Dod reliability availability and maintainability(ram guide

Definition: Reliability, availability and maintenance (RAM or RMA) are system design attributes that have a significant impact on sustainable maintenance or total life cycle costs (LCC) in a developed system. In addition, the RAM attributes affect the ability to accomplish the intended mission and affect overall mission success. The default definition of reliability is the probability of zero errors over a defined time interval (or task), while availability is defined as the percentage of time a system is considered ready to use when assigned to task. Maintenance capability is a measure of the ease and speed with which a system or equipment can be restored to operational status after an error. Keywords: availability, maintenance, RAM, reliability, RMA MITRE SE Roles and expectations: MITRE system engineers (Se's) are expected to understand the purpose and role of reliability, availability and maintenance (RAM) in the acquisition process, where it occurs in system development and the benefits of employing it. MITRE SE is also expected to understand and recommend when RAM is appropriate for a situation and if the process can be tailored to meet the program's needs. They are expected to understand the technical requirements for RAM as well as the strategies and processes that encourage and help end users and other stakeholders to participate actively in the RAM process. They are expected to monitor and evaluate contractor RAM technical efforts and acquisition program's overall RAM processes and to recommend changes when warranted. Background Reliability is the source of the other RAM system attributes of availability and maintenance. Reliability was first practiced in the early start-up days of the National Aeronautics and Space Administration (NASA) when Robert Lusser, working with Dr. Wernher von Braun's rocket program, developed what is known as the Lusser's Law [1]. Lusser's law has to say that the reliability of any system is equal to the product of the reliability of its components, which corresponds to the weakest link concept. The term reliability is often used as an overarching concept that includes availability and maintenance. Reliability in its purest form is more concerned with the likelihood of an error occurring over a certain time interval, while availability is a measure of something to be in a state (mission stand) ready to be tasked (i.e. available). Maintenance is the parameter that deals with how the system used can be restored after an error, while considering concepts such as preventive maintenance and BUILT-In-Test (BIT), required maintenance level and support equipment. When taking into account the accessibility requirement, the maintenance requirement must also be invoked, because a certain degree of repair and restoration to a mission-capable mode must be included. It is clear that logistics and logistical support strategies are also closely linked and rely on variables Requirements. This takes the form of sparse strategies, maintenance training, maintenance manuals and identification of the necessary support equipment. The linking of RAM requirements and the dependencies associated with logistics support illustrates how RAM requirements have a direct impact on maintenance and the overall LCC. In short, RAM requirements are considered the top-level, overarching requirement specified at the overall system level. It is often necessary to break down these requirements at the top level of lower-level design-related quantitative requirements, such as the use of the design. These lower level requirements are specified at the system level; however, they may be assigned subsystems and units. The most common allocation is made to the line replacement unit (LRU), which is the unit with the lowest level of repair on the field (often called organic) maintenance level. Much of this discussion has focused on hardware, but the complex systems used today are integrated solutions consisting of hardware and software. Because the software's performance affects system RAM performance requirements, software must be processed in the overall RAM requirements for the system. Wear or accumulated stress mechanisms that characterize hardware failure do not cause software failures. Instead, software exhibits behavior that operators perceive as a bug. It is critical that users, application offices, testing communities, and contractors agree early on what constitutes a software flaw. For example, software malfunctions can often be recovered with a restart, and the time of restart may be limited before a software error is declared. Another issue to consider is the frequency of occurrence, although the software restart recovers within the defined time window, as this will give an indication of software stability. The user's perception of what constitutes a software flaw will certainly be affected by both the need to restart and the frequency of glitches in the operating software. One approach to assessing software fitness is to use a comprehensive model to determine the current readiness of the software (upon shipping) to meet customer requirements. Such a model must address quantitative parameters (not just process elements). In addition, the method should organize and streamline existing quality and reliability data into a simple metric and visualization that applies across products and releases. A new model of software readiness criteria [2] has been developed to support objective and effective decision-making in product shipment. The model has been socialized in various forums and is being introduced to MITRE work programs for consideration and use on contractor software development processes for assessing maturity. The model offers: A light-energy composite index The ability to set quantitative pass criteria from requirements Easy calculation based on existing data A meaningful, insightful visualization Release-to-release comparisons Product-to-product comparisons A complete solution that incorporates almost every aspect of software development activities. Using this development test data approach, you can measure the growth or maturity of a software system along the following five dimensions [2]: Software Functionality Operating Quality Known residual defects (defective density) Test coverage and Reliability. Government interest and use Many U.S. government acquisition programs have placed more emphasis on reliability. The Defense Science Board (DSB) conducted a study on Developmental Test and Evaluation (DT&E) in May 2008 and published results [3] that linked test suitability failures to a lack of a disciplined systems engineering approach that included reliability engineering. The Department of Defense (DoD) has been the first proponent of systematic policy changes to address these findings, but similar emphasis has been seen in the Department of Homeland Security (DHS), as many government agencies leverage DoD policies and processes in the execution