Reliability, Maintainability, and Availability for Logisticians

Text Book

Defense Acquisition University
Mid-West Region

17 March 2010

This page intentionally left blank

Reliability, Maintainability, and Availability for Logisticians

Table of Contents

Title	Page
Preface	i
Description	iii
Acronyms	v
Chapter 1: Impacts of R&M on Logistics	1-1
Chapter 2: Impacts of R&M on Missions	2-1
Chapter 3: Operational and Contractual R&M Requirements	3-1
Chapter 4: Providing Insight into Designing for Reliability	4-1
Chapter 5: Providing Insight into Designing for Maintainability	5-1
Chapter 6: R&M and Risk Reduction	6-1
Chapter 7: Impacts of Manufacturing on R&M	7-1

This page intentionally left blank

17 March 2010

Preface

This textbook is intended to supplement the Reliability, Maintainability, and Availability course classroom presentation. Professor Carroll Widenhouse, Major Clint Campbell, and Professor Virgil Rehg originally developed this material for the Air Force Institute of Technology School of Systems and Logistics course, LOG 203 Reliability and Maintainability.

Any errors can be attributed to the undersigned. Comments for improvement would be appreciated.

Richard A. Di Lorenzo, course manager, LOG 203
Professor of Systems Engineering Management
Defense Acquisition University Mid-West Region
3100 Research Blvd., Pod 3, Third Floor
Kettering, Ohio 45420

E-mail: Richard.DiLorenzo@dau.mil

Commercial Voice: 937-781-1036

Commercial Fax: 937-781-1090

This page intentionally left blank

RM&A for Logisticians: Description

This course (formerly LOG 203 Reliability and Maintainability) presents a practical review of reliability, maintainability and availability by presenting an overview of acquisition policy and its application in the design and development of equipment and systems. Topics covered include: DoD RM&A Policy (**covered in Lesson 1**) ; Mission Profiles (**covered in Lesson 2**); System Level RM&A Allocations and Predictions (**covered in Lesson 4**); FMECAs (**covered in Lesson 4)**; Detailed R&M Design Predictions (**covered in Lesson 4)**; R&M Verification (**covered in Lesson 6)** and Data Collection and Analysis **(covered in Lesson 7);** and COTS RM&A Tasks (**covered in Lesson 3**). The open seminar and practical exercises format of this course will allow for maximum information to be presented. Class will also allow for questions, discussions, in-class examples and exercises to maximize the students' overall learning experience.

This page intentionally left blank

RM&A for Logisticians: Acronyms

AGREE	Advisory Group On Reliability Of Electronic Equipment
ALDT	Administrative and/or Logistics Delay Time
AMSAA	Army Material Systems Analysis Activity
A_o	Operational Availability
AoA	Analysis Of Alternatives
BCS	Bench Checked Serviceable
BIT	Built-In-Test
CASA	Cost Analysis Strategy Assessment
CDD	Capabilities Development Document
CLS	Contractor Logistics Support
CMDT	Corrective Maintenance Downtime
CND	Cannot Duplicate
DAG	Defense Acquisition Guidebook
DSMC	Defense Systems Management College
ECS	Environmental Control Systems
EPR	Essential Performance Requirement
ESS	Environmental Stress Screening
FA	False Alarm
FMC	Fully Mission Capable
FMEA	Failure Modes And Effects Analysis
FRACAS	Failure Reporting, Analysis, And Corrective Action System
GIDEP	Government Industry Data Exchange Program
IC	Integrated Circuits
ICD	Initial Capabilities Document
LCL	Lower Confidence Limit
LRU	Line Replaceable Unit
$\overline{M}$	Mean active maintenance time
MaxCMT	Maximum Correction Maintenance Time
MaxCMTOMF	Maximum Corrective Maintenance Time For Operational Mission Failures
MC	Mission Capable
MCMT	Mean Corrective Maintenance Time
MCMTOMF	Mean Corrective Maintenance Time For Operational Mission Failures
MDT	Mean Downtime
M_o	Operational Maintainability
MR	Maintenance Ratio Or Mission Reliability
MR/WSR	Mission Or Weapon System Reliability
MRT	Mean Repair Time
MTB_	Mean Time Between (Event)
MTBD	Mean Time Between Demands
MTBDE	Mean Time Between Downing Events

Acronyms (Con't)

MTBF*	Mean Time Between Failures
MTBM	Mean Time Between Maintenance
MTBMA	Mean Time Between Maintenance Actions
MTBMCF*	Mean Time Between Mission Critical Failures
MTBOMF	Mean Time Between Operational Mission Failures
MTBR	Mean Time Between Removals
MTBUM	Mean Time Between Unscheduled Maintenance
MTTFL	Mean Time To Fault Locate
MTTR*	Mean Time To Repair
NDI	Nondevelopmental Items
Pcd	Percent Of Correct Detection
Pcfi	Percent Of Correct Fault Isolation
PM	Preventive Maintenance
PMC	Partial Mission Capable
PMDT	Preventive Maintenance Downtime
PRAT	Production Reliability Acceptance Test
R&M	Reliability And Maintainability
RAC	Reliability Analysis Center
RFP	Request for Proposal
RMA	Reliability, Maintainability and Availability
RQT	Reliability Qualification Test
RTOK	Retest OK
SOO	Statement Of Objectives
SOW	Statement of Work
SRA	Shop Replaceable Assembly
SRU	Shop Replaceable Unit
TAAF	Test Analyze And Fix
TOC	Total Ownership Cost
WRA	Weapon Replaceable Assembly

*Recommended use: Contract Specification

Chapter 1: Impacts of Reliability and Maintainability on Logistics

The primary aim of this chapter is to assure the acquisition logistician, working in a program office, understands how the product's R&M will affect logistics and associated costs. Specifically, you will be able to:

1. Recognize how R&M affect support costs.
2. Recognize how R&M affect total ownership cost.
3. List the 4 keys elements in the definition of reliability.
4. List two MTB_s that are logistics reliability parameters.

Why R&M are Important to the DoD:

There are two reasons that the DoD wants to acquire systems that are reliable and maintainable. They are analogous to the reasons you and I buy a car or washing machine that is reliable and maintainable. The DoD wants more combat capability (more missions succeed if fewer fail); and lower support costs (fewer maintenance folks to train and support; fewer spares to buy, distribute and manage if there are fewer failures and easier/quicker repairs). In short, R&M hold the promise of more bang and less bucks (at least in the out-years). This chapter discusses the "less bucks", i.e., lower support costs. Chapter 2 discusses "more bang", i.e., increased combat capability.

Life Cycle Logistics and Reliability and Maintainability - per the Defense Acquisition Guidebook (DAG)

"Chapter 5 -- Life-Cycle Logistics
5.3. Supportability Design Considerations

5.3.2. Reliability

> Reliability is critical because it contributes to a system's war fighting effectiveness as well as its suitability in terms of logistics burden and the cost to fix failures. For each system, there is a level of basic reliability that must be achieved for the system to be militarily useful, given the intended CONOPS. Reliability is also one of the most critical elements in determining the logistics infrastructure and footprint. Consequently, system reliability should be a primary focus during design (along with system technical performance, functions, and capabilities). The primary objective is to achieve the necessary probability of mission success and minimize the risk of failure within defined availability, cost, schedule, weight, power, and volume constraints. While performing such analyses, trade-offs should be

conducted and dependencies should be explored with system maintainability and integrated with the supportability analysis that addresses support event frequency (i.e. Reliability), event duration and event cost. Such a focus will play a significant role in minimizing the necessary logistics footprint, while maximizing system survivability and availability.

The requirements determination process offers the first opportunity to positively influence a system from a reliability perspective. Trade-offs among "time to failure," system performance, and system life-cycle cost are necessary to ensure the correct balance and to maximize materiel availability. Options that should be considered and implemented to enhance system reliability and achieve the Materiel Reliability KSA include:

- Over-designing to allow a safety margin;
- Redundancy and/or automatic reconfiguration upon failure allowing graceful degradation;
- Fail safe features (e.g., in the event of a failure, systems revert to a safe mode or state to avoid additional damage and secondary failures). Features include real time reprogrammable software, or rerouting of mission critical functions during a mission;
- Calibration requirements; and
- Reliability Growth Program.

Reliability estimates evolve over time. Generally, the initial estimates are based on parametric analyses and analogies with like or similar systems operating in the same environment and adjusted via engineering analysis. As the design evolves and as hardware is prototyped and developed, the engineering analysis becomes more detailed. In addition to estimates and modeling, testing at the component, subsystem, or system level may be necessary to assess or improve reliability. Approaches such as accelerated life testing, environmental stress screening, and formal reliability development/growth testing, should be considered and incorporated into program planning as necessary. To assure the delivery of a system that will achieve the level of reliability demanded in field use, a methodical approach to reliability assessment and improvement should be a part of every well-engineered system development effort. The Reliability Availability and Maintainability (RAM) Guide provides a structure, references, and resources to aide in implementing a sound strategy. It is crucial the reliability approach be planned to produce high confidence the system has been developed with some margin

beyond the minimum (threshold) reliability. This will allow for the inevitable unknowns that result in a decrease between the reliability observed during development and that observed during operational testing and in-service.

5.3.3. Maintainability

The design emphasis on maintainability is to reduce the maintenance burden and supply chain by reducing the time, personnel, tools, test equipment, training, facilities and cost to maintain the system. Maintainability engineering includes the activities, methods, and practices used to design minimal system maintenance requirements (designing out unnecessary and inefficient processes) and associated costs for preventive and corrective maintenance as well as servicing or calibration activities. Maintainability should be a designed-in capability and not an add on option because good maintenance procedures cannot overcome poor system and equipment maintainability design. The primary objective is to reduce the time it takes for a properly trained maintainer to detect and isolate the failure (coverage and efficiency) and affect repair. Intrinsic factors contributing to maintainability are:

- **Modularity:** Packaging of components such that they can be repaired via remove and replace action vs. on-board repair. Care should be taken not to "over modularize" and trade-offs to evaluate replacement, transportation, and repair costs should be accomplished to determine the most cost effective approach.
- **Interoperability:** The compatibility of components with standard interface protocols to facilitate rapid repair and enhancement/upgrade through black box technology using common interfaces. Physical interfaces should be designed so that mating between components can only happen correctly.
- **Physical accessibility:** The designed-in structural assurance that components requiring more frequent monitoring, checkout, and maintenance can be easily accessed. This is especially important in Low Observable platforms. Maintenance points should be directly visible and accessible to maintainers, including access for corrosion inspection and mitigation.
- Designs that require **minimum preventative maintenance** including corrosion prevention and mitigation. Emphasis should be on balancing the maintenance requirement over the life cycle with minimal user workload.
- **Embedded training and testing**, with a preference for approved DoD Automatic Test Systems (ATS) Families when it is

determined to be the optimal solution from a TOC and Materiel Availability perspective.

- **Human Systems Integration (HSI)** to optimize total system performance and minimize life-cycle costs. (For further discussion, see Chapter 6 and section 4.4.8.) This includes all HSI domains (Manpower, Personnel, Training, Human Factors Engineering, Environment, Safety, Occupational Health, Survivability, and Habitability) to design systems and incorporate technologies that require minimal manpower, provide effective training, can be operated and maintained by users, are suitable (habitable and safe with minimal environmental and occupational health hazards), and survivable (for both the crew and the equipment).

Condition Based Maintenance Plus. When it can support the materiel availability, prognostics & diagnostics capabilities/technologies should be embedded within the system when feasible (or off equipment if more cost-effective) to support condition based maintenance and reduce scheduled and unscheduled maintenance. Health management techniques can be very effective in providing maintainers with knowledge, skill sets, and tools for timely maintenance and help reduce the logistics footprint. Condition based maintenance plus (CBM+) (the application of technologies, processes, and procedures to determine maintenance requirements based, in large part, on real time assessment of system condition obtained from embedded sensors), coupled with reliability centered maintenance can reduce maintenance requirements and reduce the system down time. (CBM+ references include the DoDI 4151.22, the CBM+ Guidebook, and the CBM+ DAU Continuous Learning Module (CLL029).) The goal is to perform as much maintenance as possible based on tests and measurements or at pre-determined trigger events. A trigger event can be physical evidence of an impending failure provided by diagnostic or prognostics technology or inspection. An event can also be operating hours completed, elapsed calendar days, or other periodically occurring situation (i.e., classical scheduled maintenance). Key considerations in implementing this concept include:

- Use of **diagnostics** monitoring/recording devices and software (e.g., built-in test (BIT) and built-in-self-test (BIST) mechanisms) providing the capability for fault detection and isolation, (including false alarm mitigation) to signal the need for maintenance. It should include user friendly features to convey system status and the effect on mission capabilities to the operator and maintainer.

- Use of **prognostics** monitoring/recording devices and software monitoring various components and indicate out of range conditions, imminent failure probability, and similar proactive maintenance optimization actions to increase the probability of mission success and anticipate the need for maintenance. (As in the case for diagnostics prognostics includes BIT and BIST mechanisms with user friendly features and false alarm mitigation.)
- Maintenance strategies that balance scheduled (preventive) maintenance and minimize unscheduled corrective maintenance with risks.

Key characteristics in implementing the CBM+ concept include:

- Hardware—system health monitoring and management using embedded sensors; integrated data
- Software—decision support and analysis capabilities both on and off equipment; appropriate use of diagnostics and prognostics; automated maintenance information generation and retrieval
- Design—open system architecture; integration of maintenance and logistics information systems; interface with operational systems; designing systems that require minimum maintenance; enabling maintenance decisions based on equipment condition
- Processes—RCM analysis; a balance of corrective, preventive, and predictive maintenance processes; trend-based reliability and process improvements; integrated information systems providing logistics system response; CPI; Serialized Item Management (SIM)
- Communications—databases; off-board interactive communication links
- Tools—integrated electronic technical manuals (i.e., digitized data) (IETMs); automatic identification technology (AIT); item-unique identification (IUID); portable maintenance aids (PMAs); embedded, data-based, interactive training
- Functionality—low ambiguity fault detection, isolation, and prediction; optimized maintenance requirements and reduced logistics support footprints; configuration management and asset visibility.

In accordance with DoDI 4151.22, it is envisioned that elements of CBM+ should be revisited as the life cycle progresses, conditions change, and technologies advance. Consequently CBM+ should be considered and revisited in each life-cycle phase. See CBM+ Guidebook, Section 4 which provides basic steps for planning and implementing CBM+ throughout the life cycle."

Note that reliability and maintainability are grouped with availability in both "RM&A" and "RAM". From a user perspective this is good because availability is even more important than either reliability or maintainability alone. R&M contribute to availability. As we shall see, operational availability is a function of Reliability (R), Maintainability (M), and the Support Structure (S).

Note also that the two reasons DoD wants R&M - more bang and less bucks (at least in the out-years) - are addressed in the DAG, above. The terminology there includes "availability" and "cost."

Why R&M are Important to DoD Logisticians

One reason the Program Manager (PM) should pursue R&M is total ownership cost considerations.

The PM should consider the R&M of not merely the mission-critical equipment but the all elements of the system, including support and training equipment, technical manuals, spare parts, and tools.

The PM should be concerned about mission reliability as well as logistics reliability: The former addresses the probability of carrying out a mission without a mission-critical failure. The latter is the ability of a system to perform as designed in an operational environment over time without any failures."

How the R&M of some of the logistics support elements contribute to driving down product support costs will be explained in the remainder of this chapter. The logistics support elements are, generally: Maintenance Planning, Manpower and Personnel, Supply Support, Support Equipment, Technical Manuals and Technical Data, Training and Training Devices, Computer Resources Support, Facilities, Packaging, Handling, Storage, and Transportation, and Design Interface.

The Reliability of Spares Affects the Number of Spares Required

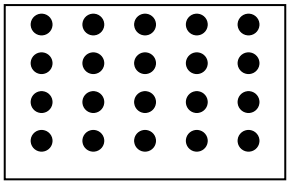
Assume an overhead projector bulb has Reliability = .80 for a 3-hour mission, e.g. 8 a.m. to 11 a.m. for classroom instruction. Assume the operator (teacher) knows how to change a bulb if one fails (and has ready access to at least one spare) and hence can salvage the mission (teaching) if he can do it without too much delay. Then the Probability of System Success P(S) depends on the number of spares as follows:

Number of spares on Hand	If projector bulb has reliability = .80 for a 3-hour mission, then P(S)	Same, except .50 instead of .80
0	.8000	.5000
1	.9784	.8466
2	.9983	.9665

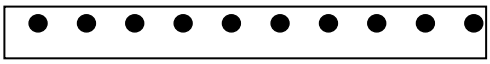
If the user requires 96% dependability how many spares should the support folks provide? Answer: one. But if the bulb has a reliability of only 50%, two spares are required. Therefore, the reliability of the bulb affects the number of spare bulbs required. So, for people in supply support, reliability affects their jobs.

Demand Rate (a Reliability Parameter) Affects the Confidence Level for Spares

A piece of equipment operates 24 hours a day. It contains 20 parts of a specific type with a demand rate of 1 per 10,000 hours of operation. A box of 10 spares is provided. What is the probability that they won't run out of spares for the next 90 days? Theoretical answer (Poisson distribution) is 99.5%. But, if the demand rate were worse, say 3 demands per 10,000 hours of operation, confidence falls to about 25.5%. Again, reliability affects supply support.



Equipment



Spares

MTBM (a Reliability Parameter) Affects the Probability of Maintenance-free Operation

A product's MTBM is 100 hours (calculated from four maintenance actions in 400 hours of operation). What is the probability of completing a 30-hour mission? The theoretical (constant failure rate assumption) answer is 73%.

However, if the MTBM were 200 hours, the probability of completing a 30-hour mission increases to 86%! So, the reliability parameter (MTBM) affects the probability of maintenance-free operation. So, reliability affects maintenance.

Reliability Affects Inventory Management

Ordering creates procurement costs. Managing inventory creates carrying cost.

Economic Order Quantity (EOQ) is affected by the demand for the item. Demand is affected by demand rate (a reliability factor).

How the R&M of Training Equipment and Support Equipment Affect the Quantities of Equipment Required

For an anticipated amount of training equipment utilization, the quantity of training equipment will be affected by how often the training equipment itself fails (reliability) and how long it takes to get it fixed (maintainability and support structure). Hence the quantity of training equipment needed for an organization depends on the reliability and maintainability of the training equipment. The same can be said about support equipment.

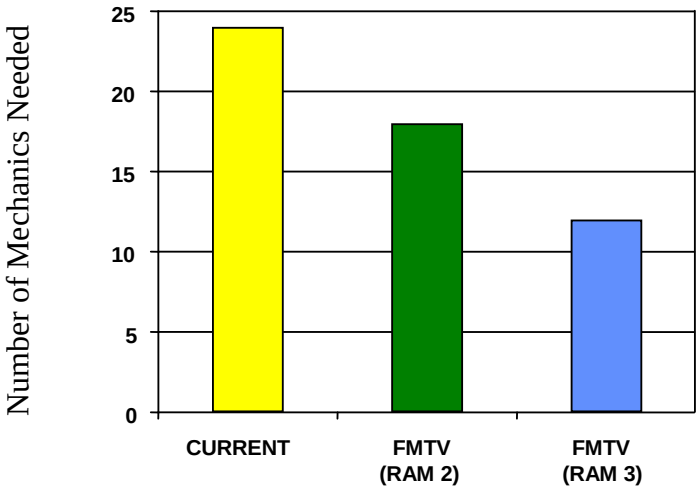
How R&M Can Drive a Maintenance Organization's Labor Requirements

Maintenance labor time for each personnel category or skill level may be expressed by maintainability factors such as:

- Maintenance man-hours per operating hour (MMH/OH).
- Maintenance man-hours per mission cycle (or segment of a mission).
- Maintenance man-hours per month (MMH/month).
- Maintenance man-hours per maintenance action (MMH/MA).

A generic example of how increased reliability can decrease maintenance manpower requirements is: A squadron of 24 follow-on aircraft will cost $30 million less to own and operate per year than the same number of predecessor aircraft because the follow-on aircraft require fewer support personnel and have higher reliability."

A real example involves the Army's Medium Truck mechanic requirements. The following chart shows how the Army's need for mechanics for the Family of Medium Tactical Vehicles (FMTV) dwindled with RAM (reliability, availability, and maintainability) improvements.



How a System's R&M Can Drive Facility Sizing

Facilities are needed for maintenance work, for storing spares and repair parts, and for training maintenance personnel. All are affected by how often products fail and how long it takes to repair them (R&M characteristics). So, facilities planning folks are affected by the reliability of the equipment they will support.

How R&M Can Affect Transportation and Handling Factors

Transportation of 1) initial spares (from contractor, depot, etc., to worldwide maintenance organizations); 2) follow-on spares; 3) maintenance pipeline flow; 4) mobilization (spares, maintenance personnel, training equipment, etc.).

Transportation factors include transportation costs, transportation time, and transportation capacity. These factors can be significantly affected by the demand for spares (a reliability parameter).

Why the Reliability of Software is Important

Software may be critical to mission equipment, training equipment and support equipment. So, a software error can be mission-critical (or, for that matter, safety-critical or cost-critical). So, software reliability is an issue for computer resources support people.

What do R&M Mean for Logistics?

As discussed above, R&M affect spares, inventory, training and support equipment, maintenance manpower, facilities, transportation, software, etc. Since all these cost money, R&M affect their costs during acquisition and/or support phase.

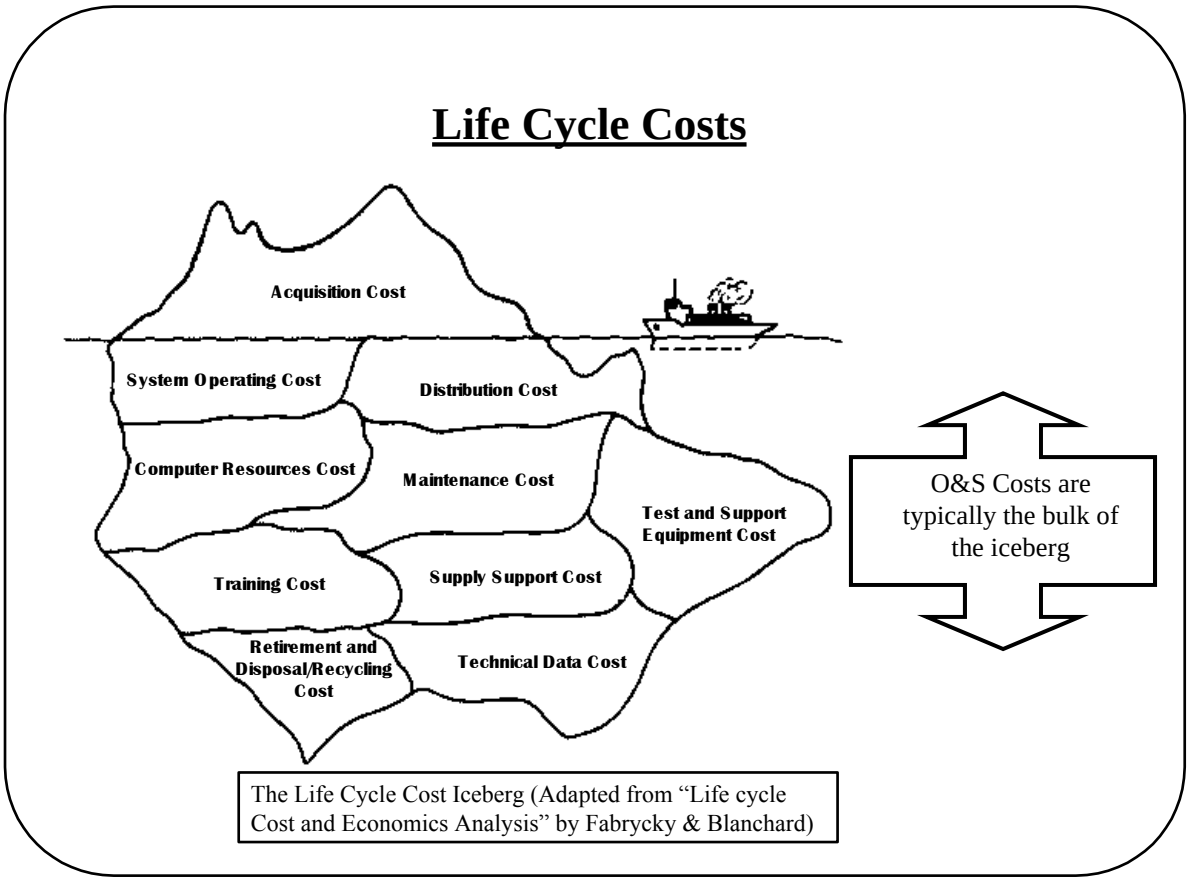
R&M and Total Ownership Cost

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

The desire for a highly reliable system may increase the acquisition cost to an unaffordable level. Even though the support costs will be driven down, the TOC may climb. Costs and mission

requirements must be properly balanced to determine the appropriate amount of reliability to seek in a weapon systems acquisition program.

Here is the well-known life cycle costs Iceberg chart from Fabrycky & Blanchard, showing that the acquisition costs are typically the tip of the iceberg.

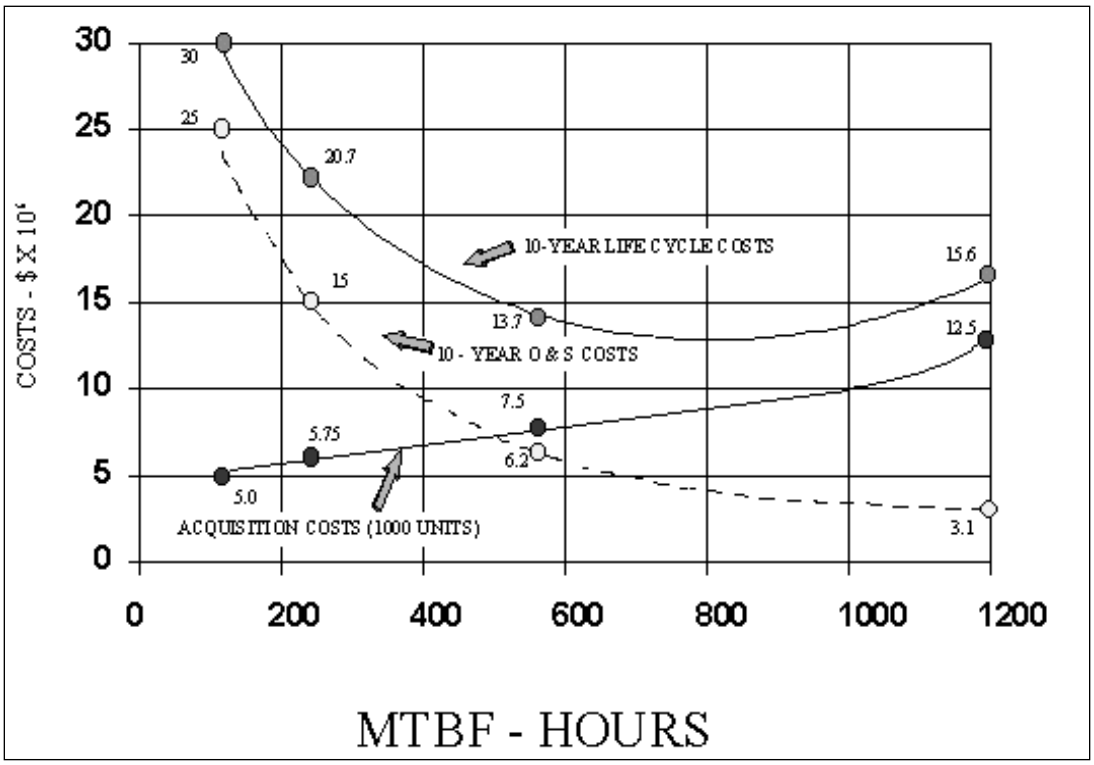


Decreased O&S Costs:

The following chart suggests that there is an optimum MTBF from a minimum life-cycle cost (LCC) perspective. That MTBF is about 800 hours. If this chart were used during design to specify a contractual MTBF, it would be misleading, however.

That's because the chart doesn't address the other reason DoD wants reliability in its weapons, i.e., combat capability. The chart doesn't show how operational availability, readiness, mission capable rate, deterrence, or national security in general might benefit from different levels of MTBF. Besides costs, the Program Manager should consider operational requirements as stated in the Capabilities Development Document or CDD.

Imagine for example that this piece of equipment is the single most critical to our national security; and that high reliability will safeguard our futures. It may well be affordable to pay the higher acquisition cost and higher life cycle cost for such an essential product.



R&M and Affordability

Today's systems must be not only CAPABLE, but also AFFORDABLE! Affordable means we have the ability and the intention to adequately fund a system for the entire life cycle. The life cycle cost of a system includes costs for both:

Acquisition Costs	**Recurring / Support Costs**
Design / Development	Operating (personnel, power, consumable)
Development and Qual. Testing	Maintenance (preventive and corrective)
Tooling and Manufacturing	Spares
Screening	Transportation
Initial Spares, Training	Training
Test Equipment	Mobility kits
Technical Manuals	
Warranties	

The point here is that Program Manager who only sees acquisition costs is blind to the larger costs, the out-years costs of operating and supporting the system.

