrate that the system can be patched and returned to operational status. Although canceled, MIL-STD-471A [Ref 43] provides detailed information on planning and execution of a Maintenance Demonstration. Another useful document is the "Maintainability Program Standard Implementation Guide," dated 24 May 2011 [Ref 44].
- **System BIT Demonstration** – The system-level BIT demonstration should be conducted with sufficient time before Government system testing in order to incorporate any corrective actions discovered as a result of this demonstration. The system-level BIT demonstration should be used to verify the adequacy of all BIT fault recording, reporting, and display functions for both the operator and the maintainer. This may be more practical to conduct in a System Integration Lab than on the test vehicle (aircraft, ship, etc.).
- **System R&M Assessment** – During system testing, it is essential to evaluate the R&M capabilities of the system to determine if there are any design problems that were not

discovered during laboratory testing and development work and to establish effective corrective actions to eliminate these problems. During all system tests, maintenance tasks should be conducted by maintenance personnel of the same type, number, and skill level to perform maintenance on the system during the operational phase in the field.

The Initial Operational Test and Evaluation (IOT&E) is conducted on production, or production representative articles, to determine whether systems are operationally effective and suitable for intended use by representative users to support the decision to proceed beyond Low Rate Initial Production (LRIP). OT&E is a fielded test, under realistic combat conditions, for an MDAP of any item or component of a weapons system, equipment, or munitions for the purposes of determining its operational effectiveness and operational suitability for combat. OT&E is conducted by independent operational testers. Operational testing of an MDAP may not be conducted until the Director of Operational Test and Evaluation approves the adequacy of test plans for OT&E to be conducted in connection with that program. Additionally, the director analyzes results of the OT&E conducted for each MDAP. At the conclusion of such testing, the Director should prepare a report for the Secretary of Defense stating completeness or incompleteness of the test.

OT&E activities continue after the FRP decision in the form of FOT&E. FOT&E verifies the operational effectiveness and suitability of the production system, determines whether deficiencies identified during IOT&E have been corrected, and evaluates areas not tested during IOT&E due to system limitations. Additional FOT&E may be conducted over the life of the system to refine doctrine, tactics, techniques, and training programs and to evaluate future increments, modifications, and upgrades.

U. PRODUCTION PLANNING

The R&M engineer / analyst needs to ensure the systems continue to meet operational thresholds but also ensure there is no unacceptable degradation of design characteristics that would present a risk to meeting operational thresholds due to Fleet environment or manufacturing changes.

- **Environmental Stress Screening (ESS) / Burn-in** – ESS or Burn-in is conducted to ensure infant mortality, workmanship defect, and other nonconformance anomalies can be identified and removed from equipment prior to delivery. MIL-STD-785B, "Task 301: Environmental Stress Screening (ESS)," [Ref 45], MIL-HDBK-2164 [Ref 46], and NAVMAT P-9492 [Ref 47] provide more information in regard to ESS / burn-in.
- **Production Reliability Acceptance Testing (PRAT)** – PRAT is conducted to detect any inherent degradation in a product's reliability over the course of production caused by tooling, manufacturing processes, workflow, parts quality, etc. MIL-STD-

785B (cancelled), "Task 304: Production Reliability acceptance Test (PRAT) Program" [Ref 45] provides more information regarding PRAT.

V. FLEET R&M DATA ANALYSIS

The R&M engineers should maintain sustained surveillance of the fielded systems to ensure the continued R&M performance, identify any R&M performance degradation, and monitor system degraders.

In order to accomplish this task, the R&M engineer should ensure the proper processes and procedures are in place to obtain the data necessary to assess the system R&M performance, identify poor performing systems, sub-systems, or components, and conduct root cause analyses. These tasks require access to organic usage, failure, maintenance, and health management data. Additionally, supplier and original equipment manufacturer (OEM) maintenance and repair data is needed. When issues are identified, the R&M engineer along with the systems and design engineers will coordinate on determining the root cause and the corrective actions needed to eliminate of minimize the failure mode occurrence. The R&M engineer will then contribute to the Business Case Analysis (BCA) by determining the R&M improvement benefits to the product reliability and maintainability performance. Once the corrective action is identified, the R&M engineer will continue to monitor the system performance to ensure the corrective action was effective. A funded FRACAS is required for a fully effective sustainment R&M program. At a minimum, the OEM and Organic I-level and Depot level repair data is needed.

All data and analyses are coordinated with logistics and engineer. The identification or new failure modes or BIT design deficiencies may result in maintenance planning changes. In a future iteration of this guidebook, R&ME interactions with Condition Based Management Plus (CBM+) efforts will be included.

W. ENGINEERING CHANGE PROPOSALS

An Engineering Change Proposal (ECP) is the management tool used to propose a configuration change to a configuration item (CI) and its Government-baselined performance requirements and configuration documentation during acquisition (and during post-acquisition if the Government is the Current Document Change Authority (CDCA) for the configuration documentation). The LSE should notify the assigned R&M engineer of all ECPs. The R&M engineer should develop quantified reliability and/or maintainability values for all proposed engineering changes within the trade space. Final down select would depend on many variables, and the LSE should consider reliability and maintainability for this decision. Some ECPs may be complex enough to require a focused R&M evaluation.

X. LIFE CYCLE SUSTAINMENT PLAN

The LCSP is the primary program management reference governing operations and support planning and execution from program inception to disposal.

R&M engineers assist the PSM to ensure that the LCSP evolves in tandem with the SEP, to ensure that JCIDS sustainment capabilities are designed into the system and integral to systems performance. Specifically, the R&M engineer contributes to the Design Interface and Sustaining Engineering portions of the LCSP.

Y. INDEPENDENT LOGISTICS ASSESSMENT

The Independent Logistics Assessment (ILA) is conducted for major weapon systems before key acquisition decision points, including Milestones B and C and the full rate production decision. The purpose of the ILA is to assess the sustainment strategy's adequacy and to identify sustainment cost elements, factors, risks, and gaps that are likely to drive future O&S cost. The PSM leads the ILA effort. The R&M engineer supports the completion of the ILAs and identifies risks associated with R&ME shortcomings.

Figure 11 is an overview of the DON's Two-Pass Seven-Gate Review process. The goal of the Two-Pass Seven-Gate Governance procedures is to ensure alignment between Service-generated capability requirements and systems acquisition, while improving senior leadership decision-making through better understanding of risks and costs throughout a program's entire development cycle. The following paragraphs discuss the R&ME objectives throughout the phases of acquisition life cycle.

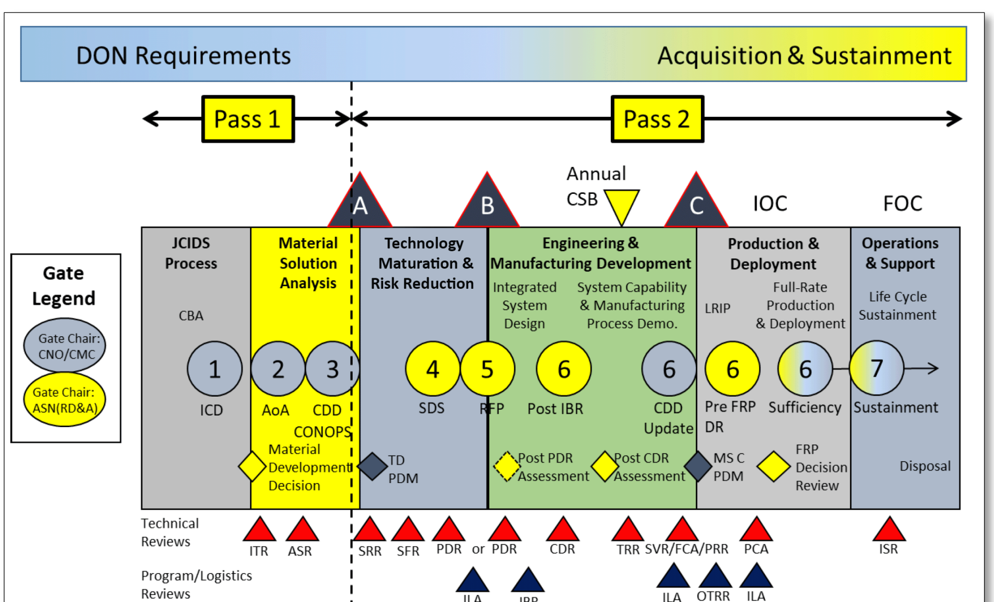


Figure 11: Two-Pass Seven-Gate Review[7]

[7] From SECNAV Instruction 5000.2G [Ref 4].

A. Materiel Solution Analysis

The R&ME objectives during the Materiel Solution Analysis (MSA) phase are to ensure that materiel development efforts include actions to identify and reduce risk of the proposed solutions. The MSA R&ME effort seeks to understand and mitigate the operational and maintenance impacts of any R&ME associated risks.

MILESTONE A REVIEW

The Milestone A (MS A) review should look for inconsistencies that may be visible with the proposed solution in an integrated, system oriented, program wide view. The following documents should be evaluated for adequacy of R&ME requirements and provisions:

- R&ME Program Planning Document(s)
- R&ME portions of the system specification(s) or Requirements Document
- MSA phase R&ME Reports
- R&ME T&E Planning
- R&ME RFP documentation (Specification, Statement of Work, Contract data requirements list (CDRLs), Section L and M, H Clauses)
- Program documentation such as Acquisition Strategy, SEP, RAM—C, TEMP, and LCSP

B. Technology Maturation and Risk Reduction

During the Technology Maturation and Risk Reduction (TMRR) phase, requirements are transformed into practical design criteria suitable for system development. System configuration begins to take shape in the form of design drawings and specifications for major components of the system. Functional requirements are allocated to lower tier components such that when recombined in the integrated system they will satisfy requirements defined in the functional baseline specification. Objectives of the TMRR phase are essentially twofold:

- Develop and verify adequacy of the allocated design for the system with respect to operational effectiveness and suitability, logistics supportability, and life cycle costs.
- Develop the allocated baseline (if the program completes a successful Preliminary Design Review (PDR) in this phase) and contract for the EMD phase, by which the preliminary design can be transformed into engineering hardware and software for test and evaluation. If the contract overlaps the EMD and subsequent phases, the data and contract should also satisfy those subsequent phases.

The following data should be available for the in-process review of R&ME analyses results during the TMRR phase:

- By SRR:
  - Preliminary environmental studies.
  - R&M block diagrams, allocations, and predictions for major system and subsystems.
  - A reliability growth-planning curve is developed and included in the SEP.
- By SFR:
  - R&ME Specification – Approved specification R&ME requirements reflecting functional baseline.
  - The OMS/MP definition (provided by the Government) is used by the contractor to provide the following:
    - Mission objectives, including what, when, and where a function is to be accomplished.
    - Constraints that affect the way objectives are to be accomplished (e.g., launch platform, design ground-rules for various flight conditions).
    - Time scale of system-level functions to accomplish the mission objectives.
  - BIT functional requirements allocated for operations and maintenance to the functional baselines and are supported by maintainer use-case analysis.
  - System architecture contains required BIT functionality.
- By PDR:
  - Design derating guide and criteria.
  - Final environmental studies.
  - R&M block diagrams, allocations, and predictions to subsystem and unit levels.
  - Current, approved version of allocated baseline R&M requirements.
  - Preliminary functional FMECA with supporting software FMEAs to the subsystem and unit that addresses 100 percent of functions and preliminary Critical Items list.

MILESTONE B REVIEW

The MS B review at the conclusion of the TMRR phase requires an R&ME assessment to provide the data necessary for an evaluation of R&M conformance to requirements in system specification. The PDR, the final systems engineering design review before entering EMD, signifies completion of all assigned activities in the TMRR phase. It verifies the acceptability of activity results as a basis for a decision to proceed into EMD.

The contractor's prediction analyses, test results, problem evaluations, and root failure cause/categorization (by which the detail design has been guided) are verified analytically. The Government review team evaluates the program's progress and effectiveness in correcting deficiencies noted in the earlier assessments, and evaluates the status of any remaining R&ME problems. The team evaluates the seriousness of problems to determine whether correction should be required before release of the design for development and manufacture. R&M requirements and provisions defined by the contractor in the proposed follow-on contract data package are critically reviewed to determine compliance with contract requirements (e.g., R&ME plans, specifications, reliability growth plans, test and evaluation plans, demonstration acceptance criteria and procedures, data requirements, and contract work statement).

C. Engineering Manufacturing and Development

The purpose of the Engineering Manufacturing and Development (EMD) phase is to develop, build, test, and evaluate a materiel solution to verify that all operational and implied requirements, including those for security, have been met, and to support production, deployment and sustainment decisions. The core R&ME activities to be addressed in this phase in approximate chronological order include:

- Describe in the SEP the R&ME program for monitoring and evaluating contractor, subcontractor, and supplier conformance to contractual R&M requirements.
- Conduct design reviews, R&ME assessments, and problem evaluations at scheduled milestones. Assign and follow up on action items to correct noted deficiencies and discrepancies.
- Conduct a CDR to ensure that the product baseline design and required testing can meet R&M requirements, the final FMECA identifies any failure modes that could result in personnel injury and/or mission loss, and detailed prediction to assess system potential to meet design requirements is complete.
- Perform specified development, qualification, demonstration, and acceptance tests to show conformance to contractual R&M requirements and assess the readiness to enter system-level reliability growth testing at or above the initial reliability

established in the reliability growth curve in the TEMP. Verify the adequacy of corrective action taken to correct design deficiencies.

- Ensure the Software Development Plan (SDP) and TEMP include software test methods to identify and correct software failures and that there is a high degree of confidence the system can be recovered from any software failures that may occur after fielding.
- Implement a FRACAS to ensure feedback of failure data during test to design for corrective actions. Provide a data collection system for data storage and retrieval suitable for R&M tracking analysis and assessment.
- Coordinate with OTAs to ensure that data collection, R&M monitoring, and failure definition and scoring processes are compatible with the processes of both the OTA and the program office to evaluate contractual and operational R&M performance and suitability characteristics.
- Ensure the configuration control program includes the total life cycle impact (including R&M) of proposed changes, deviations, and waivers. Ensure the systematic evaluation, coordination, timely approval or disapproval, and implementation of approved changes.
- Apply and evaluate allocation and prediction analyses using latest test data to identify potential R&M problem areas.
- Prepare initial production release documentation to ensure adequate R&M engineering activities in production test plans, detailed drawings, procurement specifications, and contract SOW. Ensure that documentation provides adequate consideration of R&ME in re-procurements, spares, and repair parts.

