NASA Technical Memorandum 106313

Design for Reliability:

NASA Reliability Preferred Practices for Design and Test

Vincent R. Lalli
Lewis Research Center
Cleveland, Ohio

Prepared for the
Reliability and Maintainability Symposium
cosponsored by ASQC, IIE, IEEE, SOLE, IES, AIAA, SSS, and SRE
Anaheim, California, January 24–27, 1994

National Aeronautics and
Space Administration

DESIGN FOR RELIABILITY

PART I—NASA RELIABILITY PREFERRED PRACTICES FOR DESIGN AND TEST

Vincent R. Lalli
National Aeronautics and Space Administration
Lewis Research Center
Cleveland, Ohio 44135

SUMMARY AND PURPOSE

This tutorial summarizes reliability experience from both NASA and industry and reflects engineering practices that support current and future civil space programs. These practices were collected from various NASA field centers and were reviewed by a committee of senior technical representatives from the participating centers (members are listed at the end). The material for this tutorial was taken from the publication issued by the NASA Reliability and Maintainability Steering Committee (NASA Reliability Preferred Practices for Design and Test. NASA TM-4322, 1991).

Reliability must be an integral part of the systems engineering process. Although both disciplines must be weighted equally with other technical and programmatic demands, the application of sound reliability principles will be the key to the effectiveness and affordability of America's space program. Our space programs have shown that reliability efforts must focus on the design characteristics that affect the frequency of failure. Herein, we emphasize that these identified design characteristics must be controlled by applying conservative engineering principles.

This tutorial should be used to assess your current reliability techniques, thus promoting an active technical interchange between reliability and design engineering that focuses on the design margins and their potential impact on maintenance and logistics requirements. By applying these practices and guidelines, reliability organizations throughout NASA and the aerospace community will continue to contribute to a systems development process which assures that

- Operating environments are well defined and independently verified.
- Design criteria drive a conservative design approach.
- Design weaknesses evident by test or analysis are identified and tracked.

Vincent R. Lalli has been at NASA Lewis Research Center since 1963 when he was hired as an aerospace technologist. Presently, as an adjunct to his work for the Office of Mission Safety and Assurance in design, analysis, and failure metrics, he is responsible for product assurance management and also teaches courses to assist with NASA's training needs. Mr. Lalli graduated from Case Western University with a B.S. and an M.S. in electrical engineering. In 1959 as a research assistant at Case, and later at Picatinny Arsenal, he helped to develop electronic fuses and special devices. From 1956 to 1963, he worked at TRW as a design, lead, and group engineer. Mr. Lalli is a registered engineer in Ohio and a member of Eta Kappa Nu, IEEE, IPC, ANSI, and ASME.

1.0 OVERVIEW

1.1 Applicability

The design practices that have contributed to NASA mission success represent the "best technical advice" on reliability design and test practices. These practices are not requirements but rather proven technical approaches that can enhance system reliability.

This tutorial is divided into two technical sections. Section II contains reliability practices, including design criteria, test procedures, and analytical techniques, that have been successfully applied in previous spaceflight programs. Section III contains reliability guidelines, including techniques currently applied to spaceflight projects, where insufficient information exists to certify that the technique will contribute to mission success.

1.2 Discussion

Experience from NASA's successful extended-duration space missions shows that four elements contribute to high reliability: (1) understanding stress factors imposed on flight hardware by the operating environment; (2) controlling the stress factors through the selection of conservative design criteria; (3) conducting an appropriate analysis to identify and track high stress points in the design (prior to qualification testing or flight use); and (4) selecting redundancy alternatives to provide the necessary function(s) should failure occur.

2.0 RELIABILITY PRACTICES

2.1 Introduction

The reliability design practices presented herein contributed to the success of previous spaceflight programs. The information is for use throughout NASA and the aerospace community to assist in the design and development of highly reliable equipment and assemblies. The practices include recommended analysis procedures, redundancy considerations, parts selection, environmental requirements considerations, and test requirements and procedures.

2.2 Format

The following format is used for reliability practices:

PRACTICE FORMAT DEFINITIONS

Practice: A brief statement of the practice

Benefit: A concise statement of the technical improvement realized from implementing the practice

Programs That Certified Usage: Identifiable programs or projects that have applied the practice

Center to Contact for More Information: Source of additional information, usually a sponsoring NASA Center (see page 6)

Implementation Method: A brief technical discussion, not intended to give the full dethils of the process but to provide a design engineer with adequate information to understand how the practice should be used

Technical Rationale: A brief technical justification for use of the practice

Impact of Nonpractice: A brief statement of what can be expected if the practice is avoided

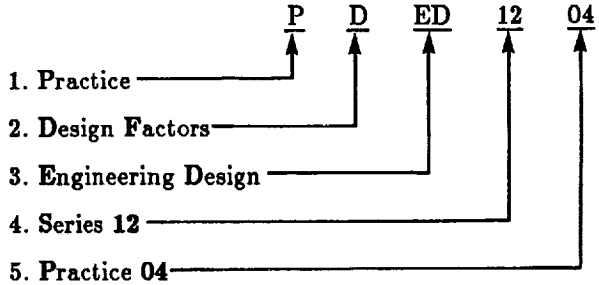
Related Practices: Identification of other topic areas in the manual that contain related information

References: Publications that contain additional information about the practice

SPONSOR OF PRACTICE

2.3 Document Referencing

The following example of the document numbering system applicable to the practices and guidelines is "Part Junction Temperature," practice number PD-ED-1204:



Key to nomenclature.—The following is an explanation of the numbering system:

Position	Code	
1.		G - Guideline P - Practice
2.		D - Design factors T - Test elements
3.		EC - Environmental considerations ED - Engineering design AP - Analytical procedures TE - Test considerations and procedures
4.	x	Series number
5.	xx	Practice number within series

2.4 Practices as of January 1993

PD-EC-1101		Environmental Factors
PD-EC-1102	**	Meteoroids/Space Debris
PD-ED-1201		EEE Parts Derating
PD-ED-1202		High-Voltage Power Supply Design and Manufacturing Practices
PD-ED-1203		Class-S Parts in High-Reliability Applications
PD-ED-1204		Part Junction Temperature
PD-ED-1205	*	Welding Practices for 2219 Aluminum and Inconel 718
PD-ED-1206	*	Power Line Filters
PD-ED-1207	*	Magnetic Design Control for Science Instruments

PD-ED-1208	*	Static Cryogenic Seals for Launch Vehicle Applications
PD-ED-1209	**	Ammonia-Charged Aluminum Heat Pipes with Extruded Wicks
PD-ED-1210	*	Assessment and Control of Electrical Charges
PD-ED-1211	*	Combination Methods for Deriving Structural Design Loads Considering Vibro-Acoustic, etc., Responses
PD-ED-1212	*	Design and Analysis of Electronic Circuits for Worst-Case Environments and Part Variations
PD-ED-1213	**	Electrical Shielding of Power, Signal, and Control Cables
PD-ED-1214	**	Electrical Grounding Practices for Aerospace Hardware
PD-ED-1215.1	**	Preliminary Design Review
PD-ED-1216	**	Active Redundancy
PD-ED-1217	**	Structural Laminate Composites for Space Applications
PD-ED-1218	**	Application of Ablative Composites to Nozzles for Reusable Solid Rocket Motors
PD-ED-1219	**	Vehicle Integration/Tolerance Buildup Practices
PD-ED-1221	**	Battery Selection Practice for Aerospace Power Systems
PD-ED-1222	**	Magnetic Field Restraints for Spacecraft Systems and Subsystems
PD-AP-1301		Surface Charging and Electrostatic Discharge Analysis
PD-AP-1302	*	Independent Review of Reliability Analyses
PD-AP-1303	*	Part Electrical Stress Analysis
PD-AP-1304	*	Problem/Failure Report Independent Review/Approval
PD-AP-1305	*	Risk Rating of Problem/Failure Reports
PD-AP-1306	*	Thermal Analysis of Electronic Assemblies to the Piece Part Level
PD-AP-1307	**	Failure Modes, Effects, and Criticality Analysis (FMECA)
PT-TE-1401		EEE Parts Screening
PT-TE-1402		Thermal Cycling
PT-TE-1403		Thermographic Mapping of PC Boards
PT-TE-1404		Thermal Test Levels
PT-TE-1405		Powered-On Vibration
PT-TE-1406		Sinusoidal Vibration
PT-TE-1407	*	Assembly Acoustic Tests
PT-TE-1408	*	Pyrotechnic Shock
PT-TE-1409	*	Thermal Vacuum Versus Thermal Atmospheric Test of Electronic Assemblies
PT-TE-1410	*	Selection of Spacecraft Materials and Supporting Vacuum Outgassing Data
PT-TE-1411	**	Heat Sinks for Parts Operated in Vacuum
PT-TE-1412	**	Environmental Test Sequencing
PT-TE-1413	**	Random Vibration Testing
PT-TE-1414	**	Electrostatic Discharge (ESD) Test Practices

*New practices for January 1992.
**New practices for January 1993.

2.5 Typical Reliability Practice

A typical reliability practice is illustrated in this section. Environmental factors are very important in the system design so equipment operating conditions must be identified. Systems designed to have adequate environmental strength perform well in the field and satisfy our customers. Failure to perform a detailed life-cycle environment profile can lead to overlooking environmental factors whose effect is critical to equipment reliability. Not including these factors in the environmental design criteria and test program can lead to environment-induced failures during spaceflight operations.

Environmental Factors

- **Practice (PD–EC–1101):** Identify equipment operating conditions.

- **Benefit:** Adequate environmental strength is incorporated into design.