Again, What is Reliability?

Reliability is the probability that an item will perform its intended function under stated conditions for either a specified interval or over its useful life. So, reliability is quantifiable (probability), has to do with getting some work done (intended function), and assumes a set of conditions (under stated conditions), and depends on the mission duration (specified interval).

The Mean Time Between (some logistics event): a Logistics Reliability Parameter

The mean time between (some event), e.g. the MTBF, is the average amount of time between occurrences of that particular event, e.g. failures, for our product. In general, a Mean Time Between (some event) is referred to as an "MTB_" and is computed as

$$= \frac{\text{Total life units (in the period being evaluated)}}{\text{Total number of events}}$$

Note that the word "time" is used to represent any unit of life when the product is stressed (subject to something bad happening to it!). Examples of life units are operating hours, calendar hours, flying hours, cycles (engines), landings (for landing gear), etc. As used here (and often in the literature), the events are assumed to occur randomly, i.e., independently of "time". Since the "events" in MTB_s are generally undesirable, we want the average (or mean) interval between occurrences to be large, i.e., larger is better.

MTB_s in general may be referred to as reliability parameters. They tell us something about the reliability characteristic of the product. Of particular interest to logisticians are events like unscheduled maintenance actions, demands on the supply system, removals, etc. Therefore, MTB_s like MTBM, MTBD, and MTBR are **logistics** reliability parameters.

Example of an MTB_ calculation: A car travels 10,000 miles in two years and has its computer repaired twice. We can compute several "mean times between unscheduled maintenance" (MTBUM), depending on the choice of life unit (arbitrary).

$$= \frac{\text{miles}}{\qquad} =$$

$$\textit{or} \frac{\text{years}}{\qquad} =$$

$$\textit{or} \frac{\text{hours}}{\qquad} =$$

So, if a car travels 10,000 miles in two years and has its computer repaired twice, the MTBUM (unscheduled maintenance) may be computed as 5,000 miles between unscheduled maintenance; or as 1 year between unscheduled maintenance.

Here are definitions of some logistics reliability parameters:

MEAN TIME BETWEEN DEMANDS (MTBD): A measure of the system reliability parameter related to demand for logistic support. The total number of system life units, divided by the total number of item demands on the supply system during a stated period of time.

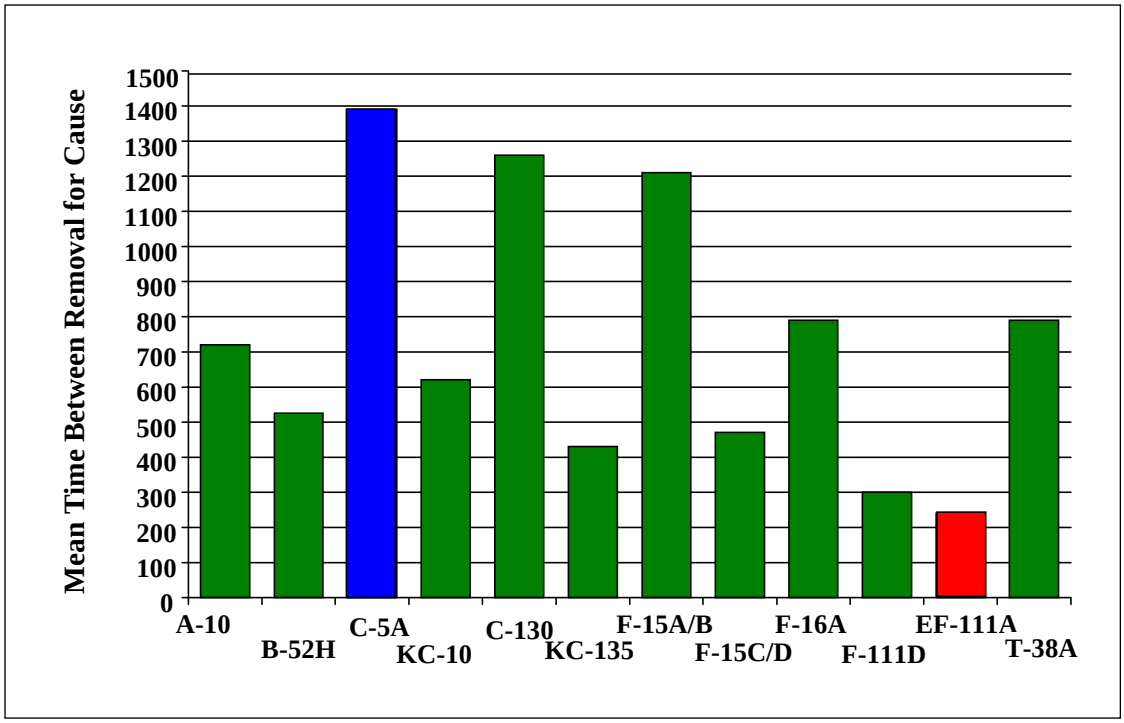
MEAN TIME BETWEEN MAINTENANCE ACTIONS (MTBMA): A measure of the system reliability parameter related to demand for maintenance manpower. The total number of system life units, divided by the total number of maintenance events (preventive and corrective) during a stated period of time.

MEAN TIME BETWEEN REMOVALS (MTBR): A measure of the system reliability parameter related to demand for logistic support. The total number of system life units, divided by the total number of items removed from that system during a stated period of time. This term is defined to exclude removals performed to facilitate other maintenance and removals for product improvement.

Reliability Depends on Environment

As stated above, reliability presumes a set of conditions. When those conditions change, so will the product's reliability.

The following chart shows how the environment may affect a reliability parameter, namely MTBR (for cause). The chart discusses a TACAN, a navigation box used on numerous platforms. The chart suggests that the box works most reliably on the C-5A aircraft and least reliably on the EF-111A; perhaps it is due to the environment. Perhaps temperature, vibration, pressure, acceleration and other environmental factors are at work here. "Handle with care" and it might last longer.



<u>Exercise: Understanding "Mean Time Between"</u>

A fleet of trucks were retrofitted with new generators. Two years later, field data for the generators showed:

1,000,000 operating hours and 100 truck breakdowns due to generator failure.

There were 1200 "events" involving generators:

a. 100 on-equipment repairs (turning wrenches, screwdrivers, etc.)
b. 200 removals to facilitate other maintenance (50 of these resulted in damage to the generators!)
c. 900 removals were forwarded to the depot for repair (of which 600 were identified as design or manufacturing related problems)

Calculate the following reliability parameters for the generator:

MTBM (TOTAL): count all maintenance events
MTBM (INHERENT): count only those maintenance events caused by design or manufacturing errors.
MTBR (TOTAL): count all removals
MTBR (FOR CAUSE): count only those removals where the generator was identified initially as requiring maintenance
MTBD
MTBOMF (How does MTBOMF differ conceptually from the MTB_s above?)

MTBF: A Contractual Design, Development, Test Reliability Parameter

Most of us are familiar with MTBF, mean time between failures. It should be used as a contractual term to drive a design and for testing. It belongs in the contract specification, as a Section 3 requirement, and in Section 4 for verification purposes. Both "time" and "failure" should be defined in the specification to limit the possibility of a dispute (and cost and schedule impacts) between the government and the contractor.

MTBF should not be used in an operational requirements document like the CDD, because the CDD should not be written in engineering terms like MTBF or MTTR (mean time to repair). These are specification requirements that should be derived from (translated from) the CDD. The logistician needs to assure that this translation is done in a manner that is technically sound – regardless of who actually writes the specification.

MTB_'s and their Corresponding Rates

If a product is assumed to have a constant failure rate, then its MTBF is generally the reciprocal of that failure rate. Similarly, if the demand rate is constant, the MTBD is the reciprocal of that demand rate. If the maintenance rate is constant, the MTBM is the reciprocal of the maintenance rate. If the removal rate is constant the MTBR is the reciprocal of the removal rate.

So, What Does Reliability Mean in Plain English?

Reliability means "sustained performance" – the watch keeps on ticking;
Reliability means "performance over time" – the product works this time and the next time;
Reliability means "quality over time" – it keeps on doing the job.

What is Maintainability?

According to MIL-HDBK-470A, maintainability is "the relative ease and economy of time and resources with which an item can be retained in or restored to a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. In this context it is a function of design."

Retaining a system in specified condition is preventive or scheduled maintenance. Changing the oil on your car every three months is an example. A Reliability Centered Maintenance Analysis (RCMA) identifies the appropriate preventive maintenance tasks and intervals for a system.

Restoring a system to specified condition is corrective or unscheduled maintenance. Changing a flat tire on a car is an example.

The definition of maintainability assumes maintainers have the appropriate skills, technical data, tools, test equipment, facilities, etc. at each level of maintenance (organizational, intermediate, depot). When these conditions don't hold, maintainability degrades.

Human factor issues include accessibility and environments. Accessibility is concerned with issues like whether the maintainer has long enough arms, enough strength and adequate visibility to see the part he/she needs to work on. Environments include the combat environments (nuclear, chemical, biological, arctic, tropical, etc.). Note that some commercial products are not designed to operate in or be repaired in such environments.

Major Areas of Concern in Maintainability

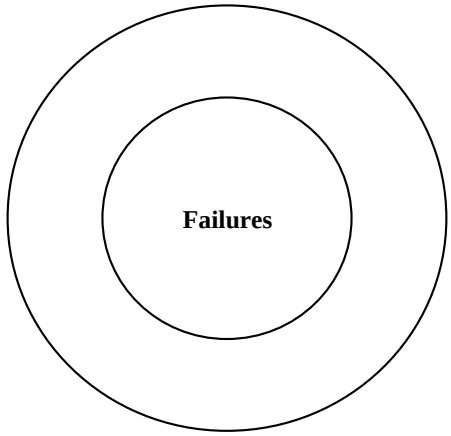
Diagnostics and human factors are the major areas of concern in maintainability. Diagnostics includes fault detection and fault isolation. Human factors include accessibility and environmental issues. The DoD has been increasing its emphasis on diagnostics in recent years as a means of decreasing its need for highly skilled maintainers. This puts added burden on diagnostics. It must perform as advertised! We may no longer have trained mechanics to fall back on! The failure of diagnostics may result in the same consequences on missions, safety and cost as when mission-essential equipment fails.

Diagnostics deals with fault detection, fault isolation and related issues. Fault detection is the ability to determine that something is amiss with equipment. Fault isolation means identifying just what component or assembly is amiss

"Fault" vs. "Failure"

As used here, a "fault" occurs when any item is not performing like it should; this could be your car's engine, oil gage, or a courtesy reading lamp. A "failure" occurs when any mission-critical, safety-critical, or cost-critical item is not performing like it should; this could be your car's engine, but not the oil gage or courtesy reading lamp. Logistics folks ultimately need to fix all faults. Operational people are primarily focused on failures. In other words, failures may be thought of as comprising a subset of faults. The following picture illustrates the relationship of failures to faults.

Faults



<u>Measures of Maintainability</u>

An example of a "diagnostics" measure is <u>built-in-test fault detection percentage</u>. It answers the question, What percentage of the faults was detected by BIT (built-in-test)?

$$= \frac{\text{Number malfunctions confirmed by built} - \text{in} - \text{test}}{\text{Total malfunctions observed by operator/technician}}$$

A truck malfunctioned 25 times in 10 years. Only 5 of 25 malfunctions were indicated by BIT (warning lights and gages).

$$\text{Built - in - test fault detection\%} = \text{———} =$$

"Workload" measures of maintainability incorporate effects of both diagnostics capability and human factors. Terms generally relate to clock time or man-hours required performing maintenance. An example of a "workload" measure of maintainability is <u>mean repair time</u> (MRT). In plain English, MRT answers the question "How long should we expect the actual repair work to take?"

$$\text{MRT} = \frac{\text{Total elapsed time (or cumulative man - hours) for repairs}}{\text{Total number of repairs}}$$

Repair of the 25 malfunctions above required a total of 100 man-hours.

Mean repair time =

Other workload measures of maintainability include:

FA rate: False alarm rate

$\overline{M}$: Mean active maintenance time; accounts for corrective and preventive maintenance.
MCMT: mean corrective maintenance time.
$MaxCMT_{.90}$: This represents the 90% confidence limit for corrective maintenance. It answers the question, "90% of the time, the corrective maintenance will take no more than how much time?"

The reason for have both a mean and a max corrective maintenance time is that the underlying probability distribution (usually normal or lognormal) is defined by two parameters, one for central tendency (mean) and one for variability (such as the 90percentile "max").

So, What Does Maintainability Mean in Plain English?

Maintainability basically means the rapid diagnosis and removal of faults. Or, it tells us how long or hard it is to perform maintenance.

Logistics R&M Definitions

The following are Army, Navy, Marine Corps, and Air Force Operational Test Agencies logistics-related R&M definitions.

Mean Time Between Unscheduled Maintenance (MTBUM): The total operating time divided by the total number of incidents requiring unscheduled maintenance.

Mean Corrective Maintenance Time (MCMT): The total number of clock-hours of corrective, on-system, active repair time due to all corrective maintenance divided by the total number of incidents requiring corrective maintenance.

Maximum Corrective Maintenance Time (MaxCMT): That time below which a specified percentage of all corrective maintenance tasks must be completed.

Percent of Correct Detection given that a fault has occured (Pcd): The number of correct detections divided by the total number of confirmed faults times 100 (to express the quotient as a percent).

Percent of Correct Fault Isolation (and Correct Fault Location) given correct detection (Pcfi): The number of correct fault isolations (and/or correct fault locations) divided by the number of correct detections times 100 (to express the quotient as a percent). "Fault isolation" and/or "fault location" must be clearly defined

Measures of False Alarms (FA): False alarms are faults, where, upon investigation, it is found the fault cannot be confirmed. Measures of FA may be expressed as a total number, a percentage, a rate of occurrence, a probability of occurrence, etc. The selected measure must be clearly stated.

Mean Time to Fault Locate (MTTFL): The total amount of time required locating faults divided by the total number of faults.

Summary, Chapter 1, Impacts of Reliability and Maintainability on Logistics:

We have seen in this chapter how a product's R&M affect logistics measures involving: spares requirements; safety levels for spares; inventory; training and support equipment; maintenance labor; facilities; transportation and handling; and software. In every case, we concluded that better reliability or maintainability result in lower costs in the out years. However, the additional acquisition investment may not be affordable. This point will be discussed more later.

Bibliography:
Logistics Engineering and Management, Fourth Edition, by Benjamin S. Blanchard; publisher Prentice-Hall.

This page intentionally left blank

Chapter 2: Impacts of R&M on Missions

The primary aim of this chapter is to assure the acquisition logistician, working in a program office, understands how the product's R&M will affect missions and combat capability. Specifically, you will be able to:

1. Identify the policy document that tells program managers to establish R&M activities early in order to assure meeting operational requirements.
2. Distinguish by trend in hazard rate among latent defect failures, random failures, and wear-out failures.
3. Identify three measures of combat capability that are enhanced by good R&M characteristics.
4. Distinguish between reliability and maintainability.
5. List two reasons the DoD wants reliable and maintainable products.

Why R&M are Important to the DoD:

Recall from Chapter 1 that there are two reasons the DoD wants to acquire systems that are reliable and maintainable. The DoD wants more combat capability (more missions succeed if fewer fail); and lower support costs (and fewer maintenance folks to train and support; fewer spares to buy, distribute and manage if there are fewer failures and easier/quicker repairs). In short, R&M hold the promise of more bang and less buck (at least in the out-years). Chapter 1 discussed the lower support costs, which is of particular interest to the support/sustainment community. Chapter 2 will now discuss the increased combat capability, of particular interest to the mission/operational folks.

Why R&M are Important to Mission Personnel

1. R&M requirements should be based on operational requirements The program manager then develops R&M system requirements based on the Initial Capabilities Document, Capability Development Document, total ownership cost (TOC) and other considerations, and states them in quantifiable, operational terms, measurable during DT&E and OT&E.

2. R&M are aimed at helping meet operational requirements. R&M system requirements address all elements of the system, including support and training equipment, technical manuals, spare parts, and tools. These requirements should be derived from and support the user's system readiness objectives.

3. R&M requirements should address mission reliability, which is the probability of carrying out a mission without a mission-critical failure."

Measures of Reliability

As mentioned, reliability is quantifiable through a probability or percentage. So, a common measure is the percentage of successes with respect to total attempts, i.e.,

$$\frac{\text{Number successful missions, events, etc.}}{\text{Total number missions attempted}}$$

For example, if 207 Delta launch vehicles were launched and 195 were successful, then:

$$R = \frac{\qquad\qquad}{} =$$

Is it wise to use this calculation as a predictor of reliability for the next launch? Only if the process of producing successful launches is stable. Here's where knowledge of statistical process control concepts can be applied.

For example, what if I told you the last twelve launches were all the failures! Would you feel confident that there's a 94% chance of success on the next launch? I don't think so. Something in the process has changed! Always check the data before predicting. Be sure it is stable. Summary data alone is not adequate for prediction.

Here's another example of a reliability calculation

Eighteen preproduction Peacekeeper ICBMs were launched during DT&E; all were considered to be successful. The calculation is 100% reliability, but does that guarantee a successful launch next time? No, even though the numbers look great.

When do you know the True Reliability of an Item?

In a sense you don't know the true reliability until all the items are used or service is terminated. That's when all the data is in. Until then the numbers may change and all we have are estimates. However, we can and should use these in predicting logistics needs (spares, labor, transportation, etc.). For example, if three successes occur on the first four trials, the reliability estimate is 75%. If the next try is a failure the reliability drops to 60%, but if it is a success, it climbs to 80%. In either case it changes. It has to. So, let's not be surprised when demand rates, maintenance rates, MTB_s or other field reliability data change over time.

Life Cycle Hazard Rate ("Bathtub") Curve

The so-called "bathtub" curve comes from actuarial tables and is used by the life insurance industry. The instantaneous failure rate indicates how hazardous life is at different stages.

Early on, failures are driven largely by defects in manufacturing. This is referred to as the infant mortality phase.

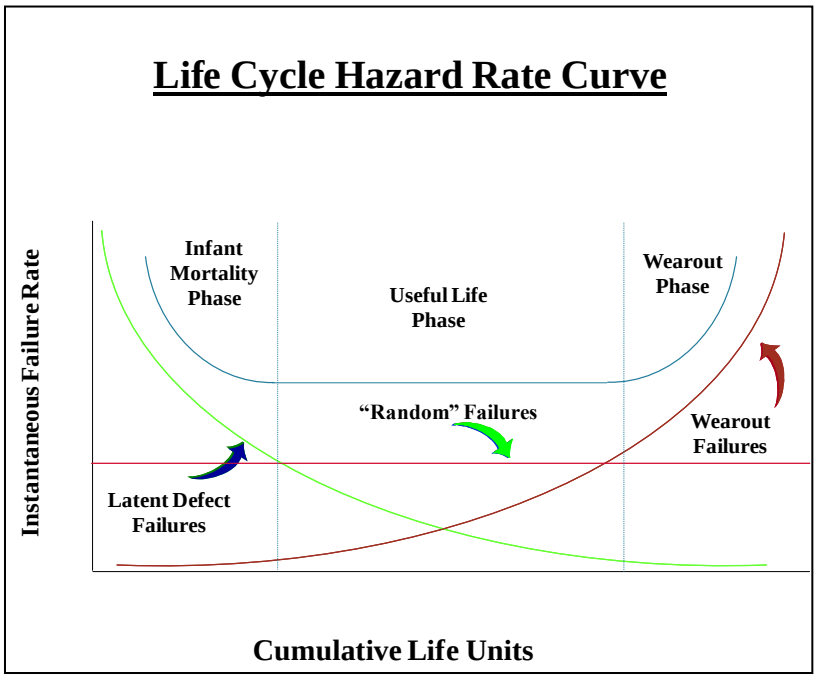
Once the defective units are weeded out and the strong survive, they are subject to randomly occurring failures like accidents; this marks the so-called useful life phase. Notice it has the lowest instantaneous failure rate (lower is better) and hopefully this is the longest phase (longer is better). Finally, we have a period where wear-out dominates and the failure rate rises. This might be a good time to remove and replace because it becomes increasingly hazardous to operate.

As an example: a tire might have latent defects such as poor bonding of the tread to the carcass. This may result in an early failure; say within a few thousand miles.

Randomly occurring failures would include road hazards like spikes causing a flat tire. The tire's age is pretty insignificant against a road hazard; young or old it is vulnerable! Finally, wear-out of the tread, at say the 50,000 mile point. Operating beyond this, and we're asking for trouble, such as hydroplaning and loss of control. So, as preventive maintenance, we replace an automobile tire when the tread thickness is 2/32nd of an inch (legal minimum in Ohio).

Not all products follow the bathtub curve. When burn-in, ESS, or other quality control efforts are effective, there may be no infant mortality period. Similarly, some products, like electronics, exhibit virtually no wear-out, or its onset is greatly delayed - often beyond the obsolescence period.

In a study performed by United Airlines fewer than six percent of the equipments examined followed the bathtub curve. The most popular exception to the "bathtub" curve is the constant failure rate (horizontal line) model. It is generally used for electronics, avionics, and complex systems like aircraft, ships, tanks, etc.



Definitions for Mission Reliability Parameters

MEAN TIME BETWEEN DOWNING EVENTS (MTBDE): A measure of the system reliability parameter related to availability and readiness. The total number of system life units, divided by the total number of events in which the system becomes unavailable to initiate its mission(s), during a stated period of time.

MEAN TIME BETWEEN OPERATIONAL MISSION FAILURES (MTBOMF): A measure of the system reliability parameter related to availability and readiness. The total number of system life units, divided by the total number of operational mission failures, during a stated period of time.

R&M are Force Effectiveness Multipliers.

Reliability is a "force effectiveness multiplier": This means that the more reliable our system is the more effectiveness it will provide. For example if we have 20 combat tanks, whose reliability in getting from point A to point B (where combat will begin) is only 50%, we can only expect 10 tanks to engage in battle. Whereas if the tanks had approximately 100% reliability we can expect all 20 tanks to engage in battle, i.e., double the combat capability. So, reliability "multiplies" the size of the combat force.

Maintainability is a "force effectiveness multiplier": The more rapidly our system can be repaired and put back into the combat arena, the more combat capability it can provide. If 8 of the 10 tanks that broke down in the desert, above, are repaired quickly enough to still cross the desert on time, then maintainability of those tanks has saved the day. In other words, maintainability has provided more combat capability – 8 of the 20 tanks (40%) completed the mission because maintenance saved 8 of the 10 (80%) failed tanks!

Dependability:

The dependability of a product is the probability it will provide acceptable performance during the mission, even if maintenance is needed to sustain it. For a single mission, dependability is the same as Mission or Weapon System Reliability (MR/WSR). For a continuously operating system dependability is the percent of time system performs its mission functions.

"Dependability is the ability of the airplane to meet schedules, require low maintenance, and be easily and quickly restored when a failure occurs." - Boeing Commercial Airplane Group 1994. Dependability is a broader concept than reliability because the former allows for maintenance to sustain the product even if fails. Dependability is, therefore, larger than reliability.

A general model for Dependability (D) is: $D = R + (1-R)M_O$

where M_O is the operational maintainability (the probability that, if a failure occurs, maintenance can be performed quickly enough to allow the mission to be completed successfully). In the example involving the tanks, Reliability is 50%, M_O is 80% and Dependability is therefore 90%.

Operational Availability

Availability is a measure of the degree to which an item is in an operable and committable state at the start of a mission when the mission is called for at a random point in time.
Operational availability (A_o) depends on field reliability and downtime.

$$A_o = \frac{MTBM}{MTBM + MDT}; where\, MDT = \overline{M} + ALDT$$

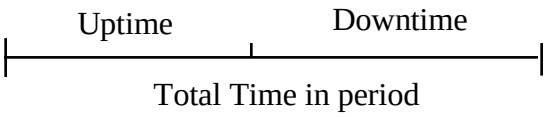
Mean Downtime (MDT) is the average elapsed time between loss of mission-capable status and restoration of the system to mission-capable status. $\overline{M}$ is the mean active maintenance (preventive and corrective) time. ALDT is the average administrative and logistics delay time. It includes delay times.

A more plain-English formula for A_o is

$$A_o = \frac{Uptime}{Uptime + Downtime}$$

Comparing these two formulae, we can see that MTBM is essentially the average Uptime; and MDT is the average Downtime.

For simplicity, equipment is either operational ("up") or not operational ("down"). So,



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

Example: Total time = 8 hr, downtime = 0.6 hr

$$A_o = \frac{\text{Total time} - \text{Down time}}{\text{Total Time}} = 1 - \frac{\text{Downtime}}{\text{Total Time}}$$

$$A_o = \frac{8 - 0.6}{8} = \frac{7.4}{8} = .925 \text{ or } 92.5\%$$

That is, the system was operational 92.5% of the time during this 8-hour interval.

<u>Automobile Example for MDT Calculation</u>

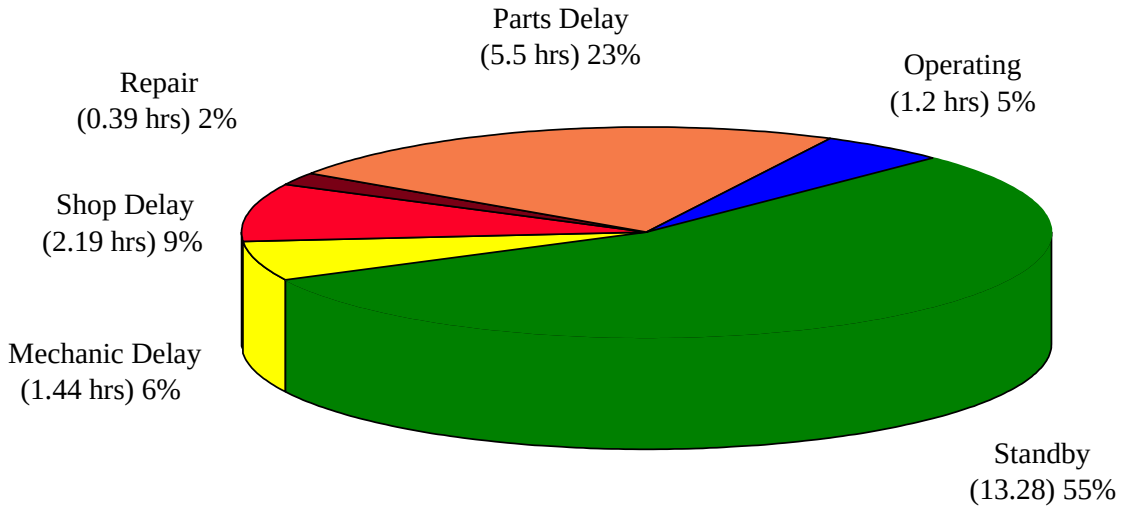
- Principal components of Downtime are:
  - <u>Corrective</u> Maintenance Downtime (CMDT); for example: my car was down for repairs on three occasions last year: 2 days, 1 day, and 3 days. So CMDT = 6days
  - <u>Preventive</u> Maintenance Downtime (PMDT); my car was down on four occasions for an oil change last year: .75 hr, .75 hr, .75 hr, .75 hr. So PMDT = 3 hrs.

- So, Downtime = CMDT + PMDT; for my car, Downtime = 6 days + 3 hours = 6x24 hours + 3 hours = 147 hours.

Downing Event #	Cause	Downtime (hr.)	Active maintenance time (hr.)	Delay time (hr.)
1	PM	0.75	0.50	0.25
2	CM	48.00	4.00	44.00
3	CM	24.00	3.00	21.00
4	PM	0.75	0.50	0.25
5	PM	0.75	0.50	0.25
6	CM	72.00	5.00	67.00
7	PM	0.75	0.50	0.25
TOTALS		147.00	14.00	133.00

MDT = 147 hr / 7 downing events = 21 hr
$\overline{M}$ = 14 hr / 7 maintenance actions = 2 hr
ALDT = 133 hr / 7 delays = 19 hr

A Day in the Life of the M1
(TRADOC/AMC Pamphlet 70-11, RAM Rationale Report Handbook, 1987)



Thus, the M1 tank was available 60% of the time; it experienced maintenance delays 38% of the time, and underwent active repair 2% of the time. Note the delays outweighed the active repair time by a ratio of 19:1. The M1 tank example suggests another formula:

A_o = 1 - [Nonavailability for Hands-on] - [Nonavailability for Delays]

ALDT - an Example

Bench stock for a certain type of aircraft (1100 frequently used, inexpensive parts, such as lights, seals, and screws) was kept in a central storage area back from flight line. Requests for bench stock items were handled by special expediter trucks, which could cause a delay of an hour or more. A new system was installed. The most frequently used items were identified (400 out of 1100). Now all 400 items are carried on all expediter trucks. User comment: "These mobile bench stocks now often deliver requested parts within eight minutes."