When the program has accomplished the objectives of the EMD phase and the system has demonstrated adequate progress toward achieving the contractual requirements, the MDA convenes a milestone review or its equivalent to consider approval for commitment of resources for initial production and deployment. Although system-level R&M requirements may have been achieved, subsystem and Component R&M failing their individual R&M requirements can affect logistics, support equipment, and manpower.

Engineering and Manufacturing Development Results

- Conformance to specified R&M requirements and maintenance concept verified by appropriate demonstration and test.
- R&M requirements and control procedures defined in production release documentation.

MILESTONE C REVIEW

Milestone C is the point at which a program is reviewed for entrance into the Production and Deployment Phase.

R&M Assessment for Milestone C

The primary criteria are:

- Applicable R&M tests satisfy conformance to quantitative R&M criteria.
- Government system test and evaluation verifies the suitability of R&M technical characteristics for the intended application.

These tests provide the data for a comprehensive R&M assessment of the production-representative article design and provide the basis for a low rate initial production (LRIP) release decision. Demonstrated R&M characteristics are compared with specified requirements in product baseline specifications.

The final review of R&M achievements in the EMD phase (performed just prior to the scheduled milestone) is intended to verify fulfillment of specified requirements and to ensure that the production release data package is adequate for proceeding to production.

The following data is generally required at this review point:

- **R&M Analysis Reports –** Final EMD phase R&M analysis reports.
- **System Specifications –** Updated product baseline specifications.
- **Integrated Test Plans –** Proposed integrated test plan for R&M in the Production and Deployment (P&D) phase.
- **R&M Program Plans –** Contractor-proposed R&M plans for the P&D phase.
- **Proposed Contract Work Statement –** Activities for achievement, monitoring, and control of R&M in the P&D phase.
- **Data Requirements Exhibit –** R&M contract data requirements and corresponding DIDs.
- **Program Documentation –** Program documentation such as the SEP, TEMP, and AS.

R&M Recommendation

On the basis of the review, make recommendations (with justification) for disposition of the program by one of the following alternatives:

- **Proceed into P&D –** Production-representative article has demonstrated conformance to specified R&M requirements and has been determined suitable by Government system test, with minor exceptions, if any.

- **Extend the EMD phase to correct deficiencies –** Production-representative article design fails by significant margin to satisfy R&M requirements; or the documentation package is seriously inadequate. The design and data package should be corrected and verified by test, including a reevaluation of the design documentation.

Production and Deployment Phase

The production-representative design is translated into a production system in accordance with the production release documentation developed during the EMD phase. The P&D phase may be initiated by a LRIP to provide additional assets for test and evaluation. At the conclusion of LRIP, a Full Rate Production (FRP) decision is made. If successful, the FRP program is implemented for procurement of quantities required for deployment. The R&M objectives of the P&D phase are as follows:

- Consistently manufacture, and deliver to operational forces, equipment and systems that meet the R&M thresholds specified in the CDD update, formerly CPD.
- Deliver technical data, support equipment, operating and maintenance instructions, etc., required for system operation and maintenance in the field.
- Provide required quantities, of specified quality and in correct proportions, of maintenance spares, repair parts, contractor augmented support, operating and maintenance manuals, trained personnel, etc., to achieve and sustain specified CDD Update thresholds.
- Update R&M predictions and FMECAs based on production tests, demonstration tests, operational evaluation, and field results and apply to models previously developed to assess maintenance procedures, spares, manpower, packaging design, test equipment, and other mission and logistics impacts.
- Continue to implement a FRACAS by maintaining surveillance of systems in the field through a maintenance data collection system to correct problems in the operational environment.

Operations and Support Phase

The Operations and Support (O&S) phase of a system begins with its introduction to service use and ends with its retirement from use. The period of useful service can range from a few years to several decades depending on the practicability and desirability of updating the design and support structure to satisfy changing requirements or to incorporate improvements made possible by technological advances.

Typically, a system begins its introductory period of service use under the surveillance and with the augmented support of the production contractor. During this period, the production contractor is required, by reference to appropriate contract tasks, to identify and investigate inherent design and manufacturing process-related problems and to submit recommendations for their correction. Corrections or improvements are then introduced as engineering changes in follow-on production systems and may be retrofitted on those systems already deployed.

Following completion of a successful introductory period, the Government continues monitoring the system's R&M performance and impact to effectiveness and logistics support by analyzing reports from maintenance data collection systems and other reporting systems. Problems are identified, corrected, and monitored on a continuing basis throughout the useful life of the system.

Objectives of the O&S phase are:

- In the field, the system consistently experiences the operational features and characteristics (including R&M) it achieved in development and maintained under control throughout production.
- Operational and maintenance documentation, training programs, spare and repair parts provisioning plans, and other features of the implemented logistics support plan are adequate to support the system in the field environment.
- Providing inputs to appropriate contractual documents including engineering change proposals and SOWs.

Sustainment Reviews

Sustainment Reviews (SRs) required for all active and in service covered weapon systems. SRs begin at five years after initial operational capability and repeat every five years thereafter. SRs end five years before a covered system's planned end of service date. The SRs will focus on statutory sustainment elements and track O&S cost growth. In support of the SR, the R&ME team will provide assessments of the systems fielded performance to the Sustainment KPP and KSAs.

4 | REQUIREMENTS DEVELOPMENT AND MANAGEMENT

SUSTAINMENT KPP

The Sustainment KPP and associated KSAs are translated into systems design and supportability requirements. They are used to influence system design, improve mission capability and availability, and decrease the logistics burden over a system's life cycle. Metrics ensure operational readiness, performance of assigned functions, and optimized operation and maintenance.

The sustainment KPP metric is used to determine if the system can be operated and maintained within the O&S cost goals. The sustainment KPP includes key supportability metrics used to develop the program's logistics footprint such that the system is sustainable during its operating life. By not adopting sustainment requirements, especially during the design phase, the logistics footprint will be insufficient to support the system resulting in the operational availability not meeting the warfighter's needs. Every program must consider sustainment during acquisition planning and develop requirements in accordance with Annex D to Appendix G to Enclosure B of the JCIDS Manual, Sustainment KPP Guide [Ref 10].

SECNAVINST 5000.2G [Ref 4] requires a Sustainment KPP for all CDDs (with inherent flexibility to allow a resource sponsor (user) to justify not including one.) The JCIDS Manual instructs that the Sustainment KPP (in addition to System Survivability, Force Protection, and Energy) must be addressed. The resource sponsor can address this by stating that the user requirement is not applicable; however, all systems have some attributes that are relevant to the Sustainment KPP.

The Sustainment KPP is comprised of several mandatory components: Materiel Availability and Operational Availability, and three mandatory KSAs: Reliability, Maintainability, and the O&S cost, as illustrated in **Figure 12**. Together these components provide Fleet-wide operational availability. The operational framework for the expected Materiel and Operational Availability must be clearly articulated during the AoA or similar studies and based on operational context in the validated ICD and/or OMS/MP. Assessment of capability requirements and performance metrics must consider the combination of the system being designed and its sustaining support infrastructure.

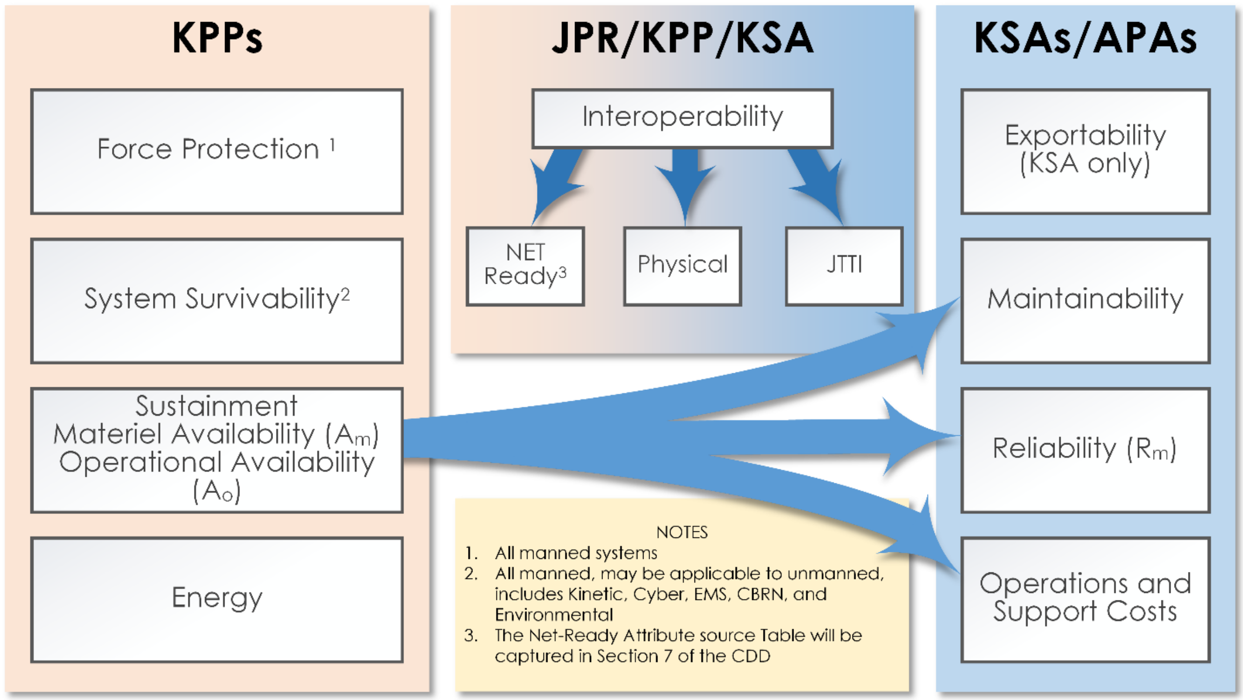


Figure 12: KPPs, KSAs, APAs

Sustainment KPP Requirements

In accordance with JCIDS, Sustainment KPP requirements shall consist of the following:

- **Materiel Availability (A_m) KPP** - Measure of the percentage of total inventory of a system operationally capable, based on materiel condition, of performing an assigned mission. This can be expressed mathematically as the number of operationally available end items divided by the total population. For single or small-quantity systems that are used intermittently, Materiel Availability can represent available time (i.e., Uptime, when the system is in operational status) as a percentage of total calendar time. Note: Materiel Availability is typically not applicable to Automated Information Systems (AIS).

$$Materiel\ Availability\ (A_m) = \frac{Quantity\ of\ Operationally\ Available\ End\ Items}{Quantity\ of\ Total\ Population\ of\ End\ Items}$$

- **Operational Availability (A_o) KPP** - Measure of the percentage of time that a system or group of systems within a unit are operationally capable of performing an assigned mission and can be expressed as:

$$Operational\ Availability\ (A_o) = \frac{Uptime}{Uptime + \ Downtime}$$

Determining the optimum value for Operational Availability requires a comprehensive analysis of the system and its planned CONOPS and/or OMS/MP, including the planned operating environment, operating tempo, reliability and maintenance concepts, and supply chain solutions.

Mandatory Attribute (KSA or APA) Requirements

In accordance with JCIDS, Mandatory Attribute (KSA or APA) requirements shall consist of the following:

- **Reliability Attribute** - Measure of the probability that the system will perform without failure over a specific interval, under specified conditions. Reliability shall be sufficient to support the warfighting capability requirements, within expected operating environments. Examples include a probability of completing a mission, a Mean Time Between Operational Mission Failures (MTBOMF) or A Mean Time Between Failures (MTBF). For AIS, a reliability attribute should not use traditional reliability metrics (e.g., MTBF, MTBCF). Subordinate attributes are:
  - ***Mission Reliability*** – Measure of the ability of an item to perform its required function for the duration of a specified mission profile, defined as the probability that the system will not fail to complete the mission, considering all possible redundant modes of operation.
  - ***Logistics Reliability*** – Measure of the ability of an item to operate without placing a demand on the logistics support structure for repair or adjustment, including all failures to the system and maintenance demand as a result of system operations.
- **Maintainability Attribute** – Measure of the ability of the system to be brought back to a readiness status and state of normal function. Subordinate attributes are:
  - ***Corrective Maintenance*** – Ability of the system to be brought back to a state of normal function or utility, at any level of repair, when using prescribed procedures and resources.
  - ***Maintenance Burden*** – Measure of the maintainability parameter related to item demand for maintenance manpower.
  - ***Built-in-Test (BIT)*** – An integral capability of the mission system or equipment which provides an automated test capability to detect, diagnose, or isolate failures.
- **Operations and Support Cost Attribute** - Provides balance to sustainment solution by ensuring that total O&S cost across the projected life cycle associated with availability and reliability are considered in making decisions. Note: Logistics Reliability is a fundamental component of O&S cost as well as Materiel Availability.

- **Logistics Footprint Attribute (Optional)** – Optional attribute is a useful metric for measuring materiel, mobility, and required space to effectively deploy, sustain, or move a weapon system. Incorporating Logistics Footprint in requirements drives design decisions that include actual usage limitations.

Note: *For complex systems and System of Systems (SoS), the Sustainment KPP and supporting Reliability attribute are to be applied to each major end item or configuration item, and whenever practical, to the system/SoS as a whole.*

The Government R&M engineer should assist the Resource Officer in establishing basic sustainment KPP and KSA/APA requirements for the AoA and ICD and numeric user sustainment KPP and KSA/APA requirements in the CDD. Per the JCIDS, the Resource Officer provides OMS/MP and architectural views to better define operational capability. If the Resource Officer decides not to include the Sustainment KPPs, the JCIDS should, at a minimum, provide sufficient readiness and mission capability information to enable acquisition R&M engineers to derive values for R&M metrics. These derived R&M metrics values will be documented in a Government performance specification and interface control documents and included in contract specifications.

The user (resource officer and operational tester), Systems Engineering, R&ME, and logistics managers must develop failure definitions and scoring criteria (FD/SC). The FD/SC provides a clear, unambiguous definition of what constitutes a failure (FD) and how each failure counts against the R&M metrics (SC). The FD/SC provides a means for problems to be identified as failures when they occur and identified as critical/non-critical/operator induced, or other necessary categories such that they can be scored properly against requirements.