- **Programs That Certified Usage:** SERT I and II, CTS, ACTS, space experiments, launch vehicles, space power systems, and Space Station Freedom

- **Center to Contact for More Information:** NASA Lewis Research Center

- **Implementation Method:** Develop life-cycle environment profile.

  - Describe anticipated events from final factory acceptance through removal from inventory.
  - Identify significant natural and induced environments for each event.
  - Describe environmental and stress conditions:
    Narrative
    Statistical

· Technical Rationale

Environment	Principal effects	Typical failures induced
High temperature	Thermal aging: Oxidation Structural change Chemical reaction	Insulation failure; alteration of electrical properties Structural failure Loss of lubrication properties
	Softening, melting, and sublimation Viscosity reduction/ evaporation Physical expansion	Structural failure; increased mechanical stress; increased wear on moving parts
Low temperature	Increased viscosity and solidification Ice formation	Loss of lubrication properties Alteration of electrical properties
	Embrittlement	Loss of mechanical strength; cracking; fracture
	Physical contraction	Structural failure; increased wear on moving parts
High relative humidity	Moisture absorption	Swelling, rupture of container; physical breakdown; loss of electrical strength
	Chemical reaction Corrosion Electrolysis	Loss of mechanical strength; interference with function; loss of electrical properties; increased conductivity of insulators
Low relative humidity	Desiccation Embrittlement Granulation	Loss of mechanical strength; structural collapse; alteration of electrical properties; "dusting"
High pressure	Compression	Structural collapse; penetration of sealing; interference with function
Low pressure	Expansion	Fracture of container; explosive expansion
	Outgassing	Alteration of electrical properties; loss of mechanical strength
	Reduced dielectrical strength of air	Insulation breakdown and arc-over; corona and ozone formation
Solar radiation	Actinic and physio-chemical reactions: embrittlement	Surface deterioration; alteration of electrical properties; discoloration of materials ozone formation
Sand and dust	Abrasion Clogging	Increased wear Interference with function; alteration of electrical properties
Salt spray	Chemical reactions: Corrosion	Increases wear Loss of mechanical strength; alteration of electrical properties; interference with function
	Electrolysis	Surface deterioration; structural weakening; increased conductivity

· Technical Rationale (continued)

Environment	Principal effects	Typical failures induced
Wind	Force application	Structural collapse; interference with function; loss of mechanical strength
	Deposition of materials	Mechanical interference and clogging; abrasion accelerated
	Heat loss (low velocity)	Acceleration of low-temperature effects
	Heat gain (high velocity)	Acceleration of high-temperature effects
Rain	Physical stress Water absorption and immersion	Structural collapse Increase in weight; electrical failure; structural weakening
	Erosion	Removal of protective coatings; structural weakening; surface deterioration
	Corrosion	Enhancement of chemical reactions
Temperature shock	Mechanical stress	Structural collapse or weakening; seal damage
High-speed particles (nuclear irradiation)	Heating	Thermal aging; oxidation
	Transmutation and ionization	Alteration of chemical, physical, and electrical properties; production of gases and secondary particles
Zero gravity	Mechanical stress	Interruption of gravity-dependent functions
	Absence of convection cooling	Aggravation of high-temperature effects
Ozone	Chemical reactions: Crazing, cracking	Rapid oxidation; alteration of electrical properties
	Embrittlement	Loss of mechanical strength
	Granulation	Interference with function
	Reduced dielectrical strength of air	Insulation breakdown and arc-over
Explosive decompression	Severe mechanical stress	Rupture and cracking structural collapse
Dissociated gases	Chemical reactions: Contamination	Alteration of physical and electrical properties
	Reduced dielectric strength	Insulation breakdown and arc-over
Acceleration	Mechanical stress	Structural collapse

- **Technical Rationale** (concluded)

Environment	Principal effects	Typical failures induced
Vibration	Mechanical stress	Loss of mechanical strength; interference with function; increased wear
	Fatigue	Structural collapse
Magnetic fields	Induced magnetization	Interference with function; alteration of electrical properties; induced heating

- **Impact of Nonpractice:**

  Failure to perform a detailed life-cycle environment profile can lead to overlooking environmental factors whose effect is critical to equipment reliability. If these factors are not included in the environmental design criteria and test program, environment-induced failures may occur during spaceflight operations.

- **References:**

Government

1. Reliability Prediction of Electronic Equipment. MIL-HDBK-217E Notice 1, January 1990.
2. Reliability/Design Thermal Applications. MIL-HDBK-251, January 1978.
3. Electronic Reliability Design Handbook. MIL-HDBK-338-1A, October 1988.
4. Environmental Test Methods and Engineering Guidelines. MIL-STD-810E, July 1989.

Industry

5. Space Station Freedom Electric Power System Reliability and Maintainability Guidelines Document. EID-00866, Rocketdyne Division, Rockwell International, 1990.
6. Society of Automotive Engineers, Reliability, Maintainability, and Supportability Guidebook, SAE G-11, 1990.

3.0 RELIABILITY DESIGN GUIDELINES

3.1 Introduction

The reliability design guidelines for consideration by the aerospace community are presented herein. These guidelines contain information that represents a technically credible process applied to ongoing NASA programs and projects. Unlike a reliability design practice, a guideline lacks specific operational experience or data to validate its contribution to mission success. However, a guideline does contain information that represents current "best thinking" on a particular subject.

3.2 Format

The following format is used for reliability guidelines:

GUIDELINE FORMAT DEFINITIONS

Practice: A brief statement of the guideline

Benefit: A concise statement of the technical improvement realized from implementing the guideline

Center to Contact for More Information: Source of additional information, usually the sponsoring NASA Center (see page 6)

Implementation Method: A brief technical discussion, not intended to give the full details of the process but to provide a design engineer with adequate information to understand how the guideline should be used.

Technical Rationale: A brief technical justification for use of the guideline

Impact of Nonpractice: A brief statement of what can be expected if the guideline is avoided

Related Guidelines: Identification of other topic areas in the manual that contain related information

References: Publications that contain additional information about the guideline

SPONSOR OF GUIDELINE

3.3 Guidelines as of January 1993

GD-ED-2201	**	Fastener Standardization and Selection Considerations
GD-ED-2202	**	Design Considerations for Selection of Thick-Film Microelectronic Circuits
GD-ED-2203	**	Design Checklists for Microcircuits
GD-AP-2301		Earth Orbit Environmental Heating
GT-TE-2401	**	EMC Guideline for Payloads, Subsystems, and Components

**New Guidelines as of January 1993.

3.4 Typical Reliability Guideline

A typical reliability guideline is illustrated in this section. Environmental heating for Earth orbiting systems is an important design consideration. Designers should use currently accepted values for the solar constant, albedo factor, and Earth radiation when calculating the heat balance of Earth orbiters. These calculations can

accurately predict the thermal environment of orbiting devices. Failure to use these constants can result in an incomplete thermal analysis and grossly underestimated temperature variations of the components.

Analysis of Earth Orbit Environmental Heating

· **Guideline (GD–AP–2301)**: Use currently accepted values for solar constant, albedo factor, and Earth radiation when calculating heat balance of Earth orbiters. This practice provides heating rate for blackbody case without considering spectral effects or collimation.

· **Benefit**: Thermal environment of orbiting devices is accurately predicted.

· **Center to Contact for More Information**: Goddard

· **Implementation Method**

- Solar constant, W/m^2
  Nominal, 1367.5
  Winter, 1422.0
  Summer, 1318.0

- Albedo factor
  Nominal, 0.30
  Hot, 0.35
  Cold, 0.25

- Earth-emitted energy (nominal, 255 K; producing 241 W/m^2)

Solar constant, W/m^2	Albedo factor	Earth-emitted energy, W/m^2	Equivalent earth temperature, K
Nominal, 1367.5	0.25	256	258
	.30	239	254
	.35	222	250
Winter solstice, 1422	0.25	267	262
	.30	249	258
	.35	231	253
Summer solstice, 1318	0.25	247	256
	.30	231	251
	.35	214	246

· **Technical Rationale**: Modification of energy incident on a spacecraft due to Earth-Sun distance variation and accuracy of solar constant are of sufficient magnitude to be important parameters in performing a thermal analysis.

· **Impact of Nonpractice**: Failure to use constants results in an incomplete thermal analysis and grossly underestimated temperature variations of components.

· **References**:

1. Leffler, J.M.: Spacecraft External Heating Variations in Orbit. AIAA paper 87–1596, June 1987.
2. Reliability/Design, Thermal Applications. MIL–HDBK–251, 1978.
3. Incropera, F.P.; and DeWitt, D.P.: Fundamentals of Heat and Mass Transfer. Second ed. John Wiley & Sons, 1985.

4.0 NASA RELIABILITY AND MAINTAINABILITY STEERING COMMITTEE

The following members of the NASA Reliability and Maintainability Steering Committee may be contacted for more information about the practices and guidelines:

Dan Lee
Ames Research Center
MS 218–7 DQR
Moffett Field, California 94035

Jack Remez
Goddard Space Flight Center
Bldg. 6 Rm S233 Code 302
Greenbelt, Maryland 20771

Thomas Gindorf
Jet Propulsion Laboratory
California Institute of Technology
MS 301–456 SEC 521
4800 Oak Grove Drive
Pasadena, California 91109

Nancy Steisslinger
Lyndon B. Johnson Space Center
Bldg. 45 Rm 613 Code NB23
Houston, Texas 77058

Leon Migdalski
John F. Kennedy Space Center
RT-ENG–2 KSC HQS 3548
Kennedy Space Center, Florida 32899

Salvatore Bavuso
Langley Research Center
MS 478
5 Freeman Road
Hampton, Virginia 23665–5225

Vincent Lalli
Lewis Research Center
MS 501–4 Code 0152
21000 Brookpark Road
Cleveland, Ohio 44135

Donald Bush
George C. Marshall Space Flight Center
CT11 Bldg. 4103
Marshall Space Flight Center, Alabama 35812

Ronald Lisk
NASA Headquarters Code QS
Washington, DC 20546

PART II—RELIABILITY TRAINING

1.0 INTRODUCTION TO RELIABILITY

"Reliability" applies to systems consisting of people, machines, and written information. A system is reliable if those who need it can depend on it over a reasonable period of time and if it satisfies their needs. Of the people involved in a system, some rely on it, some keep it reliable, and some do both. Several machines comprise a system: mechanical, electrical, and electronic. The written information defines peoples' roles in the system: sales literature; system specifications; detailed manufacturing drawings; software, programs, and procedures; operating and repair instructions; and inventory control.