Two Formulae for Operational Availability:

Operational Availability (A_o) may also be viewed from two other perspectives: the number of systems that are ready divided by the number possessed; or the total uptime divided by the uptime plus downtime when operated in an operational mission scenario. From the first perspective, operational availability may be defined as the percentage of assigned systems ready for use when needed, e.g.,

$$\text{Operational Availablity} = \frac{\text{Number of missileson alert}}{\text{Total missilesinstalled}}$$

This formula is useful for as a snapshot assessment of operational availability. It would answer a question such as "What was your operational availability at 0600 on 16Jun99?"

From the second perspective, operational availability is the percentage of time a system(s) is available for use

$$\text{Operational Availability} = \frac{\text{Uptime}}{\text{Uptime} + \text{downtime}}$$

This formula indicates operational availability for some duration. It could answer a question like "What was your operational availability for June, 2007?"

Inherent Availability

A product's inherent availability (A_i) depends on inherent R&M characteristics.

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

Note that contractual R&M parameters (MTBF and MTTR) are used in the A_i formula.

R&M May be Considered Complementary Disciplines

Technically, R&M can be traded-off to achieve a desired level of inherent availability, A_i

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

For example, if a contract specification has an A_i requirement of 95%, any of the combinations below will suffice.

A_I	MTBF (hr)	MTTR (hr)
.95	900	47.4
.95	950	50.0
.95	1900	100.0

Consider the second combination above as the baseline design (MTBF=950 hours and MTTR=50 hours. However, the contractor can trade-off reliability if they compensate by improving maintainability to still reach the 95% inherent availability (MTBF=900, MTTR=47.4). Conversely, they can trade-off maintainability if they compensate by improving reliability (MTBF=1900, MTTR=100.0).

The fallacy here is that we have discussed a specific level of inherent availability. From a pure "availability" viewpoint, "more is better"; so we should want the contractor to be thinking of how they can increase availability, not stay at some specific level. One means to achieve this might be to include an incentive for better availability. This would encourage the designer to improve both R&M.

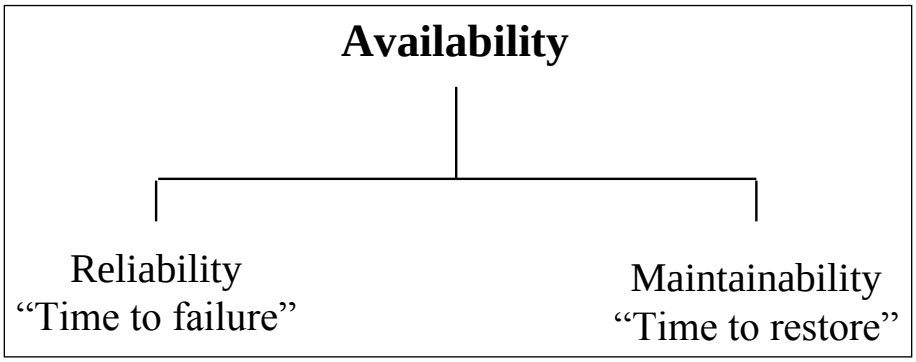
Achieved Availability

Achieved Availability (A_a) depends on field reliability and maintenance.

$$A_a = \frac{MTBM}{MTBM + \overline{M}}$$

Here MTBF has been replaced with an operational analog, MTBM. MTTR has been replaced with an operational analog, $\overline{M}$, which is the average time for corrective and preventive maintenance.

Another way to conceptualize how availability relates to R&M is to think of reliability as "time to failure" (larger is better) and maintainability as "time to restore" (smaller is better). Pictorially, this becomes



How are Readiness and Availability Related?

Readiness is a broader concept. It deals with the entire system, including having the right number and types of personnel to carry out the mission. Availability usually refers to the equipment. Availability of equipment is a part of the mission readiness concept.

R&M Benefit Operations by providing Increased Mobility

Another example of how R&M benefit mission operations is via increased mobility. The greater the reliability of a system the smaller will be the size of the logistics footprint. This means fewer people and less "stuff" to mobilize. An F-22 squadron and its support can deploy with eight C-141s rather than the 17 required for a comparable number of F-15s.

Definitions for Mission-Related Maintainability Terms

The following are Army, Navy, Marine Corps, and Air Force Operational Test Agencies mission-related maintainability terms.

Mean Corrective Maintenance Time for Operational Mission Failures (MCMTOMF): The total number of clock-hours of corrective, on-system, active repair time, which was used to restore failed systems to mission-capability status after an operational mission failure (OMF) occurs, divided by the total number of OMFs.

Maximum Corrective Maintenance Time for Operational Mission Failures (MaxCMTOMF): That time below which specified percentage of corrective maintenance tasks must be completed to restore the system to operation after an Operational Mission Failure.

Maintenance Ratio (MR): The most common expression for Maintenance Ratio (MR) is Maintenance Man-hours per Operating Hour, which is an indication of the maintenance burden associated with the system. So, the cumulative number of maintenance man-hours during a given period is divided by the cumulative number of operating hours. If appropriate, other terms such as miles or rounds may be substituted for hours. Scheduled as well as corrective maintenance, in keeping with the users' maintenance requirements, is included without regard to their effect on mission or availability of the system.

Impacts of R&M on Missions - Summary

As shown in Chapter 1, R&M reduce support costs. As shown in Chapter 2, R&M increase combat capability. That is R&M provide more bang and less buck (at least in the out years). Some measures relating to combat capability that were discussed in Chapter 2 include operational availability, readiness, dependability, and mobility.

This page intentionally left blank

Chapter 3: Developing Operational and Contractual R&M Requirements

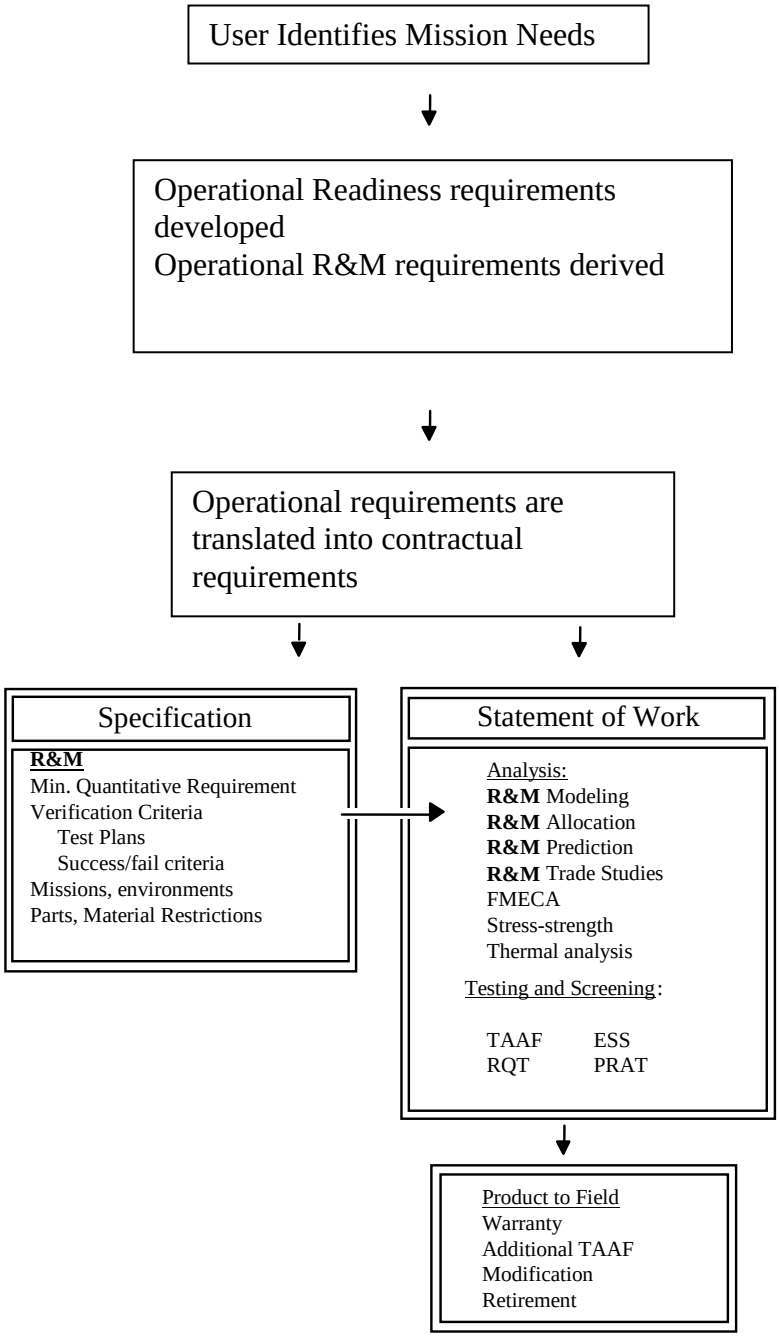
The primary aim of this chapter is to assure the logistician, working in a program office, can generate operational R&M requirements and participate in translating them into contractual R&M requirements. Specifically, you will learn:

A two-step process of developing operational R&M requirements from a ICD.
Methods for converting operational R&M requirements into contractual requirements.
Approaches for assessing the R&M of Commercial and Nondevelopmental Items.

This chapter begins the cradle-to-grave review of acquisition with a focus on R&M activities. Acquisition begins with the requirements process.

The following chart highlights R&M activities during the acquisition process.

R&M in the Acquisition Process



Chapters 3-7 will discuss the R&M activities highlighted above mentioned above.

Developing Operational R&M Requirements

a. The Initial Capabilities Document (ICD)

The using command or HQ prepares the ICD. It identifies a capabilities need or deficiency. A good example of a ICD statement would be "to kill 10,000 enemy tanks in specified conflict." A bad example: "Must be an aircraft that must fly at 600 knots and carry a minimum of ten Maverick" missiles; this is a bad example because it dictates a solution.

b. Analysis of Alternatives (AoA)

The AoA shows the sensitivity of each alternative to possible changes in key assumptions.

c. Capabilities Development Document (CDD)

The CDD documents user requirements and provides system-specific requirements such as range, speed of data transmission, and RM&A. The CDD should flow from the AoA and reflect system-level performance requirements. The CDD is used as the basis for translating operational requirements into contractual requirements. Since R&M requirements in the CDD will affect operational effectiveness, the R&M requirements should also be addressed in the TEMP (Test and Evaluation Master Plan).

Exercise: Developing R&M Requirements in an CDD

- Situation: Air pollution is still a problem. In order to help improve the quality of the air, a state mandated a percentage of vehicles (weighing less than 3750 pounds) sold in the state have **zero emissions!**

- Solution: To meet this challenge, automotive manufacturers are developing new battery - powered propulsion subsystems.

Specify R&M requirements. Identify a **MINIMUM ACCEPTABLE, THRESHOLD REQUIREMENT (T)** and an **OBJECTIVE (O).**

Battery R&M Requirements	T	O
Reliability:		
Maintainability:		

Developing Operational R&M Requirements from the Capability Need

The following is a two-step method for developing operational requirements from a capability need:

Step 1: Develop appropriate **system level models to** relate R&M to DoD combat capability and life cycle ownership cost goals.

e.g., System Effectiveness = Performance Capability X A_o X Dependability

It means a system's effectiveness depends on its inherent capability, the likelihood that it will be available when called for, and the Service's ability to sustain it during its mission.

Step 2: Select and quantify appropriate **OPERATIONAL** R&M factors, such as MTBOMF, MTBM, MTBD, MCMT, MDT, etc. This list is arbitrary; any set of appropriate operational terms may be used.

Several organizations, like the Air Force Air Combat Command, publish a RAMS (Reliability, Availability, Maintainability, and Supportability) Rationale document that provides the supporting justification for the RAMS needs in the CDD.

Operational Models Need Operational Terms

Situation: You are budgeting for support costs for depot repairs for an item for the next year. The cost per depot repair is $500. The expected utilization of the equipment in the field is 100,000 hours for the next year. The maintenance concept is: every removal-for-cause results in a return-to-depot for-repair. Someone gave you

a value of 1,000 hours mean time between failure (MTBF) for the reliability characteristic. QUESTION: HOW MUCH DO YOU BUDGET?

You should first ask yourself whether "MTBF" is the correct term to analyze support cost (or availability, or mission reliability, or any other R&M related system readiness objective)? A possible model would be:

$$\text{Annual Depot Repair Costs} = \left[\text{Expected Number Of Depot Repairs}\right] * \left[\text{Cost Per Repair}\right]$$

$$= \left[\frac{\text{Expected Life Units}}{\text{MTBR}}\right] * \left[\text{Cost Per Repair}\right] = \left[\frac{100{,}000\text{hours}}{\text{MTBR}}\right] * \left[\frac{\$500}{\text{repair}}\right]$$

Definition of Failure:

The A-10 Aircraft development contract defined a failure as "loss of mission critical function that occurred after the end of the preflight inspection and before the start of the postflight inspection". So, it excluded noncritical failures and many failures not discovered in flight. The user's definition of failure was any incident that required a maintenance action to correct an inherent defect.

Both definitions were used to develop a MTBF. So, weapon system advocates reported a MTBF over ten times higher than the more independent testers. This large discrepancy surfaced at an important program review and the chairing flag rank officers were notably displeased.

Failure Definition Exercise

- An individual's judgment as to whether an event is or is not a "failure" is dependent upon how that event affects that individual or their organization.
- Based upon your assigned perspective, identify which of the following events you consider to be a "failure".
- Assume that these 24 events occurred in an operational, field environment on a system that is still managed by the original system program office.
- The operator initially observed events 1-18. Only a maintenance technician observed events 19-24.
- All 24 events and the maintenance associated with each event were recorded in the end item/system records. All base (but no depot) maintenance actions were reported via the Service maintenance data collection and reporting system.

Failure Definition Exercise: Perspectives

- OPERATOR: The individual that operates the equipment attempts to use its various functions, and makes operational decisions based upon equipment/ software performance. The operator only observes those actual or indicated malfunctions while he/she is operating the equipment.
- LOGISTICS (On-equipment maintenance manpower): The on-equipment or first line maintenance technician. Performs troubleshooting, fault detection, fault isolation, adjustments, remove and replace actions on the end item (e.g. aircraft, simulator, missile, etc.). The on-equipment technician responds to all events listed. The on-equipment technician will probably not be aware of the subsequent actions (stated in some of the events) that take place at the intermediate/base shop or at the depot/contractor repair center.
- LOGISTICS (Spares manager at a government depot): Concerned about storing, transporting, tracking, and managing SPARE PARTS.
- LOGISTICS (Maintenance manager at a depot): Concerned with maintenance performed at a government depot or at a contractor's facility to: (1) periodically inspect/repair end items, (2) perform major modifications, or (3) repair removed items.
- PROGRAM OFFICE (PO): Has received a Program Management Directive to develop/acquire a system that (1) meets the users' needs as stated in the Capabilities Development Document, and (2) is acquired on schedule and within cost constraints.
- PRIME CONTRACTOR: Has a contract with the PO. Responsible for (1) designing and manufacturing a system that meets performance requirements and (2) keeping the program within cost and schedule constraints.

FAILURE (Y or N)?		EVENT
_____	1.	A brake assembly malfunctioned and was replaced by a line technician. Later, depot failure analysis showed that the brake was incorrectly assembled by a depot technician.
_____	2.	A pilot oxygen mask did not operate properly. A shop technician found cookie crumbs in the inhale/exhale value.
_____	3.	A mission was aborted due to an indication by a fuel leak detector. Line technicians could not find an actual leak.
_____	4.	A torn B-52 drag chute was replaced and sent to a depot repair facility. Upon inspection, the depot technician found the remains of a taxi light
_____	5.	A computer malfunctioned and was replaced. Shop technicians found sand in the unit.
_____	6.	During a pre-use check, a critical indicator did not illuminate as expected. A line technician replaced a light bulb in 5 min.
_____	7.	A transport vehicle failed to complete its mission. Depot failure

analysis identified that a piece of cleaning cloth had blocked fluid through a critical valve.

_____ 8. The radio transmitter, removed as "intermittent," was sent to the depot where the unit tested OK.

_____ 9. A back-up electronics unit malfunctioned and was replaced. A shop technician reseated all the cards and the unit checked OK.

_____ 10. During takeoff and gear retraction, a landing gear warning light stayed on. The plane aborted its mission and landed. A line technician adjusted a switch to correct the problem.

_____ 11. A radio was replaced because of a built-in-test (BIT) indication. Depot failure analysis identified a bad transistor in the BIT circuit.

_____ 12. A water pump shaft broke, causing flooding in an equipment compartment. A minor change in a manufacturing process was implemented that should prevent future breakage.

_____ 13. An aircraft made an uncommanded maneuver. A depot technician found and corrected a software error. This particular malfunction has not recurred as of this date.

_____ 14. The GFE radar-warning receiver malfunctioned and was removed. A shop technician found moisture (rain) inside.

_____ 15. After 3 months, paint began to peel from a new utility vehicle. A line technician did a "touch-up" repair.

_____ 16. Hail severely damaged a protective dome covering radar. The radar was turned off and a line technician replaced two large panels that were subsequently condemned.

_____ 17. The power generation system on one of the engines dropped off line during a mission. A line technician replaced the generator and the generator control unit. Both were sent to the depot.

_____ 18. During scheduled depot maintenance, a depot technician discovered and replaced a badly chafed wire bundle.

_____ 19. A line technician corrected a fuel leak by tightening a fluid connector.

_____ 20. Per tech data, a gearbox was replaced after 2000 hours of failure-free operation.

_____ 21. Chemical vapors from the GFE battery caused severe corrosion to a hydraulic line. The line was replaced.

_____ 22. A cut tire was discovered during a pre-use inspection and replaced before the next scheduled usage.

_____ 23. A tire (warranted for 50,000 miles) was worn beyond safe limits after accumulating 60,000 miles and was replaced.

_____ 24. During a routine, end-of-day inspection, a line technician found and replaced a broken access door latch.

Reliability Terms Exercise - Summary

Perspective	Term Name MTB ____?	# of Events
Operator: Mission critical		
On-equipment Maintenance		
Depot Spares Manager		
Depot Maintenance Manager		
Program Office: "Failures"		
Prime contractor: "Failures"		

Developing Contractual R&M Requirements

Some methods for developing contractual requirements from operational requirements are:

1. Use formal translators. The Reliability Analysis Center (later known as Alion System Reliability Center), accomplished numerous studies of translators. An example is "Translating User Requirements into System Specifications", RL-TR-96-222, February 1997. A simple example of a translator is:

> MTBF = 3 times the CDD threshold MTBM. So, if the CDD MTBM threshold were 1,000 hours, the required MTBF would be 3,000 hours.

2. Use engineering judgment. The engineer decides how much MTBF is necessary to protect the users' CDD threshold values for R, M, and A requirements.

3. Policy: For example, the Air Force R&M 2000 policy was to "Double R, Halve M" for follow-on systems.

4. Buy as much reliability as funding, schedule, or other constraints allow.

5. Buy the best the contractor can do.

Note that only the first two methods are clearly based on the users' operational needs as expressed in the CDD. However, in actual practice they are probably used less often than the other three!

Contracting for R&M

Aspects of contracting important for R&M include the system specification, the SOO, the SOW, and a warranty. These are discussed below.

Section 3 of a Contract Specification

Section 3, Requirements, describes performance characteristics required. These should be developed from operational/ user requirements. R&M requirements include MTBF, and MTTR, respectively. Requirements may also include physical constraints, interfaces, etc. Material/process limitations, repair tool limitations, or "no safety wire on flight line", may be specified, for example.

The Section 3 requirements should have a valid relationship to user needs as expressed in the CDD. However the Section 3 requirements should be expressed in understandable, contractual language.

Section 4 of a Contract Specification

Section 4 Verification describes how to assure that the item meets the Section 3 requirements.

> **A requirement in a specification is not a real requirement unless there is a corresponding method for verifying that the requirement has been achieved.**

Four basic methods for verifying that the requirements have been met are inspection, test, demonstration, and analysis. Reliability requirements are generally verified by test; maintainability by demonstration. Since Section 4 states how the contractor will be evaluated, traditionally the government could drive the design by imposing a tough test plan. However, with acquisition reform, the contractor now proposes the Section 4 test plan.

Section 4 identifies accept/reject criteria and test/analysis procedures as well as environmental conditions. Section 4 is very important since it should prevent/reduce disagreements when evaluating test data. It helps to scope the design effort.

Statement of Objectives (SOO)

The SOO states the government's high-level program objectives, including the RM&A objectives, when appropriate. The SOO is part of the Request for Proposals (RFP).

Statement of Work (SOW)

A SOW is proposed by industry in response to a SOO. It describes the minimum contractual effort necessary to achieve the RM&A (and other) requirements in specification. The SOW states what activities the contractor will perform (e.g., FMECA per best commercial practices) and when to have them accomplished/completed.

Warranties

Although warranties are no longer required for weapon system acquisitions, there may be cases where they appropriate. A warranty is a promise or affirmation given by a seller to the government regarding the nature, usefulness, or condition of the supplies or performance of services furnished under the contract. "Guarantee" and "product performance agreement" are other terms for "warranty."

Nature of Warranties (Government or Commercial Marketplace)

All warranties have certain essential elements. A warranty will always identify the warranted item, state the length of the warranty period, identify what is covered by the warranty, list the acceptable use conditions, and explain the warrantor's liability.

There are several reasons to have a warranty. It is difficult to demonstrate a product's mature reliability without actual field data; and production items may have latent defects. Warranties are designed to protect Government interest after delivery.

We warrant essential performance requirements (EPRs). There may be hundreds of performance requirements in a specification. A maximum of three to five EPRs is suggested. The Warranty for the F-117 engine for the C-17 aircraft states that:

> The engine reliability guarantee plan guarantees that the maintenance shop visit rate will not exceed 0.28 per thousand engine flying hours. A "shop visit" occurs whenever an engine must be removed from the aircraft for maintenance.

Contractor Motivations with Warranties:

When the government notifies a contractor early on in the design phase that we intend to buy a warranty, we hope this will motivate the contractor to design-in even more reliability.

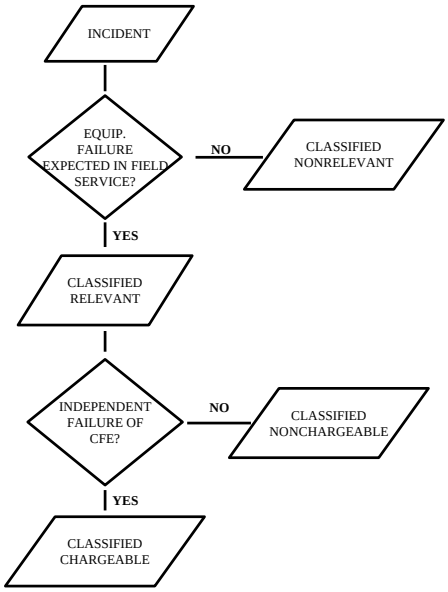
It may also motivate the contractor to provide better diagnostics (improve BITE, technical manuals, test equipment, etc.) because they don't want to "fix" good items. By enabling the military to do a better job of discriminating good items from bad, the contractor will lessen his future burden.

The contractor will also be motivated by a warranty to design-in a more efficient and effective repair process so the corrective maintenance work they do can be done less expensively.

Contractual Terms - "MTBF" Contractual Definition of "Failure"

Question: What counts as a "failure" relative to contractual reliability tests? This brings up the issue of relevant vs. non-relevant, and chargeable vs. non-chargeable failures. MIL-HDBK-781 discusses these terms. Each contract should define these times, however.

The following chart illustrates their relationships.



If a system under test experiences a failure, the first question is whether the failure is relevant or non-relevant. If the system failure was caused by a subsystem of a type that will be used in the operational environment, the failure is relevant; otherwise, it is non-relevant. An example of a non-relevant failure would be a substitute generator (not of a

type expected to be used in the field) was installed in a system merely to allow the other subsystems and the interfaces to be tested; and the generator causes the system to fail.

Assuming a failure is relevant, the next question is whether the failure is chargeable (to the contractor). If a failure is caused by contractor-furnished-equipment (CFE), the failure would be deemed chargeable. An example where it would be non-chargeable is if the government gave the subsystem to the contractor (government-furnished equipment or GFE) and it was faulty. Chargeable failures are scored against the contractor in calculating an observed MTBF.

Why Field Reliability Data Differs From Contractual Reliability Data

Field personnel often note that field reliability data (maintenance rate, removal rate, demand rate) suggests the product is less reliable than they expected based on Program Office or contractual numbers. There are many reasons for this:

> Environment not quite the same (i.e., conditions change). Sometimes we deploy equipment in parts of the world where we hadn't intended, and for which we hadn't designed or tested.
>
> Failures induced by interacting components: some field failures result from interactions that were not anticipated and for which we had not tested.
>
> Personnel-related failures: some failures in the field result from mistakes made by operators, maintainers or other personnel.
>
> No-defect removals: some removals that were counted as failures are later learned to have been no-defect - perhaps the built-in-test-equipment (BITE) was faulty.

Acquisition Reform Impact on R&M

Prior to acquisition reform, the government specified its requirements (Section 3 of the specification), wrote the SOW, and specified verification procedures (Section 4 of the specification) for R&M. This led to a rather structured, dictated approach to R&M. Under acquisition reform, however, the contractor proposes the SOW and verification plan; they may also participate in developing technical requirements. Thus, the contractor assumes a greater role and more responsibility.

Military Documents Dealing with R&M:

Since MIL-STDs cited in a contract generally denoted a requirement rather than guidance, the DoD is basically doing away with many MIL-STDs. And there are various ways of doing this.

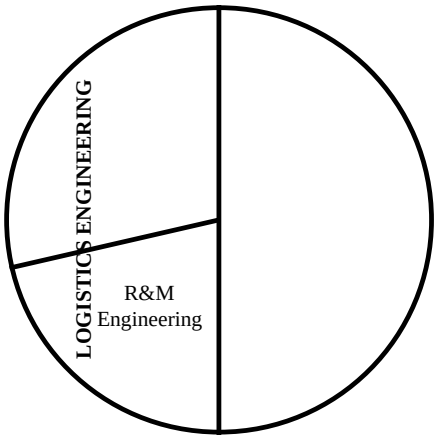
Some of the R&M standards, like MIL-STD 2164, Environmental Stress Screening Process for Electronic Equipment, have been converted to MIL-HDBKs. Others, like MIL-STD 721, Definition of Terms for Reliability and Maintainability, have been canceled, but contents retained elsewhere (like in MIL-HDBK-338 for MIL-STD-721). Still others (like MIL-STDs-470 and –471) have been consolidated and published as a new document (MIL-HDBK-470A).

How Design Interface, Logistics Engineering, Systems Engineering, and R&M are Related

A major function of an acquisition program office is systems engineering. Systems engineering includes logistics engineering, which includes R&M engineering. Acquisition Logisticians are urged, by the Design Interface logistics element, to work with the systems engineer to assure the system is designed and developed with supportability in mind.

As the Program Office "watchdog" for supportability, the acquisition logistician must assure that CDD R&M requirements are not discarded. These requirements must be translated (through logistics engineering and system engineering processes) into the solicitations and contracts. The R&M performance requirements may be expressed in terms like failure rates, MTBF, and MTTR.

SYSTEMS ENGINEERING



Open System Architecture

An open system design is one that emphasizes standardized approaches to system interfaces, both functional and physical. This approach can achieve superior warfighting capability (e.g. by a reliability upgrade) more quickly and more affordably by using multiple suppliers and commercially supported practices, products, specifications, and standards, which are selected based on performance, cost, industry acceptance, long term availability and supportability, and upgrade potential.

The open systems approach is sometimes referred to as "plug and play". An example would be removing a card from a computer slot and replacing it with a better (more reliable) card. The Army popularized an open systems approach with its Modernization through Spares (MTS) program. Legacy systems can thus be modernized via better line replaceable or shop replaceable units.

Assessing the R&M of Commercial and Nondevelopmental Items:

In plain English, if you can walk into a store and buy an item off the shelf, or order it through a catalog, it is a "commercial item". Nondevelopmental items are a little more complicated.

Example: years ago the DoD contracted for the development and manufacture of a generator set; some other DoD organization today feels that same generator could satisfy their own new requirement. They ask the supplier to build some more. Since this generator is not readily available to the public, but has been developed already, it is a "nondevelopmental item". The DoD has published "Commercial and Nondevelopmental Items: A Handbook", to assist the acquisition workforce. It is accessible at https://acc.dau.mil/CommunityBrowser.aspx?id=143255. The Handbook includes some six pages on assuring that we acquire reliable and maintainable commercial and nondevelopmental items. It outlines three approaches: market investigation, testing, and others.

a. Market Investigation: Ask the retailer, manufacturer, etc. for R&M design, development, and failure data. Use this data to assess whether the item meets your R&M needs. For example, what well-established R&M practices were incorporated in the design and development of the item? What was the MTBF (Mean Time Between Failures) and how were "time" and "failures" defined? Show me the market-generated failure data. If this investigation fails to definitively answer the question, proceed to the next approach, testing.

b. Testing: Acquire some specimens and test them to determine their R&M characteristics. Perhaps a third party; can participate in testing. Also, demonstrate the maintainability of the item. If this approach doesn't answer the question, or isn't feasible, try some other means to determine the R&M characteristics of the item.

c. Some other means include

1. Require total contractor logistics support (CLS) including an operational availability (A_0) requirement.
2. Scrutinize existing requirements (e.g. mission profiles) to determine if demonstrated R&M values of potential commercial or nondevelopmental items are acceptable under different circumstances.
3. Purchase sufficient spares to meet the specified A_0.
4. Modify the commercial or nondevelopmental item to meet R&M requirements.