FD/SC is placed into the TEMP to ensure that failures are properly identified during testing to score and report sustainment metrics. The definition of all categories of failures is important to reduce ambiguity in determining the performance of systems during all phases of testing. Finally, the FD/SC must be placed into the reliability and maintainability review board charter to ensure that the sustainment KPP is recorded and reported properly during systems engineering technical reviews, and that corrective action, which are most critical, are prioritized for the PM.

Only one set of operational FD/SC should be developed and maintained in accordance with the SECNAVINST 5000.2G [Ref 4]. FD/SCs should be consistent for all systems installed on a platform or integrated together as a SoS. The operational FD/FC may be supplemented for evaluating contract compliance with performance and interface specifications.

JCIDS requirements are to be developed by the Government during the AoA and validated against the warfighter's mission capability needs. The warfighter's Sustainment KPP requirements should be validated by a Government R&M engineer, logistics support manager and cost engineer for each program by performing and developing a Reliability, Availability and Maintainability – Cost (RAM-C) rationale study and report in accordance with the most recent DOD RAM-C Rationale Report guidance [Ref 21]. The R&M engineers should work with the PSM and cost engineers to balance the optimum sustainment cost with feasible and affordable reliability and maintainability requirements.

TRANSLATING AND ALLOCATING KPP AND KSA/APA REQUIREMENTS INTO CONTRACT SPECIFICATIONS

Warfighter (user) requirements cannot simply be placed directly on contract for a supplier or design activity to achieve. Warfighter (user) requirements must be translated into performance and interface specifications by the Government and allocated proportionally into contract specifications.

R&M performance specifications and interface control documents should be translated from the Sustainment KPP and associated attributes found in CDDs or user requirements documents, or the warfighters technical parameters detailed in **Chapter 5**. The translation accounts for differences between the operational environment and the acquisition environment. These differences are not statistical variations or confidence intervals but are, in part, attributed to the fact that the operational system includes more elements and more potential failures in the operating environment than the system under contract evaluated in a controlled environment. Government performance specifications and interface control documents and Contractor Design specifications account for components, processes, workmanship, integration, and environmental and usage factors. For these reasons, the contractual performance specifications and interface control documents should never be the same as warfighter (user) requirements values. As a result, contractual design specifications should never be the same as the warfighter (user) requirement values.

R&ME activities and technical requirements should be a part of all contracts, including performance-based contracts for design, development, and production of defense materiel.

Materiel Availability (A_m): The Availability KPPs are unique for each program and describe the total end items that are required to support the warfighter's needs. Materiel Availability must be translated into a total quantity of end items needed including any spares that will be needed given that some items will not be available for operational tasking due to training and research needs, as well as items that will be out of service for repair. Translating the Materiel Availability KPP into a total quantity requires the

Government to define peacetime as well as wartime surge requirements and forecast future anticipated development plans for the system. Failure to do so will result in falling short of meeting materiel availability requirements as mission capability matures.

Operational Availability (A_o): Placing A_o on contract requires that the Government clearly define an OMS/MP or operating profile for the system. An operating profile is needed to forecast environmental and operational usage rate of all of the components in the system such that preventive and corrective maintenance can be planned. The OMS/MP must contain an operating profile to describe the timing of events, functions, and environmental conditions that a system is expected to encounter during operational use and in support of each mission that the system will be capable of performing. The OMS/MP is used in conjunction with a reliability block diagram to predict when failures are expected to occur, when maintenance will be required and to calculate overall system reliability & maintainability metrics. The OMS/MPs operating profile provides the time that each component is expected to operate during a mission and the times that each component is expected to be idle or turned off. The timing of these events allows reliability predictions to be made normally through reliability modeling software. When a specific system supports multiple missions, the most stressing mission profile is used to make reliability and maintainability predictions; unless it is known how often each mission will occur over the systems life cycle. Operating profiles and the assumptions that are used to predict how often equipment is expected to operate are necessary in order to support the program design which is why the OMS/MP is so important to reliability engineers. Environmental profiles in the OMS/MP are also important as they may affect the failure rates of each component. More on performing reliability calculations can be found in the "DOD Guide for Achieving RAM" [Ref 48].

If an operating profile is not contained within the OMS/MP, then reliability engineers must extract and document this information from other sources such as the CONOPS and the LCSP. A system level OMS/MP is prepared by the Government and included in the system performance specification to allow the developer to understand expected usage rate of all of the functions to design for R&M. The acquisition R&M engineers must ensure a composite OMS/MP covering anticipated mission and environmental profiles is prepared to enable the derivation and evaluation of the design specifications. Failure to clearly define an OMS/MP will result in assumptions on the warfighter's usage requirements and may result in a system being down (even during an operational mission) more for maintenance than originally required and not meet the Operational Availability component of the Sustainment KPP.

Once the OMS/MP is complete, and the system's operating profile is defined in support of all mission areas, engineers must then document all functions which are mission critical/essential and which functions are not. Failure of any function can result in the system becoming non-mission capable, partially mission capable, or to remain fully mission capable. From these definitions, mission critical/essential functions can be defined, and placed into contract specifications, to allow developers to identify mission critical/essential items and deliver a critical items list. The critical items list will be used to ensure logistics support is properly planned for those components in terms of organizational, intermediate or depot level spares, and to properly plan organizational maintenance tasking.

The Government must then translate the user A_o requirement from Uptime and Downtime to something measurable for design and development and prior to fleet operations. In general, the interval of interest is calendar time, but this can be broken down into other intervals of active time and inactive time. Active time contains Uptime and Downtime, while inactive time can normally be considered neutral time or when the item is in storage or the supply pipeline. Uptime and Downtime in the A_o equation are intended to describe system operating and non-operating periods once deployed. Uptime is that element of active time during which an item is in condition to perform its required functions. Uptime may include time that the equipment is operating, in standby or off and downtime generally does not include time for preventive maintenance. Downtime is that element of active time during which an item is in an operational inventory but is not in condition to perform its required function.

Figures 13 and **14** show examples of Uptime and Downtime for a ship to provide guidance of how they must be tailored for continuously operated systems or intermittently operated systems. It is important to understand how A_o will be measured so that a translation to a procurement specification can be made.

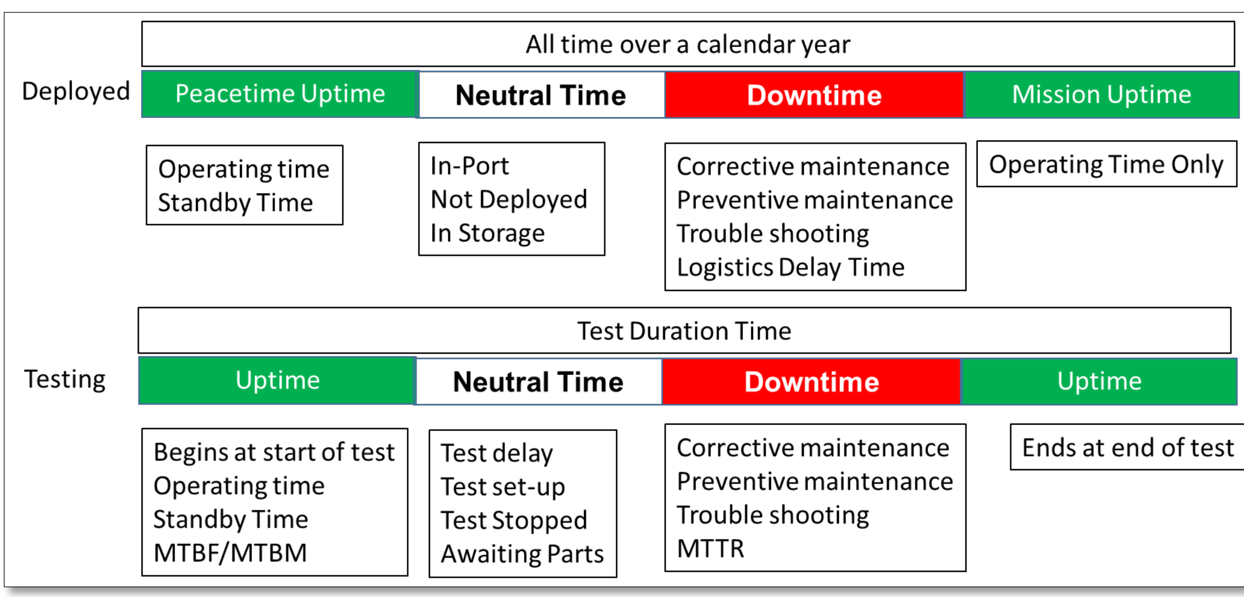


Figure 13: Operational Availability for Continuously Operating System

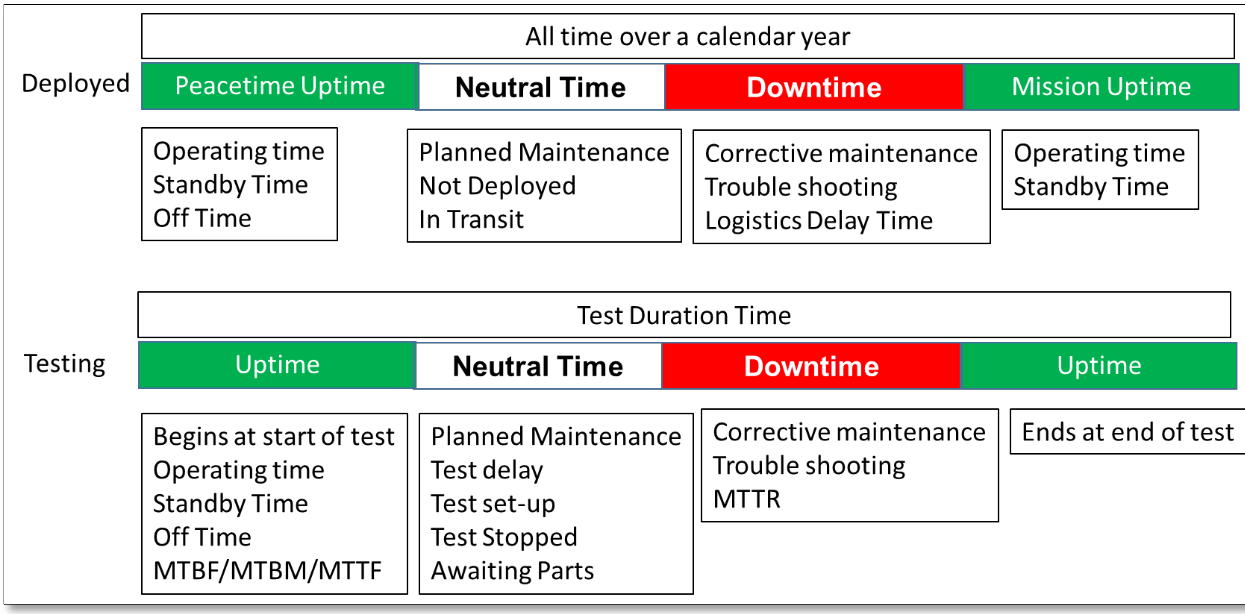


Figure 14: Operational Availability for Intermittently Operated System / One-shot System

Figure 15 shows examples of various operating and non-operating conditions that may be included in Uptime and Downtime definitions. Some programs may use neutral time to define periods of time that will not be included in either Uptime or Downtime and thus exclude these periods of time from the A_o definition. Inactive time may be considered neutral time when an item is in reserve and not in an operating state. Neutral time is used to eliminate specific periods of time over calendar time that will be excluded from the A_o equation and will not be counted as either Uptime or Downtime. Neutral time may be a weekend, or the time periods when repairs are halted due to holidays. Neutral time can account for time between operating periods when a system is intermittently operated or used only occasionally and thus availability does not apply over the entire calendar year. Neutral time can also be used during test events when testing is halted or stopped. Using neutral time makes a test event look more like an operational event because those periods of time when testing is halted are excluded from calendar time in the A_o equation. More on how Uptime and Downtime are used and affect the A_o equation can be found in MIL-HDBK-338B [Ref 31].

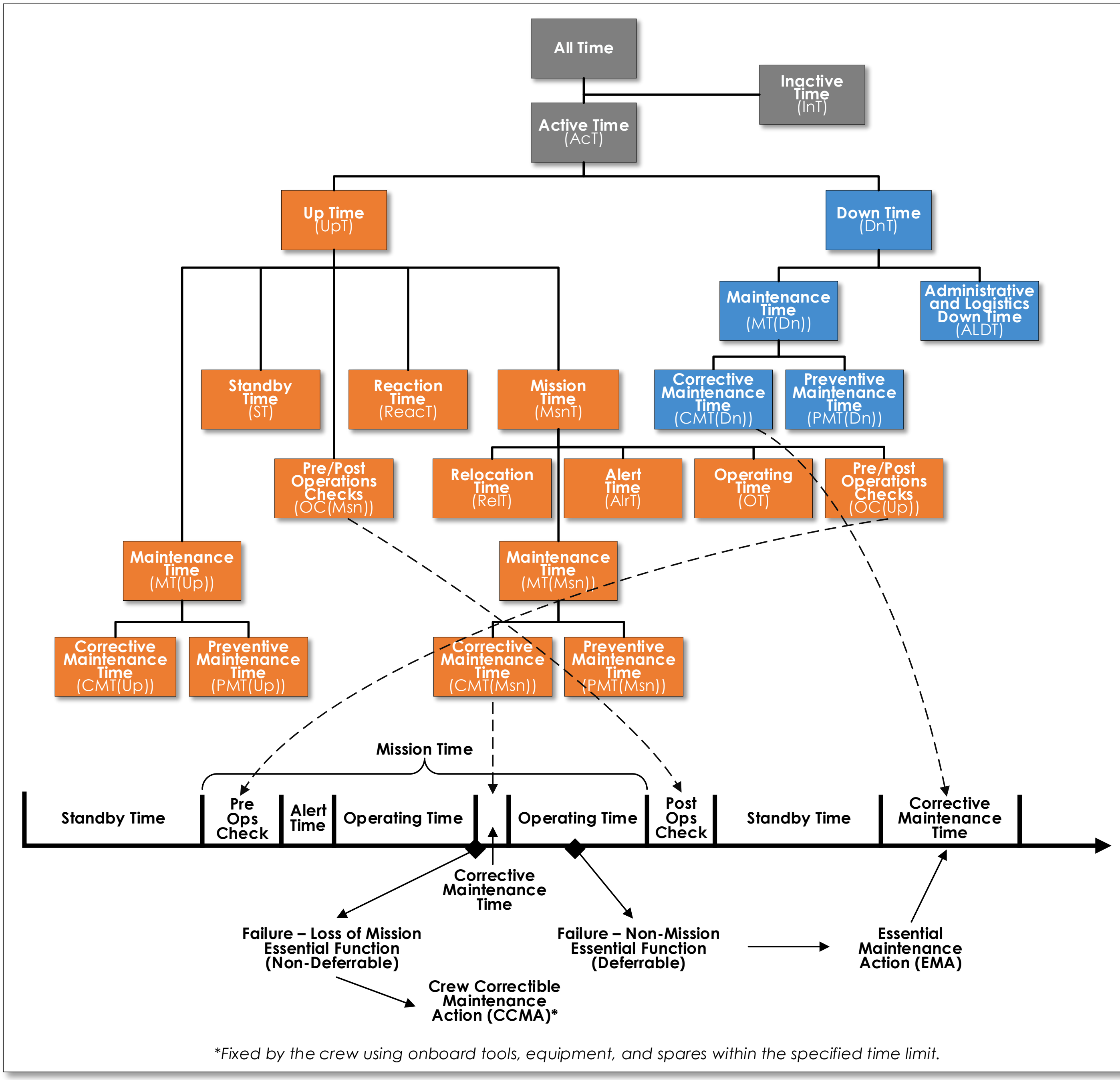


Figure 15: Examples of Uptime and Downtime Categories

In general, Inherent Availability (A_i) should be used in place of A_o when developing procurement specifications to estimate Uptime as the Mean Time Between Operational Mission Failure (MTBOMF), Mean time between failure (MTBF), Mean Time Between Maintenance (MTBM) or Mean Time To Failure (MTTF) depending on the system performance requirements. Downtime will need to be estimated during design and development through the Mean Time To Repair (MTTR) for hardware and software plus Mean Logistics Delay times for Logic's support such as waiting for parts or transit times. A_o

is an operational mission performance metric that cannot be demonstrated until fully deployed.

