LIFE

CYCLE

ASSET

MANAGEMENT

Good Practice Guide
GPG-FM-004

Reliability, Maintainability, Availability (RMA) Planning

March 1996

Department of Energy
Office of Field Management
Office of Project and Fixed Asset Management

This page intentionally left blank.

1. INTRODUCTION

1.1 Reliability, Maintainability, Availability

The control of life-cycle cost is a primary concern during the development, production, construction, operation, and decommissioning of Department of Energy (DOE) systems and facilities. Analysis used to control the cost of overhaul, maintenance, and repair is called Reliability, Maintainability, Availability (RMA). Though overhaul, maintenance, and repair are major contributors to operations costs, concern about achieving the performance objectives often dominates the development process. The extent of overhaul, maintenance, and repair required during operation is largely determined by the design of a system or facility. Thus, the operating characteristics of a system or facility are determined during the design process. Equal attention should be paid to both performance and RMA issues during the design process to control risk related to meeting the full scope of desired operational characteristics. This attention directly contributes to the control of life-cycle cost. This Guide addresses techniques that can be applied throughout the life cycle, but principally during development and construction, to minimize risk and control RMA parameters.

This Guide is one of several for implementing DOE O 430.1, LIFE-CYCLE ASSET MANAGEMENT. (See *Guide to the Guides*, GPG-FM-000.) DOE O 430.1 provides requirements for DOE, in partnership with its contractors, to plan, acquire, operate, maintain, and dispose of physical assets. Requirements within the Order focus on *what* should be done, not *how* it should be done. Chapter 2 of this Guide, Principles and Processes, explains the use of RMA planning.

1.2 Developing an RMA Program

This Guide is intended to provide a basis for tailoring an RMA program for the design and construction of DOE project end products. The first step in establishing an RMA program is to develop a requirements statement. The requirements statement is used to define the following parameters:

- operational needs for the design life of the desired end product;
- expected normal and worst-case operating conditions;
- expected downtime for either corrective or preventive maintenance actions;
- and similar parameters.

The requirements statement is used to develop an availability statement for the end product, which can be used to allocate RMA indices to major subsystems. In this process it is important to match the requirements statement to the level of complexity and the intended use of the end product. End products that are large, highly complex, or have a mission that may directly affect human or environmental safety generally require considerable RMA effort; other relatively small or simple end products require much less RMA engineering attention. This "graded" approach to establishing RMA requirements and applying engineering discipline ensures that the value received from engineering effort is in consonance with that of the end products. Chapter 3 presents the methodology for grading RMA requirements.

The RMA requirements are interpreted in engineering terms meaningful to designers and allocated to lower-tier subsystems. Following this allocation, process analysis is performed to "roll-up" allocated values to verify that they are consistent with top-level requirements. A byproduct of this analysis is the identification of items that are necessary to accomplish top-level requirements. These items are termed "critical" and subjected to specialized attention ensure they attain allocated values. This approach leads the engineer through a systematic course of action that ensures complete and accurate accounting of factors that determine the overhaul, maintenance, and repair costs of end products, thereby providing a means for continual assessment and control.

1.3 Risk Management

Risk management as related to RMA indices is accomplished through the following sequence of engineering activities proceeding from requirements analysis, to allocation, to assessment.

- Identify the desired operational characteristics of the end product against measurable risk.

- Define these characteristics at the end-product level in terms of a quantitative availability statement made against a formal operational time line. This time line is termed the Design Reference Mission (DRM) and includes the sequence of planned operations of the end product in normal and worst case conditions.

- Allocate these requirements to lower tier internal end product subsystems, equipment and components to document their respective contribution to the operation of the overall end product.

- Formally estimate the expected performance of each major system, subsystem and equipment through appeal to historical data or engineering analysis.

- Roll up these system, subsystem, and equipment level estimates to the end-product level through system simulation techniques to provide an estimate of the expected performance of the end product, which can then be compared to the end-product level requirements.

- Identify equipment that contributes to the overall system downtime.

- Designate this equipment as critical equipment and subject it to specific engineering activities to improve its expected performance, thus improving the expected ability of the overall end product to meet its top-level requirements.

1.4 Interfaces with Other Guides

Because the RMA discipline deals with all aspects of end product design and construction, it interfaces with all of the other Good Practice Guides that provide engineering information. Table 1 presents general input and output information between this RMA Guide and the other Guides.

Table 1. RMA - Guides Interface.

Guide	Input from RMA Guide	Output to RMA Guide
Project Management Overview	"Graded" project RMA program	Project top-level objectives
Project Execution and Engineering Management Planning	"Graded" RMA program	System engineering plan
Critical Decisions Criteria	Allocated requirements for critical equipment	Mission statement
Engineering Tradeoff Studies	Results of RMA analyses	Alternatives for analysis
Test and Evaluation	Assessment methods and basis	Test objectives and conditions
Status Reporting	RMA assessments	Performance measures
Project Risk Analysis	Critical equipment RMA assessments	Project baselines
Project Work Planning and Control	"Graded" project RMA program for critical equipment	Project baselines
Baseline Change Control	Proposed corrective actions	Project baselines and changes

This page intentionally left blank.

2. PRINCIPLES AND PROCESSES

2.1 The RMA Engineering Process

From an overall management perspective, the principal lesson to be learned from highly successful projects is that RMA engineering is most effective when it is initiated early in the end product design process so that potential problem areas can be recognized early enough to allow corrective action with little impact on interfacing systems, cost, or schedule. However, RMA engineering is a design discipline and, as such, should be applied at all stages of the design process.

The RMA engineering process is based on the following general concepts.

- Availability is the top-level RMA requirement for an end product. Formally, availability is defined as the ratio of total end products up-time divided by the total time. Operationally, this definition establishes bounds for overhaul, maintenance, and repair actions and their attendant cost. From an engineering perspective, the availability statement establishes the basis for allocation of requirements to subsystems and the measure of success to be applied in examining results of assessments of the design.

- Availability is an operational parameter, suitable therefore for defining a top-level end product RMA requirement. However, an availability statement includes operational considerations that are not characteristics of the end product design. Thus, availability is not directly usable as a design requirement. It should be reinterpreted in meaningful terms and under the control of the design process. In general, this reinterpretation involves the recognition that stating the total up-time for an end product in turn establishes a statement of the total downtime. This measure, the total downtime for the end product, is then allocated to the lower-tier systems in the form of design requirements. The relative complexity of subsystems is generally used as the basis for this allocation process.