MIL-SPEC vs. Commercial Parts – Buyer Beware

The bottom line is that while many commercial parts work quite well in military applications, some don't. Moreover, "standard" parts may be suspect if your intended military environment requires technical performance of material/other properties that weren't observed during the standardization process.

Therefore, the application of parts, including standard parts, is most important!

R&M Activity Guidance (General)

DoD 4245.7-M: Transition from Development to Production.
DoD Guide for Achieving Reliability, Availability, and Maintainability.
MIL-HDBK-470A: Designing and Developing Maintainable Products and Systems.

Summary, Chapter 3: Operational and Contractual R&M Requirements -

This chapter explained how R&M requirements relate to the ICD, AoA, CDD, and a contract specification. It showed a method for developing operational R&M requirements from the ICD and some means to develop contractual R&M requirements from the CDD. It also discussed the notions of relevant vs. non-relevant failures and chargeable vs. non-chargeable failures.

This page intentionally left blank

Chapter 4: Providing Insight into Designing for Reliability

The aim of this chapter is to assure that while you are reviewing a company's proposal you consider all the activities that might result in a reliable product. Specifically, you will learn about designing for supportability; allocation; modeling; integrity analysis; parts selection; derating; thermal design; failure modes effects and criticality analysis (FMECA); software R&M; reliability prediction; reliability-critical items analysis; storage, shelf-life, packaging, transportation, and handling analyses; sneak circuit analysis and failure reporting, analysis, and corrective-action system (FRACAS).

Design for Reliability

Designing for reliability is a part of designing for supportability. But supportability also includes maintainability, human factors, system safety, producibility, quality, and cost. This chapter discusses typical reliability methods.

Reliability (or Maintainability) Allocation

A reliability allocation is an apportioning of the overall system level reliability requirement in such a way that the individual item reliability characteristics support the overall system requirement. The government's reliability requirements are generally at the system level

The contractor will generally allocate the government's system-level requirement to lower levels of assembly; i.e., the allocation process is a "top-down" process. Lower tiers may be subsystems; line replaceable units (LRU), which the Navy refers to as weapon replaceable assemblies (WRA); shop replaceable units (SRU), which the Navy calls shop replaceable assemblies (SRA); or individual components.

Uses for Allocation

There are many reasons why a contractor should perform a reliability allocation. It can help establish reliability goals for the contractor's departments or its subcontractors. It can help the contractor track progress throughout development process. Also the allocations provide the "best guess" of real reliability in the mature system; as such the allocated values are the initial inputs into logistics models for spares, maintenance personnel, transportation requirements, etc.

Reliability allocations may be adjusted over time, as long as the system-level requirement is met. However, there comes a point in the design, when the allocations should be frozen, because, for example, mission and logistics planning are being finalized.

Allocating the System Failure Rate Requirement

In performing an allocation it has been found that failure rates are easier to deal with than MTBFs. This is because subsystem failure rates add up to the system failure rate (assuming the subsystems are mission-critical and in the "useful life", i.e., constant failure rate phase). Subsystem MTBFs don't add up to anything meaningful!

Reliability Allocation Methods

There are several reliability allocation methods. Three that we will examine here are the Equal Allocation Method, the Weighted Allocation Method and a General Iterative Allocation Method.

Equal Allocation Method

This method assigns equal reliability requirement to each subsystem. However, it fails to consider the relative effort required to achieve equal reliabilities. For some subsystems it may be difficult, for others, easy. Hence, the equal allocation method is of limited usefulness. Its main use is as a first-cut in making an allocation.

Equal Allocation Method Example

Assume that a new car requirement includes a system-level failure rate requirement of (not to exceed) ten failures per 100,000 miles. Assume also that the automobile's mission-critical subsystems are Electrical (EL), Drive Train (DT), Steering (ST), and

Brakes (BK). Using the Greek letter "lambda" to denote failure rate, we can then write:

$$\lambda_{car} = \frac{10 \text{ failures}}{100{,}000 \text{ miles}} = \lambda_{EL} + \lambda_{DT} + \lambda_{ST} + \lambda_{BK}$$

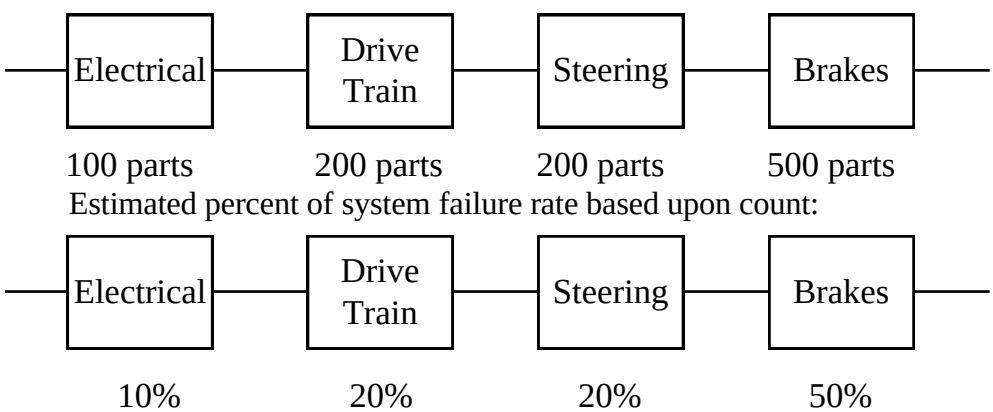
Equal Allocation means: $\lambda_{\text{EL}} = \lambda_{\text{DT}} = \lambda_{\text{ST}} = \lambda_{\text{BK}} = \dfrac{2.5 \text{ failures}}{100{,}000 \text{ miles}}$

<u>Weighted Allocation Method</u>

This method considers or weighs factors such as complexity of the system, safety/mission criticality, number of parts, physical weight of components, maturity of the technology, and past experience.

We will show an example of a "Weighted" model using expected <u>parts count</u>.

Situation<u>:</u> Same car requirement as before. Engineers have estimated the following parts count based upon past design history, new functional requirements, and new technologies.



Allocated requirement:

Electrical	10% x 10 failures/100000 miles = 1 failure/100000 miles
Drive Train	20% x 10 failures/100000 miles = 2 failures/100000 miles
Steering	20% x 10 failures/100000 miles = 2 failures/100000 miles
Brakes	50% x 10 failures/100000 miles = 5 failures/100000 miles

- System failure rate $\lambda_S = 1 + 2 + 2 + 5 = \dfrac{10}{100{,}000 \text{ miles}}$

Notice how these failure rates differ from the amounts attained in the Equal Allocation method. Can you see why the weighted allocation method is somewhat superior to the equal allocation method?

A General Iterative Allocation Method

Same car requirement as before (10fails/100,000 miles)

1. Write an equation for failure rate: $\lambda_{CAR} = \lambda_{EL} + \lambda_{DT} + \lambda_{ST} + \lambda_{BK}$
2. Estimate the most probable, achievable failure rates for each subsystem, in the model:

$$\lambda_{EL} = 3.0;\ \lambda_{DT} = 1.5;\ \lambda_{ST} = 2.0;\ \lambda_{BK} = 1.5;\ \left(\frac{\text{fails}}{100{,}000\text{mi}}\right)$$

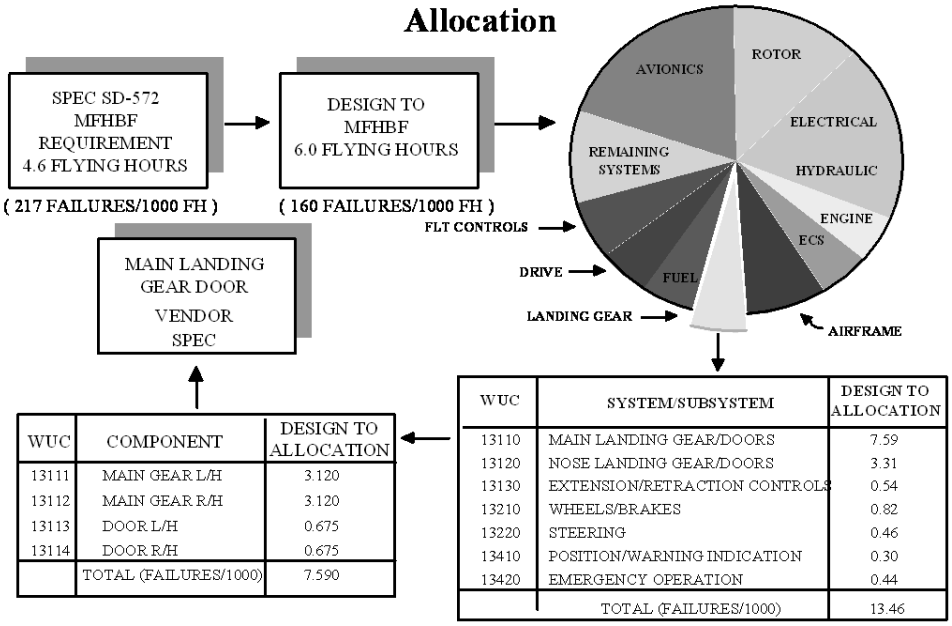
3. Calculate the resulting system-level failure rate: $\lambda_{CAR} = 3.0 + 15 + 2.0 + 1.5 = 8.0$.
4. Compare the model result with the actual system-level requirement.
   λ_{CAR} is smaller than the requirement.
5. If the model result is smaller than the required failure rate, the **input values may become the allocated values.** Otherwise:
   a. "Tweak" the model; add redundancy if practical (REQUIRES USE OF PROBABILITY MODEL). Reevaluate the failure rate inputs. Recalculate the model output. Repeat this process until the model output is less than the required value. If the desired model output cannot be achieved, go to step b.
   b. If the desired value cannot be achieved, then the system requirement is perhaps unrealistic and may have to be relaxed.

      λ_{CAR} is better than required. Accept the values in Step 2.

This iterative allocation process is applicable for all systems and is the only method that will work on large, complex systems such as an aircraft.

Aircraft Reliability Allocation Example

The figure below shows how one company, during early design activity, allocated system requirements among the major subsystems, subsystem requirements among major assemblies, and major assembly requirements to components.



WUC	COMPONENT	DESIGN TO ALLOCATION
13111	MAIN GEAR L/H	3.120
13112	MAIN GEAR R/H	3.120
13113	DOOR L/H	0.675
13114	DOOR R/H	0.675
	TOTAL (FAILURES/1000)	7.590

WUC	SYSTEM/SUBSYSTEM	DESIGN TO ALLOCATION
13110	MAIN LANDING GEAR/DOORS	7.59
13120	NOSE LANDING GEAR/DOORS	3.31
13130	EXTENSION/RETRACTION CONTROLS	0.54
13210	WHEELS/BRAKES	0.82
13220	STEERING	0.46
13410	POSITION/WARNING INDICATION	0.30
13420	EMERGENCY OPERATION	0.44
	TOTAL (FAILURES/1000)	13.46

Allocations and Predictions should be based on operational requirements, not expected laboratory performance.

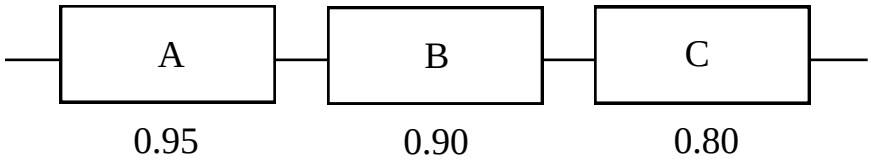
In the first block (upper left) the specified Mean Flying Hours between Failures requirement is given. Below that box is the reciprocal or failure rate. In the next box, we see the contractor is aiming higher than required. In general contractors will try to exceed the required reliability in order to: lessen their risk of failing a test; win an incentive; gain a competitive advantage; or satisfy the customer and compete for other contracts. Note below the second box is the failure rate corresponding to the design MFHBF.

In the pie chart we see the mission-critical subsystems that make up this aircraft system. Note the landing gear is highlighted. In the table below the pie chart we see the subsystems that comprise the landing gear. Note that the failure rate allocated to the landing gear has apparently been further allocated to its subsystems. Note too from the next chart that the failure rate allocated to the main landing gear and its doors has been further allocated. The process becomes more manageable with all this allocation.

Reliability Modeling

Sometimes a single unit design concept may not appear to provide sufficient safety or mission reliability. The solution sometimes focuses on employing one or more redundant items.

EXAMPLE: The initial design for a system has three mission-critical subsystems (A, B, & C) in series (each must work for the system to be successful). The mission reliability (MR) block diagram can be drawn with a series reliability model:



Note that the reliabilities for each subsystem are written below the subsystem's box. These values are easy to work with. However, they are not typical of real-world mission-critical or safety-critical values, which are generally on the order of 99% or higher. For example, if the landings at O'Hare Airport were only 99% reliable, there would be several crashes there each week!

Since all three subsystems must operate:

Mission Reliability (MR) = $\mathbf{R_A \times R_B \times R_C}$
= 0.95 x 0.90 x 0.80
= 0.684

Notice this is less than the reliability of the "weakest link", subsystem C.

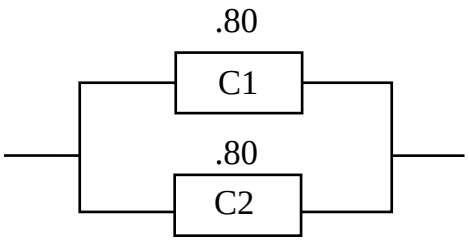
If the customer's <u>requirement</u> for this system is 0.80, will the proposed system meet the user's need? No, it's too low.

What alternatives exist to improve the system?

- Delete one or more subsystems and associated functions? We are assuming all three subsystems are critical to the mission, say, a bombing mission, so this alternative is not feasible.
- Improve reliability of A and/or B? This is not feasible since neither A nor B is the weak link and because the weak link is right at the system requirement. Perfecting A and/or B would still keep us below (or right at) the minimum requirement.
- Improve reliability of C? Yes, but there may be technological limitations that preclude improvements being feasible; or, what if subsystem C is GFE? Then, the contractor may not tamper with it.
- Incorporate REDUNDANCY? Yes, on subsystem C.

<u>Mission</u> reliability can be improved by incorporating active redundancy. Since "C" is the most unreliable subsystem, let's add a second, identical, active - redundant subsystem "C" so that either can perform mission functions. Let C be a "computer" used in the bombing mission.

Reliability (Redundant "C's") =?



"TRUTH" TABLE

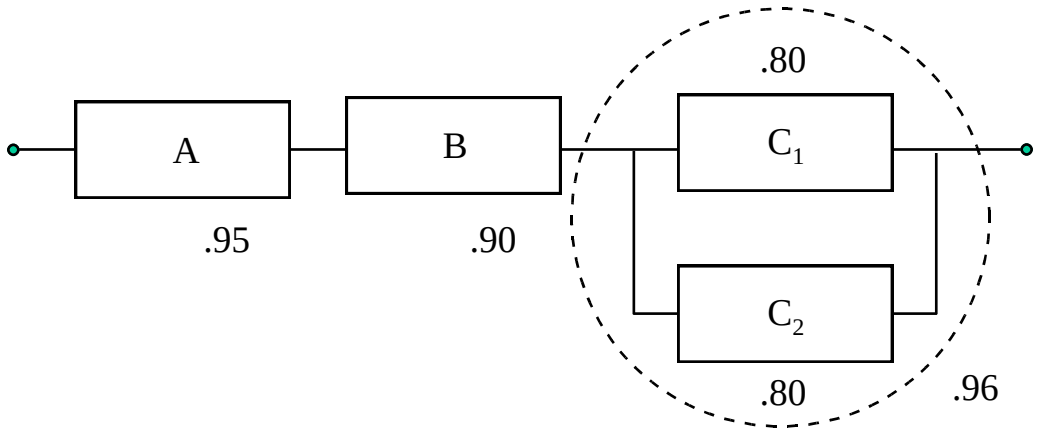
CONDITION C1	CONDITION C2	MISSION SUCCESS?	P (S)
✓	✓	✓	.8 (.8) = .64
✓	x	✓	.8 (.2) = .16
x	✓	✓	.2 (.8) = .16
x	x	x	.2 (.2) = .04
			1.00

The Truth Table provides an intuitive means of computing the reliability of the redundant configuration of computers. The Truth Table considers all possible scenarios. One scenario is that both computers work the entire mission. The mission would then be a success, at least computer-wise. What is the probability of this scenario occurring? The probability of C_1 and C_2 working is the product of their respective probabilities (reliabilities), i.e., .64. Similarly the probabilities associated with the other scenarios are computed. Note that the probability that a computer won't work (denoted by an "x") is its unreliability, i.e., .2.

To check our logic and arithmetic, the probabilities in the right hand column should add to 100%. They do.

Of the four scenarios, only the first three provide a successful mission from the computer point of view. That is, if either the first or the second or the third scenario occurs, the mission is a success from the computer standpoint. The probability that one of those scenarios will occur is the sum of their probabilities, i.e., .96. This leads to the mission reliability block diagram with redundancy, shown below.

Mission Reliability Block Diagram with Redundancy:



MR = .95(.90)(.96) =.82

I.e., Redundancy improves mission reliability; from .68 to .82 here.

Question: How many mission critical failures would you expect for the above C1/C2 subsystem in 1000 missions?
Answer: 4%(1000 missions) = 40 missions

Question: How many logistics failures (e.g. maintenance actions or removals) would you expect in for the above C_1/C_2 subsystem in 1000 missions?
Answer:
For C_1: 20% (1000) = 200 logistics failures;
For C_2: 20% (1000) = 200 logistics failures.
Total: 400 logistics failures.

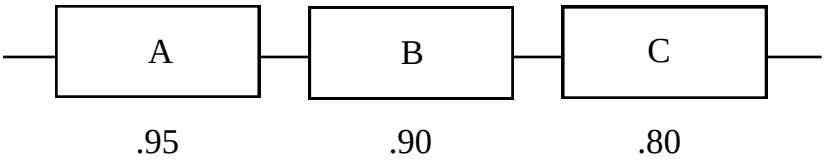
Disadvantages of Redundancy

Improved mission reliability is an apparent benefit of redundancy. What are the disadvantages of redundancy? They include more maintenance labor to care for an additional computer in the above case; increased costs for spares acquisition and transportation and inventory management; more power and cooling requirements. In a word, from a logistics viewpoint, redundancy means more work. From the mission standpoint, there are possible weight penalties such as performance degradation particularly on aircraft; also there may be volume limitations.

Logistics Reliability (LR)

Logistics reliability (LR) is the probability that the mission will not generate any corrective maintenance requirements. Equal consideration is given to non-critical and critical items. Hence, even with redundancy, for logistics reliability we treat everything as if in series. So,

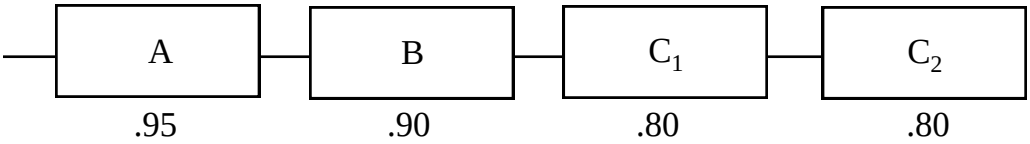
LR Block Diagram for Initial Configuration:



LR = .95(.90)(.80) =.68

Note that this is the same as the mission reliability block diagram for the initial configuration. That's because everything in the initial configuration is mission-critical (and, you could say, logistics-critical). However,

LR Block Diagram with redundancy:



LR = .95(.90)(.80)(.80) =.54

I.e., Redundancy reduced Logistics Reliability from 68% to 54%. There is a 54% chance that everything will be in working order at the end of the mission. There is a 46% chance that <u>at least one</u> of the four subsystems will come home broken.

Redundancy: Summary

In this section we learned that redundancy can help improve MISSION reliability but will decrease LOGISTICS reliability and increase support costs. It is generally better to try to improve the reliability of a single unit whenever possible; use redundancy as a last option.

Integrity Analysis

Integrity analysis is not new but it is receiving increased emphasis in the DoD today. The aim is to design a product to have a failure-free operating period. The method involves anticipating the stress-profile and designing-in adequate strength.

Integrity analysis is a "deterministic approach" to reliability design. The designers determine a failure-free operating period when they can predict (and design for) the lifetime of cumulative stresses. The traditional approach to reliability design is "probabilistic": design it, test to see how reliable it is, and answer questions like what is its probability of success for a given mission duration.

In an integrity analysis, the engineers base the design on cumulative stresses over expected lifetime, material characteristics, and manufacturing capabilities. The analysis then focuses on root cause of failures: stress exceeds strength! This should reduce the need for a Test-Analyze-and-Fix (TAAF) process.

Integrity analysis requires an understanding of the "physics of failure", - fatigue, over-stress, over-voltage, corrosion, etc. It assumes the designers can predict the cumulative stresses that the product will see. This may be easy, for say, the design of a water softener in the home, but may be impossible for a combat system whose mission may change during its operational lifetime.

Parts Selection Program

The objective of a parts selection program is to use parts of known and high reliability; and to minimize the number of new parts entering the supply system. Even if the reliability is not high, if it is at least known, then we can prepare for the failures (provide spares, maintenance labor, etc.).

A parts selection program can simplify logistic support by enhancing interchangeability, quality, reliability, and maintainability. It can also help to conserve resources. The quality of parts is a factor in failure prediction methodology for electronics (ref. MIL-HDBK-217).

Designators are used for different levels of quality. "Best" quality is generally used in space applications. The next best is usually used in aircraft applications. Examples of quality designators are JAN (World War II nomenclature for Joint Army, Navy); JANTX (TX denotes extra testing); and JANTXV (V denotes visual inspection).

While standard parts are encouraged, of utmost importance is the application of the parts. A standard part may not work well in your environment.

MIL-SPEC or Commercial?

Commercial parts may be cheaper to buy than MIL-SPEC parts but they may be more expensive in the long run. For example, there may be less expensive versions of MIL-M-38510 device types, but they may have less stringent electrical specifications than 38510 equivalents. (In many cases they are not electrically tested over the entire operating temperature range and are manufactured with less stringent process controls of uncertified lines.) good management looks at the total cost of ownership not merely the price tag.

Derating

Derating is the practice of limiting the electrical, thermal, and mechanical stresses on parts (devices) to levels below their specified or proven capabilities in order to enhance the product's reliability.

The use (application) of parts (devices) is in such a manner that the applied stresses are less than the maximum ratings. Derating and many other R&M - related activities are discussed in MIL-HDBK-338, "Electronic Reliability Design Handbook."

Example: Derating for Lamps	
Characteristic to Derate	Percent of Rated Value
Voltage (Incandescent Lamps)	94
With the above derating, the **life expectancy** (a reliability parameter) **doubles** and the light output (performance capability) decreases only 16%.	

There are four basic procedures the designer may use to increase reliability via derating.

(1) Increase Average Strength. This approach is tolerable if size and weight increases can be accepted or if a stronger material is available. This shifts the strength curve out to the right, increasing the strength-minus-stress gap.

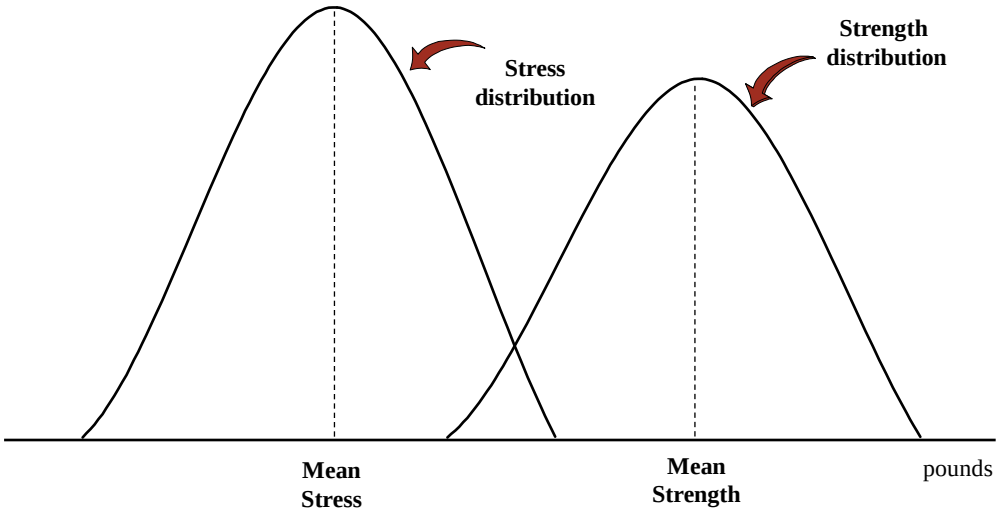
(2) Decrease Average Stress. Occasionally the average stress on a component can be reduced, by using more bolts, for example, each bolt bears less of the burden. This shifts the stress distribution curve to the left.

(3) Decrease Stress Variation. The variation in stress is usually hard to control. However, the stress distribution can be effectively truncated by putting limitations on use conditions by the use of governors, for example. This is portrayed by "pinching" the stress distribution curve.

(4) Decrease Strength Variation. The inherent part-to-part variation in strength can be reduced by improving the basic process, holding tighter control over the process, or by utilizing tests to eliminate the less desirable parts. This is illustrated by pinching the strength distribution curve.

Derating

Component Strength vs. Stress



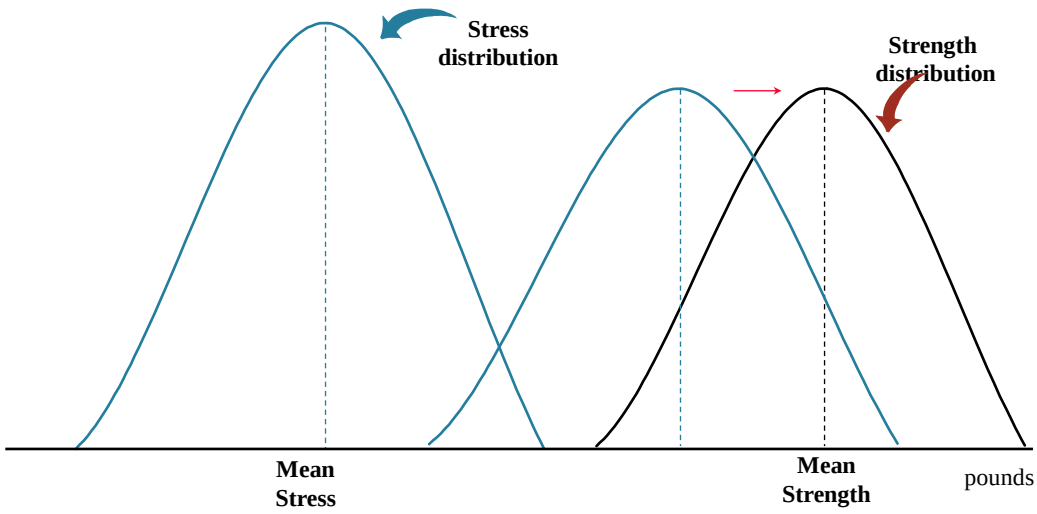
Distribution of stresses and component strength

Note: The overlap area above represents the amount of unreliability in this nominal situation.

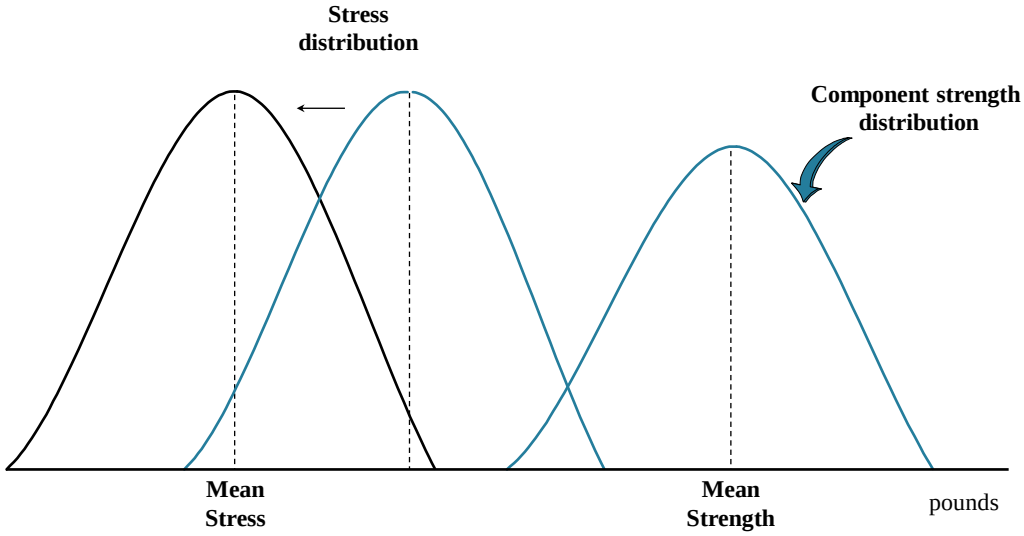
The following four graphs illustrate the four basic procedures discussed above.