Reliability engineering is the discipline that defines specific tasks done while a system is being planned, designed, manufactured, used, and improved. Outside of the usual engineering and management tasks, these tasks ensure that the people in the system attend to all those details that keep it operating reliably.

Reliability engineering is necessary because as users of rapidly changing technology and as members of large complex systems, we cannot ensure that essential details affecting reliability are not overlooked.

1.1 Period of Awakening: Failure Analysis

The theme of this tutorial is failure physics: the study of how products, hardware, software, and systems fail and what can be done about it. Training in reliability must begin with a review of mathematics and a description of the elements that contribute to product failures. Consider the following example of a failure analysis. A semiconductor diode developed a short. Analysis showed that a surge voltage was occurring occasionally, exceeding the breakdown voltage of the diode and burning it up. The problem: stress exceeding strength, a type I failure. A transistor suddenly stopped functioning. Analysis showed that aluminum metallization opened at an oxide step on the chip, the opening accelerated by the neck-down of the metallization at the step. In classical terminology, this failure, caused by a manufacturing flaw, is a random failure (type II). These two failure types are shown in figure 1. Formerly, most of the design control efforts shown in the figure were aimed at the type I failure. Although such design controls are important, most equipment failures in the field bear no relation to the results of reasonable stress analyses during design. These failures are type II (i.e., those caused by built-in flaws).

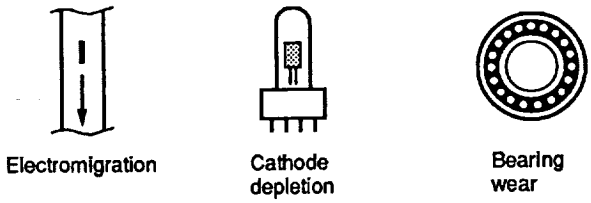
1.2 New Direction

The new direction in reliability engineering will be toward a more realistic recognition of the causes and effects of failures. The new boundaries proposed for reliability engineering are to exclude management, applied mathematics, and double checking. These functions are important and may still be performed by reliability engineers. However, reliability engineering is to be a synthesizing function devoted to flaw control. The functions presented in figure 2 relate to the following tasks:

(1) Identify flaws and stresses and rank them for priority actions.

(2) Engage the material technologists to determine the flaw failure mechanisms.

(3) Develop flaw control techniques and send information back to the engineers responsible for design, manufacture, and support planning.



(a) Type I failures (a design margin problem on stress/strength, fatigue, and wear).

(b) Type II failures (a flaw problem).

Figure 1.—Two types of failure.

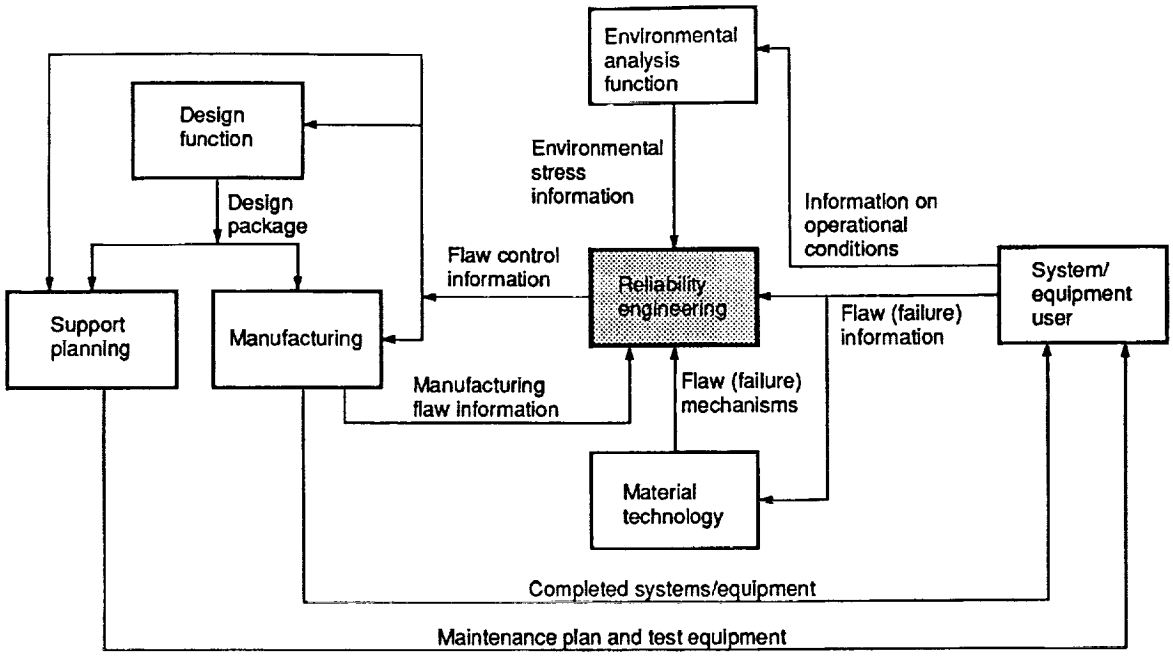


Figure 2.—Role of reliability engineering for the 1990's.

The types of output expected from reliability engineering are different from those provided by traditional engineering: stress-screening regimens; failure characteristics of parts and systems; effects of environmental stresses on flaws and failures; relationship of failure mechanisms to flaw failures; relationship of manufacturing yield to product reliability; flaw detection methods such as automated IC chip inspection and vibration signature monitoring.

Because flaws in an item depend on the design, manufacturing processes, quality control, parts, and materials, the distribution of flaws does not stay constant. Reliability engineering must act in a timely manner to provide flaw control information to the proper functions for action. It is important that customers recognize this fact and allow proper controls to be tailored to the needs of the time instead of demanding a one-time negotiation of what should be done for the total contract period.

1.3 Training as of June 1992

Although this tutorial considers only specific areas to exemplify the contents of a reliability training program, the following provides a complete list from the NASA Reference Publication 1253, "Reliability Training," available upon request from the National Technical Information Service, Springfield, Virginia; (703) 487–4650. A course evaluation form is included in the appendix.

Introduction to Reliability
- Era of Mechanical Designs
- Era of Electron Tubes
- Era of Semiconductors
- Period of Awakening
- New Direction
- Concluding Remarks
- Reliability Training

Reliability Mathematics and Failure Physics
- Mathematics Review
  - Notation
  - Manipulation of Exponential Functions
  - Rounding Data
  - Integration Formulas
  - Differential Formulas
  - Partial Derivatives
  - Expansion of $(a + b)^n$
- Failure Physics
- Probability Theory
  - Fundamentals
  - Probability Theorems
- Concept of Reliability
  - Reliability as Probability of Success
  - Reliability as Absence of Failure
  - Product Application
  - K-Factors
- Concluding Remarks
- Reliability Training

Exponential Distribution and Reliability Models
- Exponential Distribution
  - Failure Rate Definition
  - Failure Rate Dimensions
  - "Bathtub" Curve
  - Mean Time Between Failures
  - Calculations of P_c for Single Devices
- Reliability Models
  - Calculation of Reliability for Series-Connected Devices
  - Calculation of Reliability for Devices Connected in Parallel (Redundancy)
  - Calculation of Reliability for Complete System

2.0 RELIABILITY MATHEMATICS AND FAILURE PHYSICS

2.1 Failure Physics

When most engineers think of reliability, they think of parts since parts are the building blocks of products. All agree that a reliable product must have reliable parts. But what makes a part reliable? When asked, nearly all engineers would say a reliable part is one purchased according to a certain source control document and bought from an approved vendor. Unfortunately, these two qualifications are not always guarantees of reliability. The following case illustrates this problem.

A clock purchased according to PD 4600008 was procured from an approved vendor for use in the ground support equipment of a missile system and was subjected to qualification tests as part of the reliability program. These tests consisted of high- and low-temperature, mechanical shock, temperature shock, vibration, and humidity. The clocks from the then sole-source vendor failed two of the tests: low-temperature and humidity. A failure analysis revealed that lubricants in the clock's mechanism froze and that the seals were not adequate to protect the mechanism from humidity. A second approved vendor was selected. His clocks failed the high-temperature test. In the process the dial hands and numerals turned black, making readings impossible from a distance of 2 feet. A third approved vendor's clocks passed all of the tests except mechanical shock, which cracked two of the cases. Ironically, the fourth approved vendor's clocks, though less expensive, passed all the tests.

The point of this illustration is that four clocks, each designed to the same specification and procured from a qualified vendor, all performed differently in the same environments. Why did this happen? The specification did not include the gear lubricant or the type of coating on the hands and numerals or the type of case material.