of their acquisition programs. As evidenced by the above, the strongest public support for increased focus on reliability comes from DoD, which now requires most programs to integrate reliability engineering with the system engineering process and to bring reliability growth as part of the design and development phase [4]. The scope of reliability impact is further expanded by directing reliability during the Analysis of Alternatives (AoA) process to identify reliability impacts on the system's LCC performance [5]. The strongest policy directives have come from the Chairman of the Joint Chiefs of Staff (CJCS), where a RAM-related sustaining Key Performance Parameter (KPP) and supporting Key System Attributes (KSAs) have been mandated for most DoD programs [6]. Elevation of these RAM requirements to a KPP and support KSAs will bring greater focus and oversight, with programs that do not meet these requirements prone to reassessment and reassessment and program modification. Best practice and experience [7] [8] Topic expertise questions. Acquisition program offices that employ RAM subject experts (SMEs) tend to produce more consistent RAM requirements and better oversight of contractor RAM processes and activities. MITRE SE has the opportunity to reach back to bring MITRE to bear by strategically engaging MITRE-based RAM SMEs early in applications. Uniform RAM requirements. Top-level ram requirements must be consistent with lower-level ram input variables, which are typically design-related and are called out in technical and performance specifications. A review of user requirements and flow of requirements for a contractual specification document released along with a Request For Proposal (RFP) package. If the requirements are inconsistent or program is at risk of RAM performance before awarding the contract. Ensure sustained, active engagement for all stakeholders. RAM is not a stand-alone specialty encouraged to answer mail in a crisis, but rather a key participant in the acquisition process. The RAM discipline should be included early in the trade studies, where results, costs and RAM should be part of any trading-space activity. The RAM SME must be part of the development of requirements with the user drawing on a defined operating concept (CONOPS) and what realistic RAM targets can be set for the program. RAM SMEs must be a key member of several integrated product teams (IPt's) during system design and development to establish insight and cooperation with the construction team(s): RAM IPT, Systems Engineering IPT and Logistics Support IPT. In addition, RAM specialty should be part of the testing and evaluation IPT to address RAM testing strategies (reliability growth, qualification testing, environmental testing, BIT testing, and maintenance demonstrations) while interfacing with contractor testing teams and the government operational testing community. Remember – RAM is a risk reduction activity. RAM activities and technical processes are risk mitigation activities used to ensure that performance needs are achieved for the success of the mission and that LCC is delimited and predictable. A system that works as needed can be used per CONOPS, and maintenance costs can be budgeted at a low risk of cost overruns. Create technical performance measures (reliability security measures) reported during application management reviews (PMRs) throughout the program's design, development, and testing phases, and use these TPMs to manage risk and mitigation activities. Include the reliability program plan. Rampp (Reliability(or RAM) ProgramPlan (RAMPP) is used to define the scope of RAM processes and activities to be used during the application. A program office of RAMPP can be developed to help guide the contractor RAM process. Application-level rampp forms the basis of the detailed contractor RAMPP, which links RAM activities and deliveries to the Integrated Master Plan (IMS). Ane can predict and model reliability. Use reliability prediction and modeling to assess the risks of meeting RAM requirements early in the application when a hardware/software architecture is formulated. Increase and hone the model later in the acquisition cycle with design and test data during these application phases. Reliability test. Be creative and use a test phase to collect reliability performance data. Ensure that the contractor has planned an error review board (FRB) and uses a robust error and corrective action reporting system (FRACAS). When planning a reliability growth test, you should realize that the actual calendar time will be 50-100% more than the actual test time to allow for analysis of root causes and corrective detected error states. error states. forget the maintenance part of ram. Use maintenance analysis to assess the design to facilitate maintenance, and work with Human Factors Engineering (SMEs) to assess the impact on maintainers. Engage with Integrated Logistics Support (ILS) IPT to help design the maintenance strategy and discuss repair and savings levels. Look for options for collecting maintenance and testability data in all test phases. Look at Error Detection and Fault Isolation (FD/FI) coverage and the impact on repair timelines. Consider and also address software maintenance activity in the field as patches, upgrades, and new software audits. Be aware that the ability to maintain the software depends on the maintainer's software and information technology skills and on the capacity built into the maintenance facility for software performance monitoring tools. A complete maintenance picture includes defining planned maintenance tasks (preventive maintenance) and assessing the impact on system availability. Understand reliability implications when using COTS. Understand the operating environment and THE COTS hardware design envelopes and impact on reliability. Use Failure Modes Effects Analysis (FMEA) techniques to assess integration risk and characterize system behavior during error events. References and Resources Military Handbook 338, Electronic Reliability Design Handbook, October 1998. Asthana, A., and J. Olivieri, Quantifying Software Reliability and Readiness, IEEE Communications Quality Reliability (CQR) Proceedings, 2009, go to August 30, 2017. Report from the Defense Science Board Task Force on Developmental Test and Evaluation, May 2008, accessed August 30, 2017. Department of Defense Instruction, Number 5000.02, Operation of Defense Acquisition System, January 7, 2015, accessEd August 30, 2017. Department of Defense, June 2009, Reliability, Availability, Maintenance, and Cost Rationale Report Manual, access August 30, 2017. CJCSI 3170.01I, January 23, 2015, Joint Capabilities Integration and Development System, accessEd August 30, 2017. The DoD Guide for Achieving Reliability, Availability, and Maintainability, August 2005, is accessed August 30, 2017. Quanterion Solutions Incorporated, 2015, System Reliability Toolkit-V: New Approaches and Practical Applications, accessed August 30, 2017.