- After end product downtime is allocated to subsystems, analytical techniques are used to estimate the actual downtime expected to be experienced by the various subsystems during operation. These estimates include the frequency of failures and the time required to return the failed subsystem to operational status. These estimates for all subsystems are then "rolled-up" to the end-product level by a summation process to estimate the availability of the end product as designed. This estimated availability is then compared with the availability requirement as a measure of success.

- Because the engineering assessment of the design involves estimating the operating characteristics of end product subsystems, this process reveals their individual contributions to the overall downtime of the end product. In addition, since the engineering assessment is a design activity, the difficulty of achieving each subsystem's allocated requirement can be evaluated. This process provides the basis for an iterative optimization of the design for minimizing this difficulty, including designs for those subsystems estimated to offer the most difficulty.

This process of identifying a top-level availability requirement, decomposing it into the design meaningful downtime statements for subsystems, estimating subsystem downtimes through analytical methods, and formally summing these downtimes to estimate the availability of the end product is the essential outline of RMA engineering.

Modern RMA system engineering disciplines can be largely traced to two major engineering projects from the late 1950s and early 1960s. (Appendix E contains a more complete discussion of this history).

2.2 Interface with Engineering and Project Management

The principal link between RMA engineering and other engineering disciplines is the documented end product availability statement. This statement should be included in the technical baseline for the end product. In addition, the financial and schedule implications of the availability statement should be reflected in the cost and schedule baselines for the project

During the planning, design, and construction phases of a DOE end product, organizations are responsible for executing technical processes. For small-scale, simple, end products, these organizations may not be distinguishable from those performing design activities. For large, complex end products, separate engineering organizations are often established to perform these functions.

However the RMA activities are organized, the organization performing the basic design of the end product and its internal systems is responsible for performing the RMA activities described herein because their design activities determine the performance of the end item.

To accomplish the RMA activities for an end product, RMA activities should be considered on a par with other design activities directed at governing performance, cost, and schedule. Since the project management function generally accomplishes the design process through an organization assigned such responsibility, application of RMA disciplines should also be assigned by project management. This organization, be it internal DOE or an external engineering firm, should be responsible for developing the top-level availability indices for the end product and its allocation to the major systems. Through their design activities, they perform such an allocation, whether it be formally documented or not. For example, the requirement for the performance of these allocations and estimates should be made part of any prime contract for design engineering services. Subsequently, allocated requirements for major internal systems should be documented in procurement or development specifications and made part of contractual instruments. Products required to support this top-level process for large/complex projects include the following.

- Availability for the end product and an associated Design Reference Mission (DRM). Page 1 of appendix A provides an example of an end product availability statement and an associated DRM.

- Identification of the maximum allowable downtime for the end product. Page 1 of appendix A provides an example of downtime and associated operational times for an end product. An example of the derivation of these parameters is provided in section 2 of appendix B.

- Standard Task Statements for RMA actions to be either provided to internal engineering organizations or levied on performing contractors.

- Data Item Descriptions for required RMA engineering products;

Specific products from small/simple projects should be graded to meet the end user's needs. End product development generally follows the life-cycle model shown schematically as Figure 1. Table 2 shows the RMA activities by phase. These RMA activities lead to the development of a series of products which offer objective evidence of the application of the RMA disciplines and document the results of their application.

2.3 Operational Availability

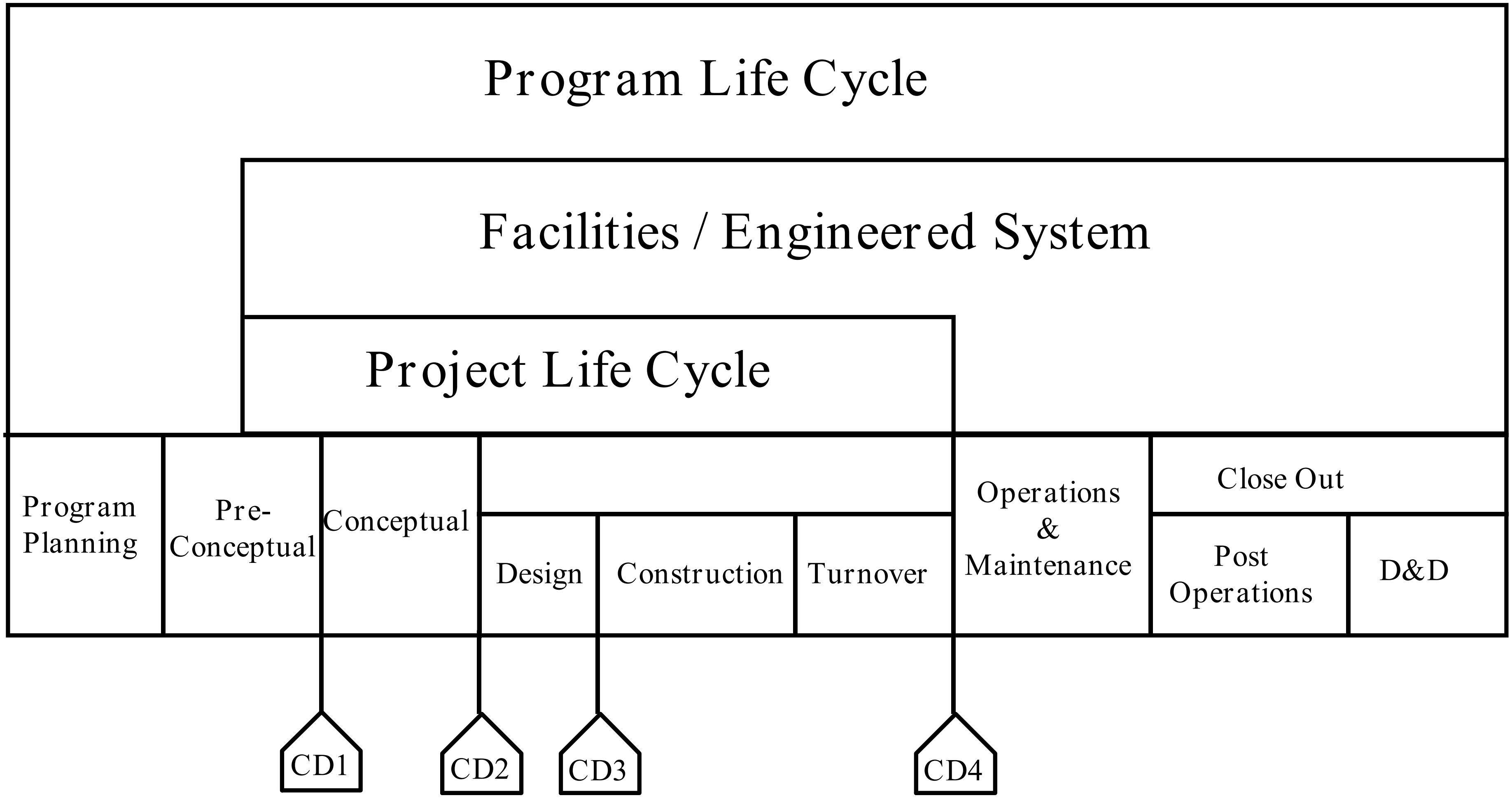
Though operational availability is a meaningful measure of end product performance for operations and management (O&M) organizations, it is of little use to the system or equipment designer because it is an operating characteristic of a system, not a design parameter. Availability does not uniquely determine a design; in fact, many designs may provide an end product with a given availability—some achievable, others wholly unrealistic. However, there is a set of parameters that is mathematically related to availability but can be controlled by the designer. The definition of operational availability as the quotient of uptime over total time may be formally recast into design meaningful numerical statements or indices in terms of the following parameters:

- mean-time-between-failure (MTBF), defined as the average interval of system uptime during the defined operation;

- mean-time-to-repair (MTTR), defined as the average system downtime, excluding logistics delays such as waiting for spare parts or maintenance personnel;

- mean-logistics-delay-time (MLDT), defined as the average time spent waiting for spare parts or maintenance personnel once a failure has occurred.

Figure 1: Life Cycle Model



CD: - Critical Decision
D&D - Decontamination and Decomissioning

Table 2. RMA Activities by Phase.

Life-Cycle Phase	Principal RMA Activity
Program Planning	Identification of RMA Activities
Preconceptual	Establishment of requirements, including availability statement and DRM
Conceptual	Requirements allocation
Execution • Design (subphase)	System analysis and identification of critical systems; formal RMA analysis and critical items programs
Execution • Construct (subphase)	Critical items programs, development test and evaluation
Execution • Turnover (subphase)	Validation of achievement of RMA allocated requirements
O&M	Surveillance and corrective actions
Closeout • Postoperations (subphase)	Project "lessons learned"
• D& D D&D (subphase)	RMA activities for specialized D&D processes

These three parameters can then be used in a formal expression of operational availability:

$$A_o = MTBF/(MTBF+MTTR+MLDT)$$

Often the contribution to downtime caused by the logistics system (MLDT) is dropped providing a definition of inherent availability:

$$A_i = MTBF/(MTBF + MTTR)$$

which is composed entirely of parameters that are controlled by the designer.

This end-product level availability statement is now interpreted in terms of a compatible MTBF, MTTR, and MLDT. The first two parameters are then provided to equipment designers in specifications to govern their design efforts, and the last is provided to the logisticians to develop the overall maintenance and support philosophy.

2.4 RMA Products by Program Life Cycle

RMA engineering efforts and products generally follow the life cycle phases for development and operation of the end product.

2.4.1 Program Planning Phase

During the program planning phase, RMA activities should be directed at determining the appropriate RMA program for the planned end product.

- To the extent possible obtain historical operating and maintenance histories for end products of a similar nature.

- Determine significant deviations between end products providing historical data and the planned end product. Examples of such deviations include use of new technologies, operation in harsher environments, greater required uptime, which might result in the assessment that the planned end product offers a greater challenge to develop, construct, and operate;

- From historical data and its variations select RMA engineering activities appropriate to the planned end product.

RMA engineering activities to be employed during an end product's life cycle are selected using a graded approach. An end product for which historical data, estimated complexity, or criticality of mission suggest considerable risk exists that may adversely affect the cost of overhaul, maintenance, or repair should receive a greater RMA effort than an end product assessed as offering less challenge when judged by the same criteria.

2.4.2 Preconceptual Phase

During the preconceptual phase, RMA activities pertain to establishing top-level requirements for the end product:

- establish operational availability as a requirement;

- incorporate operational availability into a formal mission statement;

- define an operational time line including specification of uptime (life or annual) and downtime (life or annual); and

- analyze the realism/credibility of requirements based on O&M data from other similar facilities or systems and adjust requirements based on these results.

The operational availability and mission profile for the end product is generally established by the “customer,” which usually represents the ultimate user. These requirements are developed to establish that the end product will meet user needs and expectations during operation.

RMA analysis of an end product starts with the specification of its availability. As described previously, the DRM of an end product provides a target for desired total operational time and maximum uptime. This fraction is called the average availability for the end product and can be simply described by the expression:

Average Availability = Total Uptime/Total Time

Because this measure includes all downtime from any source (planned and unplanned maintenance, major end product overhaul, and any other downtime), over the described mission profile, this measure is usually called the mission operational availability, or A_{om}.

Specification of total uptime and total time provides the maximum allowable downtime through simple subtraction:

Maximum Allowable Downtime = Total Time - Total Uptime

If, however, the downtime estimates used exclude any time arising from waiting for replacement parts for any that might have failed, or for maintenance personnel to become available, this figure of merit is called the mission inherent availability, or aim. This measure, aim, represents an upper bound of the performance capability of the system under evaluation in that all logistics effects are removed from the analysis.

If, for example, one is given an objective to "build a power plant," no work could begin until a few basic parameters are provided. The desired output wattage, peak and average, is clearly an important example. Regulatory and financial considerations might dictate the specification of fossil over nuclear fuel with a further focus narrowing the choice between coal or natural gas. Similarly, the location of the power plant is of critical importance. Coastal or inland, seismically active or inactive, soils composition, and similar parameters each imply a distinguishing set of special environments which, in turn, directly affect the design of the overall power plant, its structure, and functional systems. Finally, cost-of-ownership targets are usually given to bound such parameters as average maintenance costs, anticipated maximum downtime, and life of the power plant. Given this set of characteristics, defined in engineering terms in a formal mission statement, the developer can then proceed with the design and construction of the power plant.

For the power plant model, this profile would account for both short- and long-term variations in operation. Daily minimum, average, and peak output profiles would be provided against a 24-hour clock. These daily profiles would then be adjusted against an annual calendar detailing expected seasonal variations dictated by demand. Long-term, but planned, variations in this cycle due to annual climatic extremes over the prescribed life of the power plant; such events as power plant shutdowns for major system overhaul would also be identified.