Absent careful attention to the Requirements process discipline, reliability may not be treated as a performance parameter and hence a design criteria. Consequently, the developer must use Logistics-based metrics to demonstrate the ability to achieve A_o. As shown in **Figure 16**, the solution is to focus on design-controllable MTBF and MTTR (A_i), in the requirement generation, decomposition, and design process. Thus, Mean Logistics Delay Time (MLDT) remains an integrated logistic support (ILS) item, not a design topic.

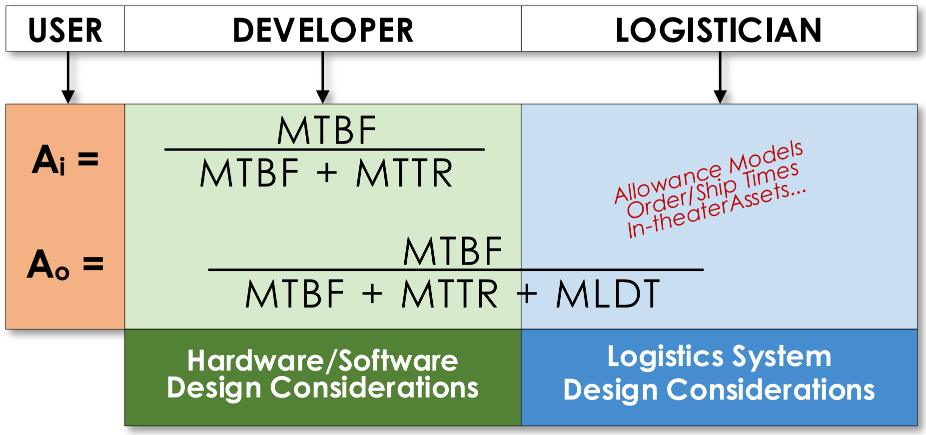


Figure 16: MLDT is Not a Design Criteria

ASN (RDA), Component DASNs, SYSCOM technical authorities, and reliability SMEs are well versed in this process and available to support the PM as needed to ensure reliability and maintainability are treated as design requirements.

Use of R&M measures, time-based R&M metrics provide the contractor with objective, quantifiable criteria to guide the system design, and engineering and manufacturing process. By requiring that all R&M metrics are allocated to, and included in, all system subcontracts (flowed down), the PM will assure that any trade analysis will be supported in a consistent manner, without surprises, and that testable provisions exist at all levels. Deficiencies will be promptly identified at the source, not subsequently at integrated system levels.

Allocating the A_o Requirement into Contract Specifications

Once A_o has been translated, it must be allocated properly into Government performance and contract specifications especially when several contracts are being used by Government to procure a system, or if parts of the system is Government furnished. A_o must be allocated between the multiple subsystems that will make up the warfighter's system. The simplest way to understand this is that the warfighter's A_o is the product of all of the subsystem A_o values. All the subsystem A_o values must multiply together to meet the warfighter's A_o requirement. Note, if all the subsystems' A_o were at the required user A_o for the system, when multiplied together, the resulting A_o for the system would be much lower than the required A_o for the system. As a result, when multiple subsystems are being integrated, each subsystem's A_o will need to be much higher than the warfighter's required system A_o simply because all subsystem A_o's must be multiplied together to properly measure and achieve the warfighter's A_o requirement shown in **Figure 17**.

$$A_o = \prod_{i=1}^{n} Ai(n) = Ai(1) \text{ x} \ldots \ldots Ai(n)$$

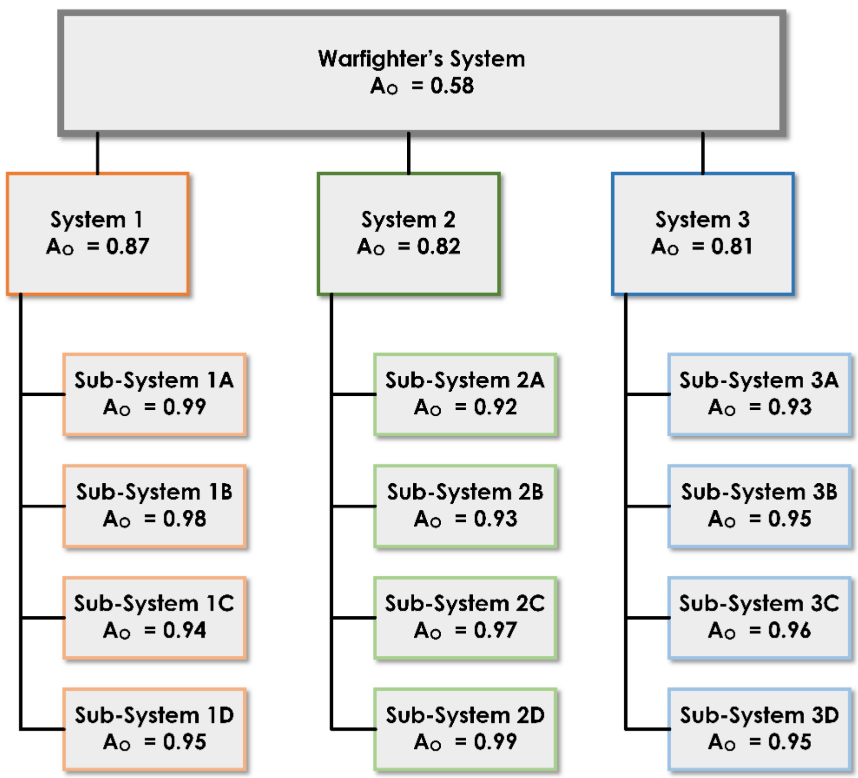


Figure 17: Warfighter's Required System A_o

Reliability Attribute

Reliability and maintainability requirements in performance and contract design specifications should be identified as critical technical requirements (CTRs) for all contracts. Reliability performance and contract specifications should be testable and verifiable and in a form that the developer (Government or contractor) can demonstrate prior to delivery of the equipment to the Government acquisition office. Requesting that the developer demonstrate a Mean Time Between Operational Mission Failures (MTBOMF) for example may not be practical especially when the developer will not be testing or demonstrating mission operations or success. Placing an operational mission requirement into a Government RFP may require that the developer demonstrate the requirement by analysis only. Translating a MTBOMF into a simple failure rate (failures/hour) or MTBF (time/failure) is typically the most practical method of specifying a reliability specification when the developer (Government or contractor) is not being asked to analyze or demonstrate mission capabilities. Suppliers can deliver parts (electronic, mechanical, or other COTS components) that meet MTBF requirements, but those parts cannot be guaranteed to meet MTBOMF because MTBOMF is a system level measure. When translating user reliability requirements into Government performance specifications, interface control documents, and contract specifications, R&M engineers must consider two types of failures: 1) Predictable component and subcomponent failures, and 2) Unpredictable operationally-induced failures.

Component and subcomponent failures are typically predictable because they generally fall within their design expected failure rate. While failed subcomponents ("piece parts") are not repairable when they occur, their failure rates are directly translatable to their failure rate requirements and ultimately the failure rate requirement of the component.

Operationally-induced failures are normally unpredictable. They can occur unexpectedly during test and evaluation or normal operations when equipment is exposed to conditions outside its operational design limits, such as unanticipated environmental conditions, stress on components from external sources, operator error or bypassing rigorous engineering during design. Because of the unpredictability, operational failure effects on the mission profile must be considered in the allocation of user reliability KSA/APAs in government acquisition performance specifications, interface control documents and contract specifications.

To anticipate the effect operationally-induced failures may have on the overall mission profile, R&M and systems engineers should conduct a function level FMECA to assess the level of risk expected from new technologies, untested environmental effects, and integration and interoperability of the equipment used in the design. Based on this analysis, user reliability KSA/APAs can be more accurately defined for optimum mission success.

Translating Reliability Attribute into Contract Specifications

Figure 18[8] represents an example of the distribution of root failure causes that can ultimately impact the ability of a system to meet its reliability requirement. The figure graphically illustrates a nominal percentage of operational failures attributable to each of eight identified failure-cause categories based on historical failure mode data collected on DOD electronic systems. For each program, historical records should be used to develop a similar pie chart identifying the failure categories that make up operational failures. This distribution can be used to decompose user requirements to a contract specification requirement. Definitions of failure must exist for user requirements and for all requirements decomposed in a complete set of failure definitions and scoring criteria so that there is no misunderstanding of what a failure means, especially when decomposing requirements into contract specifications. The definitions of the eight failure-cause categories all contribute directly to the level of operational reliability that the end-user will experience. Unfortunately, when specifying a reliability requirement that is the same as fielded performance requirements, contractor's predictions may only account for a fraction of them. For this reason, contract specification requirements must account for how the developer proves that a system has met the needs.

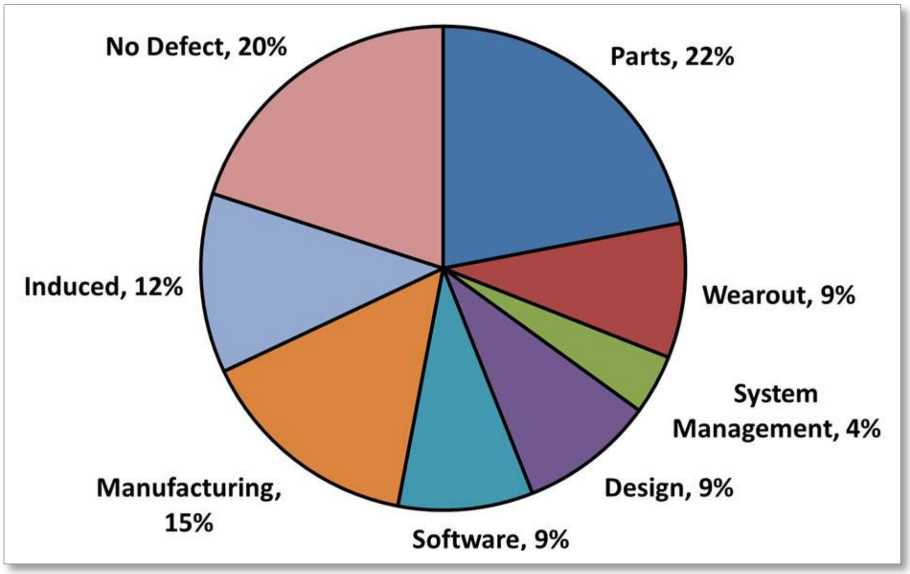


Figure 18: Nominal Failure Cause Distribution of Electronic Systems

- **Parts (22%):** Failures resulting from a part failing to perform its intended function before its expected "end-of-life" (or wearout) limit is reached (random failures, typically based on part quality variability issues).
- **Wearout (9%):** Failures resulting from "end-of-life" or "age related" failure mechanisms due to basic device physics (e.g., mechanisms associated with electrolytic capacitors, solder joints, microwave tubes, switch/relay contacts, etc.).
- **System Management (4%):** Failures traceable to incorrect interpretation or implementation of requirements, processes or procedures; imposition of "bad"

[8] Nicholls, David and Lein, Paul, "When Good Requirements Turn Bad," 2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS), 2013, pp. 1-6, DOI: 10.1109/RAMS.2013.6517616 [Ref 49].

requirements (missing, inadequate, ambiguous or conflicting); or failure to provide sufficient resources (funding, schedule, manpower) to design, build and test a robust, compliant system.

- **Design (9%):** Failures resulting from inadequate design approaches (e.g., tolerance stack-up, unanticipated logic conditions (sneak paths), inadequate design margins for the environment, etc.). This should include infant mortality.
- **Software (9%):** Failure to perform intended functions due to the manifestation of a software fault.
- **Manufacturing (15%):** Failures that result from problems in the manufacturing process, such as bad solder joints, wire routing issues, bent connector pins, lack of training, documentation problems, etc. They are not attributable to deficiencies in the inherent reliability of the design.
- **Induced (12%):** Failures resulting from externally applied stresses not associated with normal operation, such as electrical overstress, maintenance, human operator error, etc.
- **No defect (20%):** Reported field failures that cannot be reproduced. These may or may not represent an actual failure; however, they do represent removals that may be “scoreable” based on OT&E FD/SC and cause a system to not meet its operational reliability/suitability requirement. This includes multiple nuisance issues that ultimately cause an operator to become frustrated and stop work.