Many similar examples could be cited, ranging from requirements for glue and paint to complete assemblies and systems, and the key to answering these problems can best be stated as follows: *To know how reliable a product is or how to design a reliable product, you must know how many ways its parts can fail and the types and magnitude of stresses that cause such failures.* Think about this: if you knew every conceivable way a missile could fail and if you knew the type and level of stress required to produce each failure, you could build a missile that would never fail because you could eliminate

(1) As many ways of failure as possible
(2) As many stresses as possible
(3) The remaining potential failures by controlling the level of the remaining stresses

Sound simple? Well, it would be except that despite the thousands of failures observed in industry each day, we still know very little about why things fail and even less about how to control these failures. However, through systematic data accumulation and study, we learn more each day.

As stated at the outset, this tutorial introduces some basic concepts of failure physics: failure modes (how failures are revealed); failure mechanisms (what produces the failure mode); and failure stresses (what activates the failure mechanisms). The theory and the practical tools available for controlling failures are presented also.

2.2 Reliability as Absence of Failure

Although the classical definition of reliability is adequate for most purposes, we are going to modify it somewhat and examine reliability from a slightly different viewpoint. Consider this definition: *Reliability is the probability that the critical failure modes of a device will not occur during a specified period of time and under specified conditions when used in the manner and for the purpose intended.* Essentially, this modification replaces the words "a device will operate successfully" with the words "critical failure modes . . . will not occur." This means that if all the possible failure modes of a device (ways the device can fail) and their probabilities of occurrence are known, the probability of success (or the reliability of a device) can be stated. It can be stated in terms of the probability that those failure modes critical to the performance of the device will not occur. Just as we needed a clear definition of success when using the classical definition, we must also have a clear definition of failure when using the modified definition.

For example, assume that a resistor has only two failure modes: it can open or it can short. If the probability that the resistor will not short is 0.99 and the probability that it will not open is 0.9, the reliability of the resistor (or the probability that the resistor will not short or open) is given by

$$R_{\text{resistor}} = \text{Probability of no opens} \times \text{Probability of no shorts} = 0.9 \times 0.99 = 0.89$$

Note that we have multiplied the probabilities. Probability theorem 2 therefore requires that the open-failure-mode probability and the short-failure-mode probability be independent of each other. This condition is satisfied because an open-failure mode cannot occur simultaneously with a short mode.

2.3 Product Application

This section relates reliability (or the probability of success) to product failures.

2.3.1 Product failure modes.—In general, critical equipment failures may be classified as catastrophic part failures, tolerance failures, and wearout failures. The expression for reliability then becomes

$$R = P_c P_t P_w$$

where

P_c probability that catastrophic part failures will not occur

P_t probability that tolerance failures will not occur

P_w probability that wearout failures will not occur

As in the resistor example, these probabilities are multiplied together because they are considered to be independent of each other. However, this may not always be true because an out-of-tolerance failure, for example, may evolve into or result from a catastrophic part failure. Nevertheless, in this tutorial they are considered independent and exceptions are pointed out as required.

2.3.2 Inherent product reliability.—Consider the inherent reliability R_i of a product. Think of the expression $R_i = P_c P_t P_w$ as representing the potential reliability of a product as described by its documentation, or let it represent the reliability inherent in the design drawings instead of the reliability of the manufactured hardware. This inherent reliability is predicated on the decisions and actions of many people. If they change, the inherent reliability could change.

Why do we consider inherent reliability? Because the facts of failure are these: When a design comes off the drawing board, the parts and materials have been selected; the tolerance, error, stress, and other performance analyses have been performed; the type of packaging is firm; the manufacturing processes and fabrication techniques have been decided; and usually the test methods and the quality acceptance criteria have been selected. At this point the design documentation represents some potential reliability that can never be increased except by a design change or good maintenance. However, the possibility exists that the actual reliability observed when the documentation is transformed into hardware will be much less than the potential reliability of the design. To understand why this is true, consider the hardware to be a black box with a hole in both the top and bottom. Inside are potential failures that limit the inherent reliability of the design. When the hardware is operated, these potential failures fall out the bottom (i.e., operating failures are observed). The rate at which the failures fall out depends on how the box or hardware is operated. Unfortunately, we never have just the inherent failures to worry about because other types of failures are being added to the box through the hole in the top. These other failures are generated by the manufacturing, quality, and logistics functions, by the user or customer, and even by the reliability organization itself. We discuss these added failures and their contributors in the following paragraphs but it is important to understand that, because of the added failures, the observed failures will be greater than the inherent failures of the design.

2.4 K-Factors

The other contributors to product failure just mentioned are called K-factors; they have a value between 0 and 1 and modify the inherent reliability:

$$R_{\text{product}} = R_i(K_q K_m K_r K_\ell K_u)$$

- K-factors denote probabilities that inherent reliability will not be degraded by
  - K_m manufacturing and fabrication and assembly techniques
  - K_q quality test methods and acceptance criteria
  - K_r reliability engineering activities
  - K_ℓ logistics activities
  - K_u the user or customer
- Any K-factor can cause reliability to go to zero.
- If each K-factor equals 1 (the goal), $R_{\text{product}} = R_i$.

2.5 Variables Affecting Failure Rates

Part failure rates are affected by (1) acceptance criteria, (2) all environments, (3) application, and (4) storage. To reduce the occurrence of part failures, we observe failure modes, learn what caused the failure (the failure stress), determine why it failed (the failure mechanism), and then take action to eliminate the failure. For example, one of the failure modes observed during a storage test was an "open" in a wet tantalum capacitor. The failure mechanism was end seal deterioration, allowing the electrolyte to leak. One obvious way to avoid this failure mode in a system that must be stored for long periods without maintenance is not to use wet tantalum capacitors. If this is impossible, the best solution would be to redesign the end seals. Further testing would be required to isolate the exact failure stress that produces the failure mechanism. Once isolated, the failure mechanism can often be eliminated through redesign or additional process controls.

2.6 Use of Failure Rates in Tradeoffs

Failure rate tables and derating curves are useful to a designer because they enable him to make reliability tradeoffs and provide a more practical method of establishing derating requirements. For example, suppose we

have two design concepts for performing some function. If the failure rate of concept A is 10 times higher than that of concept B, one can expect concept B to fail one-tenth as often as concept A. If it is desirable to use concept A for other reasons, such as cost, size, performance, or weight, the derating failure rate curves can be used to improve concept A's failure rate (e.g., select components with a lower failure rate, derate the components more, or both). An even better approach is to find ways to reduce the complexity and thus the failure rate of concept A. Figure 3 illustrates the use of failure rate data in tradeoffs. This figure gives a failure-rate-versus-temperature curve for the electronics of a complex (over 35 000 parts) piece of ground support equipment. The curve was developed as follows:

(1) A failure rate prediction was performed by using component failure rates and their application factors K_A for an operating temperature of 25 °C. The resulting failure rate was chosen as a reference point.

(2) Predictions were then made by using the same method for temperatures of 50, 75, and 100 °C. The ratios of these predictions to the reference point were plotted versus component operating temperature, with the resulting curve for the equipment. This curve was then used to provide tradeoff criteria for using air-conditioning versus blowers to cool the equipment. To illustrate, suppose the maximum operating temperatures expected are 50 °C with air-conditioning and 75 °C with blowers. Suppose further that the required failure rate for the equipment, if the equipment is to meet its reliability goal, is one failure per 50 hr. A failure rate prediction at 25 °C might indicate a failure rate of 1 per 100 hr. From the figure, note that the maximum allowable operating temperature is therefore 60 °C, since the maximum allowable failure rate ratio is $\lambda = 2$; that is, at 60 °C the equipment failure rate will be $(1/100) \times 2 = 1/50$, which

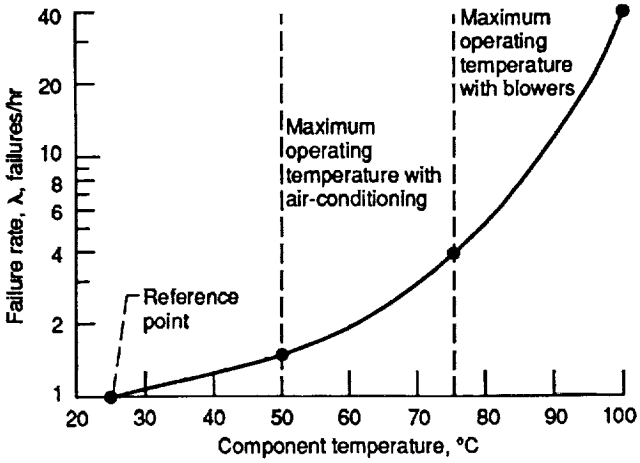


Figure 3.—Predicted failure rate ratios versus temperature for ground support equipment (electronics).

is the required failure rate. If blowers are used for cooling, the equipment must operate at temperatures as high as 75 °C; if air-conditioning is used, the temperature need not exceed 50 °C. Therefore, air-conditioning must be used if we are to meet the reliability requirement.

Other factors must be examined before we make a final decision. Whatever type of cooling equipment is selected, the total system reliability now becomes

$$R_T = R_s R_c$$

Therefore, the effect on the system of the cooling equipment's reliability must be calculated. A more important consideration is the effect on system reliability should the cooling equipment fail. Because temperature control appears to be critical, loss of it may have serious system consequences. Therefore, it is too soon to rule out blowers entirely. A failure mode, effects, and criticality analysis (FMECA) must be made on both cooling methods to examine all possible failure modes and their effects on the system. Only then will we have sufficient information to make a sound decision.

2.7 Importance of Learning From Each Failure

When a product fails, a valuable piece of information about it has been generated because we have the opportunity to learn how to improve the product if we take the right actions.