Superimposed on this "normal operation" profile would be abnormal events that might directly affect the overall operation of the power plant. If, for example, the power plant were to be sited in a seismically active area the mission profile should describe the occurrence of these events. Once again, expected annual occurrences and "worst-case" events over the life of the power plant should be included. Similarly, the occurrence of catastrophic weather events should be detailed. In such cases both the direct and indirect effects on the power plant should be identified. Direct impacts, such as stress on operating components of a coastal power plant during a tropical hurricane may be dramatic; but indirect effects, such as major load fluctuations and temporary isolation from spare parts and maintenance personnel in the immediate aftermath, may also be critical.

In general, then, a proper DRM for a power plant, or an end product provides a time line that delineates all potential operational conditions ("normal" and "worst-case") throughout its expected life. Furthermore, conditions should be specified in sufficient detail to allow the design engineer to interpret them in terms that constrain the design of the end product and its systems. Reference to seismic activity, for the power plant example, should specify expected magnitude and duration.

The overall mission statement for the end product, its operating time line, and supporting engineering notes describing the conditions of each operating "phase" within the time line provide a DRM for the end product. The DRM should be delivered as a formal document.

Finally, at the end-product level, the rationale behind allocating total downtime to the various categories (corrective maintenance, overhaul, preventive maintenance, etc.) should be documented. Presumably, for example, a level of preventive maintenance is selected to preclude catastrophic failures that might have major impact to safety or downtime. Tradeoffs may be conducted where the "cost" of a run-to-failure operational philosophy should be weighed against a philosophy of manning and sparing preventive maintenance activities. Numbers and availability of maintenance and repair personnel as well as spare parts inherent in the assumption should be documented because they provide an upper level of available resources to be allocated to major subsystems.

The mission statement, profile, and supporting data and rationale should be reviewed at major project development stages as part of the normal review process.

2.4.3 Conceptual Phase

During the conceptual phase (formulation of the end product design and subtier development of internal systems), the allocation process proceeds, followed by initial estimation or prediction efforts:

- allocation of end product downtime to major systems consistent with the DRM. (Table 5.l appendix A provides an example);

- expand the DRM to a greater degree of detail for the end product and develop those for major systems (see appendix B);

- analyze the realism/credibility of system-level allocations based on O&M data on similar systems; and

- prepare MTBF, MTBR, MLDT, and related indices. (Table 3, page 3, appendix A provides an example).

Because operational availability is the fundamental, or top-level, RMA parameter for the end product, it should be allocated to major internal systems. In actual practice, this allocation process is accomplished by distributing the maximum available downtime for the end product. The total downtime for the end product, provided in its mission statement, should be first allocated at an end-product level over the entire time line prepared for the mission profile. This allocation will provide an end-product level upper limit on such activities as overhaul, repair, and preventive maintenance, whether scheduled or unscheduled. The reasonableness of this end-product level distribution of downtime should be demonstrable through appeal to historical data on end products that are either similar in function or complexity. Where no existing end product is considered wholly comparable in mission, or if the new end product is to make use of new technologies or processes, background information from the development of these technologies or processes to support the downtime estimated for the end product should be provided. These downtime estimates will provide the basis for the specification of RMA indices to subsystems. Hence, it is of considerable importance that the downtime estimates at the end-product level have a firm historical or engineering foundation.

As with the determination of downtime at the end-product level, system-level allocation should proceed from historical or engineering data. Where firm historical data exist for operational subsystems, it should be used and the source of the data, and its assumptions, referenced. In its absence, data on systems of similar complexity and operation should be used, once again suitably supported by reference materials.

The functional level to which this allocation process should proceed is largely determined by the validity and comprehensivness of the available data. If, for example, a large volume of historical data exists for a similar end product, and their mission profiles are also largely compatible, allocation need not proceed lower than that of the major subsystems to be procured as functional units. If, however, the functionality of the end product is new, its siting is peculiar in some aspect, or its desired performance (including availability) is greater, the allocation process should be similarly more detailed.

This process of review should proceed at each major level of allocation; each subsystem need not be treated equally. For example, if the total heat load of an end product can be accurately estimated to be within normal bounds (including peak conditions) of operating products of similar complexity, specification of indices for the entire end product may be sufficient. If, however, the power requirements, and resulting thermal loading, are particularly demanding, allocation of requirements to major components such as compressors and heat exchangers may be warranted.

In each case, the governing principle should be one of recognizing and addressing the level of risk involved. If the effects of the failure of a particular subsystem are not significant, the probability of occurrence small, and a significant operating margin exists, detailed allocation and analysis may not be necessary. If , however, the impact of system failure on the overall end product would be great, and analysis suggests that such a failure could occur, detailed allocation and analysis should proceed.

Once allocated, the individual downtime for the subsystems may be used to develop availability figures of merit for subsystems. A mission profile for each system should be derived from that of the overall end product. Each mission profile should reflect the operational phases required of the particular system to allow the end product to achieve its mission profile.

2.4.4 Execution Phase: Design Subphase

Throughout the execution phase (design, construction, and turnover subphases), but specifically during the execution design subphase, it is necessary to perform engineering activities to assess whether the emerging end product can be expected to exhibit the overall operational characteristics desired. As with functional parameters, computations may be made to evaluate whether the desired availability levels will be achieved over the life of the end product. The techniques employed to perform these assessments are statistical and provide an estimate of expected performance in a probabilistic statement.

- Perform specialized RMA analyses on subsystems and equipment as the design progresses to evaluate the probability of meeting allocated values and identify particular problem areas by performing such RMA engineering activities as failure modes, effects, and criticality analysis (FMECA), stress analysis, and similar studies. (See section 4.2 of appendix A for an example).

- Identify what prohibits a particular subsystem or equipment from attaining its allocated requirement and determine corrective action. (Section 4 of appendix B provides a detailed example of this process.).

- Perform an end-product level "roll-up" of actual RMA values to assess achievement of the overall end product availability requirement. (Table 3 of appendix A provides an example of the results of this type of analysis).

- Develop and perform necessary test and evaluations to confirm end product and subsystem RMA indices.

Historically, techniques were developed to estimate the probable number of failures of a component of the system over a defined time. Then, from other considerations, an estimate was made of the average downtime each failure was expected to cause. If this accumulated downtime was subtracted from the total time chosen for the analysis, an uptime resulted, which allowed an estimate of availability by simple division.

Whatever the availability estimated, the crucial factor contributing to its ultimate value is the estimate of the number of failures of the item. It is in this estimate that statistical techniques are used.