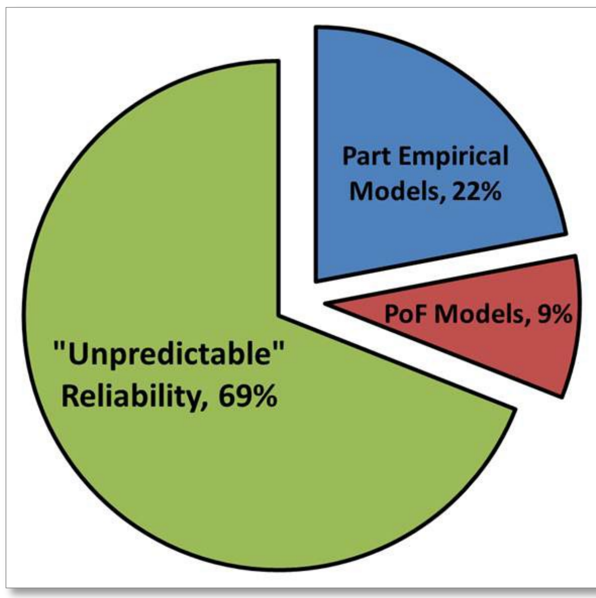


Figure 19: Unpredictable Reliability

In this example, MIL-HDBK-217 and its derivatives for electronics and surrogate databooks (such as the “Non-electronic Parts Reliability Data (NPRD)” databook from RIAC [Ref 50] that addresses mechanical items) will address only 22% of the overall system failure rate – the “useful life” portion of the reliability bathtub curve. Physics-based approaches will address only 9% of the overall system failure rate—the “wearout” portion of the bathtub—unless they account for part variability in the model. A hardware-centric system engineering design focus, then, has caused us to overlook approximately 70% of the failure contribution of the system, what **Figure 19**[9] calls “Unpredictable Reliability.” Yet these failures are significantly more likely to contribute to unsatisfactory operational reliability performance. (Note that there are numerous software

[9] D. Nicholls and P. Lein, [Ref 49].

reliability and human factor reliability models that do exist, but software reliability requirements are not always adequately specified in contracts, and human factor requirements are rarely, if ever, called out). For these reasons, predicted component failure rates are insufficient and must predict performance 70% higher than what you would expect to see in the fielded product.

Some contracts will require that the developer demonstrate reliability performance during factory acceptance testing in the engineering and manufacturing development phase, long before operational test and evaluation. Factory acceptance testing will not account for induced failures due to the operational environment and from interoperability with the entire system. For this reason, specifying reliability requirements in contracts must take into account which of the eight failure-cause categories will not be accounted for in the developer's predictions.

In this example, if the contract will be specifying a reliability requirement that will require the developer to demonstrate reliability using MIL-HDBK-217 predictions or similar reliability handbooks:

- The Government performance specification should require a failure rate that is 70% lower than what is required in the field, or a 70% higher MTBF, since MTBF is the inverse of the failure rate.

If the system design is evolutionary where there are years of data to predict performance of the existing hardware, there are minor changes in the design, and the contract will require the developer to use a combination of field data and MIL-HDK-217 predictions:

- The Government performance specification should require that the developer increase predicted failure rates by 70% for any MIL-HDBK-217 prediction used.

If the contract specification will require that the developer demonstrate the system will meet its reliability requirement through factory acceptance testing and not in the environment which it will be used:

- The Government performance specification should require a failure rate that is 41% lower than the expected fielded performance. This is because failures due to manufacturing, software, design, system management will be accounted for in the factory acceptance test but failures due to wearout, induced failures and those identified as "no defect" will not.

Managing Data Sources

Some programs find it easier to manage the data sources for making reliability predictions rather than place more stringent reliability requirements into contract specifications.

Methods of controlling the developer sources for reliability data can be used such as defining a priority list of data sources based on risk. The best data sources will come directly from the Fleet when there are years of evidence of performance of the equipment. Higher risk data sources, such as MIL-HDBK-217, will require adjustments to be made in the predicted failure rates. A priority list of data sources is described below to assist with requiring adjustments to the predicted failure rates.

- **Real Fleet/Field Data**
  - Highest Fidelity data source where no adjustment to the failure rate used for reliability predictions are needed.
- **Identical equipment used in a similar environment**
  - When this data source is used, environmental differences will stress the equipment differently and adjustments to the failure rates typically from 10% to 20% will be needed.
- **Similar equipment where Fleet/Field data is available**
  - When performing similarity analysis, consider applying a percentage to how similar the equipment and environment is to the actual equipment that the failure rate is to be applied to. For example, equipment from the same manufacturer, which is very similar in design and used in the same environment, may only require a slight modification to the data rate. Equipment from different manufacturers, with major differences in design complexity, will require a higher risk rating and a higher adjustment to the failure rate to make accurate predictions.
- **Test Data of the actual equipment in a similar operational environment**
  - When using this data, the difference between the test environment and the actual environment may be significant. An attempt should be made to determine environmental effects on the equipment such as:
    - Bench testing in a pristine environment: Increase the failure rate from 60% to 70%.
    - Testing in a similar operational environment: Increase the failure rate from 5% to 10%.
- **Test Data of the actual equipment from commercial sources**
  - This data source is performance data of the actual equipment used in a different application, such as the automobile industry, a factory or communications systems. This data source will require a failure rate adjustment due to military applications. Attempt to modify the failure rate from 20% to 40%.
- **Manufacturers Performance Data (lowest fidelity data source)**
  - Manufacturers may bench test thousands of items and define defects per thousand or failures during a test in a lot size. In some cases, manufacturers will

perform actual life cycle testing or reliability testing. An attempt should be made to understand what the manufacturer is advertising as the failure rate and apply conservatism in using the failure rate. An adjustment to the failure rate from 40% to 60% is recommended.

As the fidelity of the source of data diminishes as described above, the developer's reliability predictions should contain methods to translate the data to accommodate the level of risk being assumed with the source of data.

Reliability Allocations

Reliability requirements, once translated into contract specifications, must be allocated by the Government into several contract specifications or between GFE and CFE. OM/MP engineers can determine the operating duration of each function during a mission and develop reliability block diagrams to assist with calculating the appropriate system-level failure from subsystem and component-level failure rates. Failure rate allocations can be determined by the amount of time that a system must operate during a mission, and from those allocations reliability block diagram complexity can be determined. More information on calculating failure rates can be found in many standard reliability textbooks and in the DOD guide to achieving RAM of 2005. Once allocations are completed, subsystem failure rates (failures/hour) can be directly added together to meet end items or system level failure rate requirements where MTBF must be inverted into a failure rate (failures/hour) prior to addition.

Commercial Off-The-Shelf Hardware Selection

Commercial Off-The-Shelf components should be chosen based on the expected failure rate in its operating environment. Determining the effect that the environment will have on COTS failure rates may require analysis or testing in a simulated environment or past experience of similar components in the same operating environment. COTS equipment is manufactured for environments that are not representative of what can be expected in an operational environment (e.g., under the ocean, under extreme vibrations, or at high altitudes). The use of COTS is ideal for keeping acquisition costs low and allow for replacement items to be used when the equipment is no longer supported by the manufacturer. However, it also comes at the cost of managing obsolescence through diminishing manufacturing sources and material shortages. COTS is not designed for military use. It is frequently repackaged into enclosures for the military operational environment. R&M engineers should be aware and should caution design engineers of sources that provide less reliable or imitation parts.

MIL-HDBK-217 [Ref 34] provides common metrics that apply to a manufacturer's failure rate based on its expected operating environment. However, MIL-HDBK-217 predicted failure rates are solely based on "piece part" failure rates predicted from bench testing in a pristine environment and will not represent all suppliers and sources of material. The use of COTS requires extensive testing in the expected operating environment to gain confidence that the equipment is compatible and reliable for military needs.

If Prognostic and Health Management (PHM), Reliability Centered Maintenance (RCM) or Condition Based Management Plus (CBM+) are to be implemented, the necessary design elements (sensors, timers, data storage…) must be coordinated with the BIT design features to insure there are no conflicts and to maximize common utilization of available data streams. Product Support Managers, R&ME and ISEA engineers, and maintainers must work together to ensure the integrity of both real time (BIT) and stored/recorded (PHM, RCM, and CBM+) sensor and data systems and to prevent any modifications from interfering with the other functions. Ideally, they will be designed together but may be expanded or added after initial design.

Engineering activities necessary to ensure achievement of the design specifications must be included in the technical specifications. RBDs, allocations, FMECA, FRACAS processes, maintainability, health sensor net architecture, and BIT demonstrations should always be employed. Other appropriate engineering activities such as environmental stress analysis, reliability testing, and accelerated life testing may be implemented as necessary for the system or the environment of use.

Durability and material properties should be specifically considered in the mandatory early FMECA required by PDR and in the root cause analysis phase of the mandatory FRACAS that is done throughout the life of the system.

Maintainability Data

Maintainability predictions can be managed similarly to reliability data when attempting to determine the MTTR. Maintainability predictions must be made even when no data exists or when no testing is planned. In these extreme conditions, engineers will need to qualitatively assess the level of effort required by maintenance personnel when making maintenance predictions. An effort should be made to understand the difficulty in performing repairs and maintenance. When maintenance data is determined from analytical 3D models demonstrating the repair, a risk assessment like translating reliability data sources can be used. When maintenance data will be obtained from a maintenance demonstration, engineers should attempt to understand the effects of performing the demonstration in the actual location where it will be used by the operator, or if the demonstration will be performed on a bench or at a factory where access to the equipment may be unrestricted. In this case, attempts to increase the MTTR should be made.

Allocating Mean Time To Repair

Allocating MTTR requirements are an important step in managing systems maintainability. Maintainability is a characteristic of the design and installation of an item that is expressed as the MTTR or the probability that an item will be retained in or restored to a specified condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources. When including the maintainability requirement in contract specifications, engineers should understand that corrective maintenance occurs only after failures occur and repairs are not performed until something requires it. Maintainability allocation is essential prior to completion of the contract specification to allow the equipment to be maintained in less time, and at the lowest cost to the Government. When only one system is being placed under contract the actual MTTR requirement may be used in the contract specification. A number of methods may be used to allocate maintainability requirements to several subsystems such as the equivalent allocation method, availability-based allocation method, and failure rate-based allocation method. It may not be feasible for the Government to specify how the developer should allocate the maintainability requirement down to the component level. However, the methodology used and resulting data should be requested in the contract specification so that information can be used for Government modeling, predictions, and reliability-centered maintenance activities.

AVAILABILITY-BASED MTTR ALLOCATION METHOD

An availability-based allocation method is used when the program is controlling repair times in order to achieve its operational availability requirements. In this case, no top-level MTTR requirement has been specified by the warfighter but an operational availability and reliability requirement exist. This method is also used when the availability and reliability have already been allocated to the various subsystems and engineers are now allocating MTTR. The availability method assumes that an operational availability equation has been derived, such as:

$$A_o = \frac{MTBF}{MTBF + MTTR + MLDT}$$

Or reorganized to:

$$MTTR = \frac{MTBF}{A_o - 1 - \frac{MTBF}{MLDT}}$$

This equation assumes that the program has allocated A_o and MTBF, and can determine the appropriate MLDT to assume for each subsystem.

FAILURE RATE-BASED ALLOCATION METHOD

All programs should attempt to ensure that maintainers will not have to remove components that do not fail often when performing repairs on components that are expected to require maintenance or fail often. It is not desired to handle or disturb equipment that is operating correctly. A failure rate method is used when a MTTR by the warfighter has been specified and is essential, or is a MTTR requirement has been derived from the operational availability requirements and must be broken down into components or subsystems. In this case, the program must develop reliability models to predict the failure rates for each subsystem, or has allocated the reliability requirement to each subsystem. The following equation applies:

$$MTTR(S1) = \frac{MTTR\ x\ MTBF(S1)}{n\ x\ MTBF}$$

Where:

MTTR(S1) is the mean time to repair of the system

MTTR is the mean time to repair for the entire system

MTBF(S1) is the mean time between failures for subsystem 1

MTBF is the mean time between failures for the entire system

n is the total number of subsystems

This method is independent of operational availability since it is known that the system-level MTTR will support the A_o requirement.

EQUIVALENT ALLOCATION METHOD

The equivalent allocation method is used when all repairs are independent activities and do not require repairs or replacements of other subsystems / components within the system. For this method, the top-level MTTR may be placed within the system specification. This method may be used when the Government is allocating a maintainability requirement on separate subsystems which will be developed by different vendors under separate contracts. This method can only be used when the Government is certain that repairs made to each subsystem are independent and will not require work or repair to another system. When using this method, it is important to leave some margin between contract specifications and warfighter requirements because some components will not be capable of meeting their overall MTTR requirement.

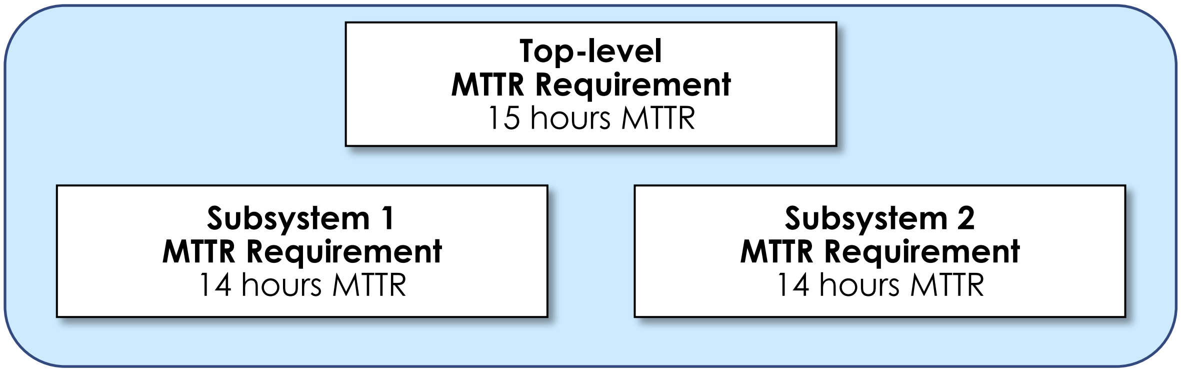


Figure 20: MTTR Equivalent Allocation Example

In **Figure 20**, a one-hour margin is used as an example for placing the top-level MTTR requirement on several contracts or between subsystem 1 and subsystem 2.