Failures can be classified as:

(1) Catastrophic (a shorted transistor or an open wire-wound resistor)
(2) Degradation (change in transistor gain or the resistor value)
(3) Wearout (brush wear in an electric motor)

These three failure categories can be subclassified further:

(1) Independent (a shorted capacitor in a radiofrequency amplifier being unrelated to a low-emission cathode in a picture tube)
(2) Cascade (the shorted capacitor in the radiofrequency amplifier causing excessive current to flow in its transistor and burning the collector beam lead open)
(3) Common mode (uncured resin being present in motors)

Much can be learned from each failure by using these categories, good failure reporting, analysis, and a concurrence system and by taking corrective action. Failure analysis determines what caused the part to fail. Correc-

tive action ensures that the cause is dealt with. Concurrence informs management of actions being taken to avoid another failure. These data enable all personnel to compare the part ratings with the use stresses and verify that the part is being used with a known margin.

2.8 Effects of Tolerance on a Product

Because tolerances must be expected in all manufacturing processes, some important questions to ask about the affects of tolerance on a product are

(1) How is the reliability affected?

(2) How can tolerances be analyzed and what methods are available?

(3) What will affect the term P_t in the product reliability model?

Electrical circuits are often affected by part tolerances (circuit gains can shift up or down, and transfer function poles or zeros can shift into the righthand s-plane, causing oscillations). Mechanical components may not fit together or may be so loose that excessive vibration causes trouble (refs. 1 to 3).

3.0 TESTING FOR RELIABILITY

3.1 Test Objectives

It can be inferred that 1000 test samples are required to demonstrate a reliability requirement of 0.999. Because of cost and time, this approach is impractical. Furthermore, the total production of a product often may not even approach 1000 items. Because we usually cannot test the total production of a product (called product population), we must demonstrate reliability on a few samples. Thus, the main objective of a reliability test is to test an available device so that the data will allow a statistical conclusion to be reached about the reliability of similar devices that will not or cannot be tested. That is, the main objective of a reliability test is not only to evaluate the specific items tested but also to provide a sound basis for predicting the reliability of similar items that will not be tested and that often have not yet been manufactured.

To know how reliable a product is one must know how many ways it can fail and the types and magnitudes of the stresses that produce such failures. This premise leads to a secondary objective of a reliability test: to produce failures in the product so that the types and magnitudes of the stresses causing such failures can be identified. Reliability tests that result in no failures provide some measure of reliability but little information about the population failure mechanisms of like devices. (The exceptions to this are not dealt with at this time.)

In subsequent sections, we discuss confidence levels, attribute test, test-to-failure, and life test methods, explain how well these methods meet the two test objectives, show how the test results can be statistically analyzed, and introduce the subject and use of confidence limits.

3.2 Confidence Levels

Mr. Igor Bazovsky, in his book, Reliability Theory and Practice (ref. 4), defines the term "confidence" in testing:

> **We know that statistical estimates are more likely to be close to the true value as the sample size increases. Thus, there is a close correlation between the accuracy of an estimate and the size of the sample from which it was obtained. Only an infinitely large sample size could give us a 100 percent confidence or certainty that a measured statistical parameter coincides with the true value. In this context, confidence is a mathematical probability relating the mutual positions of the true value of a parameter and its estimate.**
>
> **When the estimate of a parameter is obtained from a reasonably sized sample, we may logically assume that the true value of that parameter will be somewhere in the neighborhood of the estimate, to the right or to the left. Therefore, it would be more meaningful to express statistical estimates in terms of a range or interval with an associated probability or confidence that the true value lies within such interval than to express them as point estimates. This is exactly what we are doing when we assign confidence limits to point estimates obtained from statistical measurements.**

In other words, rather than express statistical estimates as point estimates, it would be more meaningful to express them as a range (or interval), with an associated probability (or confidence) that the true value lies within such an interval. Confidence is a statistical term that depends on supporting data and reflects the amount of risk to be taken when stating the reliability.

3.3 Attribute Test Methods

Qualification, preflight certification, and design verification tests are categorized as attribute tests (refs. 5 and 6). They are usually go/no-go and demonstrate that a device is good or bad without showing how good or how bad. In a typical test, two samples are subjected to a selected level of environmental stress, usually the maximum anticipated operational limit. If both samples pass, the device is considered qualified, preflight certified, or verified for use in the particular environment involved (refs. 7 and 8). Occasionally, such tests are called tests to

success because the true objective is to have the device pass the test.

In summary, an attribute test is not a satisfactory method of testing for reliability because it can only identify gross design and manufacturing problems; it is an adequate method of testing for reliability only when sufficient samples are tested to establish an acceptable level of statistical confidence.

3.4 Test-To-Failure Methods

The purpose of the test-to-failure method is to develop a failure distribution for a product under one or more types of stress. The results are used to calculate the demonstrated reliability of the device for each stress. In this case the demonstrated population reliability will usually be the P_t or P_w product reliability term.

In this discussion of test-to-failure methods, the term "safety factor" S_F is included because it is often confused with safety margin S_M. Safety factor is widely used in industry to describe the assurance against failure that is built into structural products. Of the many definitions of safety factor the most commonly used is the ratio of mean strength to reliability boundary:

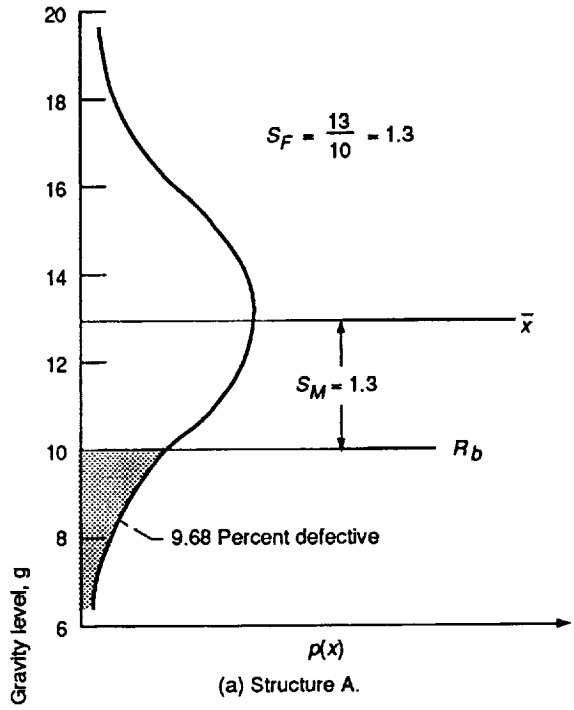
$$S_F = \frac{\bar{x}_s}{R_b}$$

When we deal with materials with clearly defined, repeatable, and "tight" strength distributions, such as sheet and structural steel or aluminum, using S_F presents little risk. However, when we deal with plastics, fiberglass, and other metal substitutes or processes with wide variations in strength or repeatability, using S_M provides a clearer picture of what is happening (fig. 4). In most cases, we must know the safety margin to understand how accurate the safety factor may be.

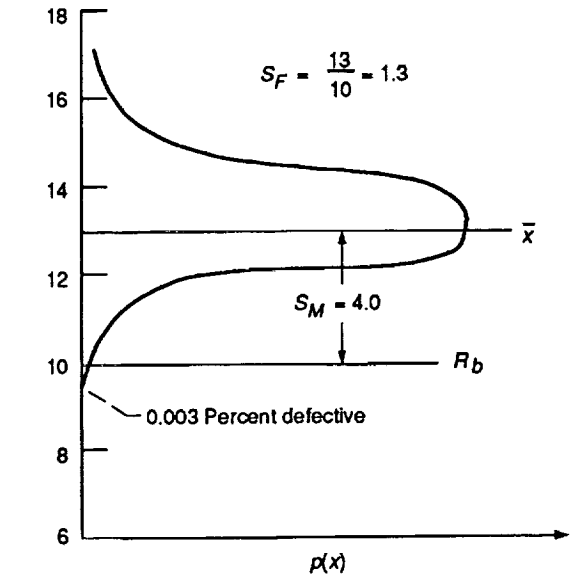
In summary, test-to-failure methods can be used to develop a strength distribution that provides a good estimate of the P_t and P_w product reliability terms without the need for the large samples required for attribute tests; the results of a test-to-failure exposure of a device can be used to predict the reliability of similar devices that cannot or will not be tested; testing to failure provides a means of evaluating the failure modes and mechanisms of devices so that improvements can be made; confidence levels can be applied to the safety margins and to the resulting population reliability estimates; the accuracy of a safety factor can be known only if the associated safety margin is known.

3.5 Life Test Methods

Life tests are conducted to illustrate how the failure rate of a typical system or complex subsystem varies during its operating life. Such data provide valuable guidelines for controlling product reliability. They help to establish burn-in requirements, to predict spare part requirements, and to understand the need for or lack of need for a system overhaul program. Such data are obtained through laboratory life tests or from the normal operation of a fielded system.



(a) Structure A.



(b) Structure B.

Figure 4.—Two structures with identical safety factors (S_F = 13/10 = 1.3) but different safety margins.

In summary, life tests are performed to evaluate product failure rate characteristics; if failures include all causes of system failure, the failure rate of the system is the only true factor available for evaluating the system's performance; life tests at the part level require large sample sizes if realistic failure rate characteristics are to be identified; laboratory life tests must simulate the major factors that influence failure rates in a device during field operations; the use of running averages in the analysis of life data will identify burn-in and wearout regions if such exist; and failure rates are statistics and therefore are subject to confidence levels when used in making predictions.

Figure 5 illustrates what might be called a failure surface for a typical product. It shows system failure rate versus operating time and environmental stress, three parameters that describe a surface such that, given an environmental stress and an operating time, the failure rate is a point on the surface.