As discussed in appendix D, detailed failure mechanisms for both mechanical and electrical systems are physical manifestations of some form of stress; this model can be extended to systems using computer programs. Hence, a comprehensive estimation of failure frequency of a particular item is based on an understanding of these stress producing processes.

Fortunately for the vast majority of components one might use in the production of major subsystems required for an end product, one need not perform detailed studies into the physics of failure of the device. The failure history of virtually all devices in common use, mechanical or electrical, are accumulated by the U.S. Government for use in estimating failure frequency of the components. The Government Industry Data Exchange Program (GIDEP) has provided a forum for the submittal of such information for almost a half century. In addition, specialized test and evaluation programs have been developed to analyze the reliability of most components. In addition, most major equipment suppliers have developed and maintained detailed failure and maintenance histories on their equipments as a basis for costing warranty programs. This information represents billions of operating hours and is classified in a manner that allows one to estimate the variations in expected failure rates arising from intended use of the device and the anticipated level of stress.

Using this information, the developer of major end-product subsystems and equipment should estimate the failure rate over the defined end product mission profile. Early in the design process this estimate may take the form of obtaining data from prior users of the equipment or from manufacturers. If substantial variations in equipment design or operating conditions are present, such estimates should proceed from the component level. The resulting product of such analysis is a reliability analysis document detailing the expected failure rates of system equipment and the sources of part failure information.

For simple equipment that operates only under steady-state conditions, this analysis may be performed using analytical means. The failure rate per hour of each component in the equipment is estimated. This may only require a simple table lookup; in other cases, actual stress levels may need be calculated and used in the estimate. For equipment of moderate complexity, the effects of redundancy should be considered if present.

At the level of major subsystems, and certainly at the end-product level, estimates of RMA characteristics should include the various phases of operation described in the mission profile as well as the effect of logistics considerations. The final stage of statistical estimation of these parameters is the performance of an all-up end-product level simulation of RMA characteristics. For complex systems, with various operating rules, and including logistics consideration, such "open form" techniques are required.

Using such techniques as the U.S. Navy's TIGER simulation program, the RMA characteristics of entire ships and petrochemical end products containing several thousand components have been estimated. Such simulations provide a comprehensive view of the failure frequency and maintenance times of the entire end product reflected against the DRM. This failure and maintenance information is provided for each equipment item included in the analysis. This allows the designer to immediately identify equipment that is a major contributor (critical items) to system downtime either through the total number of failures or through the time required for individual maintenance actions. In either event this critical items listing provides a basis for the management of risk and improvement actions. The results of this end-product level analysis, the availability and reliability critical items, and any programs developed to improve them, should be formally documented.

The point in the design process when the initial system-level RMA analyses have been completed and the reliability and maintainability critical items and the results of these system-level analyses have been "rolled up" to demonstrate the achievability of the end product availability requirement is often identified with the end of a major RMA engineering milestone. The two phases of an end product's design process are commonly called the “preliminary design phase” and the “critical design phase.” When a program makes such a distinction, the demonstrated achievability of the end product's availability requirement should be accomplished by the end of the preliminary design phase.

Following this RMA program milestone, emphasis should be placed on achieving the estimated values. This is accomplished through the continuing assessment of design activities to ensure that assumptions made during the design process are valid. During major system procurement, RMA efforts should concentrate on those items identified as critical to the performance of detailed equipment- and component-level engineering, such as stress analysis, FMECA and similar activities appropriate to the equipment level.

RMA activities during the critical design phase are generally focused on eliminating risk areas identified in earlier analyses through critical item programs and the iterative assessment of results through continuing analysis and simulation to the end-product level.

Though the actual engineering techniques applied are not different during this stage of development, the degree of application is performed at an ever-increasing level of component detail, principally focused on critical items. During this process items judged as critical at one stage are removed from the list as focused engineering attention mitigates the fundamental causes for their designation. In contrast, other items emerge as critical as the designs become more definite and greater insight into their expected operational characteristics is obtained.

Ideally, the final result of the critical design stage is a product technical baseline that will meet the intended operational availability of the end product when analyzed against the defined mission profile. A companion to the technical baseline is a list of critical items that have characteristics that can be controlled during the manufacturing and construction processes to mitigate the causes of failure or high-maintenance times. These items, and their manufacturing and construction processes, will be the major focus of RMA surveillance during the next life-cycle stage.

2.4.5 Execution Phase: Construction Subphase

Principal RMA activities during the execution construction subphase (production of systems and equipment) involve the surveillance of equipment and systems to ensure that they meet their allocated requirements.

This surveillance takes two forms:

- review of all production and test documentation of major systems and equipment to identify potential problem areas and to verify expected performance; and

- focused attention to critical items, including conduct of specialized tests such as stress screening or demonstrations to eliminate latent defects or validate requirements. (Appendix D provides an example of this type of effort).

The final product of the construction process should be a formal end product data package describing the as-built configuration of at least the major subsystems and equipment which have been identified as critical and subjected to specific management actions. The significant element of this data package is identification of critical equipment sources and any waivers or deviations that may have been granted during system production or construction. This information can be used if unexpected problems arise.

2.4.6 Execution Phase: Turnover Subphase

The execution turnover subphase is a formal process of certifying that the end product meets or exceeds its requirements. RMA activities during this phase pertain to:
(1) formal installation, testing, commissioning, and turnover activities to validate the as-installed systems and (2) development of documentation supporting the acceptance actions.

RMA products during this stage include contributions to acceptance reports, test reports, and contribution to the installation and checkout formal documentation.

2.4.7 O&M Phase

RMA activities during end-product operations involve surveillance of subsystems and equipments to ensure that they continue to meet their allocated requirements over time:

- Establish and maintain a Failure Data Collection, Analysis, and Corrective Action (FRACAS) program;
- Establish and maintain RMA programs for development of replacement or improved items.

During operation, a formal FRACAS program should be maintained to capture data and accomplish corrective action for critical systems. This process allows for the ongoing assessment of system performance and possible recognition of operational problems prior to the occurrence of catastrophic events.

In addition, participation in formal activities such as GIDEP to disseminate information to other potential developers of like systems is appropriate.

2.4.8 Closeout Phase: Postoperations Subphase

The closeout postoperations subphase of an end product is governed by dismantling the facility or similar activities. RMA has a single activity during this phase: documentation of "lessons learned" during the end product life cycle. This information is of use in establishing future RMA programs for new end products.