5 | R&ME WARFIGHTER REQUIREMENTS AND TECHNICAL PARAMETERS

This chapter establishes limits on the use of warfighter (user) requirements values and establishes the top-level process acquisition R&M engineers must use when no numerical warfighter requirements are provided for reliability and maintainability, including BIT. A more detailed process should be developed by each SYSCOM for their type weapons systems. This chapter is intended to be consistent with JCIDS [Ref 10] however the necessity to translate requirements to contract design specifications may result in the use of different terms than those used in the warfighter (user) requirements documents.

The warfighter (user) requirements documents, such as JCIDS capabilities documents (ICD/CDD/CPD/CDD update), normally provide operational system requirements for reliability and maintainability (including BIT) as KSAs, CTPs, or APAs. Reliability requirements must first be described in the form of a probability of operating over a specified period of time without failure. An OMS/MP along with a single set of clear failure definitions must exist before these probabilities can be expressed in terms of time, e.g., MTBOMF, MTBF, and MTTR. These warfighter operational (user) requirements pertain to the integrated operational system, do not provide the necessary derived technical requirements, and should not be used as Government performance and contract design specifications.

Reliability and maintainability (R&M) performance requirements and contract design specifications are design-controllable attributes of the system and, as such, should be developed and managed in the CHENG, SDM, or SIM engineering domain.

The system's reliability and maintainability performance, combined with Government management decisions, including the sustainment strategy, form the basis for meeting Operational Availability requirements. A_0 and the sustainment management decisions and strategies are in the Product Support domain. The program R&M engineer must work with the PSM or Lead Logistician and Cost Engineer to balance operational availability, reliability, maintainability, and cost as described below.

Reliability and maintainability warfighter requirements should be derived or refined for the CDD in concert with the PSM and Cost Engineer in order to balance the achievable reliability and maintainability requirements within the specified sustainment cost limit. The program R&M engineer should support the PSM and Cost Engineer in the balancing process to prepare the RAM-C Rationale Report per the DOD RAM-C Guide [Ref 21].

- If no warfighter requirements for reliability and maintainability are provided in the updated capabilities document, the R&M engineer should inform the LSE and PM with the risk to contracting without R&ME design specifications and proceed to determine the appropriate parameters to be used in the balancing process and further translated to contract design specifications.
- After the PSM and Cost Engineer determine the optimum Availability-Cost ratio, the R&M engineer will determine the corresponding reliability and maintainability factors, including BIT, necessary to achieve the availability at that point. After technical feasibility is established and affordability determined, the reliability and maintainability thresholds and objectives can be set. This is an iterative process requiring all three participants to work together to balance their objectives until an affordable and technically feasible solution is reached.

When numerical reliability and maintainability values are not provided by the warfighter requirements documents, reliability and maintainability parameters should be derived by the acquisition R&M engineers based on operational availability requirements and the OMS/MP. If sufficient information is not provided by the warfighter requirements documents, the R&M engineer must work with the requirements officer to derive the missing details from available information. The resultant "technical parameters" are used to develop contractual design requirements and are not warfighter operational requirements.

An operational requirement or technical parameter must be provided for each of the following (Note: When any of these do not exist as a warfighter requirement, a technical parameter must be developed by the R&M engineer in order to derive the design specifications).

- Mission Reliability should first be defined in terms of a probability of a successful operation throughout the duration of a specified mission. Systems or combinations of systems with multiple missions should be addressed. Probabilities of operating without a mission critical failure in the expected environment over the mission timeframe should be the basis for determining MTBOMF or MCBOMF parameters.
  - Multi-mission platforms may also require a Mean Time Between Abort Parameter.
  - Large, complex platforms may address critical missions and their critical systems individually rather than assign a requirement or R&ME parameters to the large, complex platform. This approach is recommended for new technology or new development systems (e.g., CVN-78s EMALS, AAG, AWE, and DBR).
- Logistics Reliability in terms of MTBF/MCBF to provide a measure of the maintenance and logistics load a system or component will present. In addition to meeting mission needs, the probabilities of operating without failure in the expected

environment between planned maintenance cycles, when corrective actions can be made, or between acceptable unscheduled corrective maintenance opportunities should be the basis of determining MTBF parameters.

- Maintainability in terms of MTTR should be derived from the expected time to perform the necessary corrective actions following failures. MTTR is the total elapsed time (clock hours) for corrective maintenance divided by the total number of corrective maintenance actions during a given period. MTTR must support the A_o, A_M, and readiness requirements.
- Maintenance ratio in terms of maintenance man hours per operating hour or flight hour may also be required.

BIT should be implemented whenever feasible to minimize repair time. BIT specifications should be provided for systems implementing BIT. These specifications are usually expressed as a percentage for Fault Detection and Fault Isolation and may be time, cycle, or percentage based for False Alarms.

System boundaries should be defined with any excluded (legacy and/or GFE) equipment specifically identified.

The terms and parameters above should be explicitly defined to clarify seemingly common terms that create recurring problems due to unclear meanings, such as time or cycle parameters. For example, time parameters must clarify or differentiate between flight hour versus operating hour, or operating hours versus power on or standby hours. Aviation operating days (12 hours) versus 24 hours days must be reconciled, and requirements or technical parameters adjusted accordingly.

6 | RELIABLE SOFTWARE

ORIGIN

Hardware reliability engineering was first applied in military applications during World War II to determine the probably of success of ballistic rockets. Throughout the 1950s, life estimation methods for mechanical, electrical, and electronic components were created and used in the development of military products. By 1960s the practice of life estimation of products had proven integral to developing successful military and commercial systems. These new methods were grouped under the name of Reliability Engineering. Reliability Engineering evolved from an understanding of physical components, their arrangement in the system, and how their interaction supports the functions of the system. At that time, software, although present and critical in some systems, was not part of reliability engineering.

Early software was utilized in systems to execute basic programs quickly and accurately, often numerical calculations too numerous or complex to be done manually. Once developed and tested, the software was simple enough to be depended on to perform 100% consistently. This meant it was 100% reliable and therefore not a consideration in the system reliability analysis. The term software reliability was first coined in the 1970s as an evolution of software quality efforts of software engineers wanting to improve the reliability of their software. Software and software development has evolved at an ever-increasing pace since then, and the need for reliable software has and will continue to increase.

PRESENT

Today, system reliability is not only affected by the hardware in the system, but also by the software. Software is installed in the hardware of nearly all military systems. This software includes executable programs, operating systems, virtual environments, and firmware. Increasingly system functions are dependent on the interaction of hardware and software. It is rare, and becoming rarer, to find a system that contains no software. Any time software supports or performs a system function, the reliability of that software's impact to the system should be considered as part of system reliability analysis.

FUTURE

Increased use and reliance on digital engineering technologies will make it possible to evaluate the reliability of the system more quickly and more accurately. Models used for system development and realization will be evolved into operational models (digital twins). In the future, system reliability will be evaluated in the digital model which will include all relevant interactions between the hardware and software. Such a complete digital model will display the impact of proposed changes to system reliability in real-time. Operational reliability models will be perfected from the design models and will enable prognostic capabilities that optimize system availability and maximize mission readiness.

WHAT IS RELIABLE SOFTWARE?

What is reliable software? It is not a simple question to answer. People's notion of reliability is gleaned through personal experience with the physical world. They notice when something persists in its operation throughout time and therefore ascribe it to being "reliable" (even if only in their mental model of the item). This item could be organic: a rock, a tree, a planet, a person; or it could be human made: a toaster, a car, an airplane, a telephone. All these things do something, even the rock, which persists without change to some degree, over time (how long will a granite countertop last?). People also notice when an item that they previously considered reliable starts to become, in their estimation, "unreliable." The item may begin to occasionally lose functionality due to broken parts. These parts may be broken from a catastrophe or simple accumulation of wear.

Hardware reliability engineering endeavors to quantify the reliability of physical items through in-depth understanding of the interplay between relevant physical elements. Some software only operates on specific hardware. Some software may be completely agnostic to the hardware environment, but in all cases, software is dependent on hardware to provide the physical environment upon which the software will establish the virtual environment. Software, although unaffected by the physical world (other than as it impacts the host hardware), still has the potential to fail, although the mechanisms are wholly different from the mechanisms that cause hardware to degrade and fail.

Hardware Versus Software Reliability

Determining the reliability of hardware is a matter of evaluating how the material will respond to physical stresses of operation. The act of exposing materials to physical stresses causes the item to break down in a predicable way; however, this is not the case with software. Software is not limited nor constrained by its physical properties; instead, software fails when it encounters a situation that has not been provisioned for in the design. Like hardware, software that has shown itself to be reliable may become less reliable, but unlike hardware, the root cause of the reduced reliability will not be due to material degradation. The root causes are that the inputs to the software have changed and the software cannot cope with the change.

Hardware Reliability is generally defined as:

- The probability a system will operate as expected without failure in a given environment for a given period of time.

This definition contains elements that are relevant to hardware in a way fundamentally different than they could be related to software. The IEEE 1633-2016 [Ref 36] defines software reliability in two ways:

- The probability that software will not cause the failure of a system for a specified time under specified conditions.
- The ability of a program to perform a required function under stated conditions for a stated period of time.

Notice that the spirit of both the software and hardware reliability definitions are the same; however, some of the language has been adjusted to account for the fundamental differences between them. Also, notice the use of "time" as a relevant factor in all the equations. Time refers to time elapsed in the physical environment (hardware) and not the virtual environment (software). One may ask why the software reliability definitions include time (physical world). The answer: only physical time is relevant to evaluation of system function in the operating environment. More simply, system users live in the physical world so both software and hardware reliability must be represented in a way that shows the impact of a loss of functionality to the user in the physical world. Since hardware exists in the physical world, the conversions are based on usage (mission) profiles (e.g., converting miles requirement to a time requirement). On the other hand, software does not change or degrade over time, so quantifying the functional time of software in the physical world is a matter of determining how often existing errors, defects, or bugs present themselves and cause the system to lose functionality.

Concepts and Desired Outcomes

There is no single universally accepted methodology for evaluating the reliability of software. Software reliability is like hardware reliability in that the methods used are dependent on many factors. And, similar to hardware reliability, there are numerous models and analytical techniques depending on the constraints and requirements of the system or program. In short, one size does not fit all! The desired outcome of engineering reliable software is the same as the desired outcome for engineering reliable hardware: a reliable system. When hardware, software, or firmware are present in a system they must be engineered to work together to achieve the required system reliability and maintainability.

RELIABILITY BLOCK DIAGRAMS

System reliability block diagrams (RBDs) should include hardware, software, and when relevant firmware so they can be used as a basis for understanding dependencies between the various elements in the system. RBDs are also useful in capacity modeling because they represent the available pathways for flow of information (signal, electricity, data, fluid, even stress) between the elements. Capacity modeling is relevant to reliability if the potential exists that when the capacity between two or more elements is exceeded the system functionality could be negatively impacted or cause a system failure. Capacity is not normally discussed alongside reliability probably because capacity analyses differ between engineering disciplines both in method and critically. Nonetheless, broaching the limits of capacity can cause system failures and negatively impact system reliability and maintainability; therefore, system capacity is generally relevant to the reliability engineering. However, capacity is discussed in this chapter because the interaction between software and hardware is often awash with software demands that overwhelm the hardware (e.g.: processor, storage system, memory, network bandwidth). Software should be designed with consideration of hardware capacity and should adopt best practices that protect for safety margins relevant to hardware capacity. Examples could be:

- Conducting a worst-case analysis that considers hardware resource loading
- Evaluating the correlation between system latency and specific software demands/activities
- Developing telemetric instrumentation that provides feedback to software to allow for the preservation system resources for mission essential functions
- Built-in or automatic or manual activated software overrides that disable or pause non-mission essential functions in favor of mission essential functions when required (battle override function or software battle short)

Consider an electronic control unit for an electro-mechanical fuel pump that supplies fuel to an engine that is mounted to a framework. The electronic control unit has a network connection that enables basic two-way communication (commands, BIT status, response) between it and other network connected systems via a local area network. The RBD in **Figure 21** represents the basic elements of the system described. Notice how the RBD depicts the “chain of reliability” for the function of controlling the engine speed. This RBD spans varied connection types between the elements, each with potential capacity limitations that if breached could cause a system failure.

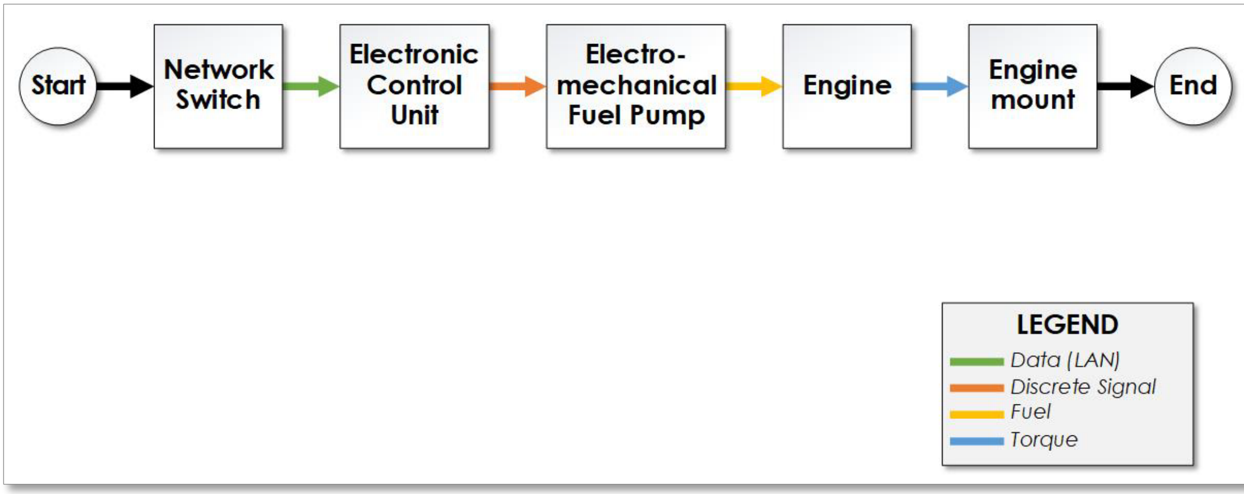


Figure 21: Reliability Block Diagram Example

The RBD above is meant to draw attention to the various engineering disciplines that a system relies upon to provide a function. The reliability engineer cannot be a specialist in all engineering disciplines, so to develop a meaningful reliability block diagram the reliability engineer must rely on engineering analyses performed by engineers of those respective specialties. Each of the elements could be further decomposed into sub-elements as necessary to support the needs of the analysis.