Derating

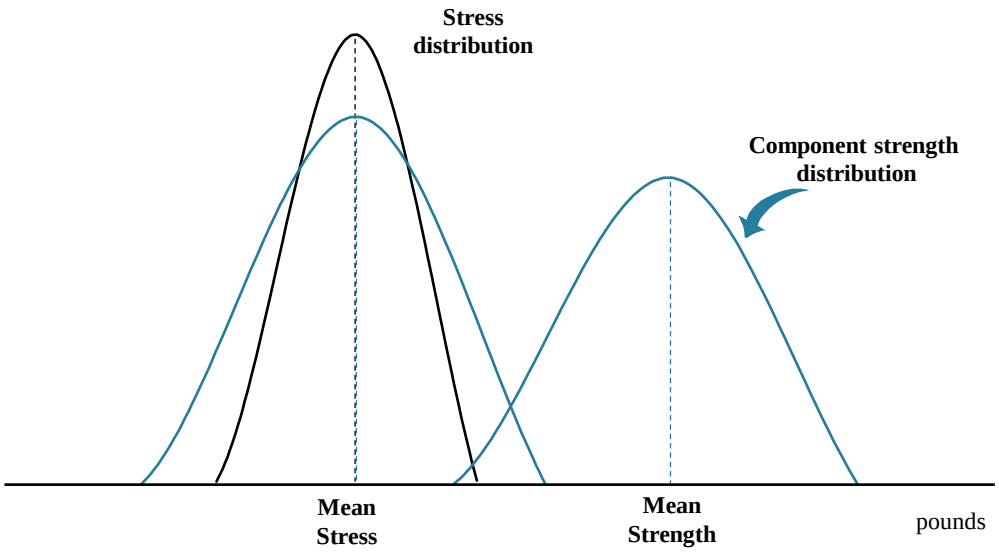
Component Strength vs. Stress



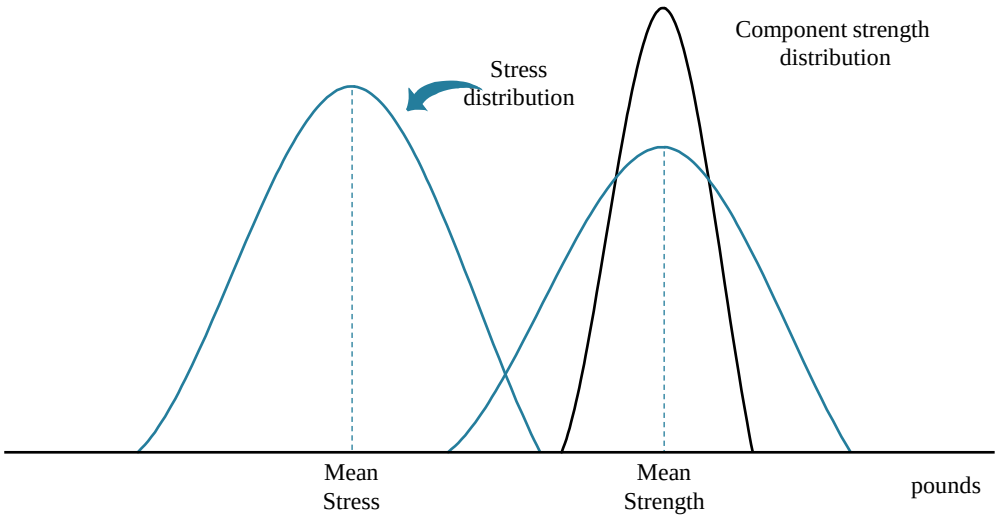
1. Increasing the average strength of components increases reliability



2. Decreasing the average stress on components increases reliability



3. Decreasing the stress variation on components increases reliability



4. Decreasing the strength variation on components increases reliability

Thermal Design

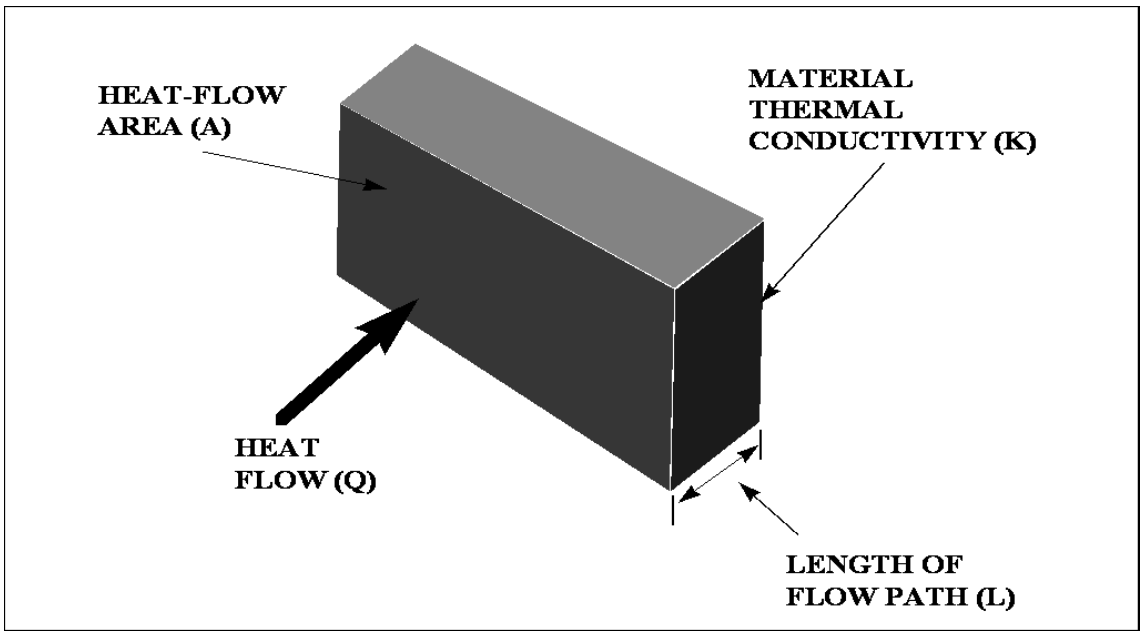
Heat can cause product failure. All processes are less than 100% efficient and generate heat. Heat raises equipment-operating temperature, which generally reduces reliability. Designers need to select "stronger" parts or reduce temperatures.

Two basic methods for reducing temperature are to generate less heat by more efficient designs; and to move or transfer heat away from sensitive devices.

Several independent studies (Boeing, Collins, et al.) have shown that a one-degree Celsius drop in operating temperature reduces the failure rate of electronics by approximately 3%.

Cooling by Conduction

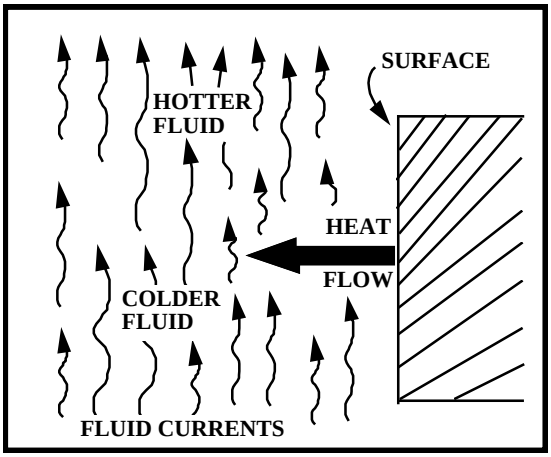
Some designs use heat sinks (solids) to conduct heat away from sensitive devices and to places where no harm will come.



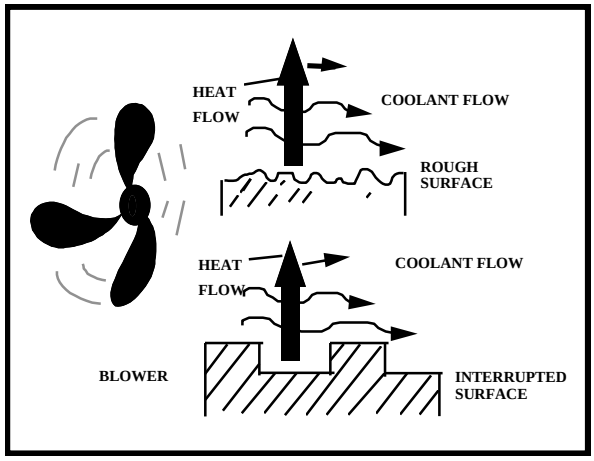
Cooling by Convection

Another cooling technique involves heat transfer through a fluid, such as a liquid or gas. This is called convection. When a fan is used to facilitate the heat transfer, we have forced convection. A good example is in the video projector used in the classroom.

FREE CONVECTION

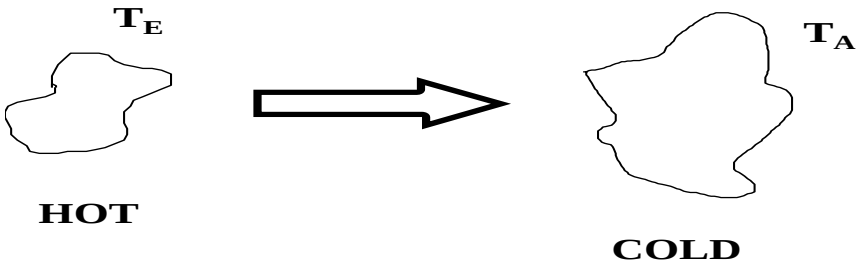


FORCED CONVECTION



Cooling by Radiation

Heat transfer from one body to another, even in a vacuum, may occur via radiation. This is not the dangerous kind of radiation. The rate of heat transfer is increased when the surface areas are large; there is a good view between the two bodies; and when the bodies have high emissivity properties.



Thermal Design for a Device

The aim is to provide enough cooling so the device's field failure rate won't surpass the maximum tolerable failure rate. How do the engineers achieve this? First, they determine how hot the device is likely to get in its operational environment without cooling, say, 100°C. Then they determine how hot they can allow the device to get before its failure rate would exceed the maximum tolerable failure rate, say, 40°C. Then they design-in enough cooling so that the device's temperature won't exceed 40°C.

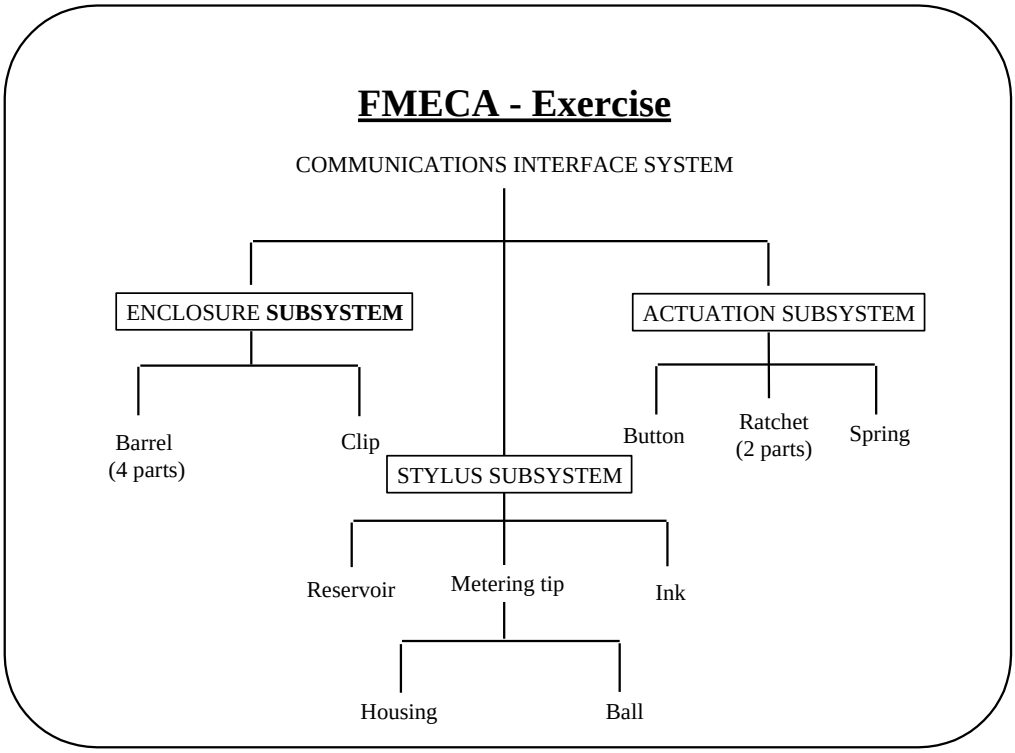
Failure Modes, Effects and Criticality Analysis (FMECA)

Here is a definition of FMECA from MIL-HDBK-338B, 1 October 1998: "A procedure for analyzing each potential failure mode in a product to determine the results or effects thereof on the product. When the analysis is extended to classify each potential failure mode according to its severity and probability of occurrence it is called a Failure Modes, Effects, and Criticality Analysis (FMECA)." Since a FMECA identifies the different ways an item can fail, it leads to the development of the required corrective maintenance capabilities.

The Society of Automotive Engineers (SAE) standard, SAE ARP-5580 Recommended Failure Modes and Effects Analysis (FMECA) Practices for Non-Automobile Applications effectively replaced the government's FMECA military standard, MIL-STD-1629A.

The overall purpose of a FMECA is to develop a safer and more reliable initial design. To achieve this, the designer analyzes the parts (bottom-up) from a potential physics of failure viewpoint. How can this component fail? What happens if it does fail? That is, what is the impact on the next higher assembly, and on the overall system? How critical would this failure be in the intended operating environment or mission? Interface and software failures should be considered also.

Associated with each possible failure is the likelihood of occurrence. Risk takes into account not only the effect of failure but also the probability. If the risk is deemed unacceptable, change the design, now. For example, change the layout, the parts, materials, or manufacturing processes. Ideally, make such changes before releasing the design to manufacturing. Along with these changes to the design it may be appropriate to add or change the preventive maintenance program (e.g., Reliability Centered Maintenance).



This diagram shows the components of the design for a "Communications Interface Device" or government ballpoint pen. Analyze a part from a "physics of failure" viewpoint and complete the table below.

Assigned Item: _____

Function of Assigned Item	Possible failure mode for assigned item	Effect of failure mode on assigned item	Effect of failure mode on next higher assembly	Effect of failure mode on Communications Interface Device

For example, the function of the "clip" may be "to attach the pen to a shirt pocket". The clip could fail from fatigue. It then would be unable to attach the pen to a shirt pocket. There would be minimal effect on the next higher assembly, the overall enclosure subsystem, such as possible cracking of the barrel. The major effect on the overall

system might be loss of the pen if it had been attached to the outside of a shirt pocket. Otherwise it should operate satisfactorily. The clip, then, would not appear to be a mission-critical part of the pen.

Below is a process FMEA for the Space Shuttle solid rocket motor. A process FMEA answers the question "What can go wrong in the manufacturing process that could lead to a problem in the field?" Although this process FMEA mentions o-rings, it is not applicable to the Challenger accident, which was due to operating outside the safe temperature range, not due to a manufacturing error. The right hand column lists steps that can prevent the errors.

FAILURE MODE EFFECTS ANALYSIS

Thiokol / WASATCH DIVISION

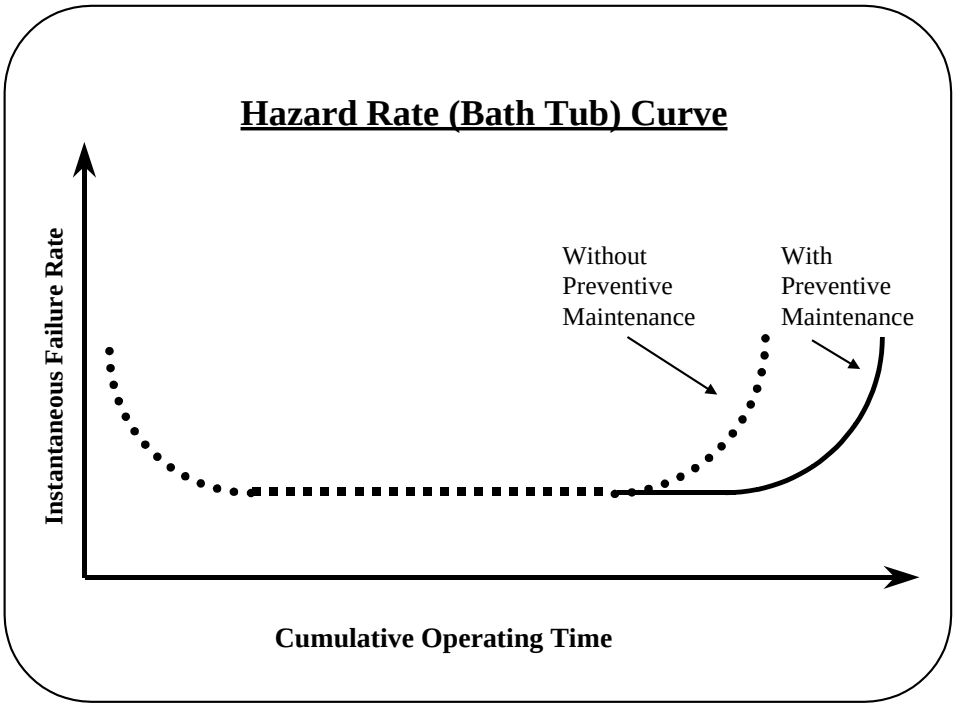
SYSTEM NAME	SUBSYSTEM NAME	COMPONENT NAME AND PART NO.	COMPONENT FUNCTION
Space Shuttle MP SRM 10-00	SRM Case 10-05	Case Assembly, Forward Segment 10-05-01 1U50147-08	
AUTHOR AND COMPANY	**DATE**	**REVISION**	
W. L. Hankins Thiokol Corporation	June 1983		

MISSION PHASE	COMPONENT FAILURE MODE AFFECTED COMPONENT PARTS REASONS FOR FAILURE	FAILURE EFFECT ON A. SUBSYSTEM FUNCTION B. SYSTEM FUNCTION C. MISSION D. VEHICLE AND PERSONNEL	CRITICALITY CATEGORY	CONTROL METHODS TO INSURE A RELIABLE PRODUCT
B	**ASSEMBLY JOINTS LEAK** **Part No** — **Part Name** — **Quantity Per Component** 1U50131-09 — Case Segment, Cylinder — 2 1U501473-01 — Case Segment, Forward — 1 1U50228-24 — Packing (O-rings) — 2/Joint 1U100269-01 — Test Plug — 1/Joint 1U50228-15 — Packing (Test Plug) — 1/plug 1. Tang-A-diameter exceeds upper limit or surface finish nonconforming, or is gouged or burred across both seal surfaces. 2. Clevis nonconforming (diameter, thickness, finish). 3. Clevis O-ring grooves exceed width and/or depth upper limits or corroded. 4. O-ring nonconforming or damaged during assembly. 5. Leak check plug loose or without O-ring, innermost seal ineffective per 1 above or the conditions of O-ring are per 4 above. 6. Foreign material in O-ring grooves. 7. Igniter flange nonconforming, flatness finish. 8. Case assembly joint rotation cases "lift-off" from secondary O-ring (primary O-ring will remain in compression). 9. Expansion of clevis gap because of residual strains resulting from manufacturing processes	A. High temperature gas flow will cause metal erosion and probable burnthrough and case burst. B. Catastrophic failure of SRM C. Mission loss. D. Vehicle and personnel loss.	1 (1) (1R) (1R) (1R) (1) (1R) (1R) (1R) (1R)	See CIL 1. Trained, qualified machinist to perform machining operation 2. Special profile template to control lathe cutting head. 3. 100% Inspection of tang diameter, clevis dimensions and O-ring grooves using Pl tape and standard measuring instruments. Surface finish sample inspected by surf-Indicator. 7. a. Trained, qualified machinist to perform machining operating. b. 100% Inspection of Igniter flange flatness by TIR readout finish is sample Inspected using surf-Indicator.

PAGE OF

Reliability Centered Maintenance Analysis (RCMA)

RCMA is an analysis aimed at determining the appropriate preventive maintenance tasks and intervals. The goal is to enjoy all the useful life that the design has to offer. Consider how long your "60,000 mile" tires would last if you never checked/adjusted the pressure or rotated them.
For a new product under development, the output of an FMECA may provide the input for an RCMA. For an in-service product, field data will generally be input for an RCMA.



Software R&M

Here is a formal definition of software reliability: "The probability of failure-free operation of a software component or system in a specified environment for a specified time." -C. R. Vick and C. V. Ramamoorthy, Handbook of Software Engineering, Van Nostrand Reinhold Co., Inc., NY, 1984.

Note, too, the following quote from MIL-HDBK-338: "An assumption that all software is completely reliable shall be stated in instances where software reliability is not incorporated into the item reliability prediction." This means that a system's software must be modeled in its reliability block diagram; otherwise, we're presuming it will never fail.

Software errors are incorporated during the requirements, design and coding process. Software errors lead to software failures in the field.

“Year 2000” Software Error

In some software, only the last 2 digits of the year were used in a calculation. This led to a problem in computing the duration of a time period. Example: If a product entered service in 1990, how many years would it have by 2002?

02 - 90 = -88 years!

The correct answer, of course, is 12 years. Which brings us to the notion that, while software may not “fail,”…

It may contain errors, which could be costly.

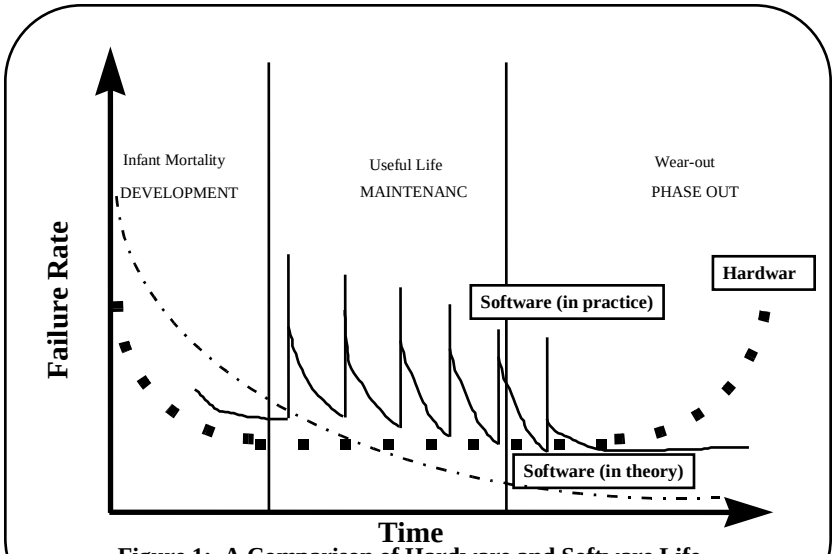


Figure 1: A Comparison of Hardware and Software Life Cycle Trends [Pressman, 1991]

Software Defects and Rework

Data and Analysis Center for Software, Sept 1996 reported: Software released with 15% of defects remaining. Companies spend 30-44% of their resources on software rework.

Software R&M Tools

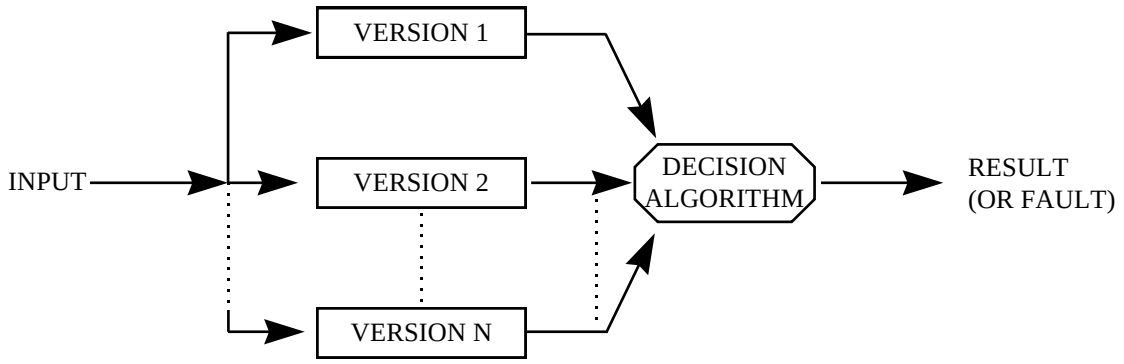
1. Good identification of requirements. Often the software developers are changing a moving requirements target, or the requirements change after development. Several studies have shown the requirements process is the biggest reason for software failures.
2. Modular design. By keeping the lines of code for a particular function packaged together, there is less chance of making a software error, and less difficulty in trouble-shooting one that might occur.
3. Use of higher order languages (HOL). HOLs like C++ and Ada are more English-like than assembler language or machine language. Hence, software developers are less likely to make a mistake writing in HOLs.
4. Re-usable software: like pre-packaged, debugged software packages. Like buying a car with a proven engine, re-usable software has less of the "unknown" quality.
5. Use of a single language. Using multiple languages requires a means of translating, converting, or otherwise communicating amongst them. Such translation is a possible source of error. That's why using a single language should provide better software reliability. However, there may be overriding reasons to use several languages, such as the fact that one language may be more suitable for a computation, while another might be better for word processing.
6. Fault tolerance. This is the ability to withstand a fault without having an operational failure. It may be achieved by active or inactive redundancy.

   An example of software fault tolerance is through N-version (or multi-version) Programming. Multiple versions of software are developed and deployed. The input (see figure below) gets exercised by all n versions. All n outputs pass through a decision algorithm, which determines the best output. Only if all n versions have a common error should this method fail. N-Version Programming utilizes active redundancy and can be very expensive.

   Another means of achieving fault tolerance is with Recovery Blocks (see Figure below). If the primary program's output fails an acceptance test, the input gets exercised by a standby or recovery program.

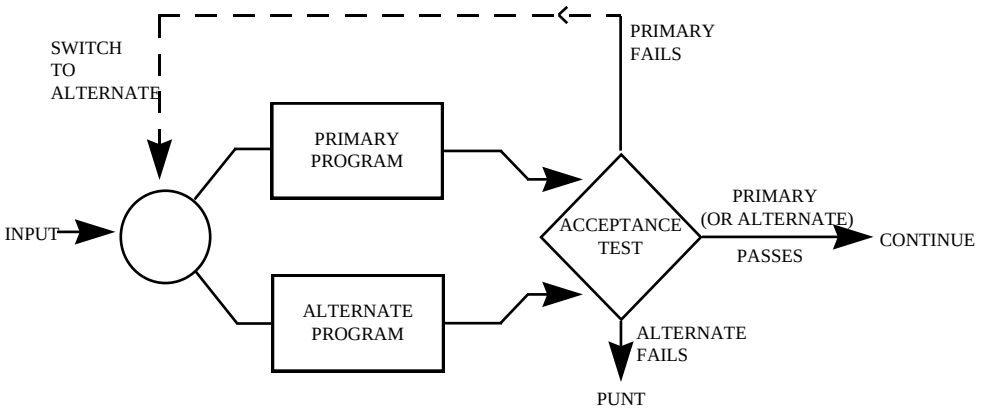
7. FMEA. If a system includes software, then the FMEA should recognize software as a possible failure point. To neglect the software is to assume it will be error-free.
8. Review and verification via second team. This allows a second independent team to look at the software before it is released.
9. Functional testing - “debugging” the software. The software can be checked on a simulator before it is released. This can save time, money, and missions and safety are not jeopardized.
10. Good documentation will facilitate software maintenance. Good documentation will make it easier to trouble-shoot or upgrade software.