Test-to-failure methods generate lines on the surface parallel to the stress axis; life tests generate lines on the surface parallel to the time axis. Therefore, these tests provide a good description of the failure surface and, consequently, the reliability of a product.

Attribute tests result only in a point on the surface if failures occur and a point somewhere within the volume if failures do not occur. For this reason, attribute testing is the least desirable method for ascertaining reliability.

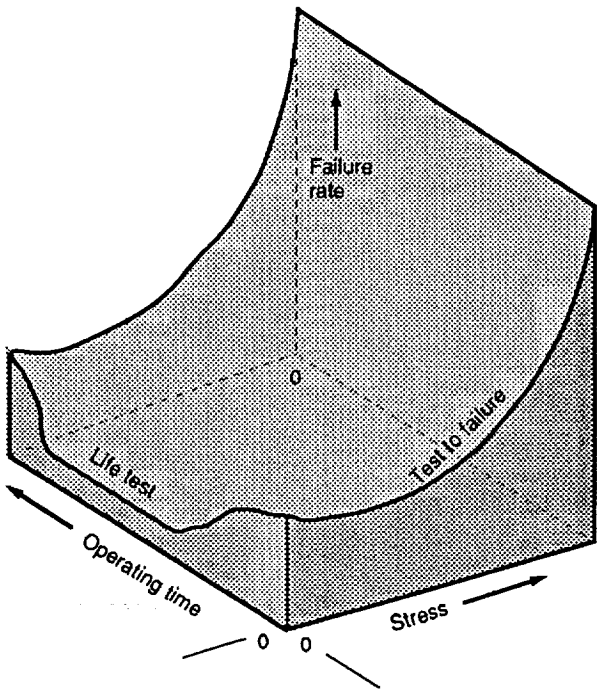


Figure 5.—Product failure surface.

Of course, in the case of missile flights or other events that produce go/no-go results, an attribute analysis is the only way to determine product reliability.

4.0 SOFTWARE RELIABILITY

Software reliability management is highly dependent on how the relationship between quality and reliability is perceived. For the purposes of this tutorial, quality is closely related to the process, and reliability is closely related to the product. Thus, both span the life cycle.

Before we can stratify software reliability, the progress of hardware reliability will be reviewed. Over the past 25 years, the industry observed (1) the initial assignment of "wizard status" to hardware reliability for theory, modeling, and analysis, (2) the growth of the field, and (3) the final establishment of hardware reliability as a science. One of the major problems was aligning reliability predictions and field performance. Once that was accomplished, the wizard status was removed from hardware reliability. The emphasis in hardware reliability from now to the year 2000 will be on system failure modes and effects.

Software reliability became classified as a science for many reasons. The difficulty in assessing software reliability is analogous to the problem of assessing the reliability of a new hardware device with unknown reliability characteristics. The existence of 30 to 50 different software reliability models indicates the organization in this area. Hardware reliability began at a few companies and later became the focus of the Advisory Group on Reliability of Electronic Equipment. The field then logically progressed through different models in sequence over the years. Similarly, numerous people and companies simultaneously entered the software reliability field in their major areas: cost, complexity, and reliability. The difference is that at least 100 times as many people are now studying software reliability as those who initially studied hardware reliability. The existence of so many models and their purports tends to mask the fact that several of these models showed excellent correlations between software performance predictions and actual software field performance: the Musa model as applied to communications systems and the Xerox model as applied to office copiers. There are also reasons for not accepting software reliability as a science, and they are discussed next.

One impediment to the establishment of software reliability as a science is the tendency toward programming development philosophies such as (1) "do it right the first time" (a reliability model is not needed) or (2) "quality is a programmer's development tool," or

(3) "quality is the same as reliability and is measured by the number of defects in a program and not by its reliability." All of these philosophies tend to eliminate probabilistic measures because the managers consider a programmer to be a software factory whose quality output is controllable, adjustable, or both. In actuality, hardware design can be controlled for reliability characteristics better than software design can. Design philosophy experiments that failed to enhance hardware reliability are again being formulated for software design (ref. 9). Quality and reliability are not the same. Quality is characteristic and reliability is probabilistic. Our approach draws the line between quality and reliability because quality is concerned with the development process and reliability is concerned with the operating product. Many models have been developed and a number of the measurement models show great promise. Predictive models have been far less successful partly because a data base (such as MIL-HDBK-217E, ref. 10) is not yet available for software. Software reliability often has to use other methods; it must be concerned with the process of software product development.

4.1 Hardware and Software Failures

Microprocessor-based products have more refined definitions. Four types of failure may be considered (1) hardware catastrophic, (2) hardware transient, (3) software catastrophic, and (4) software transient. In general, the catastrophic failures require a physical or remote hardware replacement, a manual or remote unit restart, or a software program patch. The transient failure categories can result in either restarts or reloads for the microprocessor-based systems, subsystems, or individual units and may or may not require further correction. A recent reliability analysis of such a system assigned ratios for these categories. Hardware transient faults were assumed to occur at 10 times the hardware catastrophic rate, and software transient faults were assumed to occur at 100 to 500 times the software catastrophic rate.

The time of day is of great concern in reliability modeling and analysis. Although hardware catastrophic failures occur at any time of the day, they often manifest themselves during busier system processing times. On the other hand, hardware and software transient failures generally occur during the busy hours. When a system's predicted reliability is close to the specified reliability, a sensitivity analysis must be performed.

4.2 Manifestations of Software Bugs

Many theories, models, and methods are available for quantifying software reliability. Nathan (ref. 11) stated, "It is contrary to the definition of reliability to apply reliability analysis to a system that never really works. This means that the software which still has bugs in it really has never worked in the true sense of reliability in the hardware sense." Large complex software programs used in the communications industry are usually operating with some software bugs. Thus, a reliability analysis of such software is different from a reliability analysis of established hardware. Software reliability is not alone in the need for establishing qualitative and quantitative models.

In the early 1980's, work was done on a combined hardware/software reliability model. A theory for combining well-known hardware and software models in a Markov process was developed. A consideration was the topic of software bugs and errors based on experience in the telecommunications field. To synthesize the manifestations of software bugs, some of the following hardware trends for these systems should be noted: (1) hardware transient failures increase as integrated circuits become denser; (2) hardware transient failures tend to remain constant or increase slightly with time after the burn-in; and (3) hardware (integrated circuit) catastrophic failures decrease with time after the burn-in phase. These trends affect the operational software of communications systems. If the transient failures increase, the error analysis and system security software are called into action more often. This increases the risk of misprocessing a given transaction in the communications system. A decrease in the catastrophic failure rate of integrated circuits can be significant (ref. 12). An order-of-magnitude decrease in the failure rate of 4K memory devices between the first year and the twentieth year is predicted. We also tend to oversimplify the actual situations. Even with five vendors of these 4K devices, the manufacturing quality control person may have to set up different screens to eliminate the defective devices from different vendors. Thus, the system software will see many different transient memory problems and combinations of them in operation.

Central control technology has prevailed in communications systems for 25 years. The industry has used many of its old modeling tools and applied them directly to distributed control structures. Most modeling research was performed on large duplex processors. With an evolution through forms of multiple duplex processors and load-sharing processors and on to the present forms of distributed processing architectures, the modeling tools need to be verified. With fully distributed control systems, the software reliability model must be conceptually matched to the software design in order to achieve valid predictions of reliability.

The following trends can be formulated for software transient failures: (1) software transient failures decrease

as the system architecture approaches a fully distributed control structure, and (2) software transient failures increase as the processing window decreases (i.e., less time allowed per function, fast timing mode entry, removal of error checking, removal of system ready checks).

A fully distributed control structure can be configured to operate as its own error filter. In a hierarchy of processing levels, each level acts as a barrier to the level below and prevents errors or transient faults from propagating through the system. Central control structures cannot usually prevent this type of error propagation.

If the interleaving of transaction processes in a software program is reduced, such as with a fully distributed control architecture, the transaction processes are less likely to fail. This is especially true with nonconsistent user interaction as experienced in communications systems. Another opinion on software transient failures is that the faster a software program runs, the more likely it is to cause errors (such as encountered in central control architectures).

A "missing link" needs further discussion. Several methods can be used to quantify the occurrence of software bugs. However, manifestations in the system's operations are detrimental to the reliability analysis because each manifestation could cause a failure event. The key is to categorize levels of criticality for bug manifestations and estimate their probability of occurrence and their respective distributions. The importance of this increases with the distribution of the hardware and software. Software reliability is often controlled by establishing a software reliability design process. The final measure is the system test, which includes the evaluation of priority problems and the performance of the system while under stress as defined by audits, interrupts, re-initialization, and other measurable parameters. The missing link in quantifying software bug manifestations needs to be found before we can obtain an accurate software reliability model for measuring tradeoffs in the design process on a predicted performance basis. If a software reliability modeling tool could additionally combine the effects of hardware, software, and operator faults, it would be a powerful tool for making design tradeoff decisions. Table I, an example of the missing link, presents a five-level criticality index for defects. These examples indicate the flexibility of such an approach to criticality classification.

We can choose a decreasing, constant, or increasing software bug removal rate for systems software. Although each has its application to special situations and systems, a decreasing software bug removal rate will generally be encountered. Systems software also has advantages in that certain software defects can be temporarily patched and the permanent patch postponed to a more appropriate date. Thus, this type of defect manifestation is treated in general as one that does not affect service, but it should be included in the overall software quality assessment. The missing link concerns software bug manifestations. Until the traditional separation of hardware and software systems is overcome in the design of large systems, it will be impossible to achieve a satisfactory performance benchmark. This indicates that software performance modeling has not yet focused on the specific causes of software unreliability.