2.4.9 Closeout Phase: Decontamination & Decommissioning Subphase

Decontamination & Decommissioning (D&D) efforts often involve development of specialized equipments to aid in dismantling the end product. The specialized equipment and systems are themselves end products with missions to support D&D actions: application of the RMA disciplines previously described for specialized equipment or facilities developed solely for the purpose of decommissioning the end product. The complexity and criticality of the original end product often is directly related to the complexity and criticality of the specialized equipment developed for the closeout D&D subphase.

2.5 Integration of RMA Information with Risk Management

The principal programmatic tools required for the successful execution of RMA efforts are (1) the early establishment of data requirements and (2) means of access to the data because the data provide the measure of accomplishment against risk. This is usually accomplished through contractual documents that establish contract data requirements, including their format and informational content. (See section 2.8)

The Project Management Office should consider the results of RMA estimates and progress in critical item programs of risk management activities performed against technical, cost, and schedule baselines as part of the overall management assessment. Clearly, the timeliness of required information should support major program decisions.

Programmatically, the specific RMA tasks described herein, together with the resources to perform them, should be tasked via contract deliverables.

An overall view of the allocation document for an end product will identify that some subsystems and equipment can be expected to meet their allocated downtime requirements with a comfortable margin. If a particular piece of equipment is expected to exhibit greater-than-desired downtime for accumulated corrective maintenance, it could be designated as reliability critical and efforts could be initiated to lower its frequency of failure. An item that has a marginal amount of accumulated preventive maintenance time would be designated as maintainability critical and effort could be expended to reduce this time by either extending the interval between maintenance requirements or reducing the time required for servicing the equipment.

The methods for reducing risk include identifying critical equipment and aggressively pursuing improvement actions. Because failures and maintenance activities directly affect cost and schedule, any risk reduction resulting from critical equipment programs will benefit technical, cost, and schedule baselines.

2.6 Integration of RMA Information with Quality Assurance

In general, quality assurance has come to refer to two somewhat distinct but deeply intertwined arenas of activity. The first is those broad organizational actions generally termed "Total Quality Management" (TQM); the other is those specific product-directed actions involved with product acceptance. RMA activities directly influence and are influenced by each level of quality assurance activity but in somewhat different ways.

One of the primary principles of TQM is the establishment of performance measures that are meaningful indicators of organizational effectiveness. For an organization charged with performing any of the life-cycle stages of an end product, the achievability of the overall availability statement for that end item is a natural performance measure in the TQM context.

Availability is an appropriate TQM performance measure in that it:

- is directly related to the overall end product's mission, hence that of the implementing organization;
- is measurable;
- is within the organization's ability to achieve.

Naturally, accomplishing the programmatic activities such as flow-down of allocated values to system and equipment levels through contractual or similar documents, and similar activities can be used as performance measures for those administrative or business management personnel charged with such activities. Thus, these RMA indices provide a unique ability to be used as TQM measures for technical, management, and administrative personnel and the organizations in which they reside.

In the second context, the critical item programs should directly influence quality assurance activities involved with qualification and/or acceptance of equipment, systems, and the end product.

Often the physical characteristic of a particular item that causes it to be judged as critical is one that can be inspected or tested. Accordingly, RMA activities should contribute to the preparation of test and evaluation planning and results assessment. In this manner RMA activities are an integral part of the formal quality assurance process.

2.7 Integration of RMA Information with Configuration Management and Change Control

As with quality assurance, configuration management and change control operates on two levels. In the first instance the evolving product design may result in changes to product technical, cost, or schedule baselines, which are considered to be top-level or global program parameters. The ongoing RMA activities during the development process may directly affect these baselines in two ways:

- by forcing changes in the selection of equipment or components to meet required RMA parameters; or

- by forcing changes in life-cycle cost or schedule to accommodate these changes if analysis shows previously established baselines to be unachievable.

In the other instance, RMA engineering directly participates in formal configuration management activities such as functional and physical configuration audits and review of proposed changes representing end product RMA interests.

2.8 RMA Documentation

Though a large variety of formal RMA documentation is specified in military and other government requirements documents specific to the subject, the following are considered to be applicable to a broad class of end products. The level of detail required, in both these documents and subtier implementing ones, should be determined using the tailoring or "graded" approach discussed in section 3.

- Operating and maintenance histories for end products of a similar nature.

- Significant deviations between end products providing historical data and the planned end product.

- List of RMA engineering activities appropriate to the planned end product.

- Statement of required operational availability.
- Formal mission statement incorporating the required operational availability.
- An operational time line, including specification of uptime (life or annual) and downtime (life or annual).
- Analysis of the realism/credibility of requirements based on O&M data from similar end products and adjusted requirements based on these results.
- Allocation of end-product downtime to major systems consistent with DRM.
- Expansion of DRM to greater degree of detail for end product and development of those for major systems.
- Analysis of realism/credibility of system-level allocations based on O&M data on similar systems.
- MTBF, MTTR, MLDT, and related indices.
- Results of specialized RMA analyses on subsystems and equipment as the design progresses to evaluate the probability of meeting allocated values and identification of particular problem areas.
- Identification of the fundamental reason which prohibits a particular subsystem or equipment from attaining its allocated requirement and proposed corrective action.
- Results of end-product level "roll-up" of actual RMA values to assess achievement of overall end-product availability requirement.
- Plans, procedures and results of necessary test and evaluations to confirm end product and subsystem RMA indices.
- Results of review of all production and test documentation of major systems and equipments to identify any potential problem areas and to verify expected performance.
- Results of specialized critical item efforts, including conduct of specialized tests such as stress screening or demonstrations to eliminate latent defects or validate requirements.
- Results of formal installation, test, and commissioning activities to validate the as-installed systems.
- Documentation supporting the acceptance actions.

- FRACAS reports.
- Documentation required by RMA programs for development of replacement or improved items.
- Documentation of "lessons learned" during the end product life cycle.
- Documentation of the entire RMA disciplines for specialized equipment or facilities developed solely for the purpose of decommissioning the end product.

There are potentially a host of subtier system and equipment level documents of like designation for reporting the results of highly specific analyses. These documents are identified in the various documents referenced in section 2.9 and can be selected as determined through the grading process.