A SOFTWARE FAULT TOLERANCE TECHNIQUE: N-VERSION PROGRAMMING



- 2 OR MORE VERSIONS OF SAME SOFTWARE WRITTEN BY DIFFERENT TEAMS OR ORGANIZATIONS
- DECISION ALGORITHM DECIDES WHICH OUTPUT(S) TO USE
- ANALOGOUS TO ACTIVE REDUNDANCY FOR HARDWARE
- MAY NOT PROTECT AGAINST COMMON ERRORS

A SOFTWARE FAULT TOLERANCE TECHNIQUE: RECOVERY BLOCKS



- INDEPENDENT PRIMARY AND ALTERNATE VERSIONS OF SAME PROGRAM OR “BLOCK” WRITTEN
- IF PRIMARY PROGRAM FAILS ACCEPTANCE TEST, ALTERNATE PROGRAM IS EXECUTED
- ANALOGOUS TO PASSIVE REDUNDANCY FOR HARDWARE

GAO Summary of DoD Programs With S/W Problems

1. Management
   - Lack of management attention/oversight 7
   - Lack of adequate S/W management concepts, methods, practices 6
   - Lack of adequate planning 4
   - Development proceeded despite serious problems 7

2. Requirements Definition
   - Lack of well defined requirements 10
   - Requirements change to meet new missions 4
   - Lack of overall system perspective 5
   - System not readily able to adapt to change 4
   - S/W cannot/may not meet security requirements

3. Testing
   - Lack of adequate testing methods and approaches 8
   - Lack of system level integration testing 5

GAO/IMTEC-93-13 Software Challenges in Mission-Critical DOD Systems

This study revealed the largest number of software problems was traced to the lack of well-defined requirements. In this Chapter we discussed the concept of software errors, software failures and what can be done to prevent software errors and to facilitate the software change process.

The Purpose of Reliability Prediction: Overview

Why predict reliability or maintainability characteristics periodically during the design and development phases (PDRR and EMD)? Predictions can enable the contractor or the government to evaluate the feasibility of their design with regard to its reliability goal. Predictions can be used to compare competing designs. And the predictions provide inputs to design and support activities (e.g. FMECA, maintainability analysis, provisioning, transportation).

We will look at the following prediction methods: Comparative analysis, Parts Count, Stress Analysis, and Translators.

Reliability Prediction Using Comparability Analysis

This is most useful when there's not enough data for a more sophisticated prediction model. This method was used for the Advanced Tactical Fighter's Concept Exploration Phase in the 1982-83 time frame. In particular to predict ATF Flight Control mechanical components' MTBM-Inherent, the program office applied the following steps:

Step 1: Choose a comparable system: F-16 Assess multiplier in mechanical reliability since F-16 design:	1.1
Step 2: Extract field data from F-16: F-16 MTBM-Inherent	105 hours
Step 3: Multiply. Predicted MTBM-inherent = (1.1) (105) =	116 hours

The multiplier in Step 1 represented the engineers' judgment of how much the MTBF of mechanical equipment in general had improved from the time frame when the baseline system (F-16) was developed to the time-frame when the ATF would be developed. In other words, the multiplier expresses how much improvement occurred in the science of mechanical reliability.

The Step 2 MTBM-inherent value is a reflection of the maintenance data analysis for the F-16. The Step 3 prediction is simply the product of the Step 1 and Step 2 values. Clearly, the goodness of the prediction is largely dependent on the goodness of the multiplier and the field data.

Reliability Prediction Using Parts Count

This method is useful when the design is still soft. MIL HDBK 217F "Reliability Prediction of Electronic Equipment" is often used for this prediction. The input consists of a list of parts, their failure rates under a nominal stress, and their quantities. The following table shows how to combine these values to predict MTBF.

Example

Component Part	**Quantity of Parts**	**λ/part**	**Quantity X λ**
Part A	10	.000001	.00001
Part B	15	.000002	.00003
Part C	15	.000004	.00006
MTBF = 1/.0001 = 10,000 hours			$\sum$ = .0001

Reliability Prediction Using Stress Analysis

This method is useful when the design is rather firm and the stresses are understood. It requires a list of parts, their quantities, their failure rates under nominal stress, and, very importantly, the anticipated operational environmental stresses.
Failure rates for a hypothetical board as predicted by various failure rate models (Source: 1986 RAMS Proceedings, page 162.):

FAILURE RATE PREDICTION MODEL	
RPP	Bell Communications Research
217D	MIL-HDBK-217D (New "F" version is out)
BT	British Telecom
CNET	French National d'Etudes des Télécommunications
NTT	Nippon Telegraph and Telephone
"A"	Supplier unique model
(Under "Pkg." H = Hermetic, NH = Nonhermetic)	

Stress environment was specified as: 40 degrees Centigrade ambient, ground benign environment, quality factor approximately MIL-HDBK-217D, D-1.

Variations Among Failure Rate Prediction Models (per Million hrs.)

Device	Pkg	Qty.	RPP	217D	BT	CNET	NTT	"A"
NMOS Digital:								
15 gates	H	8	120	216	200	216	56	
1750 gates	H	2	420	694	150	1,094	328	
15 gates	NH	12	288	2,592	300	324	132	
1750 gates	NH	1	350	5,135	75	569	263	
Bipolar Digital:								
400 gates	H	2	120	316	100	398	134	
88 gates	NH	4	120	1,592	20	276	108	
NMOS DRAM:								
64K bits	NH	6	3,300	363,468	60	3,246	3,252	4,824
CMOS SRAM:								
4K bits	NH	3	1,530	33,642	30	2,835	543	1,104
64K bits	H	1	2,050	7,863	25	3,065	1,002	2,030
Bipolar RAM:								
16K	NH	4	2,920	126,852	188	2,628	2,660	3,808
CMOS ROM:								
512 bits	NH	2	180	2,632	10	394	118	112
NMOS EEPROM:								
64K	NH	1	660	163,266	10	705	947	
Linear:								
24 trans	NH	4	144	4,408	60	236	100	
250 trans.	H	2	300	3,108	30	728	124	
TOTAL:			12,502	715,784	1,258	16,714	9,525	14,070

MIL-HDBK-217D agreed with several other models in identifying the "bad actor" (highest failure rate device) as the NMOS DRAM 64K Bits. However, we see that MIL-HDBK-217D's failure rate prediction is two orders of magnitude greater than that of several other models. One of MIL-HDBK-217D's major weaknesses is that its failure rate prediction value is not a good predictor of actual field reliability. However, a major strength is that it is useful for relative comparisons, for, say, comparing one design against another.

Using "Translators" to Predict Field Reliability for a Black Box from Contractual Test Data

Problem: Near the end of EMD the developmental test data for a black box (e.g. 4000 operating hours resulting in 4 "failures," as defined in the contract specification) lead to an estimate of 1000 operating hours between failures (MTBF). But the user is more interested in a prediction of mean flying hours between removals (MFHBR).

Task: What Field Reliability (MFHBR) can we Predict?

There are two "disconnects" between the test data evaluation and what the user wants. We need to change life units from operating hours to flying hours. We also need to change "events" from failures as defined in the contract specification to removals in the field.

Approach: Use "translators" based on historical data for this type of black box:

Translator 1 (Converting operating hours to flying hours): On average, 1 out of every 2 operating hours is a flying hour.

So, 1000 (OH) / "failure" = 500 (FH) / "failure". This translator has solved the life units disconnect.

Translator 2 (Converting "failures" to "removal"): On average, 1 out of every 4 removals is for a "failure."

So, 500 FH/ "failure" = 500 FH/ 4 removals = 125 FH/Removal. This translator has solved the "events" problem. We now have the "MTB" which the user wants, MFHBR.

That is, MFHBR = 125 hours

Reliability Prediction - Summary

In this section we showed some of the reasons for predicting reliability. We also illustrated four methods for predicting reliability: Comparability analysis, Parts count, Stress Analysis and Translators. Each of this represents a model. But remember this quote from industrial statistician George Box "All models are wrong, but some are useful" and the following quote from Paul Gottfried, RAC Journal, Vol. 2, No. 1, pg. 13:

> "There is no universal [prediction] model; all models are flawed; and there is no substitute for the application of intelligence and engineering judgment, on a case-by-case basis, to the problems of reliability modeling [for prediction]."

Reliability-Critical Items Analysis

The purpose of this analysis is to identify and control the design and manufacturing (e.g. by detailed analysis growth, reliability qualification test, and statistical process control) of reliability critical items. Criticality is addressed from the perspectives of safety, mission, and cost.

Storage, Shelf-Life, Packaging, Transportation, and Handling Analysis

There is the possibility of degradation in reliability due to shipping from factory to operational site, storage as spares, and during return to supplier or depot for repair. An example of storage problems is that a propane gas grill that sits outdoors for an extended period may have the venture clogged up due to spiders or other insects.

Sneak Circuit Analysis

As discussed in a Rome Laboratory technical report, sneak circuits (also referred to as latent circuit paths) are electrical paths that can cause unwanted functions to occur or inhibit desired functions from occurring. No component failure is assumed to have taken place.

Adverse circuit conditions that can give rise to sneak circuits are mostly a result of external asynchronous inputs uncontrollable and often unforeseeable by the circuit designer. For example, the end-user may unexpectedly operate two switches simultaneously or out of sequence, a condition which the circuit designer may have never envisioned during the design phase. Another example might be the unexpected loss of one several power sources in a circuit, possibly giving rise to unintended electrical paths.

A realistic example may portray the problem at hand more clearly. Figure 1 shows a simple aircraft circuit used to control the landing gear and the cargo door.

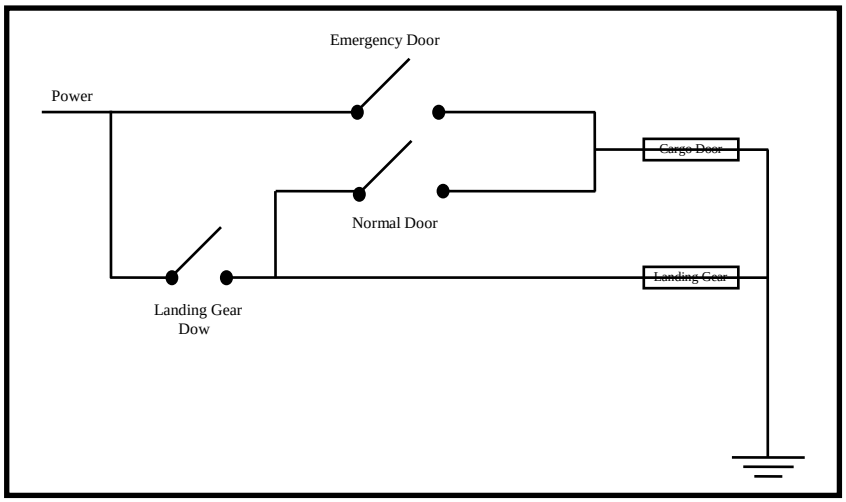


Figure 1: Sample Schematic

Under normal operating conditions the landing gear is lowered or raised depending on the position of the "Landing Gear Down" switch. The cargo door can be normally opened only if the gear has been lowered and the "Normal Door Open" switch is closed (see Figure 2). In emergency situations, the cargo door can alternatively be opened by closing the "Emergency Door Open" switch, irrespective of the state of the landing gear or the "Normal Door Open" switch. (See Figure 3).

Now imagine the following scenario:

> *Let's assume the pilot and airplane are currently in mid-flight, and a situation occurs requiring the pilot to open the cargo door. The circuit designer*

expects the pilot to now turn on the "Emergency Door Open" switch to force the cargo door to open.

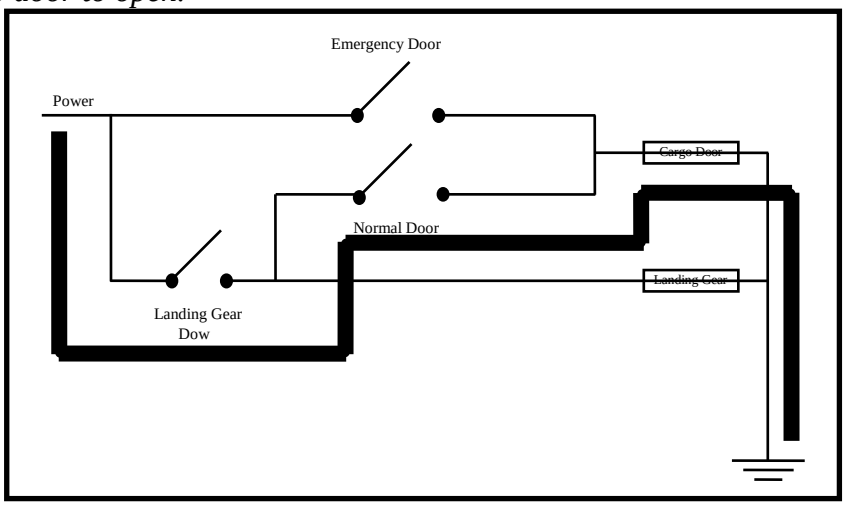


Figure 2: Normal Door Open

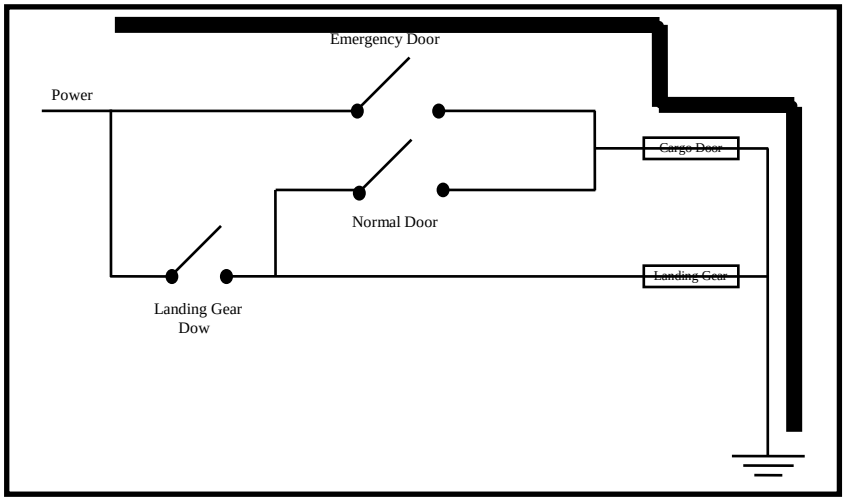


Figure 3: Emergency Door Open

Let's assume, however, that the pilot first attempts to open the cargo door using the "Normal Door Open" switch. This will not work, of course, due to the raised landing gear since the airplane is currently in flight. Upon realizing that closing the "Normal Door Open" switch did not achieve the desired result, the pilot now closes the "Emergency Door Open" switch without first disengaging the "Normal Door Open" switch. The cargo door opens as expected. However, both cargo door activation switches are now closed in mid-flight with the landing gear raised, giving rise to a sneak circuit (see Figure 4). The result of this sneak circuit is that, in addition to the cargo door opening, the landing gear will now be lowered during flight causing excessive drag, decreased maneuverability of the aircraft and possible damage to the landing gear if the horizontal airspeed is sufficiently high. Once identified, the problem can be solved quite easily by adding a diode after the "Normal Door Open" switch.

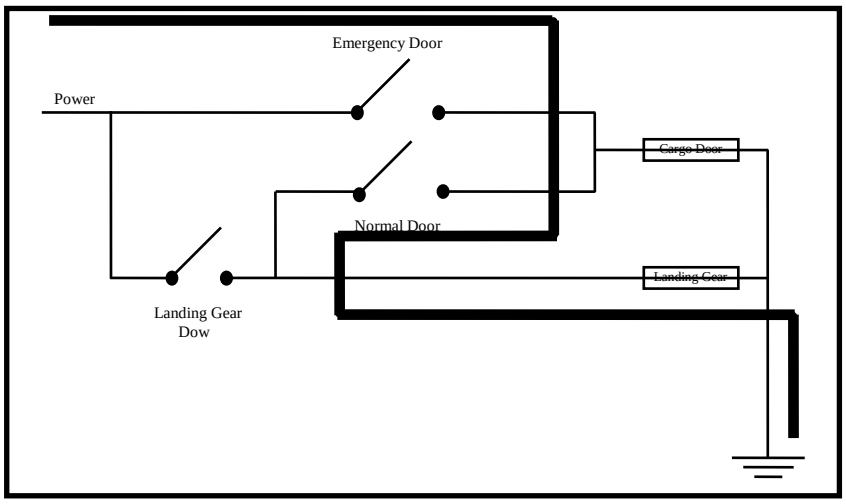


Figure 4: Identified Sneak

Failure Reporting, Analysis, and Corrective-Action System (FRACAS)

A FRACAS is a feedback and corrective-action loop. It is a method for reporting failures, analyzing the causes of failures, and recommending corrective action. It also identifies "bad actors" for maintenance.

Summary Chapter 4, Providing Insight into Designing for Reliability

This chapter was aimed at providing the acquisition logistician with insight into the traditional reliability design activities of logistics engineering. Now the logistician is better prepared to interface with the program office's systems engineer with regard to designing for reliability.

Chapter 5: Providing Insight into Designing for Maintainability

The aim of this chapter is to assure that while you are reviewing a company's proposal you consider all the activities that might result in a reliable product. Specifically, you will learn about designing for good diagnostics and human factors. We will discuss the relationship between maintenance and maintainability; the types of diagnostics errors and their associated effects; how human factors affect maintainability; the differences among MDT, MCMT, and MTTR; some basic maintainability measures; why the maintainability of a system depends on the reliability and maintainability of its subsystems.

Maintainability:

Recall that maintainability is the ability of an item to be **retained** in or **restored** to specified condition when **maintenance** is performed by personnel having specified **skill levels**, using prescribed **procedures** and **resources,** at each prescribed **level of maintenance** and repair. Briefly, then, maintainability is the "rapid diagnosis and removal of faults."

Maintenance vs. Maintainability

Maintenance is concerned with those actions taken by a system user to retain an existing system in, or restore it to, an operable condition. Maintainability is concerned with those actions taken by the system designer during development, to incorporate those design features which will enhance ease of maintenance. It is important to understand that good tech manuals can increase actual maintenance efficiency, but not MTTR.

An analogy is that maintainability is to maintenance as quality control is to quality assurance. Maintainability is putting the quality (ease of maintenance) into the product; maintenance data is the "proof of the pudding" that reveals just how well the maintainability engineer did.

Recall, also, that there are two major areas of concern in maintainability, diagnostics and human factors. These will be discussed in more detail below.

Diagnostics Systems - Operational Needs

Today, mission success is dependent upon total system: hardware, operator, software, etc. Unfortunately, hardware and software do not always perform as advertised. And, operators must make mission-critical or safety-critical decisions based on performance characteristics of the weapon system. However, many of a weapon system's performance characteristics can not be observed directly by the operator. A solution is to incorporate a diagnostics system. However, as the DoD becomes more dependent on diagnostics, it becomes less dependent on the need for highly trained (expensive) maintainers and so the demand for maintainers decreases. This means the diagnostics must work! When they don't, we are in trouble. That is why diagnostics are a big concern to the DoD.

Diagnostics Systems - Functions

Let's consider the functions of diagnostics and examine them in light of say, the oil pressure indicator on a car. First, diagnostics monitor the status of equipment: the pressure of the oil flowing through the engine. Diagnostics detect and/or verify faults, anomalies, and malfunctions; this would be a too-low or too-high pressure. The diagnostics report the status to operators or to automatic reconfiguration systems as appropriate; via a red light on the dashboard of your car.

Some diagnostics can identify what has malfunctioned, i.e., the nature of the malfunction, whether it is a hard fail or a degradation; and help the operator and/or the automatic reconfiguration system assess impacts and compensate if possible; however, the engine oil pressure indicator system in cars today doesn't go quite this far. The same diagnostics that helps the operator can also be used by maintenance to confirm malfunctions reported via the operator, the integral fault reporting system, or by other maintenance personnel.

Additionally, some diagnostics also isolate malfunctions to a level at which corrective maintenance can be effective (that is, they find the faulty item) and efficient (requiring only a minimum amount of time and manpower); again, the oil pressure indicator system doesn't go this far; it can't say the cause is a loose fitting oil filter, for example. Diagnostics are used to verify effectiveness of corrective actions; the maintainer uses the oil pressure indicator after taking corrective action, as a means of assuring the action was successful.

Automated Diagnostics Systems

The increased complexity of systems and the reduction in maintenance manpower requires the automation of the fault detection, reporting, and isolation processes. Built-in-test (BIT) equipment (BITE) is replacing direct observation. Basically, BIT is any of several methods of performing fault detection and/or fault isolation using automated test equipment that is an integral part of the end item. BIT may be applied at the part (e.g., microcircuit), card, unit, or system level.

Diagnostics Problems and Solutions - Overview

Problems with current diagnostics in electronics systems include the fact that they often provide inadequate fault detection and fault isolation capabilities. Also, manual diagnostics are slow.

There is an ongoing effort to improve diagnostics capability. One such effort is designing for testability, which will be discussed below.

Problems with Diagnostics Systems - Definitions

Some of the classical problems with diagnostics are BIT false alarms, Cannot Duplicates (CND), Bench Check Serviceable (BCS) and Re-test OK (RTOK). A BIT false alarm is a BIT indication of a malfunction that is not accompanied by observable system malfunction or degradation, and in the opinion of the operator, does not require maintenance. False alarms may be due to BIT malfunctions, but they may also result from the circuit sensitivity, operational environment, operator error or actual malfunctions such as intermittent connections. False alarms are usually **not documented.**

Cannot duplicate (CND): an on-equipment malfunction, generally reported by the operator that cannot be confirmed via **on-equipment maintenance**. The reported CND maintenance action may be the result of a BIT "error," intermittent operation, operator error/ inexperience, etc. CNDs are sometimes referred to as A-799s or as NEOFs (no evidence of failure).

The Organizational level to Depot level maintenance concept (O to D) is being utilized more and more on our aircraft as predicted reliability rates increase for weapons systems (and LRUs and WRAs). This puts more emphasis on our ability to accurately identify a failure at the O-level of maintenance. The Services currently use Built-in-Test to accomplish this task. One of the biggest problems is high CND rates. A CND occurs when a BIT causes us to remove a box that is ultimately found to be operating.

With no Intermediate level of maintenance capability we don't find out about the no-fault condition until the Depot tries to repair the item. The extended turn-around time to the Depot exacerbates the situation often causing the user to feel that we should have bought more spares to support them. The worst thing that has been happening is when the CND rate is very high, the user just starts ignoring the BIT.

In reality, the user may install the box on another aircraft and run a system check before they would send it to the Depot. What this means is that the quality of the BIT can greatly influence the number of spares you need and the number of maintenance actions you are taking to keep the aircraft up. As reported by one A-10 Aircraft R&M Report: "CNDs are very significant whether the apparent malfunction really exists or not. If the malfunction does not exist we waste personnel hours for nothing. On the other hand, if the problem really is there, we cannot identify and correct it. Frequent CNDs may indicate unreliable test equipment or deficient troubleshooting procedures."

BCS: is basically the same phenomenon as a CND except this label is generally used at the Intermediate level of maintenance. Similarly, RTOK is the preferred term at the depot level of maintenance. They can both be characterized as the event when an item is isolated as being the cause of a malfunction, is removed from the end item, and passes all subsequent testing at the next level of maintenance.

Effects of Diagnostics Reporting

The following table summarizes the effects of diagnostics. Note that in the upper left and lower right hand cells, the diagnostics is performing "as advertised." For example when the engine oil pressure is adequate, the red light is not coming on (upper left). When the pressure is too low (or too high) the red light is coming on to warn us (lower right). However, the other two cells show

how diagnostics can be misleading. Upper right: oil pressure is too low (or too high) but red light doesn't come on; so we keep on driving until a major problem occurs (overheating, engine seizing, etc.; this can lead to an expensive repair). The other possibility is the lower left cell: this occurs when the pressure is fine, but the red light comes on. The first time it happens we may stop and check it out. If we are convinced the pressure is OK (false alarm) we ignore it and future occurrences and will never benefit from the gauge when we really need it!

		Actual Condition of Equipment	
		GOOD	BAD
Reported Condition of Equipment	GOOD	No Maintenance Required	Undesirable or UNSAFE Condition
	BAD	**FALSE ALARMS** or **Unnecessary Corrective Maintenance**	Perform Necessary Maintenance

Impacts of Inadequate Diagnostics

Effects of inadequate diagnostics include adverse effects on safety, missions, schedules, and manpower. One DoD safety problem occurred when UH-60 Blackhawk pilots began ignoring fire detection indications (false alarms). In at least one situation there was a real fire onboard.

An example of a schedule impact was the postponement of a NASA launch due to a fuel flow meter indication. Upon analysis they found the fuel flow was fine, only the gauge was in error.

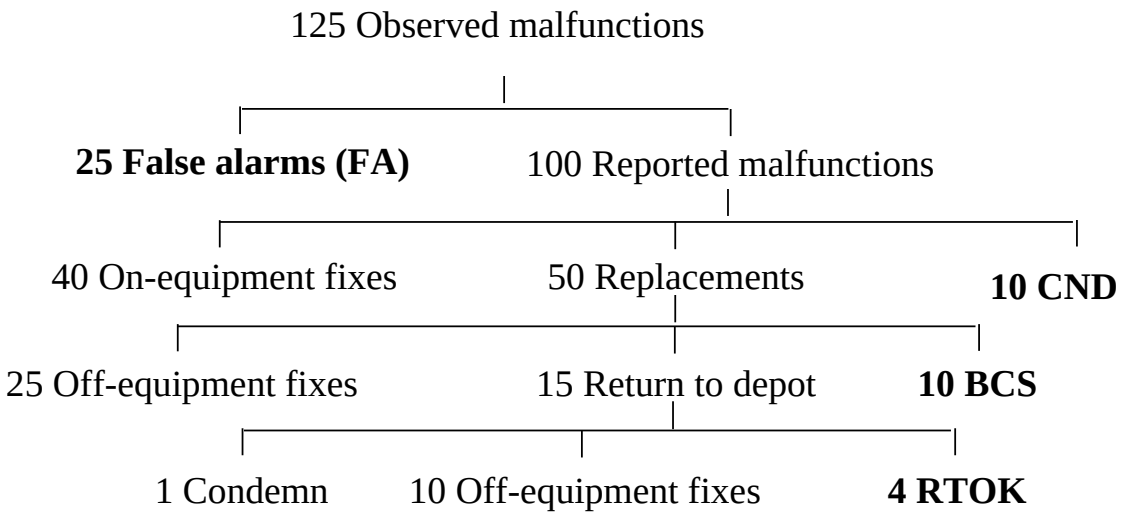
One mission-related problem occurred when the Air Force lost confidence in a turbofan engine low-pressure oil switch. They simply deactivated the switch (they had alternate means of detecting engine problems, however).

In general, manpower is wasted when CNDs, BCSs, RTOKs occur without any problems with the mission equipment. Also, the reliability of the mission equipment decreases with extra handling.

The following scenario shows typical effects that poor diagnostics have on logistics support. Efforts to solve a problem represent corrective maintenance actions, even if the problem is not actually fixed. On-equipment repairs may require only the use of a hand-tool, such as tightening a bolt with a wrench. Or a removal of a bad LRU or WRA (weapon replaceable assembly) and its replacement with a good like item may occur. Another possibility is the CND. Similar actions may occur at the intermediate or depot levels.

Exercise - Computing Diagnostics Effectiveness Terms

Assume that test results for 1000 hours of operation covering some 500 missions showed there were 125 total observed malfunctions broken down as shown below.