4.3 Concept of Quality

Consider the concept of quality before we go on to software quality. The need for quality is universal. The concepts of "zero defects" and "doing it right the first time" have changed our perspective on quality management. We changed from measuring defects per unit and acceptable quality levels to monitoring the design and cost reduction processes. The present concepts indicate that quality is not free. One viewpoint is that a major improvement in quality can be achieved by perfecting the process of developing a product. Thus, we would characterize the process, implement factors to achieve customer satisfaction, correct defects as soon as possible, and then strive for total quality management. The key to achieving

TABLE I.—CRITICALITY INDEX

Bug manifestation rate	Defect removal rate	Level of criticality	Failure type	Failure characteristic
4 per day	1 per month	5	Transient	Errors come and go
3 per day	1 per week	4	Transient	Errors are repeated
2 per week	1 per month	3	Transient or catastrophic	Service is affected
1 per month	2 per year	2	Transient or catastrophic	System is partially down
1 per two years	1 per year	1	Catastrophic	System stops

quality appears to have a third major factor in addition to product and process: the environment. People are important. They make the process or the product successful.

The next step is to discuss what the process of achieving quality in software consists of and how quality management is involved. The purpose of quality management for programming products is to ensure that a preselected software quality level has been achieved on schedule and in a cost-effective manner. In developing a quality management system, the programming product's critical life-cycle-phase reviews provide the reference base for tracking the achievement of quality objectives. The International Electrotechnical Commission (IEC) system life-cycle phases presented in their guidelines for reliability and maintainability management are (1) concept and definition, (2) design and development, (3) manufacturing, installation, and acceptance, (4) operation and maintenance, and (5) disposal.

In general, a phase-cost study shows the increasing cost of correcting programming defects in later phases of a programming product's life. Also, the higher the level of software quality, the more life-cycle costs are reduced.

4.4 Software Quality

The next step is to look at specific software quality items. Software quality is defined as "the achievement of a preselected software quality level within the costs, schedule, and productivity boundaries established by management" (ref. 10). However, agreement on such a definition is often difficult to achieve because metrics vary more than those for hardware, software reliability management has focused on the product, and software quality management has focused on the process. In practice, the quality emphasis can change with respect to the specific product application environment. Different perspectives of software product quality have been presented over the years. However, in todays' literature there is general agreement that the proper quality level for a particular software product should be determined in the concept and definition phase and that quality managers should monitor the project during the remaining life-cycle phases to ensure the proper quality level.

The developer of a methodology for assessing the quality of a software product must respond to the specific characteristics of the product. There can be no single quality metric. The process of assessing the quality of a software product begins with the selection of specific characteristics, quality metrics, and performance criteria.

With respect to software quality, several areas of interest are (1) characteristics, (2) metrics, (3) overall metrics, and (4) standards. Areas (1) and (2) are applicable during both the design and development phase and the operation and maintenance phase. In general, area (2) is used during the design and development phase before the acceptance phase for a given software product. The following discussion will concern area (2).

4.5 Software Quality Metrics

The entire area of software measurements and metrics has been widely discussed and the subject of many publications. Notable is the guide for software reliability measurement developed by the Institute for Electrical and Electronics Engineers (IEEE) Computer Society's working group on metrics. A basis for software quality standardization was also issued by the IEEE. Software metrics cannot be developed before the cause and effect of a defect have been established for a given product with relation to its product life cycle. A typical cause-and-effect chart for a software product includes the process indicator. At the testing stage of product development, the evolution of software quality levels can be assessed by characteristics such as freedom from error, successful test case completion, and estimate of the software bugs remaining. For example, these process indicators can be used to predict slippage of the product delivery date and the inability to meet original design goals.

When the programming product enters the qualification, installation, and acceptance phase and continues into the maintenance and enhancements phase, the concept of performance is important in the quality characteristic activity. This concept is shown in table II where the 5 IEC system life-cycle phases have been expanded to 10 software life-cycle phases.

4.6 Concluding Remarks

This section presented a snapshot of software quality assurance today. Continuing research is concerned with the use of overall software quality metrics and better software prediction tools for determining the defect population. In addition, simulators and code generators are being further developed so that high-quality software can be produced.

Process indicators are closely related to software quality and some include them as a stage in software development. In general, such measures as (1) test cases completed versus test cases planned and (2) the number of lines of code developed versus the number expected give an indication of the overall company or corporate progress toward a quality software product. Too often,

TABLE II.—MEASUREMENTS AND PROGRAMMING PRODUCT LIFE CYCLE

[The 5 International Electrotechnical Commission (IEC) life-cycle phases have been expanded to 10 software phases.]

System life-cycle phase	Software life-cycle phase	Order of precedence	
		Primary	Secondary
Concept and definition	Conceptual planning (1) Requirements definition (2) Product definition (3)	---------- ---------- Quality metrics[a]	---------- ---------- ----------
Design and development	Top-level design (4) Detailed design (5) Implementation (6)	Quality metrics Quality metrics Process indicators[b]	Process indicators Process indicators Quality metrics
Manufacturing and installation	Testing and integration (7) Qualification, installation, and acceptance (8)	Process indicators Performance measures[c]	Performance measures Quality metrics
Operation and maintenance	Maintenance and enhancements (9)	Performance measures	----------
Disposal	Disposal (10)	----------	----------

[a]Metrics, qualitative assessment, quantitative prediction, or both.
[b]Indicators, month-by-month tracking of key project parameters.
[c]Measures, quantitative performance assessment.

personnel are moved from one project to another and thus the lagging projects improve but the leading projects decline in their process indicators. The life cycle for programming products should not be disrupted.

Performance measures, including such criteria as the percentage of proper transactions, the number of system restarts, the number of system reloads, and the percentage of uptime, should reflect the user's viewpoint.

In general, the determination of applicable quality measures for a given software product development is viewed as a specific task of the software quality assurance function. The determination of the process indicators and performance measures is a task of the software quality standards function.

5.0 RELIABILITY MANAGEMENT

To design for successful reliability and continue to provide customers with a reliable product, the following steps are necessary:

(1) Determine the reliability goals to be met.

(2) Construct a symbolic representation.

(3) Determine the logistics support and repair philosophy.

(4) Select the reliability analysis procedure.

(5) Select the data sources for failure rates and repair rates.

(6) Determine the failure rates and the repair rates.

(7) Perform the necessary calculations.

(8) Validate and verify the reliability.

(9) Measure reliability until customer shipment.

5.1 Goals and Objectives

Goals must be placed into the proper perspective. Because they are often examined by using models that the producer develops, one of the weakest links in the reliability process is the modeling. Dr. John D. Spragins, an editor for the IEEE Transaction on Computers, corroborates this fact with the following statement (ref. 13):

> Some standard definitions of reliability or availability, such as those based on the probability that all components of a system are operational at a given time, can be dismissed as irrelevant when studying large telecommunication networks. Many telecommunication networks are so large that the probability they are operational according to this criterion may be very nearly zero; at least one item of equipment may be down essentially all of the time. The typical user, however, does not see this unless he or she happens to

be the unlucky person whose equipment fails; the system may still operate perfectly from this user's point of view. A more meaningful criterion is one based on the reliability seen by typical system users. The reliability apparent to system operators is another valid, but distinct, criterion. (Since system operators commonly consider systems down only after failures have been reported to them, and may not hear of short self-clearing outages, their estimates of reliability are often higher than the values seen by users.)

Reliability objectives can be defined differently for various systems. An example from the telecommunications industry (ref. 14) is presented in table III.

5.2 Specification Targets

A system can have a detailed performance or reliability specification that is based on customer requirements. The survivability of a telecommunications network is defined as the ability of the network to perform under stress caused by cable cuts or sudden and lengthy traffic overloads and after failures including equipment breakdowns. Thus, performance and availability have been combined into a unified metric. One area of telecommunications where these principles have been applied is the design and implementation of fiber-based networks. Roohy-Laleh et al. (ref. 15) state "...the statistical observation that on the average 56 percent of the pairs in a copper cable are cut when the cable is dug up, makes the copper network 'structurally survivable.'" On the other hand, a fiber network can be assumed to be an all or nothing situation with 100 percent of the circuits being affected by a cable cut, failure, etc. In this case study (ref. 15), "...cross connects and allocatable capacity are utilized by the intelligent network operation system to dynamically reconfigure the network in the case of failures." Figure 6 (from ref. 16) presents a concept for specification targets.

TABLE III.—RELIABILITY OBJECTIVES FOR TELECOMMUNICATIONS INDUSTRY

Module or system	Objective
Telephone instrument	Mean time between failures
Electronic key system	Complete loss of service
	Major loss of service
	Minor loss of service
PABX	Complete loss of service
	Major loss of service
	Minor loss of service
	Mishandled calls
Traffic service position system (TSPS)	Mishandled calls
	System outage
Class 5 office	System outage
Class 4 office	Loss of service
Class 3 office	Service degradation

5.3 Human Reliability

The major objectives of reliability management are to ensure that a selected reliability level for a product can be achieved on schedule in a cost-effective manner and that the customer perceives the selected reliability level. The current emphasis in reliability management is on meeting or exceeding customer expectations. We can view this as a challenge, but it should be viewed as the bridge between the user and the producer or provider. This bridge is actually "human reliability." In the past, the producer was concerned with the process and the product and found reliability measurements that addressed both. Often there was no correlation between field data, the customer's perception of reliability, and the producer's reliability metrics. Surveys then began to indicate that the customer distinguished between reliability performance, response to order placement, technical support, service quality, etc.