2.9 Reference Material, Standards, Procedures, and Manuals

- MIL-STD-470B, Maintainability Program Requirements, May 1989.
- MIL-STD-471A, Maintainability Verification/Demonstration/ Evaluation, Notice 3, March 1973.
- MIL-STD-721C, Definitions of Effectiveness Terms for Reliability, Maintainability, Human Factors, and Safety, June 1981.
- MIL-STD-756B, Reliability Prediction, November 1981.
- MIL-STD-785B, Reliability Program for Systems and Equipment Development and Production, September 1980.
- MIL-STD-1629A, Procedures for Performing a Failure Mode and Effects Analysis, November 1980.
- MIL-HDBK-217F, Reliability Prediction of Electronic Equipment, December, 1991.
- NSWC-94/L07, Handbook of Reliability Prediction Procedure for Mechanical Equipment, March 1994.
- NPRD-95, Nonelectronic Parts Reliability Data, January 1995.
- AVCO, Reliability Engineering Data Series Failure Rates, April 1962.

3. GRADED APPROACH

3.1 General Approach

The RMA program applied to a specific end product should be graded to suit the criticality of the product and its intended use. Some global project issues that govern this process can be made without reference to the size of the project, the complexity of the end product, or its actual implementation in hardware. These issues usually refer to potential worst-case results from a major end-product catastrophic failure. If a catastrophic failure could result in loss of either life or expensive or irreplaceable material or in major contamination or destruction of the environment, then, regardless of the size or complexity of the project, the RMA program selected should be of sufficient depth and detail to preclude such events.

Such a principle can be similarly applied at the subsystem or equipment level. Even if the project's end product is simple enough not to exhibit failure mechanisms meeting the scope of critical criteria just described, major project systems or equipment may exhibit them to varying degrees. In this case, the project may invoke an RMA program far more detailed than that executed at the end-product level for the equipment and systems.

The principles used to decide the degree to which RMA engineering disciplines should be applied to a project, regardless of size and complexity, are (1) the effect of a worst-case failure of the end product and (2) the likelihood of its occurrence. As this statement suggests, at least the establishment and evaluation of a top-level mission profile and FMECA may be required to make this assessment.

Another global consideration in grading an RMA program to meet end-product requirements is the degree to which the design and operation of either the end product or its major systems are understood. When an end product is one of a relatively long history of similar items with considerable operational experience and known design, the RMA program need only be designed to ensure that the evolving end product adheres to the assumption of similarity. This effort is not only conducted through the design phase but also through construction to ensure that as-built is as-designed. Surveillance to avoid acceptance of substandard materials is an example of this activity.

If the end product, either itself or in its major subsystems, employs new technologies, applies familiar ones in new applications, or the required availability is more challenging than previously encountered, a more detailed RMA program may have to be employed.

3.2 Large/Complex Projects

The RMA products listed in section 2.4 are considered a minimum list which should be obtained for any large/complex project with an engineered end product, though the complexity may vary to reflect the end-product characteristics.

At the equipment or major system level the tailoring should be according to the identified critical items. Items so identified should be subjected to comprehensive RMA analyses, including appropriate stress analysis, test, and demonstration; other items may be subjected to periodic surveillance actions alone. As this statement indicates, the degree of application of RMA disciplines on a particular item is difficult to predict at the outset of a program. As items are identified as critical, their RMA efforts should be expanded to be contracted as they are judged to no longer warrant such designation.

3.3 Small/Simple Projects

Small and/or simple projects should review the following list of questions as a way of exploring the possible need for RMA considerations on a particular project.

- Will unplanned and/or frequent facility failures have a large impact on the effectiveness of the facilities for the user?

- Will frequent or long downtimes have a large impact on the effectiveness of the facilities for the user?

- Do equipment or subsystem designs that are identical or similar in function but radically different in terms of reliability make a difference on the effectiveness of the facilities for the user?

- Do equipment or subsystem designs that are identical or similar in function but radically different in terms of preventive or corrective maintenance requirements make a difference on the effectiveness of the facilities for the user?

- Do equipment or subsystem designs that are identical or similar in function but radically different in terms of cost of ownership make a difference on the effectiveness of the facilities for the user?

If the answer to any of the above questions is “yes,” an RMA program for that particular project may be warranted.

4. MEASURING FOR RESULTS

Two methods of measuring the results of RMA programs are commonly used: the first is an organizational measure; the second refers to a specific end product.

When a single organizational entity is responsible for several end products over its life cycle, the effectiveness of that organization may be measured in the trend of RMA indices of the end product over time. If the trend is toward more uptime and lower operating cost, the organization can be assessed as effectively executing its RMA responsibilities.

The case of a single program measurement is discussed in section 2.5 by appealing to achievement of end product and allocated RMA requirements.

This page intentionally left blank.

5. SUGGESTED READING

The following examples are provided in the appendices to this document and are example products of the application of RMA discipline to a variety of products:

- Summary of Reliability, Maintainability, and Availability (RMA) Applied to the Superconducting Super Collider (SSC);
- Blackford, B., "Model, Top-Down," October 7, 1992, RMA Notebook, Vol. I, 1.11;
- Blackford, B., "Model, Bottom-Up," October 7, 1992, RMA Notebook, Vol I, 1.12; and
- Blackford, B., "Safety Engineering Design Analysis for Tunneling Equipment," November 30, 1993, National Research Council, U.S. National Committee on Tunneling Technology, National Academy of Sciences, Library of Congress 95-68330.

This page intentionally left blank.

6. ASSISTANCE

For assistance in the application of this Guide, the DOE point of contact is Mr. Lindsay Coffman, who can be contacted at (214) 935-9000, extension 2581.

This page intentionally left blank.

7. RELATED TRAINING

A variety of courses in both RMA program management and specialized engineering techniques are commercially available. Assistance in identifying these courses can be obtained from Mr. Lindsay Coffman, who can be contacted at (214) 935-9000, extension 2581.

This page intentionally left blank.

Appendix A
Reliability, Maintainability, and Availability (RMA)
Applied to the Superconducting Super Collider (SSCL)

This page intentionally left blank.

Appendix B
Design Reference Mission and Operational Time lines for RMA Allocations for the Collider Subsystems

This page intentionally left blank.

Appendix C
RMTC LINAC RMA Top-Level Review

This page intentionally left blank.

Appendix D
Safety Engineering Design Analysis for Tunneling

This page intentionally left blank.

Appendix E
History of the RMA Engineering Process

The modern system engineering disciplines of Reliability, Maintainability, and Availability, collectively known under the acronym "RMA," can be largely traced to two major engineering projects that originated in the late 1950s and early 1960s: the Mercury, Gemini, and Apollo manned spaceflight programs of the National Aeronautics and Space Administration (NASA) and the U.S. Navy's Fleet Ballistic Missiles Programs known as Polaris, Poseidon, and Trident. Arguably, the success of each of these efforts depended on systems engineering on a scale not previously required in the history of man.