Now, compute the following diagnostics measures:

- False Alarm Rate $= \dfrac{\text{FAs}}{\text{Operating time}} = \underline{\qquad\qquad}$

- % Cannot Duplicate (CNDs)

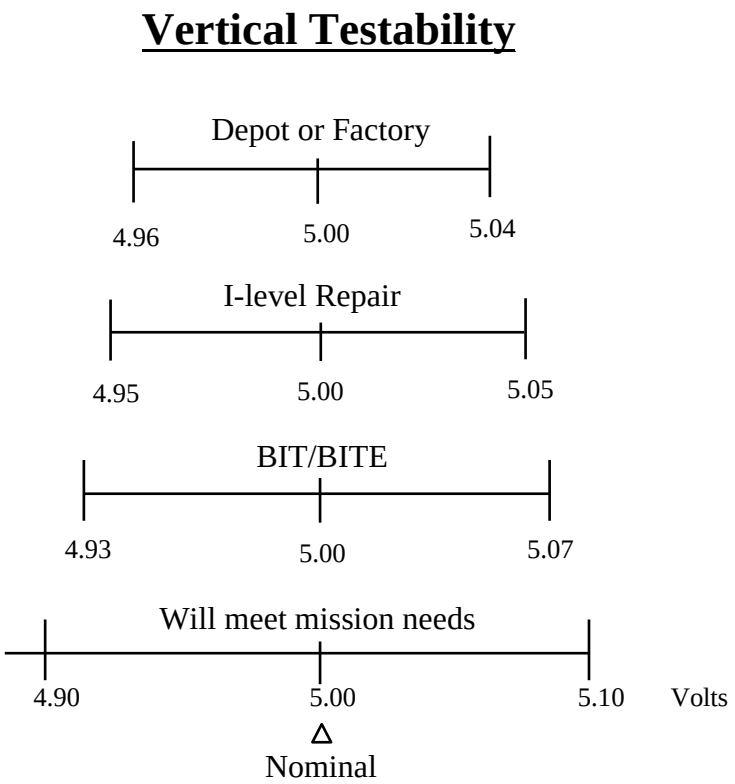
  $\% \text{ CNDs} = \dfrac{\text{Number of CNDs}}{\text{Total Number of corrective Maintenance Evensts}} = \underline{\qquad\qquad}$

- % Re-test OK (RTOK) or Bench Checked Serviceable (BCS)

  $= \dfrac{\text{RTOKs} + \text{BCSs}}{\text{All shop / depot actions}} = \underline{\qquad\qquad}$

Vertical Testability

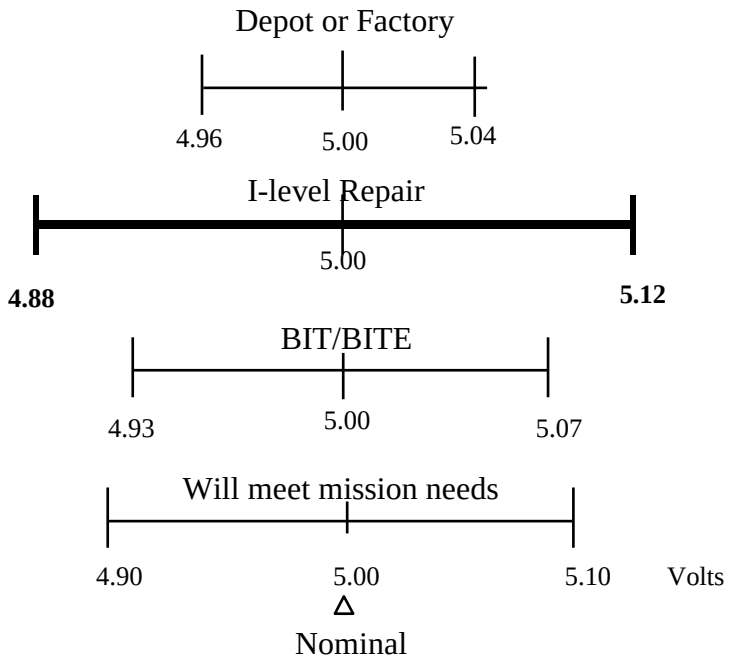
A means of limiting the occurrences of CNDs, BCSs, and RTOKs is the achievement of vertical testability. This means that the test equipments at the various levels of maintenance agree with one another. So, if the BIT indicates a problem with a box, the test equipments used by maintainers at the O-level, I-level and Depot level will also report the box is faulty. This can occur if there is a narrowing of the sensitivities of the test equipment as the maintenance progresses from O to I to depot levels, as shown by the "cone of tolerance" below.



Possible Reality Regarding Diagnostics:

Sometimes the cone of tolerance does not exist. Instead there is a hodgepodge of sensitivities as shown below. This will lead to a BCS if, for example, the actual voltage is slightly greater than the upper specification limit of 5.1 volts. Do you see why?

Possible Reality



Effective Diagnostics Systems - a Structured Approach

Vertical testability will only be achieved by design. In general, it will not occur spontaneously.

An effective diagnostics system requires program management's:

1. Understanding the operations concept - mission objectives, critical equipment, software
2. Determining the overall maintenance concept including the appropriate levels of maintenance, the mix of BIT and external test equipment, and training objectives.
3. Establishing a strategy for system diagnostics: the appropriate mix of gages and warning indicators; simple BIT/BITE; artificial intelligence; and external support equipment; troubleshooting and tech data.

Diagnostics Systems - Summary

In this section we discussed why diagnostics are used in DoD weapons systems, why diagnostics are a concern, the benefits of vertical testability and an approach for achieving it.

Maintainability - Human Factors

Human factors problems with current systems include accessibility (will the maintainer be able to see the work, reach it, and have enough strength to remove an item?); environments (nuclear, biological chemical warfare; arctic, tropics, etc.); fasteners (does the long screw or the short screw go into this hole?); and hand tools (if peculiar hand tools are provided, is there one available when I need it?).

One means of achieving better maintainability through human factors is by listening to the field! An example of a formal program to do just that was the Air Force Blue Two Program. Acquisition program office and contractor design personnel would visit an operational sight, observe maintenance, and then actually perform the maintenance themselves. The goal was to show them how difficult the tasks can be when maintainability wasn't carefully designed-in. The hope is that they would be more conscientious about it in the future. Many positive responses developed from the Blue Two Program.

Human Engineering

Human engineering or human systems integration (HSI) views users, operators and maintainers as "components" in the system. HSI seeks to optimally allocate functions to people and machines. HSI also involves determining how to present information to personnel; how to design controls (recognizing some learn best by reading, by pictures, by sound, by touch, etc.) HSI also involves, anthropometry, the fact that people come in different sizes, shapes, and with different strengths, etc.

Specifying and Measuring Operational and Contractual Maintainability Characteristics

MAINTENANCE "TIME" PERSPECTIVES

This section aims to distinguish between three maintainability-related terms, $\overline{M}$, MDT, and MTTR. Mean Down Time (MDT) has a maintenance management (and operations) perspective. One formal definition of MDT is "The average elapsed time [clock hours] between loss of mission capable (MC) status and restoration of the system to MC status." (Air Force Instruction 10-602). Mission capable status refers to the ability of a system to be available for use. A mission capable system is one that is either in **FMC** (fully mission capable) or **PMC** (partial mission capable) status.

$\overline{M}$ is the mean active maintenance time. It is a weighted average of corrective and preventive maintenance times. Recall that: MDT = $\overline{M}$ + ALDT. This means that MDT is a function of a product's maintainability as well as the Services' support of that product.

Mean Time to Repair (MTTR) has a contractor's design perspective. MTTR should be defined in each contract. Basically, it represents the time to perform those activities for which the contractor has design responsibility.

MTTR for a System

The aim of this section is twofold: to show that the maintainability of a complex system depends on both the reliability and maintainability of its subsystems; and to show that there may be a better way of contracting for R&M than to list separate reliability and maintainability requirements.

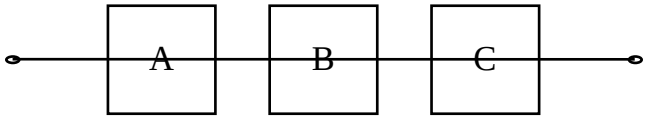
The value of MTTR for a single task is generally dependent only upon maintainability and maintenance characteristics. However, the MTTR for a set of different tasks for the same item or for a system of different items is also dependent upon one other factor.

Maintainability is most frequently quantified via terms that measure the "time" required performing a specific maintenance activity or group of activities. "Time" can be either in elapsed time (i.e. clock hours) or in man-hours (product of elapsed time and number of personnel). Times are frequently expressed either as means or averages.

Example: If a contract for designing and developing a pump calls for a Mean Time to Repair (MTTR), the demonstration may require "x" number of repairs, and specify that the estimate of MTTR would be made as follows:

$$\textbf{MTTR} = \frac{\textbf{Sum of elapsed times for x repairs}}{\textbf{x}}$$

Pump:



Assume that the initial design calls for the pump to consist of three subsystems, all mission-critical. And that their MTTRs are envisioned as follows:

Subsystem	Subsystem MTTR
A	7 clock hours
B	4 clock hours
C	1 clock hour

Then, the overall MTTR for the pump would appear to be:

(7 + 4 + 1) /3 = 12/3 = 4 hours. (What presumption exists here?)

What if the contract says the MTTR shall not exceed 3 hours? Is this design adequate?

What if the contract also has a reliability requirement that the pump's frequency of repair (failure rate) shall not exceed 20 fails/100 days and the initial design shows the

Subsystem	Failure rate
A	1/100 days
B	1/100 days
C	1/100 days

What is the system failure rate, per this design?

How is the contractor doing in the initial design with regard to the R&M requirements? Contractor is unacceptable with regard to maintainability (takes too long) but acceptable with regard to reliability (failure rate is below the maximum allowable). How might the contractor recover? One approach might be to simply use lower quality parts in the quick-fix subsystem, C. This would drive the MTTR downward, which is favorable. It would also drive the failure rate up, which is unfavorable, but may still be below the maximum allowable. The following table shows how this could happen.

Subsystem	Failure Rate	Number of Tasks (in 100 days)	Total Task Time (clock hours)		
A	1/100 days	1	1 task x 7 hours	=	7
B	1/100 days	1	1 task x 4 hours	=	4
C	1/20 days	5	5 task x 1 hour	=	5
Item		**7 tasks**	**Total clock hours**	**=**	**16**

So, the MTTR of the modified design would be = 16/7 = 2.3 clock hours, which meets the specification. The failure rate of the modified design = 7/100 days . . . which also meets the specification. So, what's wrong with this picture? Check to see that modified design gives a lower A_i than the initial design.

Has the contractor done anything illegal? Probably not. Anything unethical? Possibly. Has the government been a party to it? It would appear so. What could have prevented this situation? An alternative approach would be to contract for an "A_i" requirement (rather than for separate reliability and maintainability requirements) and to provide an incentive to maximize A_i.

Summary, Chapter 5: Designing For Maintainability

In this chapter we showed how maintainability and maintenance differ. We discussed the major areas of maintainability, namely, diagnostics and human factors. We distinguished among three maintainability-related terms. We showed that the MTTR for a system depends on the reliability and maintainability of its subsystems. Finally, we suggested an alternative approach for specifying reliability and maintainability requirements.

This page intentionally left blank

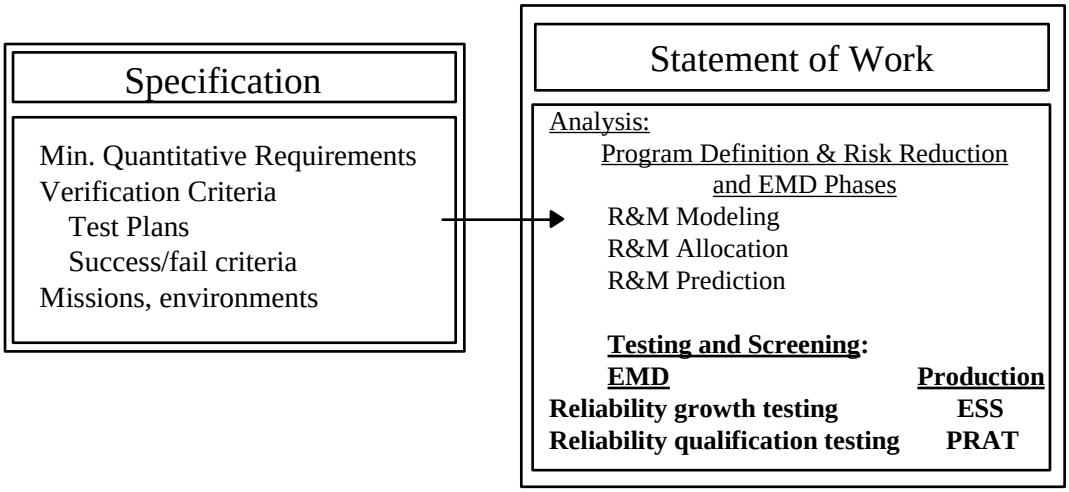
Chapter 6: R&M Risk Reduction

The aim of this chapter is to assure the acquisition logistician understands the purpose of various R&M test activities toward reducing the risk of accepting an unreliable product.

First, you will learn the Duane model for achieving reliability growth through a Test-Analyze-and-Fix (TAAF). Then, you will learn the concept of decision risk with regards to RQT and the purpose for employing a statistical test plan for an RQT.

R&M Measures of Effectiveness

Contractual (developmental) testing is aimed at assuring that the inherent characteristics identified and defined in the contract specification have been met. Operational testing is aimed at verifying that systems about to be fielded meet the requirements identified in the CDD. These types of tests occur as shown in the flow chart below.



Test and Evaluation of R&M: Overview

The DAG calls for RAM modeling and simulation, which are aimed at risk reduction. However, reliability testing and maintainability demonstration are still in widespread use. This chapter deals with reliability testing, focussing on two types: Reliability Growth Testing and Reliability Qualification Testing (which entails decision risk).

R&M testing in general poses certain challenges. There may be program constraints. Examples include: insufficient number of test articles or test time; the test environment may differ from the expected operational environment; the system may be incomplete

when testing begins, so that substitute subsystems may be called upon; and the system will likely be immature with regards to R&M.

Reliability Growth - a Perfecting Process

A formal definition of reliability growth is "The positive improvement in a reliability parameter over a period of time due to changes in product design or the manufacturing process," per MIL-HDBK-189.

The "TAAF" process for achieving reliability growth is an iterative method consisting of the following steps:

TEST: Stimulate equipment to malfunction
Capture and report associated facts

ANALYZE: Determine root cause of malfunction

And

FIX: Formulate corrective action
Verify effectiveness of fix
Incorporate corrective action

Example of a TAAF Program: Suppose the Army wants to motivate soldiers for physical training by introducing a new "gadget." - This may be a radio that can be programmed to give pulse rate, blood pressure and other physical characteristics that may vary during exercise; and to provide this data to the soldier audibly and visibly while, say, cycling on a stationary bike. The Program Manager, seeking to buy commercial, visits the local Radio Shack in search of such a device and is told it doesn't exist. But the friendly salesman tells him to return in a couple of weeks.

Two weeks later, the salesman has a bag full of parts, a list of assembly instructions, some solder, etc. The Program Manager returns to the work site, puts the radio together, and tries it out on a bike. After thirty minutes or so, it stops working. So he returns to Radio Shack, where the salesman takes it apart and determines that a certain electronic device would have worked better if it had been placed in a cooler corner of the circuit board (change #1 to the design). The PM returns to the office, implements this "fix" and resumes testing on the cycle. A few days later, however, the radio fails again. Back to Radio Shack. This time the salesman determines the cause was corrosion of a wire terminal, apparently due to the salt in perspiration; so he devises a "sweat shield" (Change #2). This process continues for, several months, until the PM is satisfied that the design is satisfactory from a reliability viewpoint. He then puts in an order for 5,000 radios. This was a TAAF process aimed at growing the reliability of a product.

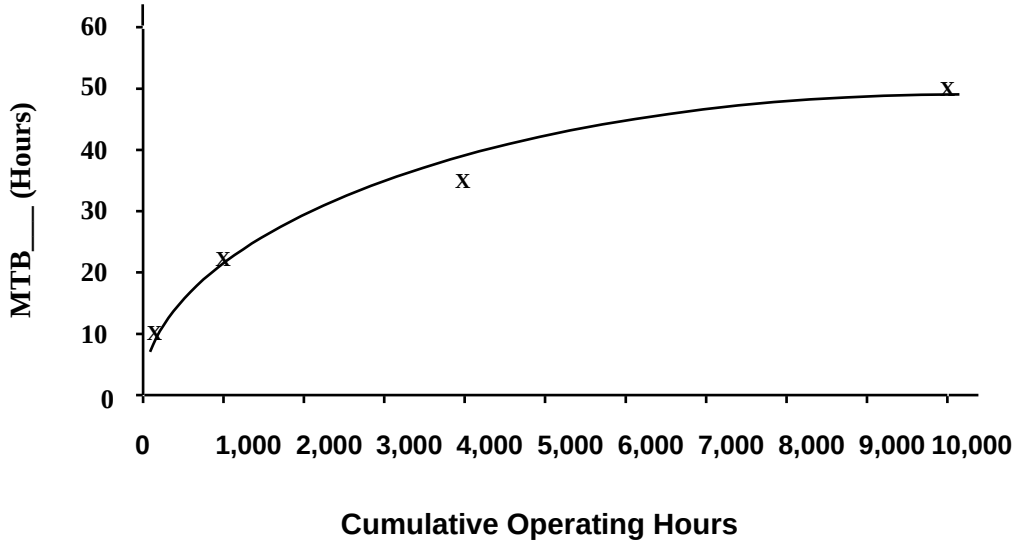
Example of Growth Data

Data from a growth program can be tracked. Although the following numbers are not realistic for the Radio Shack example, they are "easy-to-work-with" and informative. The four periods could represent, say, months of January through April. The data shows some 250 configuration changes and some 10,000 hours of testing! Notice how the reliability parameter, MTBF, has increased from month to month; this indicates positive growth. The use of Cumulative Operating Hours will be explained later.

Data for each period				CUM
Period	**Oper Hrs**	**Changes**	**MTBF**	**Oper Hrs**
1	100	10	10.0	100
2	900	40	22.5	1,000
3	3,000	83	36.1	4,000
4	6,000	117	51.3	10,000

Linear Plot of Reliability Growth

The monthly MTBFs are plotted against cumulative operating hours on linear scales below. Notice how the points seem to fall in a smooth curve that climbs rapidly then tapers off. This suggests the "low hanging fruit" (of improvement opportunities) was easy to find and correct early on but that diminishing returns set in afterwards.



Quantifying the TAAF Process - Duane Reliability Growth Model

One individual who was involved in reliability growth testing in the 1962 time frame was J.T. Duane, a General Electric employee. He recognized that reliability growth data resembled "learning curve" data, commonly found in manufacturing. Duane outlined a method for tracking (and also for planning) reliability growth programs. This method has become known as the Duane model and consists of the following steps.

Steps in the Duane Model for reliability growth:

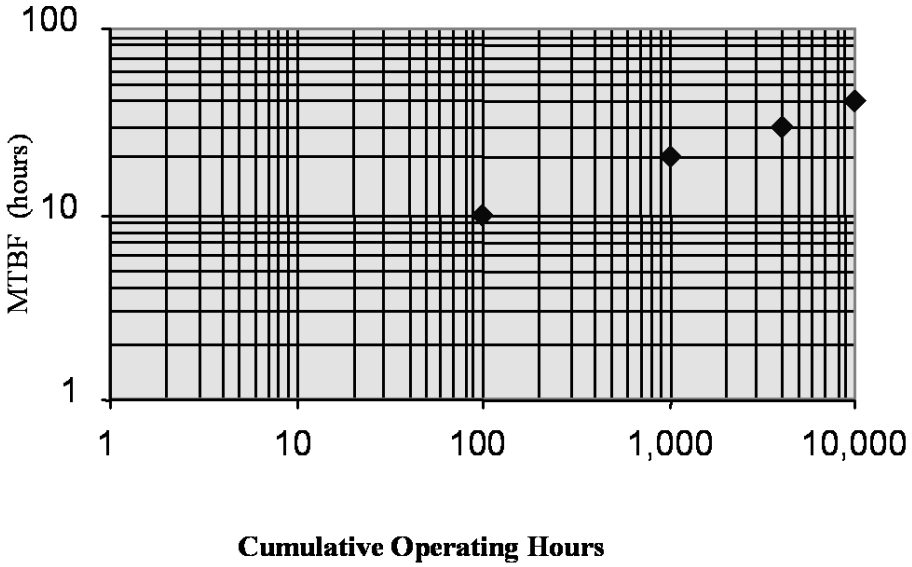
1. Plot cumulative data on log-log graph.
2. Construct the best-fit line.
3. Compute the slope of the line.
4. Estimate the current or instantaneous MTBF.
5. Project future values (optional).

The Duane model is in widespread use; it is generally applicable to mechanical, electrical or electronic equipment. It basically assumes the units under test are effectively in "useful life" (constant failure rate). Let's look at the Duane model steps more closely.

1. Calculate cumulative data: The following table is the same as that above except that two columns have been added at the right. The cumulative number of changes and the cumulative MTBF, a nebulous concept which will be explained later.

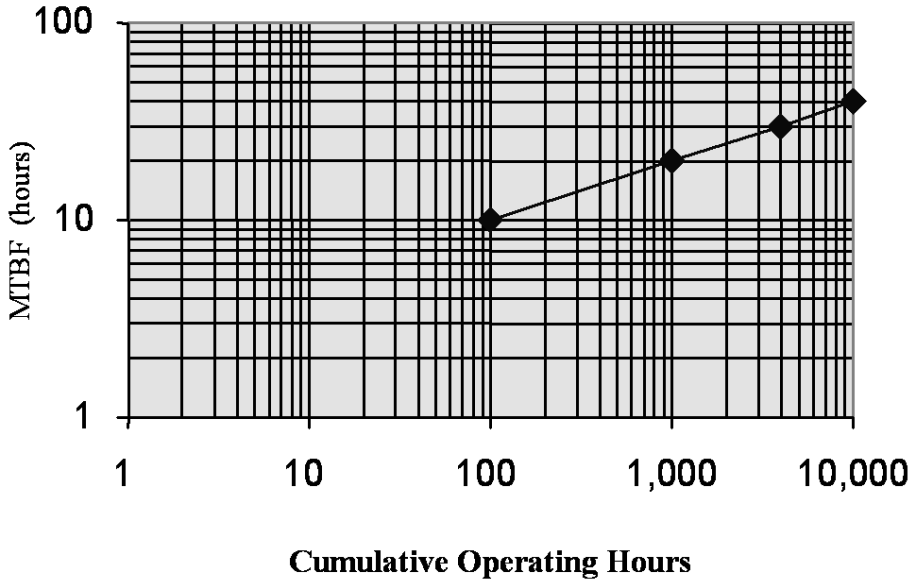
Data for each period				Cumulative Data		
Period	Op Hrs	Changes	MTBF	Op hrs	Changes	MTBF
1	100	10	10.0	100	10	10
2	900	40	22.5	1000	50	
3	3000	83	36.1	4000		
4	6000	117	51.3	10000		

Step 1: Plot Cumulative Data on Log-Log Graph



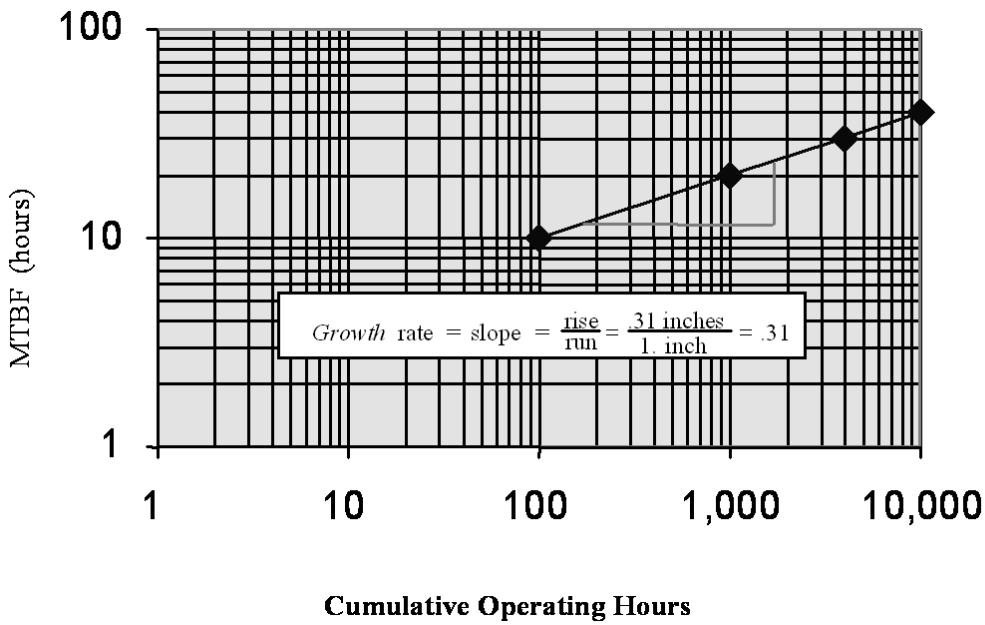
The second step is to construct the best straight line that fits the data. In this example, the four points fall on a straight line, so constructing the line is trivial. In real life, the data points will typically fall close to a straight line. Linear regression is used or "eyeball regression" may provide the needed accuracy.

Step 2: Construct Best-Fit Line



The third step is to compute the line's slope, i.e., the reliability growth rate. The steeper the slope the better, because a steep slope suggests a rapid rise in the reliability parameter, i.e., more "return" for the operating hour "investment"; more "bang for the buck."

Step 3: Compute slope of line



The fourth step is to estimate the MTBF of the latest (or current or instantaneous) configuration. This would be change number 250 in our example. Hopefully, it is also the best configuration. Duane's formula is based on learning curve theory, assuming a constant growth rate. In this example it provides the best guess of the MTBF for configuration number 250.

STEP 4: Estimate current or instantaneous MTBF

$$\text{Instantaneous MTBF} = \frac{\text{Cumulative MTBF}}{1-\text{slope}} = \frac{40}{1-.31} = \frac{40}{.69} = 58\,\text{hours}$$

Of what use is this prediction? Suppose the contract specification requires an MTBF of less than 58 hours, like 50 hours. The program manager might feel that enough growth testing has been done, and would proceed into a real test, a reliability qualification test (RQT) to verify that the specification has been met. If the specified value was much higher than 58 hours the PM might want to continue with the growth program.

Factors That Contribute to Rate of Growth

In general a high growth rate can be achieved if the specimens are tested in a severe environment (more rapid occurrence of failures) and there are high talent experts (metallurgists, physicists, chemists, etc.) available for the analysis. Both of these cost money.

		RELATIVE GROWTH RATES
RESOURCES		
Low cost	=	.3
Medium cost	=	.4
High cost	=	.5
SEVERITY OF ENVIRONMENT		
Benign (less severe than mission environment)	=	.2
Actual or simulated mission	=	.35
TAAF/stimulating (more severe than mission)	=	.5

Planning and Managing a Reliability Growth Program

Reliability growth programs should only be used when there is a significant amount of technical risk. Only then should we expect the contractor to have difficulty "getting it right the first time." In such a case it is wise to establish the reliability growth management plan early, such as in PDRR.

The growth rate is generally anticipated based on past experience. That is, companies that have had reliability growth programs before have a sense of how much investment is needed to achieve a particular growth rate, particularly with regard to similar equipment. Determine test time and associated test assets, chambers, equipment, etc.

One US Navy Program (at NAVAIR) which had unit production costs of approximately $9,000 - $10,000 for 300 production units planned a growth program for 24 units designated for TAAF. The total test time was estimated to require 72,000 hours.

Multiple units allowed the program to cheat "Father Time." After all, 72,000 hours is equivalent to many years of calendar time! Implicit here is the assumption of constant failure rate, a good assumption for a complex system.

To have a good growth program it is important to establish a good failure reporting, analysis, and corrective action (FRACAS) system. This should identify the type of events to be analyzed or tracked (for both hardware and software). It should assign responsibilities for corrective action, etc.; and it should set deadlines for completing failure analysis, corrective actions, etc.

In implementing a reliability growth program it is imperative to preclude the "fear of failures" attitude from the contractor. Instead, it should be treated as practice or spring training. The real test, RQT, will follow. So, don't use growth testing as a measure of achieved reliability. Don't censor data to reflect "projected" corrective action. Report the data "as is."

Duane vs. AMSAA (Army Materiel Systems Analysis Activity) Reliability Growth Models

Besides the Duane model, the AMSAA model is widely used in the DoD and industry for reliability growth. The AMSAA model is sometimes viewed as an improvement to the Duane model because it allows for a statistical treatment of the data, i.e., the development of confidence interval estimates for the MTBF. On the other hand, it is probabilistic not deterministic and hence is not as suitable for planning a growth program and is not as mathematically simple as the Duane model.

Reliability Qualification Testing (RQT)

RQT is needed to assess the ability of a product or system to meet the customer's requirement. Remember that R&M characteristics cannot be **measured** directly. There is no reliability tape or scale, only testing or actual use will reveal reliability.

Risk in the Decision-Making Process

In RQT, we must recognize that we may be misled by the data into making an erroneous decision. If the quality (reliability) is truly acceptable, but we unwittingly reject, we are making the only possible erroneous decision. Conversely, if the quality is unacceptable, the only erroneous decision is to accept. The probability of making an erroneous decision may be quantified.

Actual (but unknown) product population characteristic		
	Meets requirement	Does not meet requirement
Accept		
Reject		

The α (Alpha) error represents the probability of rejecting "good" product, i.e., product that meets or exceeds the contractor's design goal. The probability of making this error is known as the seller's, producer's, and contractor's risk. The contractor's design will be rejected if they fail the RQT test plan. Then the contractor has to correct problems and retest; or the program may be canceled, cut back, etc. The reject decision may affect schedule and/ or require additional funds.

The β (Beta) error represents the probability of accepting a bad product. The probability of making this error is known as the buyer's, consumer's, and government's risk. Contractor is happy - system passes! However, system will be fielded with less than required/desired reliability, resulting in additional costs to the buyer. These effects may not be observed for several years. It also represents a serious error to the logistics community because there will be more maintenance than anticipated.

<u>Decision Risk - an Example</u>

Situation: You are trying to estimate the annual budget requirement for an item that is removed and sent to the depot for repair. You have estimated the cost to remove and replace, package, transport, and repair at depot to be $500 per unit removed. You expect to operate the fleet of this system for 100,000 hours each year. You will use the translator: MTBR = .3 times MTBF. As the depot repair manager you are anxiously watching the RQT estimate of MTBF so you can apply it to your logistics model for depot repair budgeting.