SOFTWARE RELIABILITY AND MAINTAINABILITY PREDICTIONS

A software reliability prediction forecasts or assesses the reliability and maintainability of the software based on parameters associated with the software product its development and support environments. Software R&M predictions are particularly useful when combined with hardware R&M predications to establish an overall system prediction. As discussed in **Chapter 3**, predictions are used to assess system potential to meet design requirements. Credible predictions provide decision information for design considerations; they are not objective quality evidence that a system will meet the reliability or maintainability requirement. More information can be found on software reliability predictions and methods of performing them in the IEEE 1633-2016 [Ref 36].

SOFTWARE FAILURE MODES AND EFFECTS ANALYSIS

Performing a Software Failure Modes Effects Analysis (SFMEA) early in the development cycle provides the best opportunity to address critical software issues that would negatively affect system reliability. “Effective Application of Software Failure Modes Effects Analysis” [Ref 51] is an excellent source of information for conducting a SFMEA. A SFMEA uses the same bottom-up analysis as a hardware FMEA except that it evaluates software failure modes, root causes from software viewpoint: requirements, design, code or other artifacts. Below are some compelling purposes of conducting a SFMEA.[10]

Identifying serious problems before they impact safety: The complexity of modern software means testing cannot be depended on to exhaust all paths and combinations of inputs that result in system failure

Uncovering multiple instances of one failure modes: The bottom-up approach provides the ability for entire types of failures to be eliminated if a corrective action is applied at the failure mode level since one failure mode could cause several instances of failures.

Finding software failure modes that of difficult to find in testing: Hidden or latent failure modes are those failure modes that aren't observed during development or testing but can become known one the software is operational. Some failure modes are simply more visible when looking at the requirements, design, code, etc., then by testing.

Finding single point failures: Particularly single point failures that cannot be mitigated by restarting, workarounds, hardware redundancy or other hardware controls.

Uncovering missing or incomplete requirements and design: Hidden failures can happen when unstated assumptions result in incomplete requirements and design which then result in system failures. Things typically missing from the requirements and design specifications are abnormal events that the software needs to detect and how to recover from those events.

SFMEA combined with design or code review can improve the focus of the reviews: During design and code reviews, it is typical for the reviewers to focus on what the software should do. A SFMEA focuses on the design or code should not do so combining the SFMEA with a design and code review increases the cost and effectiveness of both.

Providing a greater understanding of both the software and the system: Executing a SFMEA may be tedious, but when done properly there is an improvement in the overall understanding of the system and software. It is often an eye-opening experience for software engineers.

TELEMETRY

The nature of software requires fundamentally different techniques to analyze, detect, and test failures. Software offers one major advantage over hardware; it can be tested to failure repeatedly without requiring additional test artifacts or repairs. Because of this, a key tool for ensuring reliable software is telemetry (sometimes referred to as "software instrumentation.") Instrumenting software with the ability to detect and report on failures

[10] Excerpted from Neufelder, Ann Marie, "Effective Application of Software Failure Modes Effects Analysis," [Ref 51].

allows software reliability to be measured and managed. Telemetry allows the "virtual environment" of the software to be monitored and measured. Telemetry provides the scaffolding to do fault insertion testing (all can be called "chaos testing") allowing the reliability and software engineers to understand failure conditions and impact. Since software can be tested repeatedly without need to procure more components or perform repairs, running multiple tests with and without fault injection will allow for software reliability to be characterized.

Software telemetry is conceptually similar to built-in-test (BIT) for hardware and can provide many of the same advantages. Instrumenting software early in the design provides insight into failures that occur both in test and operational environments. Also similar to hardware BIT, software telemetry can increase system maintainability in the areas of troubleshooting paths and start points, automated readiness testing, mission readiness status, and identification of failed or failing hardware. Telemetry is best when designed into the software from the start and evolved throughout the system life cycle. A SFMEA conducted early in the design provides valuable information in selecting the software components that will be instrumented. SFMEAs help decide how to utilize the scarce system resources to create optimal instrumentation coverage approaches by identifying the most critical or troublesome failures (or potential failure conditions).

SITE RELIABILITY ENGINEERING

Systems that rely on connectivity to online resources such as the cloud or other network resources should utilize Site Reliability Engineering (SRE) practices to ensure the availability of services. SRE is a practice pioneered by Google as a result of iterative adaption and improvement of system and network administrator roles. Site reliability engineering is quickly grown into an industry best practice for delivering reliable and available services through the internet. Google describes site reliability engineering as: "…what you get when you treat operations as if it's a software problem." SRE is typically identified to the "Monitor" phase of the Development, Security, and Operations (DevSecOps) software life cycle because it is focused on ensuring reliable delivery of services. Some of the tenants of SRE are: reduction of toil, utilization of automation, software monitoring and alerting, utilizing service level objectives, and conducting blameless post mortems. There are numerous resources available to obtain more information on this growing technical domain such as: Site Reliability Engineering, How Google Runs Production Systems.[11]

[11] https://sre.google/sre-book/table-of-contents/ [Ref 52].

DOD and Reliable Software

The DOD–Industry Reliability and Maintainability Roundtable is engaged with the services (including the Navy), industry, academia, and NASA to research how to develop DOD systems with reliable software. The results will be documented in the DOD RM BoK [Ref 19]. This effort will be the basis of Navy policy and guidance that will enable programs to develop and maintain reliable software.

OBJECTIVE

Develop R&ME guidance, along with associated contract language, for defining, estimating, analyzing, testing, and identifying occurrences of software failures (that would occur) in an operational (field) environment. The approach is to use DevSecOps (Development, Security, and Operations), Iterative, and Agile Practices to deliver reliable software. All types of software are within the scope of this effort (e.g., application, cloud computing, fog computing, edge computing, embedded, and firmware in certain instances). It includes software acquired through all acquisition pathways (e.g., DoDI 5000.75 [Ref 53], DoDI 5000.85 [Ref 54], and DoDI 5000.87 [Ref 55]).

GOALS

- Define acceptable system metrics supported by R&ME to measure and evaluate (define how software related failures impact current R&ME system metrics and establish guidance for failure definition and scoring criteria (FD/SC) development).
- Effectively implement R&ME into software development programs by emphasizing the use of DevSecOps as a key for reliable software. This includes development and methods of gathering operational software performance metrics to identify, characterize, and address or correct software failures through CI/CD (continuous integration/continuous delivery) updates.
- Enhance programs' ability to contract for reliable software and effectively evaluate the risks of contractor's proposal to achieve reliable software.
- Differentiate roles and responsibilities for reliability, software, development, safety, certification, security, and operations. Describe interface between each role.
- Explore the concept of architecting software using design patterns that incorporate reliability concepts to build software that is more failure resistant and fault tolerant.
- Reduce the occurrence or impact of software failures during operations.

DELIVERABLES

- Guidance for specifying, developing, and assessing reliable software.
- Contract language and guidance on implementation (including tailoring) for delivering reliable software.
- Guidance for evaluating proposals for reliable software (Government only).

7 | SCORECARD/CHECKLIST

INTRODUCTION

Evaluation of the R&ME Program is an important step to understanding its health. A detailed evaluation of the maturity of the R&ME Program provides valuable information that should be used to determine where effort should be placed to bring the reliability program to a state that it supports the overall program goals. Utilizing a standardized scorecard ensures a repeatable, methodological approach of the evaluation. Standardization and repeatability enable comparison between past and present states of health, therein providing important decision information to shape the program to meet future state goals.

The DON is developing an R&ME scorecard that provides such a standardized, repeatable method to evaluate the maturity of the Reliability and Maintainability Program for SETR events or periodic reviews over the acquisition life cycle. The Naval R&ME scorecard will guide the user in the evaluation of the R&ME Program across four phases of the program life cycle. It will enable reliability engineers and program managers the ability to perform a reliability and maintainability program self-evaluation by providing scores to a question set for each sub-area and phase. The scores are then combined to provide an overall maturity index and grade percentage for each sub-area. The scores for each sub-area are used to calculate the combined score for the phase, and the scores for each phase are further combined to determine an overall R&ME Program score. The phases and respective sub-areas that will be included in the R&ME scorecard are listed in **Table 4**.

Table 4: Scorecard Disciplines and Sub-Areas

PHASE	SUB-AREA	
Design	▪ Operational Mode Summary/Mission Profile ▪ Design Requirements ▪ Trade Studies ▪ Design Process for Reliability ▪ Design Analysis ▪ Parts and Materials Selection ▪ Software Design ▪ Built-in-Test	▪ Design Reviews ▪ Spec Development Allocation/ Validation ▪ Prototype Development and Review ▪ Prepare Design Requirements Documents ▪ Quality Assurance (QA)

PHASE	SUB-AREA	
Test	▪ Integrated Test Plan ▪ Failure Definition Scoring (and FMEA/FMECA) ▪ Software Test	▪ Design Limit ▪ Life ▪ Test, Analyze, and Fix (TAAF) ▪ TEMP Development/Execution
Production	▪ Piece Part Control ▪ Requirements Flow Down - Subcontractor Control	▪ Defect Control ▪ Manufacturing Screening
Supportability-Logistics	▪ Sustainment/Provisioning Analysis ▪ Maintenance/Manpower Ratio ▪ Support and Test Equipment ▪ Training Materials and Equipment	▪ Spares ▪ Technical Manuals ▪ Logistics Analysis/ Documentation

SCORING

The basis for the effectiveness of the scorecard are the consistent and accurate responses to the probing questions for each sub-area. The questions included in the scorecard template will be based on existing policy and guidance and the best practices of other referenced materials; however, the template will provide options for tailoring the question set to meet the needs of the user. Similar to the way a FMEA should not be performed as the effort of a single individual nor should the scoring in of the R&ME program be done as the effort of one person. The best practice is to organize a group that will evaluate and present objective quality evidence to support the recommended score for each question. This approach will ensure that when completed the final scores will represent the consensus of the group and provide an accurate estimation of the efficacy of the R&ME program.

The evaluation process requires that each question be scored from 1 to 3. The score provided represents the group's opinion of how well the program is complying with the detailed criteria of the question. The group will determine the Compliance Value (CV) for each question using scoring values in **Table 5**.

Table 5: Compliance Value Scoring

USER EVALUATION	COMPLIANCE VALUE
No Compliance	1
Partial Compliance	2
Total Compliance	3

The Sub-area Maturity Index (SMI) is the calculation of the maturity of each sub-area for each phase. The SMI is calculated by averaging the Compliance Values provided by the group for all questions within a specific sub-area using the equation below:

$$SMI = \frac{\sum_{i=1}^{n} CV_i}{n}$$

Where:

n = the quantity of questions

The Phase Maturity Index (QMI) is calculated by averaging the values of the SMIs within the respective phase (Design, Test, Production, or Sustainability / Supportability). It is calculated using the equation below:

$$QMI = \frac{\sum_{i=1}^{n} SMI_i}{n}$$

Where:

n = the quantity of SMIs in the discipline

The Program Maturity Index (PMI) is calculated by averaging the values of the four QMIs (Design, Test, Production, or Sustainability/Supportability). It is calculated using the equation below:

$$PMI = \frac{\sum_{i=1}^{4} QMI_i}{4}$$

A common maturity scale, applied across all three evaluation levels, allows for a universal comparison of the R&ME maturity at all three levels (program, phase, sub-area). The maturity index scale is shown in **Table 6**.

Table 6: Maturity Index Scale

USER EVALUATION	MATURITY INDEX RANGE
Not mature	1.00 to 1.79
Marginal	1.80 to 2.49
Mature	2.50 to 3.00

The R&ME Scorecard will be able to be calculated manually; however, an automatic calculating template is being developed using Microsoft Excel. The automatic calculating Excel version of the Naval R&ME Program Scorecard will remove the calculation burden and will allow users to focus on the evaluation criteria instead of performing numerous manual calculations. The Excel template will also be able to store the results for up to three user-defined milestones to establish an historic record of the progress or regress of the R&ME program. The Excel template will have conspicuously marked user-definable fields to enable tailoring as needed to meet the needs of different Naval organizations, programs, or system types.

APPENDIX A | REFERENCES

1. GAO 20-151, "Defense Acquisitions: Senior Leaders Should Emphasize Key Practices to Improve Weapon System Reliability," Report to the Committee on Armed Services, U.S. Senate, January 2020.
2. Title 10, United States Code, Section 2443, "Sustainment Factors in Weapon System Design," 31 January 2019.
3. GAO-20-2, "Navy Shipbuilding: Increasing Focus on Sustainment Early in the Acquisition Process Could Save Billions," Report to the Committee on Armed Services, U.S. Senate, March 2020.
4. SECNAVINST 5000.2G, "Department of the Navy Implementation of the Defense Acquisition System and the Adaptive Acquisition Framework," 08 April 2022.
5. Office of the Deputy Assistant Secretary of Defense for Systems Engineering, "Department of Defense: Digital Engineering Strategy," June 2018.
6. Deputy Assistant Secretary of the Navy Research, Development, Test and Evaluation, "U.S. Navy and Marine Corps Digital Systems Engineering Transformation Strategy," 2020.
7. "Operational Availability Handbook: A Practical Guide for Military Systems, Sub-Systems and Equipment," Published by the Office of the Assistant Secretary of the Navy (Research, Development and Acquisition), NAVSO P-7001, May 2018.
8. National Research Council 2015. "Reliability Growth: Enhancing Defense System Reliability." Washington, DC: The National Academies Press, page 112. https://doi.org/10.17226/18987.
9. Dallosta, Patrick M and Simcik, Thomas A. "Designing for Supportability: Driving Reliability, Availability, and Maintainability In...While Driving Costs Out." Defense AT&L: Product Support Issue, March-April 2012, page 35.
10. CJCSI 5123.01I, "Charter of the Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration and Development System (JCIDS)," 30 October 2021.
11. Reliability Information Analysis Center (RIAC), "System Reliability Toolkit: A Practical Guide for Understanding and Implementing a Program for System Reliability," 15 December 2005.
12. Commander Operational Test and Evaluation Force, "Operational Suitability Evaluation Handbook," 26 March 2019.

13. Marine Corps Operational Test and Evaluation Activity (MCOTEA), "Operational Test & Evaluation Manual," Third Edition, 22 February 2013.

14. MIL-STD-721C, "Definitions of Terms for Reliability and Maintainability," 12 June 1981.

15. ISO/IEC 25023:2016, "Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of system and software product quality," 15 June 2016.