Early on it was recognized that any such evaluation should be broadened to include consideration of all factors that might influence the operation of the product. Hence, the "system" under consideration was expanded to include interactions arising from the environment, internally or externally induced, the production line, the operator, and the maintainer. This expansion of point of view quickly encompassed the traditional disciplines of quality assurance and safety and the newly emerging ones labeled reliability and maintainability, incorporating them as subdisciplines under the system engineering umbrella.

NASA's major contribution to the development of this new way of engineering discipline was an ever deepening focus on the design of each component of the system, down to the smallest, and on their manufacturing processes. The philosophy was "design it right and build it right," which shifted the major effort from tests on prototypes to tests on components. This was largely a recognition of the financial, political, and human dimensions of the end product. It was simply too costly, on each of these fronts, to suffer failure "in flight.” Similarly, from an engineering and scientific perspective, it was a recognition that the "system" was of such complexity that it was impossible to examine it "holistically." A system failed to perform because the individual components failed to perform. The engineering problem became one of describing the mechanisms by which each component might fail, at what frequency, what caused that mechanism to be present, and the effect of this failure on the end product. We call this process by its formal name: Failure Modes, Effects, and Criticality Analysis (FMECA). Hence, the engineer focused efforts on identifying the weakest link in a system and either removing it altogether, making the chance of failure more unlikely, or mitigating the effects should failure occur. By this means, the concepts of design margin, redundancy, and the like arose anew.

It is a curious fact that, to a large extent, this journey was long and laborious for the electronics engineer and very short for the structural and mechanical engineer. (And remains, today, a largely unfinished trek for the software engineer!) Structural and mechanical engineers have an intimate familiarity with stress, design margins, and similar considerations from their first introduction to their disciplines, but such issues were slower to come to the electronics engineer and remain elusive to the software developer. Structural and mechanical engineers understand the importance of providing a design that offers a wide margin over the stress likely to be encountered by the product in use. The design process for a structure or mechanical device usually starts with a loads analysis, proceeds through materials selection and analysis, to fatigue and fracture analysis, to the production line or construction site.

The great leap in understanding of this problem by electronic engineers and the most successful software engineers, occurred with the recognition that this process is no different for electronic or software systems. One should identify the sources of stress under which the system is to operate; how and to what extent those stresses are transmitted to the system components; the effects of that stress on the components; and the methods available to eliminate or mitigate either these stresses or their effects on the system as a whole.

For electronic systems, stress arises as a byproduct of the operating electrical parameters of the circuits themselves, such as applied voltages and currents. At the physical level these stresses are directly attributable to mechanical effects on the material structures comprising the various components of the circuit. Current pulses, for example, flex conductors imparting fatigue-inducing mechanical stress. Similarly, heat dissipated by resistive conductors change their material properties over time which result in wearout mechanisms from these thermal effects. In microelectronic devices, where current densities may be extremely high due to submicron sized conducting or semiconducting structures, and the pulse rate of the application of these currents in the megahertz range these mechanical stress levels may be extreme.

In addition, the manufacturing methods of microelectronic devices employ processes which are reversible over time. An example of this type of process is ion implantation used to control the semiconducting properties of device structures. These reversible processes are accelerated with elevated temperature, such as would result from greater applied current or higher pulse rate.

These characteristics of the components and their underlying physical structures of electronic systems are controlled through the same means as that employed for mechanical systems - establishing and maintaining design margins. The voltage, current, and similar ratings established for electronic devices are interpretations, in electrical terms, of fatigue and yield mechanical stress levels of their mechanical constituents.

Understanding of the underlying mechanical basis of the electrical stresses imposed on a circuit during operation illuminates the importance placed by reliability engineers on workmanship in the production of electronic components and assembly of electrical circuits. Minute reductions in conductor thickness, for example, can result in large increases in current density in the thinned region, which, in turn, may dramatically increase the mechanical stress on the conductor at that point thereby shortening the number of fatigue-producing cycles of the circuit before failure occurs. Parts quality programs have been established over the last thirty years to ensure both the understanding of the range of results of a particular manufacturing process and to identify the methods of achieving product uniformity.

Software development was, and to some extent continues to be, slower to recognize the applicability of RMA engineering principles to computer programs. There is, however, an obvious relationship between a computer program and the stress its execution applies on processing electronics. From a hardware design perspective the execution time of a computer program establishes constraints on the size of processing hardware architecture. This is evidenced by the push to ever smaller active elements on microelectronic devices and desires to reduce both the area and length of conductors used to pass information between such devices as processor, memory, and peripherals. Since it is the software which largely determines both the number and rate of current pulses in such devices it then largely determines both the magnitude and rate of application of such stress-inducing events. From this view the RMA characteristics of a processing system arise from the combined hardware/software system rather than being some mathematical construction of separate hardware and software indices.

In addition to these characteristics of software systems which may be viewed as inseparable from the processing hardware there are those which may be considered without appeal to the executing processing hardware. Complex computer programs often have an extremely large number of potential pathways, many being executed in response to the occurrence of extremely rare events, some wholly unanticipated by the designer. Accordingly, as the number of branches, interrupts, lookups, and similar executable structures grow in a computer program so does the number of available pathways and hence the opportunity for an unanticipated sequence of processing events. It is therefore appropriate to consider such structures as "stress" producers in a software sense justifying efforts to reduce their presence in the name of RMA improvement.

Finally, workmanship in computer programming is meaningful in at least two senses. First, is the rather obvious coding error where the program fails to execute the desired series of instructions due to a mistake in the higher order code prior to compiling. Another example of this type of error is the failure to set proper ranges to variables used by the program which either impede program execution or allow it to accept invalid values resulting in undesirable output which can result in such phenomena as instability in a control circuit. The second workmanship issue is, however, a bit more subtle in its manifestation and root cause. Since the vast majority of computer programming is performed in a "higher-order language" rather than in that of the processor itself such programs should be translated into machine usable code for execution. This process is termed "compiling" of the code. Compiling is, itself, performed by a piece of software aptly termed a "compiler." Unfortunately, compilers are, themselves, subject to all the inefficiencies and error producing problems as any other software as well as others arising from their proximity to the processor itself. Workmanship in this sense refers to the efficiency in both the higher order code and in the ability of the compiler to convert it to machine usable language. While the code itself may be error free it may nevertheless by unusable in a desired application.