Based on the required, predicted and test data, how much should you budget for the next year?

$$\text{Budget} = (\text{Expected \# of Repairs})\text{x}(\text{Cost per Repair}) = \left(\frac{\text{Expected operating time}}{\text{est. MTBR}}\right) \text{x (Cost per removal)}$$

$$= \frac{100{,}000 \text{ hours}}{\text{est. MTBR}} \text{ x \$500}$$

Assume the contract specification calls for a required MTBF of 1000 hours. And the contractor's predicted value (design goal) is 1500 hours MTBF.

Let's also assume the RQT Test Plan is:

$$\text{Total test hours} = (16 \text{ units})\text{x}(125 \text{ test hours each}) = 2000 \text{ test hours}$$

$$\text{Then, Your estimate of MTBF} = \frac{2000 \text{ hours}}{\#\text{failures}} \text{ and estimate of MTBR} = \frac{.3(2000 \text{ hours})}{\#\text{failures}}$$

Evaluating RQT Failure Data (2,000 Test Hours)

In a classroom demonstration each student plays the role of the PM, randomly pulling 16 chips from a bag containing 480 chips, some blue (good units) and the remainder red (bad units). You count the number of red chips and put all 16 chips back in the bag before passing the bag to the next PM. In real life, there would be only one PM and only one test. The reason for allowing everyone to be PM is to show how frequently a PM may be misled by test data into making the erroneous decision. Half the class samples from Contractor A and the other half from Contractor B.

# Failure (Red Chips)	**Point Estimate of MTBF**	**Confidence in meeting requirement (1,000 hr)**
0	Infinite or undefined	86%
1	2,000	59%
2	1,000	32%
3	667	14%
4	500	5%
5	400	2%

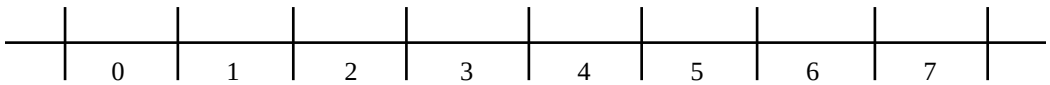
A reasonable test plan for 2000 hours of testing would seem to be to allow two failures because this leads to an estimate of 1,000 hours MTBF, right at the required value. So, this is where we would "draw the line." The demonstration for Contractor A should show about 48% of the PMs accepting (2 reds: 26%; 1 red: 17%; 0 reds: 5%). Unfortunately, Contractor A had too many red chips (80) leading to a true (but unknown to the PM) MTBF of 750 hours, computed as:

$$\frac{480\ total\ chips\ \ x\ 125\,\frac{hr}{chip}}{80\ red\ chips, i.e., (potential) failures} = 750\ hr/failure$$

Suppose a contractor's true MTBF is around 1400 hours. Notice that there is no way the test data would produce that figure. The closest possible estimates are 1000 and 2000 hours. What if the true MTBF is about 5,000 hours? Again, you'd never know it from the estimates that test data could produce!

Contractor A: Distribution of Failures (Red Chips)

Test plan: 2000 test hours
allow 2 failures



A frequency distribution of the red chips may be drawn on the scale above.

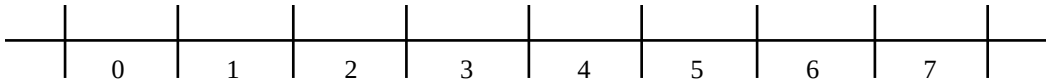
Calculate the risk of making the erroneous decision when subjecting Contractor A's quality to this test plan: The percentage of PMs that make the erroneous decision represents the risk associated with subjecting this level of reliability (750 hours) to this test plan (test for 2000 hours; allow 2 failure). Again, this number is typically about 48%.

Identify a test plan that would lessen the risk of making the erroneous decision: One test plan that would lessen the beta risk would be to draw the line at 1 failure, not 2. This is legitimate as long as the contractor is aware, agrees, and negotiates with such a test plan in mind. Other risk-reducing test plans might require additional testing, which may include unacceptable cost and schedule impacts.

Calculate the risk of using this test plan: Only those PMs with 1 or 0 red chips would be "accepting." This should result in about 22% (1 red: 17%; 0 red: 5%) of the PMs making the erroneous decision.

Contractor B: Distribution of Failures (Red Chips)

Test plan: 2000 test hours
allow 2 failures



Calculate the risk of making the erroneous decision when subjecting Contractor B's quality to the original test plan: Contractor B's bag has only 40 red chips in a total of 480. Hence the true MTBF may be calculated to be 1500 hours, acceptable. The only erroneous decision, then, would be to reject. Using the original test plan of 2000 hours and allowing 2 failures, we would expect that 86% would make the correct decision (2 reds: 25%; 1 red: 37%; 0 reds: 24%); thus 14% would make the erroneous decision. However, if the more stringent test plan were used (2000; 1), we would expect only 51% to make the correct decision (1 red: 37%; 0 reds: 24%); hence 49% would be expected to make the wrong decision.

In summary, by decreasing the government's risk we are increasing the contractor's risk. This doesn't sound fair. In reality, we would take into account both the government's and contractor's desired risk levels, and the specified and desired MTBFs, then consult, say, MIL-HDBK-781 for a statistical fixed length test plan, as discussed below.

Statistical Test Plans

If the government specified a 1,000 MTBF requirement and was willing to take a 30% chance of accepting an MTBF of 1,000; and if the contractor was predicting a 1500 hour MTBF and was willing to take a 20% chance of being rejected even if the true MTBF was 1500 hours, the statistical fixed-length test plan from MIL-HDBK-781A (p. 238, FIGURE 20) would be: test for 13,550 hours and allow as many as 11 failures. Real

world constraints on funding, schedule, and test range availability, etc. may dictate that this test plan will not be used, however.

Confidence and MTBF

Assume you have tested one or more pieces of equipment for a total of 10,000 hours and have observed 5 failures. What is the MTBF of the equipment?

$$\text{Point estimate} = \frac{\text{Total time}}{\#\,\text{failures}} = \frac{10{,}000 \text{ hours}}{5 \text{ failures}} = 2000 \text{ hr MTBF}$$

How confident are you that the equipment's true MTBF is:

Exactly 2,000 hours?
Between 1,990 and 2,010 hours?
Between 1,900 and 2,100 hours?
Between 1,000 and 3,000 hours?
Equal to or greater than 1,500 hours?

Logisticians are generally interested in the latter type question: "How confident are you that the reliability is equal to or greater than some important value"? As an aside, let's discuss confidence with regard to the red chips exercise above:

- If there are no failures in 2000 hours, we can state with 86% confidence, theoretically, that the true MTBF is at least 1000 hours. Similarly, if there were five failures, we can state with about 2% confidence that the true MTBF is at least 1,000 hours (even though the point estimate is only 400 hours!) These confidence values were determined through software provided by the Air Force Operational Test and Evaluation Center.
- Confidence tables, such as those found in MIL-HDBK-781A enable you to make confidence statements at commonly used confidence levels, like 90% and 80%. For example: 10,000 hours, 5 failures.

Instructions:

- Compute point estimate: 10,000 hours ÷ 5 failures = 2000 hours MTBF
- Select a desired confidence level (e.g. 90%)
- Enter the appropriate confidence column in the table below (from MIL-HDBK-781A) and the row with number of observed failures (5).
- Read the lower confidence limit multiplier = 0.539
- Multiply by the point estimate: 0.539 x 2,000= 1,078

Statements about this calculation:
(1) "I am 90% confident that the true (but unknown) MTBF is at least 1,078 hours."
(2) "I am willing to accept a 10% RISK the true (but unknown) MTBF is less than 1,078 hours."

Note that this value (1,078 hours) is significantly lower than the point estimate (2,000 hrs).

Demonstrated MTBF Multipliers (MIL - HDBK - 781A, p. 133)

Number of Observed Events	Lower Confidence Limit Multipliers		
	70 Percent	**80 Percent**	**90 Percent**
1	.410	.334	.257
2	.533	.467	.376
3	.630	.544	.449
4	.679	.595	.500
5	.714	.632	.539
6	.740	.661	.570
7	.760	.684	.595
8	.777	.703	.616
9	.790	.719	.634
10	.802	.733	.649
11	.812	.744	.663

Reliability Testing: References

DoD 3235.1-H, Test and Evaluation of System Reliability Availability and Maintainability
MIL-HDBK-781A, Reliability Test Methods, Plans, and Environments for Engineering Development, Qualification and Production
MIL-HDBK-189, Reliability Growth Management
DoD RAM Guide

Summary, Chapter 6, R&M Risk Reduction

In this chapter we studied Reliability Growth "Testing" - aimed at improving the reliability of the design. Then we examined Reliability Qualification Testing, whose purpose is to verify that the design meets contractual reliability requirements; RQT is aimed basically at reducing the risk of having an unacceptable number of mission failures and an unacceptable cost of support.

This page intentionally left blank

Chapter 7: Impacts of Manufacturing on R&M

The aim of this chapter is for you to learn how to assure the manufacturing process provides all the reliability the design has to offer. First, you will learn the effects that latent defects have on the field. Then, you will learn three lines of defense to assure the field does not receive latent defects.

Perfecting the Manufacturing Process

Manufacturing is an opportunity to make things worse, reliability-wise! Manufacturing processes are imperfect. This is evident because variation is inevitable in manufacturing. Some variation is extreme enough to result in defects in even the best-designed equipment.

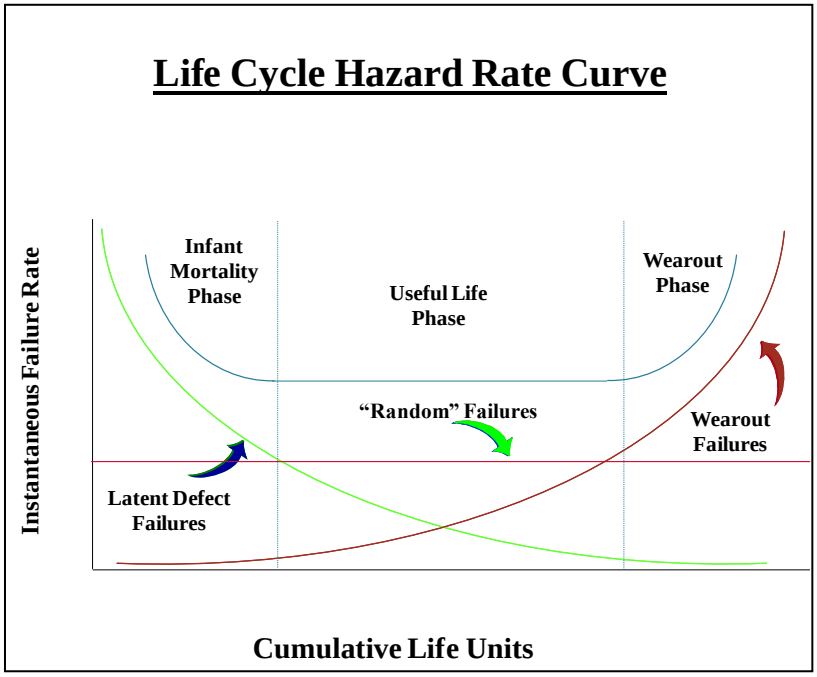
Defects are evidenced by high scrap/rework rates in factory. When failures occur early in operation, we have what are called "infant mortality" failures. An example was a Space Shuttle Failure in which a microcircuit failed a fraction of a second before lift-off. The cost impact was $10 million for the launch delay and $500,000 for replacement and failure analysis. Upon investigation, they found the root cause was human spittle (full of corrosive salts) had been sealed into the microcircuit at time of manufacture. Moisture eventually leaked in, activated the salts, and resulted in corrosion that destroyed circuit paths on the microcircuit.

Other Effects of Latent Defects

Latent defect field failures tend to reduce system availability. They also require more resources - manpower and spares. The remainder of this chapter will show how to recognize, from field data, the existence of manufacturing defects; and we will present three lines of defense.

Manufacturing Defects - Recognizing the Problem

If we suspect manufacturing defects are a problem, how can we verify? Study the factory or field failures using your understanding of the life cycle hazard rate curve aka reliability "bathtub" curve.



We will compare actual failure data to an expected, constant failure rate, using an example. Starting the first period (say, January) with 20 units and ending last period with 13. We will examine field data from three different type products, Items A, B, and C. We will calculate the period failure rate and see if it is relatively constant, which would expect for "useful life".

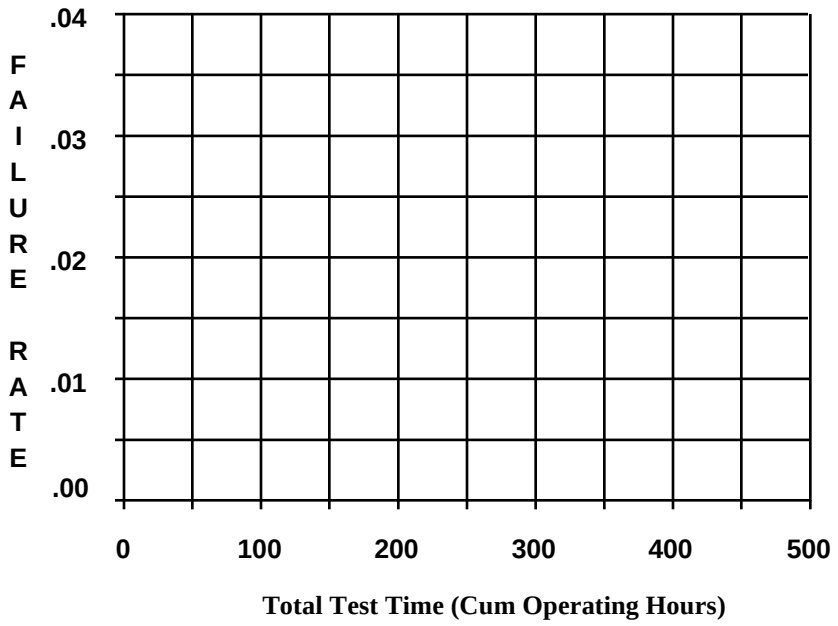
Period	Cum	Item A	Item B	Item C
100	100	1	4	0
100	200	2	2	0
100	300	1	1	1
100	400	2	0	2
100	500	1	0	4

For Item A, below, since each period is 100 hours, the period failure rates are .01, .02, .01, .02, and .01 failures per hour, respectively. This up - down - up - down pattern suggests random failures, i.e., useful life phase.

For Item B, however, the calculated failure rates are .04, .02, .01, .00, and .00 failures per hour, a decreasing trend. This suggests that infant mortality may be the cause. It might be wise to investigate the manufacturing process before the next production lot is built.

Item C's failure rates are .00, .00, .01, .02, and .04 failures per hour, an increasing trend. Thus, it appears Item C is in wear-out. It might be wise to remove and replace the remaining 13 units, or suffer many failures in the next period!

The failure rates of Items A, B, and C may be plotted below.

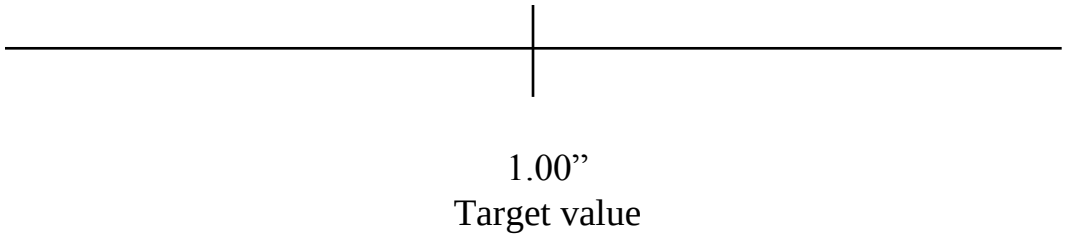


How do We Reduce or Eliminate the Number of Defects?

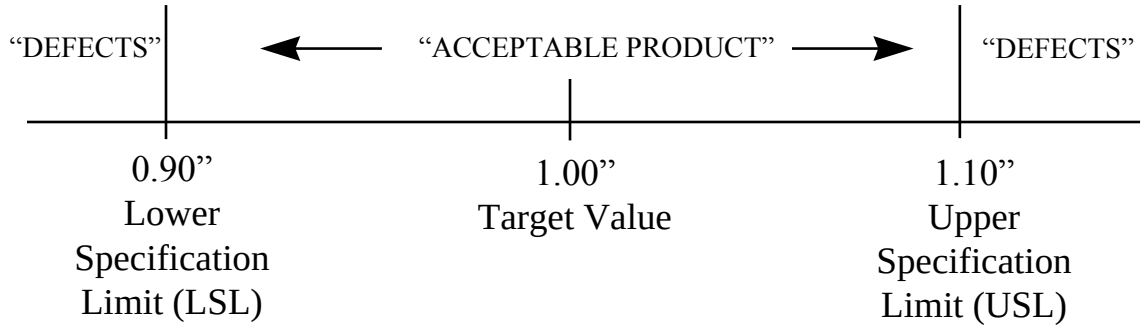
Three Lines of Defense for reducing or eliminating the number of latent defects are prevention, the identification and removal of observable defects, and the forced precipitation of non-observable, latent defects. These will be discussed below.

First Line of Defense: Preventing Defects

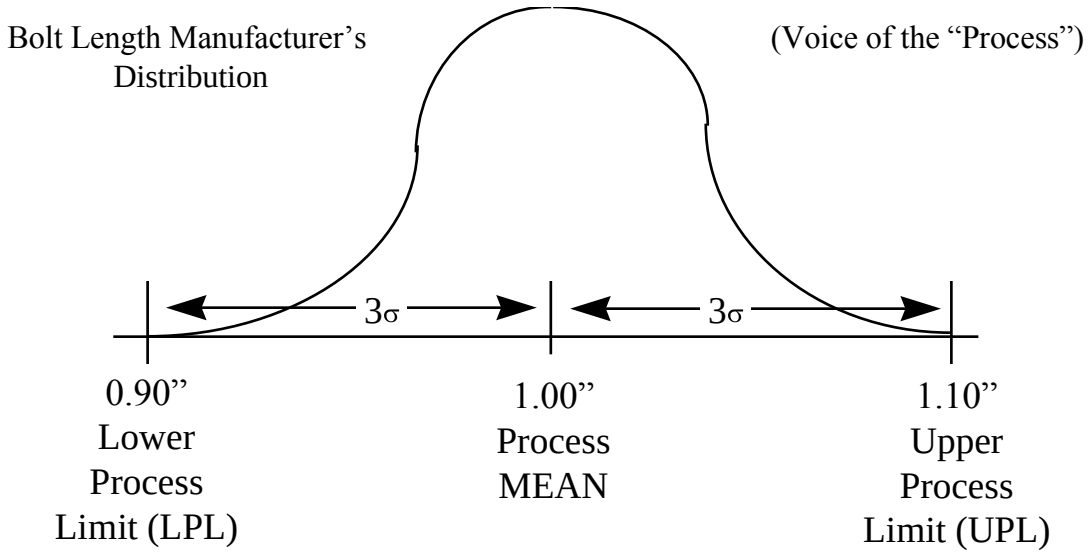
Let's consider the design of a bolt to hold an engine in place on an aircraft. The voice of the customer might say the function of the bolt is to keep the engine from shaking loose and falling off. To the engineer, this might mean many things, strength and length, for example. We will consider length as a critical quality characteristic. Let's assume the optimum or target length is 1.00 inches, no more, no less.



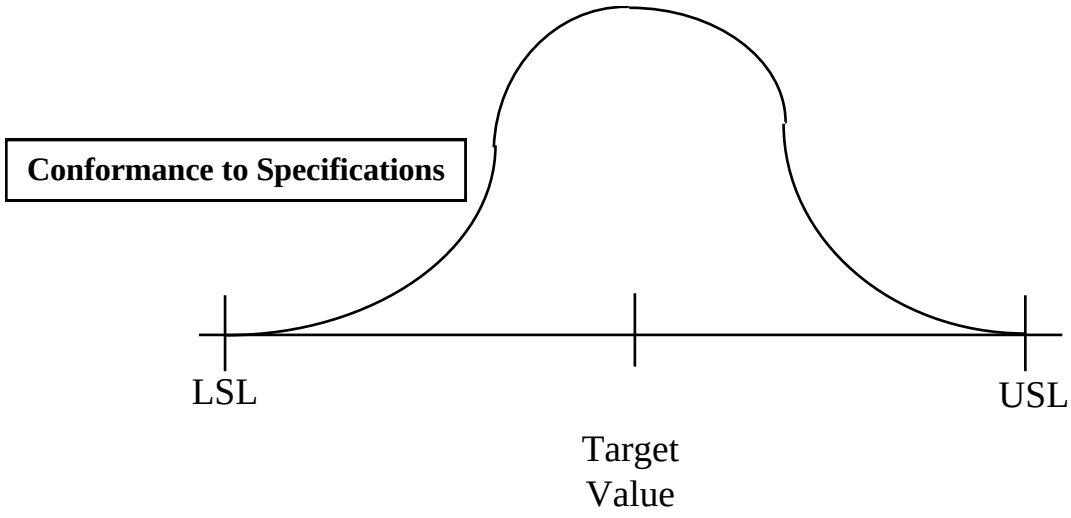
Somewhere along the line, bolt length specification limits will be imposed. Specification limits represent a "compromise" between what the designer really wants and what the draftsman or manufacturing or QA folks say they can reasonably achieve with some consistency. However, in the case where specification limits are set arbitrarily (company policy of ±10% or ±0.10 inches, for example) it is not likely that such limits will relate well to the customer's perception of quality - bolts that hold the engine in place on the aircraft. However, if testing, experimentation, or analysis determines the limits, those limits may serve the customer quite well.



The drawing below shows a possible source of supply for bolts. It depicts a special case known as Conformance to Specifications. This means that the process average coincides with the target value, which is ideal. And the upper and lower process limits coincide with the upper and lower specification limits, which is good, but not great. The process limits are by definition, three standard deviations above and below the mean. So, "conformance to specifications" is a 3σ (standard deviation) process. 4σ, 5σ, and 6σ processes are even better. Motorola, Hewlett-Packard and other companies have highly touted 6σ programs. These are aimed at reducing the variation in their processes so that 6 standard deviations can be fit between the target value and, the upper specification limit.



The conventional depiction of "Conformance to Specifications" appears below. The bell-curve is drawn touching (or stopping at) the horizontal line; by inference this truncation depicts the upper and lower process limits. By labeling these same points as the upper and lower specification limits, one can infer that the process conforms to specifications.



To quantify how much better a 4σ process is compared to a 3σ process consider the following situation: A company's manufacturing processes are such that the ± 3σ values for all processes coincide with the LSL and USL values, i.e., "conformance to specifications" exists. What is the probability of building a functional assembly from 100 parts selected without inspection?

All 100 parts in an assembly must be "good" or the assembly will fail. Any part with a characteristic value beyond the upper or lower specification limits is a "bad" part. Based on normal distribution theory the probability of a part being good is:

- P (any single part being good) = 0.9973

Therefore, the probability of 100 consecutive parts being "good" is

- Probability (100 good parts) = $(0.9973)^{100} = 0.763$

This can be interpreted as the first-time yield being about 76.3%.

If the company reduces the variability of the process such that the $\pm 4\sigma$ values coincide with the LSL and USL, what is the first-time yield or "reliability" of the manufacturing and assembly process?

- P (any single part being good) = 0.999936 (from Normal distribution).
- P (100 good parts) = $(0.999936)^{100} = 0.9936$

That is, the first-time yield is now 99.36%, a marked improvement.

Second Line of Defense: Identification and Removal of Observable Defects

A second line of defense against latent defects is to identify and remove observable latent defects via quality checks. These include the traditional QA methods of visual inspections, physical measurement, electrical and functional checks, and advanced technology inspection techniques. Automated laser inspection of solder joints, Radiographic inspection of boards, 2D/3D "smart" TV, and CAT scan are some of the advanced techniques.

Third Line of Defense: Forced Precipitation of Non-Observable, Latent Defects

Some defects are not easily preventable or can not be observed directly. However, we can precipitate such defects in the factory thereby avoiding field failures via Environmental Stress Screening (ESS). ESS is a process which involves the application of one or more specific types of environmental stresses for the purpose of precipitating to hard failure, latent, intermittent, or incipient defects/flaws, which would cause product failure in the use environment. The stress may be applied in combination or in sequence on an accelerated basis but within product design capabilities, to assure that ESS doesn't damage good units.

ESS Effectiveness - US Navy Experience

Equipment (Avionics)	MFHBR Without ESS	MFHBR With ESS	% Improvement
A	32	70	119
B	66	127	92
C	83	149	80
D	92	278	202
E	570	1100	95

Conclusion: ESS improves long-term, field reliability

Characteristics of a "Good" Environmental Screen

A good screening program is effective, efficient, and non-destructive. Effective means the process must detect various types of faults and have a high "batting average" against each. Efficient means the "cost" of the process should be minimized with regard to both time and money. Non-destructive means the ESS process doesn't damage good parts. The item's utility must be preserved, its useful life maintained, and no additional defects may be induced.

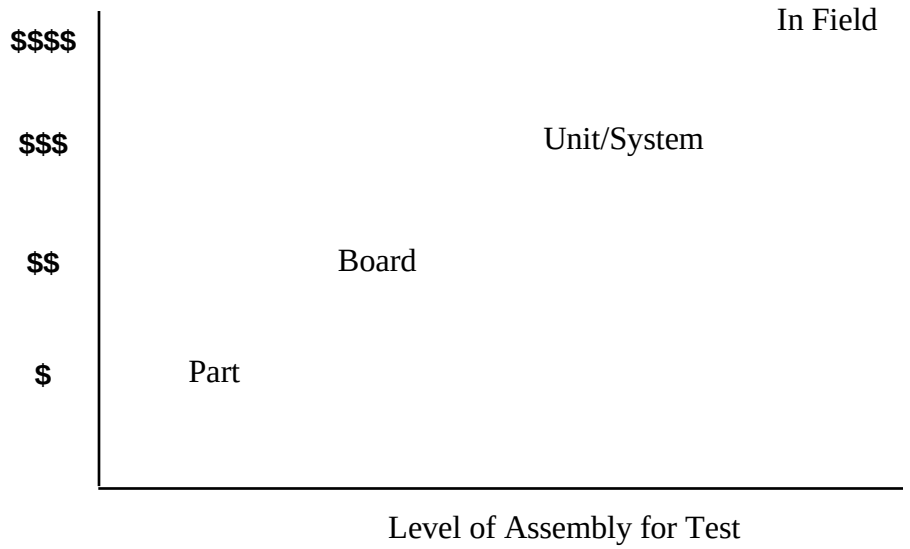
Tailoring Environmental Screens

Different types of hardware contain different types of latent defects. Different latent defects respond to different environments. Hence, there is no universal screen!

Most Common Screens

The most common screens are temperature and vibration cycling. The rate of change, the extremes of temperature and the number of cycles specify temperature cycling. The duration and the number of axes of vibration characterize random vibration.

Screening - at What Level of Assembly?



An Integrated Screening Program

It is often appropriate to screen at various levels of assembly. First at the part level to assure that only good parts remain in the manufacturing cycle. Then at the subassembly level to assure that assembly onto circuit cards, for example, has been done properly. It may also be necessary to screen at the complete assembly/system level.

Once defects are identified, it may be appropriate to repair the failed item, identify root cause of those latent defects, and initiate corrective action to PREVENT recurrence. So, ESS is **essentially a TAAF process aimed primarily at improving the manufacturing process.**

ESS - Summary: Where Applicable

ESS may be applicable in all material acquisitions that include electrical, electronic, electro-optical, electro-mechanical or electro-chemical components. It can also be accomplished in Depot overhaul programs where opportunities exist for substantial cost savings and overhaul/repair effectiveness. For commercial and nondevelopmental items, ESS may be appropriate to the extent it was implemented and documented during either current or previous production.

ESS is an effective tool for surfacing remaining latent defects, but . . . ESS is a temporary fix. Users of ESS need to analyze root cause of defects, correct parts, materials, processes, workmanship, and work toward eliminating the need for ESS.

Another type of reliability testing is PRAT (Production Reliability Acceptance Testing). The aim of PRAT is to assure that changes to the manufacturing process have improved, or at least not degraded, product reliability. Reliability testing, as discussed here, is summarized below:

TESTING/SCREENING SUMMARY			
Type of Test or Screen	Reasons for Test/Screen		Types of Environment
	Primary	Secondary	
Reliability Growth Testing	Improve design	Improve parts/ manufacturing processes	Mission/ spec +
Reliability Qualification Test	Verify design integrity	Identify pattern or other problems	Mission/ Spec
ESS	Remove latent defects	Improve design and manufacturing processes	Tailored
PRAT	Verify manufacturing integrity	Identify production anomalies	Mission Spec

Screens - Sources for Guidance

DoD RAM Guide
MIL-HDBK-2164A
MIL-HDBK-781A

Summary, Chapter 7, Impacts of Manufacturing on R&M

Manufacturing processes are imperfect. Such imperfections lead to latent defects and ultimately the loss of combat capability and/or increased support requirements. Efforts to ameliorate the effects of latent defects, in order of preference, are to prevent defects via variability reduction; remove observable defects; and screen 100%.

This page intentionally left blank