Human reliability is defined (ref. 17) as "...the probability of accomplishing a job or task successfully by humans at any required stage in system operations within a specified minimum time limit (if the time requirement is specified)." Although customers generally are not yet requiring human reliability models in addition to the requested hardware and software reliability models, the science of human reliability is well established.

5.4 Customer

Reliability growth has been studied, modeled, and analyzed—usually from the design and development viewpoint. Seldom is the process or product studied from the customer's perspective. Furthermore, the reliability that the first customer observes with the first shipment

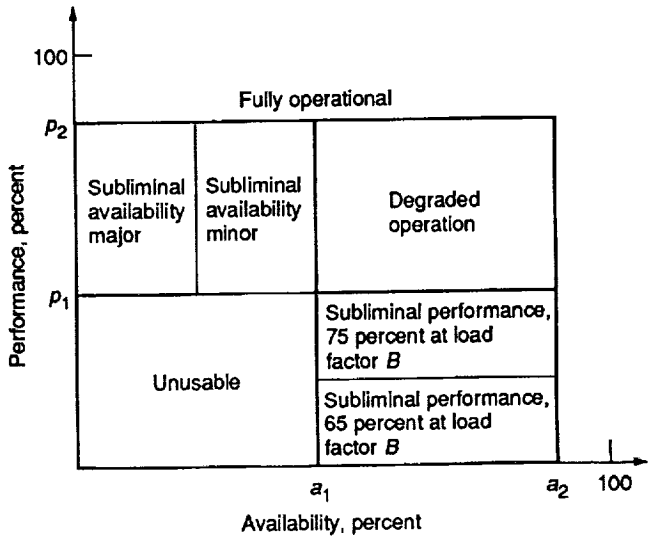


Figure 6.—Specification targets (ref. 16).

can be quite different from the reliability that a customer will observe with a unit or system produced 5 years later, or with the last shipment. Because the customer's experience can vary with the maturity of a system, reliability growth is an important concept to customers and should be considered in their purchasing decisions.

One key to reliability growth is the ability to define the goals for the product or service from the customer's perspective while reflecting the actual situation in which the customer obtains the product or service. For large telecommunications switching systems, the rule of thumb for determining reliability growth has been that often systems have been allowed to operate at a lower availability than the specified availability goal for the first 6 months to 1 year of operation (ref. 18). In addition, component part replacement rates have often been allowed to be 50 percent higher than specified for the first 6 months of operation. These allowances accommodated craftspersons learning patterns, software patches, design errors, etc.

Another key to reliability growth is to have its measurement encompass the entire life cycle of the product. The concept is not new; only here the emphasis is placed on the customer's perspective.

Reliability growth can be specified from "day 1" in product development and can be measured or controlled with a 10-year life until "day 5000." We can apply the philosophy of reliability knowledge generation principles, which is to generate reliability knowledge at the earliest possible time in the planning process and to add to this base for the duration of the product's useful life. To accurately measure and control reliability growth, we must examine the entire manufacturing life cycle. One method is the construction of a production life-cycle reliability growth chart.

In certain large telecommunications systems, the long installation time allows the electronic part reliability to grow so that the customer observes both the design and the production growth. Large complex systems often offer an environment unique to each product installation, which dictates that a significant reliability growth will occur. Yet, with the difference that size and complexity impose on resultant product reliability growth, corporations with large product lines should not present overall reliability growth curves on a corporate basis but must present individual product-line reliability growth pictures to achieve total customer satisfaction.

APPENDIX—COURSE EVALUATION

NASA SAFETY TRAINING CENTER (NSTC) COURSE EVALUATION

Name:	Course Title:	
Sponsor:	Grade: (academic course only)	Date:

1. What were the strengths of this course/workshop?

2. What were the weaknesses of this course/workshop?

3. How will the skills/knowledge you gained in this course/workshop help you to perform better in your job?

4. Please give the course/workshop an overall rating.

5	4	3	2	1
Excellent		Fair		Poor

5. Please give the instructor an overall rating.

5	4	3	2	1
Excellent		Fair		Poor

6. Please rate the applicability of this course to your work.

5	4	3	2	1
Excellent		Fair		Poor

(OVER)

7. As a customer of the NASA Safety Training Center (NSTC), how would you rate our services?

5	4	3	2	1
Excellent		Fair		Poor

Comments:

8. Please rate the following items:

	Excellent		Fair		Poor
1. Overall course content	5	4	3	2	1
2. Achievement of course objectives	5	4	3	2	1
3. Instructor's knowledge of subject	5	4	3	2	1
4. Instructor's presentation methods	5	4	3	2	1
5. Instructor's ability to address questions	5	4	3	2	1
6. Quality of textbook/workbook (if applicable)	5	4	3	2	1
7. Training facilities	5	4	3	2	1
8. Time allotted for the course	5	4	3	2	1

Comments:

9. Training expense other than tuition (if applicable):

Travel (including plane fare, taxi, car rental and tolls) _____

Per Diem _____

Total _____

10. Please send this evaluation to:

NASA Safety Training Center
Webb, Murray & Associates, Inc.
1730 NASA Road One, Suite 102
Houston, Texas 77058

THANK YOU!

REFERENCES

1. Reliability Prediction of Electronic Equipment. MIL–HDBK–217E, Jan. 1990.

2. Electronic Reliability Design Handbook. MIL–HDBK–338, vols. 1 and 2, Oct. 1988.

3. Reliability Modeling and Prediction. MIL–STD–756B, Aug. 1982.

4. Bazovsky, I.: Reliability Theory and Practice. Prentice-Hall, 1963.

5. Reliability Test Methods, Plans, and Environments for Engineering Development, Qualification, and Production. MIL–HDBK–781, July 1987.

6. Laubach, C.H.: Environmental Acceptance Testing. NASA SP–T–0023, 1975.

7. Laube, R.B.: Methods to Assess the Success of Test Programs. J. Environ. Sci., vol. 26, no. 2, Mar.-Apr. 1983, pp. 54–58.

8. Test Requirements for Space Vehicles. MIL–STD–1540B, Oct. 1982.

9. Siewiorek, D.P.; and Swarz, R.S.: The Theory and Practice of Reliable System Design. Digital Press, Bedford, MA, 1982, pp. 206–211.

10. Reliability Prediction of Electronic Equipment, MIL–HDBK–217E, Jan. 1990.

11. Nathan, I.: A Deterministic Model To Predict 'Error-Free' Status of Complex Software Development. Workshop on Quantitative Software Models, IEEE, New York, 1979.

12. Schick, G.J.; and Wolverton, R.W.: An Analysis of Computing Software Reliability Models. IEEE Trans. Software Eng., vol. SE–4, no. 2, Mar. 1978, pp. 104–120.

13. Spragins, J.D., et al.: Current Telecommunication Network Reliability Models: A Critical Assessment, IEEE J. Sel. Topics Commun., vol. SAC–4, no. 7, Oct. 1986, pp. 1168–1173.

14. Malec, H.A.: Reliability Optimization in Telephone Switching Systems Design. IEEE Trans. Rel., vol. R–26, no. 3, Aug. 1977, pp. 203–208.

15. Roohy-Laleh, E., et al.: A Procedure for Designing a Low Connected Survivable Fiber Network. IEEE J. Sel. Topics Commun., vol. SAC–4, no. 7, Oct. 1986, pp. 1112–1117.

16. Jones, D.R.; and Malec, H.A.: Communications Systems Performability: New Horizons. 1989 IEEE International Conference on Communications, vol. 1, IEEE, 1989, pp. 1.4.1–1.4.9.

17. Dhillon, B.S.: Human Reliability: With Human Factors. Pergamon Press, 1986.

18. Conroy, R.A.; Malec, H.A.; and Van Goethem, J.: The Design, Applications, and Performance of the System–12 Distributed Computer Architecture. First International Conference on Computers and Applications, E.A. Parrish and S. Jiang, eds., IEEE, 1984, pp. 186–195.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	October 1994	Technical Memorandum

4. TITLE AND SUBTITLE

Design for Reliability:
NASA Reliability Preferred Practices for Design and Test

5. FUNDING NUMBERS

WU-323-44-19

6. AUTHOR(S)

Vincent R. Lalli

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Lewis Research Center
Cleveland, Ohio 44135-3191

8. PERFORMING ORGANIZATION REPORT NUMBER

E-8053

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, D.C. 20546-0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

NASA TM-106313

11. SUPPLEMENTARY NOTES

Prepared for the Reliability and Maintainability Symposium cosponsored by ASQC, IIE, IEEE, SOLE, IES, AIAA, SSS, and SRE, Anaheim, California, January 24-27, 1994. Responsible person, Vincent R. Lalli, organization code 0152, (216) 433-2354.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Category 18

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

This tutorial summarizes reliability experience from both NASA and industry and reflects engineering practices that support current and future civil space programs. These practices were collected from various NASA field centers and were reviewed by a committee of senior technical representatives from the participating centers (members are listed at the end). The material for this tutorial was taken from the publication issued by the NASA Reliability and Maintainability Steering Committee (NASA Reliability Preferred Practices for Design and Test. NASA TM-4322, 1991). Reliability must be an integral part of the systems engineering process. Although both disciplines must be weighted equally with other technical and programmatic demands, the application of sound reliability principles will be the key to the effectiveness and affordability of America's space program. Our space programs have shown that reliability efforts must focus on the design characteristics that affect the frequency of failure. Herein, we emphasize that these identified design characteristics must be controlled by applying conservative engineering principles.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Design; Test; Practices; Reliability; Training; Flight proven	27
	16. PRICE CODE: A03

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	