16. DoDI 5000.88, "Engineering of Defense Systems," Office of the Under Secretary of Defense for Research and Engineering, 18 November 2020.

17. DoDI 5000.91, "Product Support Management for the Adaptive Acquisition Framework," Office of the Under Secretary of Defense for Acquisition and Sustainment, 4 November 2021.

18. The Assistant Secretary of the Navy (Research, Development and Acquisition). Memorandum For Distribution, Subject: "Gate 7 Sustainment Reviews," 27 September 2021.

19. "Department of Defense Reliability and Maintainability Engineering Management Body of Knowledge," (DOD RM BoK) Office of the Deputy Assistant Secretary of Defense Systems Engineering, August 2018.

20. "Systems Engineering Guidebook," Office of the Under Secretary of Defense for Research and Engineering, Washington, D.C., February 2022.

21. "Reliability, Availability, Maintainability, and Cost (RAM-C) Rationale Report Outline Guidance, Version 1.0," Office of the Deputy Assistant Secretary of Defense for Systems Engineering, 28 February 2017.

22. "Engineering of Defense Systems Guidebook," Office of the Under Secretary of Defense for Research and Engineering, Washington, D.C., February 2022.

23. "Department of Defense Systems Engineering Plan (SEP) Outline, Version 4.0," Office of the Under Secretary of Defense for Research and Engineering, Washington, D.C., September 2021.

24. Office of the Assistant Secretary of Defense. Memorandum for Assistant Secretaries of the Military Departments Directors of the Defense Agencies, Subject: "Life-Cycle Sustainment Plan (LCSP) Outline Version 2.0," 19 January 2017.

25. "Director, Operational Test and Evaluation (DOT&E) Test and Evaluation Master Plan (TEMP) Guidebook," Version 3.1, 19 January 2017. https://www.dote.osd.mil/Guidance/DOT-E-TEMP-Guidebook

26. T9070-BS-DPC-010_076-1 Reliability and Maintainability Engineering Manual, 21 Feb 2017.

27. Adaptive Acquisition Framework, Defense Acquisition University, AAF.dau.edu.

28. DI-SESS-81613A, “Reliability & Maintainability (R&M) Program Plan,” 15 July 2014.

29. R&M Engineering Community of Practice, Defense Acquisition University, https://www.dau.edu/cop/rm-engineering/Pages/Default.aspx.

30. MIL-STD-961E, “Defense and Program-Unique Specifications Format and Content,” Change 4 dated 16 July 2020

31. MIL-HDBK-338B, “Electronic Reliability Design Handbook,” 1 October 1998.

32. Reliability Information Analysis Center (RIAC) [formerly Reliability Analysis Center (RAC)], “Maintainability Toolkit,” 30 June 2000.

33. MIL-HDBK-245E, “Preparation of Statement of Work (SOW),”14 June 2021.

34. MIL-HDBK-217F, “Reliability Prediction of Electronic Equipment,” 2 December 1991.

35. “Managing Life Modeling Knowledgebase for the Naval Air Systems Command (NAVAIR),” Cybersecurity and Information Systems Information Analysis Center (CSIAC), Deliverable 4.7: Final Technical Presentation, FA807519FA051, CAT 19-1972.

36. IEEE 1633-2016: “IEEE Recommended Practice on Software Reliability,” IEEE Reliability Society, 18 January 2017.

37. MIL-STD-1629: “Procedures for Performing a Failure Mode, Effects and Criticality Analysis (FMECA),” 24 November 1980.

38. DI-SESS-81495B, “Failure Modes, Effects, and Criticality Analysis,” 16 May 2019.

39. DI-SESS-82495, “Model-Based Engineering Failure Modes, Effects, and Criticality Analysis Profile (SYSML Version),” 4 February 2021.

40. DI-SESS-80685A, “Reliability Critical Items List,” 9 July 2019.

41. MIL-HDBK-2155, “Failure Reporting, Analysis and Corrective Action Taken,” 11 December 1995.

42. DI-SESS-81927, “Failure Analysis and Corrective Action Report (FACAR) (Navy), 1 July 2013.

43. MIL-STD-471A, “Maintainability Verification/Demonstration/Evaluation,” 27 March 1973.

44. SAE International Standard, “Maintainability Program Standard Implementation Guide,” JA1010/1_201105, 24 May 2011.

45. MIL-STD-785B, “Reliability Program for Systems and Equipment Development and Production,” 15 September 1980.

46. MIL-HDBK-2164A: “Environmental Stress Screening Process for Electronic Equipment,” 19 June 1996.

47. NAVMAT P-9492, “Navy Manufacturing Screening Program: Decreased Corporate Costs Increase Fleet Readiness,” Department of Defense, Naval Material Command, May 1979.

48. “DoD Guide for Achieving Reliability, Availability, and Maintainability,” Department of Defense, Under Secretary of Defense for Acquisition, Technology, and Logistics, 3 August 2005.

49. Nicholls, David and Lein, Paul, “When Good Requirements Turn Bad,” 2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS), 2013, pp. 1-6, DOI: 10.1109/RAMS.2013.6517616.

50. Mahar, David; Fields, William; and Reade, John, “Nonelectronic Parts Reliability Data,” January 2015.

51. Neufelder, Ann Marie, “Effective Application of Software Failure Modes Effects Analysis – 2nd Edition,” January 2017.

52. Site Reliability Engineering, How Google Runs Production Systems, https://sre.google/sre-book/table-of-contents/

53. DoDI 5000.75, “Business Systems Requirements and Acquisition,” Office of the Under Secretary of Defense for Acquisition and Sustainment, Change 2 Effective 24 January 2020.

54. DoDI 5000.85, “Major Capability Acquisition,” Office of the Under Secretary of Defense for Acquisition and Sustainment, Change 1 Effective 4 November 2021.

55. DoDI 5000.87, “Operation of the Software Acquisition Pathway,” Office of the Under Secretary of Defense for Acquisition and Sustainment, 2 October 2020.

APPENDIX B | GLOSSARY & REFERENCE GUIDE

AAF	Adaptive Acquisition Framework
ACAT	Acquisition Category
A_i	Inherent Availability
AI	Artificial Intelligence
AIS	Automated Information System
ALDT	Administrative and Logistics Delay Time
A_m	Materiel Availability
ANSI	American National Standards Institute
A_o	Operational Availability
AoA	Analysis of Alternatives
APA	Additional Performance Attribute
AS	Acquisition Strategy
ASN	Assistant Secretary of the Navy
BCA	Business Case Analysis
BFA	BIT False Alarm
BFA*h*	BIT False Alarms per hour
BIT	Built-in-Test
BoK	Body of Knowledge
CBM+	Condition Based Maintenance Plus
CDCA	Current Document Change Authority
CDD	Capability Development Document
CDRL	Contract Data Requirements List
CF	Critical Failure
CHENG	Chief Engineer
CI/CD	Continuous Integration/Continuous Delivery
COI	Critical Operational Issue
CONOPS	Concept of Operations
Corrective Maintenance (CM)	Corrective Maintenance is the ability of the system to be brought back to a state of normal function or utility, at any level of repair, when using prescribed procedures and resources. (JCIDS 2021)

COTF	Operational T&E Force
COTS	Commercial-Off-The-Shelf
CTP	Critical Technical Parameter
CTR	Critical Technical Requirement
CV	Compliance Value
DASN	Deputy Assistant Secretary of the Navy
DAU	Defense Acquisition University
DevSecOps	Development, Security, and Operations
DID	Data Item Description
DMI	Discipline Maturity Index
DMSMS	Diminishing Manufacturing Sources and Material Shortages
DOD	Department of Defense
DoDI	Department of Defense Instruction
DOE	Design of Experiment
DON	Department of the Navy
DT	Developmental Testing
DT&E	Developmental Test and Evaluation
EFF	Essential Function Failure
EMD	Engineering and Manufacturing Development
ESS	Environmental Stress Screening
FACAR	Failure Analysis and Corrective Action Report
FD/SC	Failure Definition/Scoring Criteria
FMC	Fully Mission Capable
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Modes and Effects Criticality Analysis
FRACAS	Failure Reporting, Analysis, and Corrective Action System
FRB	Failure Review Board
FRP	Full Rate Production
FTA	Fault Tree Analysis
FYDP	Fiscal Year Defense Plan
GAO	Government Accountability Office
GEIA	Government Electronics and Information Technology Association
GFE	Government-Furnished Equipment

HM	Health Management
HW	Hardware
ICE	Independent Cost Estimate
ICD	Initial Capabilities Document
ILA	Independent Logistics Assessment
ILS	Integrated Logistic Support
IOC	Initial Operational Capability
ITRA	Independent Technical Review Assessment
JCIDS	Joint Capability Integration and Development System
JRMET	Joint Reliability and Maintainability Evaluation Team
JTTI	Joint Training Technical Interoperability
KPP	Key Performance Parameter
KSA	Key System Attribute
LCC	Life Cycle Cost
LCSP	Life Cycle Sustainment Plan
LFT&E	Live Fire Test and Evaluation
Logistics Reliability (R_L)	Logistics Reliability is the measure of the ability of an item to operate without placing a demand on the logistics support structure for repair or adjustment, including all failures to the system and maintenance demand as a result of system operations. [Note: Logistics Reliability is a fundamental component of an O&S cost as well as Materiel Availability.] (JCIDS 2021)
LRFS	Logistics Requirements and Funding Summary
LRIP	Low Rate Initial Production
LRU	Line Replaceable Unit
LSE	Lead Systems Engineer
M	Maintainability
Maintainability Attribute [KSA or APA]	Maintainability is the measure of the ability of the system to be brought back to a readiness status and state of normal function. [Note: Subordinate attributes which may be considered as KSAs or APAs: 1) Corrective Maintenance, 2) Maintenance Burden, and 3) Built in Test.] (JCIDS 2021)
Maintenance Burden	Maintenance Burden is a measure of the maintainability parameter related to item demand for maintenance manpower. It is the sum directed maintenance man hours (corrective and preventive), divided by the total number of operating hours. (JCIDS 2021)

MAXTTR	Maximum Time to Repair
MBE	Model Based Engineering
MCA	Major Capability Acquisition
MCBF	Mean Cycles Between Failure
MCMT	Mean Corrective Maintenance Time
MCOTEA	Marine Corps Operational T&E Agency
MCSC	Marine Corps Systems Command
MDAP	Major Defense Acquisition Program
MEF	Mission Essential Function
MIL-STD	Military Standard
Mission Reliability (R_M)	Mission Reliability is the measure of the ability of an item to perform its required function for the duration of a specified mission profile, defined as the probability that the system will not fail to complete the mission, considering all possible redundant modes of operation. (JCIDS 2021)
ML	Machine Learning
MLDT	Mean Logistics Delay Time
MMH	Mean Man Hours
MP	Mission Profile
MR	Maintenance Ratio
MRT	Mean Reboot Time
MSA	Materiel Solution Analysis
MTA	Middle Tier of Acquisition
MTBBFA	Mean Time Between BIT False Alarms
MTBCF	Mean Time Between Critical Failure
MTBEFF	Mean Time Between Essential Function Failure
MTBF	Mean Time Between Failure
MTBM	Mean Time Between Maintenance
MTBOMF	Mean Time Between Operational Mission Failure
MTBR	Mean Time Between Repairs
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
NAVAIR	Naval Air Systems Command
NAVSEA	Naval Sea Systems Command

NAVWAR	Naval Information Warfare Systems Command
NDAA	National Defense Authorization Act
NPRD	Non-electronic Parts Reliability Data
O&S	Operations and Support
O&S Cost Attribute [KSA or APA]	Measuring O&S cost provides balance to the sustainment solution by ensuring that the total O&S costs across the projected life cycle associated with availability and reliability are considered in making decisions. (JCIDS 2021)
OH	Operating Hour
OMF	Operational Mission Failure
OMS	Operational Mode Summary
Operational Availability (A_o) [KPP]	Operational Availability is the measure of the percentage of time that a system or group of systems within a unit are operationally capable of performing an assigned mission and can be expressed as (uptime/ (uptime + downtime)). (JCIDS 2021)
OT	Operational Testing
OTA	Operational Test Agency
OT&E	Operational Test and Evaluation
P&D	Production and Deployment
PBL	Performance Based Logistics
PDR	Preliminary Design Review
PHM	Prognostic and Health Management
PM	Program Manager or Preventive Maintenance
PMI	Program Maturity Index
PRAT	Production Reliability Acceptance Testing
PSM	Product Support Manager
QA	Quality Assurance
R	Reliability
R&D	Research and Development
R&ME	Reliability and Maintainability Engineering
RAM	Reliability, Availability and Maintainability
RAM-C	Reliability, Availability, Maintainability – Cost
RBD	Reliability Block Diagram
RCM	Reliability Centered Maintenance

RDA	Research, Development and Acquisition
RDGT	Reliability Development Growth Test
RDT&E	Research, Development, Test and Evaluation
Reliability Attribute [KSA or APA]	Reliability is a measure of the probability that the system will perform without failure over a specific interval, under specified conditions. Reliability should be sufficient to support the warfighting requirements, within expected operating environments. [Note: Considerations of reliability must support both availability metrics and be reflected in the O&S Cost attribute.] (JCIDS 2021)
RFP	Request for Proposal
RGC	Reliability Growth Curve
RIAC	Reliability Information Analysis Center
RIL	Reliability Intensity Level
RMRB	R&ME Review Board
S&T	Science and Technology
SDM	Ship Design Manager
SECNAVINST	Secretary of the Navy Instruction
SEP	Systems Engineering Plan
SETR	Systems Engineering Technical Review
SIM	Systems Integration Manager
SME	Subject Matter Expert
SMI	Sub-area Maturity Index
SOS	Systems of Systems
SOW	Statement of Work
SPB	Sustainment Program Baseline
SR	Sustainment Review
SRE	Software Reliability Engineering
SUBSAFE	Submarine Safety
SW	Software
SWP	Standard Work Package
SYSCOM	Systems Command
T&E	Test and Evaluation
TA	Technical Authority

TAAF	Test, Analyze and Fix
TEMP	Test and Evaluation Master Plan
TLCSM	Total Life Cycle Systems Management
TMRR	Technology Maturation and Risk Reduction
TRB	Technical Review Board
UCA	Urgent Capability Acquisition
USD (R&E)	Under Secretary of Defense for Research and Engineering