SECTION 3

RELIABILITY

Reliability of a component or a system can be considered a design parameter, but, in fact, the intrinsic design reliability may not be realized because of manufacturing defects or misapplication. Thus, the definition of reliability is the probability that a device or system will perform a specified function for a specified period of time under a specific set of conditions. The conditions may also include required maintenance procedures. The first chapter in this section expands on the definitional issues of reliability, including parts and systems modeling, reliability theory and practice, and failure analysis and prediction techniques. Chapter 3.2 discusses very high reliability techniques developed for military and aerospace applications. The special issues involved in semiconductor component reliability are covered in Chap. 3.3.

In a completely new chapter (3.4) the exceptional considerations needed in predicting reliability when using electromechanical and microelectromechanical devices are treated. Although many of the stress-strength relationships applicable to conventional electromechanical components apply to microelectro-mechanical devices, too, differences in the reliability of microelectromechanial systems (MEMS) that may be related to materials, geometries, and failure mechanisms are still under study. Thus far there is a limited amount of parts failure data available; it will be augmented as MEMS technologies mature and as the application of MEMS broadens. Additional material related to this chapter is included on the accompanying CD-ROM.

The design and modeling of electronic systems is covered in greater detail in Chap. 3.5. Finally, in another completely new chapter (3.6), the special concerns of designing software and assuring its reliability are treated. Because military specifications and standards underlie the reliable design and operation of many electronic systems, a summary description of important military reliability documents is included on the CD-ROM. D.C.

In This Section:

On the CD-ROM:

- *Reliability Standards and Handbooks*. A brief description of 8 MIL handbooks and 12 standards that cover sampling procedures, reliability growth, reliability prediction, reliability/design thermal applications, electrostatic discharge, stress screening, definition of terms, reliability modeling, design qualification, test methods, reliability of space and missile systems, FMECA techniques, failure reporting, analysis, and corrective action.
- *Commonly Used Formulas*. Formulas and equations useful in electromechanical reliability analysis.
- Concepts and Principles useful in probabilistic stress and strength analysis of electromechanical components.

CHAPTER 3.1
RELIABILITY DESIGN AND ENGINEERING

Ronald T. Anderson, Richard L. Doyle, Stanislaw Kus, Henry C. Rickers, James W. Wilbur

RELIABILITY CONCEPTS AND DEFINITIONS

Intrinsic Reliability

The intrinsic reliability of a system, electronic or otherwise, is based on its fundamental design, but its reliability is often less than its intrinsic level owing to poor or faulty procedures at three subsequent stages: manufacture, operation, or maintenance.

Definitions

The definition of reliability involves four elements: *performance requirements, mission time, use conditions,* and *probability.* Although reliability has been variously described as "quality in the time dimension" and "system performance in the time dimension," a more specific definition is *the probability that an item will perform satisfactorily for a specified period of time under a stated set of use conditions.*

Failure rate, the measure of the number of malfunctions per unit of time, generally varies as a function of time. It is usually high but decreasing during its *early life*, or *infant-mortality* phase. It is relatively constant during its second phase, the *useful-life period.* In the third, *wear-out* or *end-of-life*, period the failure rate begins to climb because of the deterioration that results from physical or chemical reactions: oxidation, corrosion, wear, fatigue, shrinkage, metallic-ion migration, insulation breakdown, or, in the case of batteries, an inherent chemical reaction that goes to completion.

The failure rate of most interest is that which relates to the useful life period. During this time, reliability is described by the single-parameter exponential distribution

$$R(t) = e^{-\lambda t} \tag{1}$$

where $R(t)$ = probability that item will operate without failure for time t (usually expressed in hours) under stated operating conditions
e = base of natural logarithms = 2.7182
λ = item failure rate (usually expressed in failures per hour) = constant for any given set of stress, temperature, and quality level conditions

It is determined for parts and components from large-scale data-collection and/or test programs. When values of λ and t are inserted in Eq. (1), the *probability of success*, i.e., reliability, is obtained for that period of time.

The reciprocal of the failure rate $1/\lambda$ is defined as the *mean time between failures* (MTBF). The MTBF is a figure of merit by which one hardware item can be compared with another. It is a measure of the failure rate λ during the useful life period.

Reliability Degradation

Manufacturing Effects. To access the magnitude of the reliability degradation because of manufacturing, the impact of manufacturing processes (process-induced defects, efficiency of conventional manufacturing and quality-control inspection, and effectiveness of reliability screening techniques) must be evaluated. In addition to the latent defects attributable to purchased parts and materials, assembly errors can account for substantial degradation. Assembly errors can be caused by operator learning, motivational, or fatigue factors.

Manufacturing and quality-control inspections and tests are provided to minimize degradation from these sources and to eliminate obvious defects. A certain number of defective items escaping detection will be accepted and placed in field operation. More importantly, the identified defects may be over-shadowed by an unknown number of *latent defects*, which can result in failure under conditions of stress, usually during field operation. Factory screening tests are designed to apply a stress of given magnitude over a specified time to identify these kinds of defects, but screening tests are not 100 percent effective.

Operational Effects. Degradation in reliability also occurs as a result of system operation. Wear-out, with *aging* as the dominant failure mechanism, can shorten the useful life. Situations also occur in which a system may be called upon to operate beyond its design capabilities because of an unusual mission requirement or to meet a temporary but unforeseen requirement. These situations could have ill-effects on its constituent parts.

Operational abuses, e.g., rough handling, over stressing, extended duty cycles, or neglected maintenance, can contribute materially to reliability degradation, which eventually results in failure. The degradation can be a result of the interaction of personnel, machines, and environment. The translation of the factors which influence operational reliability degradation into corrective procedures requires a complete analysis of functions performed by personnel and machines plus fatigue and/or stress conditions which degrade operator performance.

Maintenance Effects. Degradation in inherent reliability can also occur as a result of maintenance activities. Excessive handling from frequent preventive maintenance or poorly executed corrective maintenance, e.g., installation errors, degrades system reliability. Several trends in system design have reduced the need to perform adjustments or make continual measurements to verify peak performance. Extensive replacement of analog by digital circuits, inclusion of more built-in test equipment, and use of fault-tolerant circuitry are representative of these trends.

These factors, along with greater awareness of the cost of maintenance, have improved ease of maintenance, bringing also increased system reliability. In spite of these trends, the maintenance technician remains a primary cause of reliability degradation. Reliability is affected by poorly trained, poorly supported, or poorly motivated maintenance technicians where maintenance tasks require careful assessment and quantification.

Reliability Growth

Reliability growth represents the action taken to move a hardware item toward its reliability potential, during development or subsequent manufacturing or operation. During early development, the achieved reliability of a newly fabricated item or an off-the-board prototype is much lower than its predicted reliability because of initial design and engineering deficiencies as well as manufacturing flaws. The reliability growth process, when formalized and applied as an engineering discipline, allows management to exercise control of, allocate resources to, and maintain visibility of, activities designed to achieve a mature system before full production or field use.

Reliability growth is an iterative test-fail-correct process with three essential elements: detection and analysis of hardware failures, feedback and redesign of problem areas, and implementation of corrective action and retest.

RELIABILITY DESIGN AND ENGINEERING

Glossary

Availability. The availability of an item, under the combined aspects of its reliability and maintenance, to perform its required function at a stated instant in time.

Burn-in. The operation of items before their ultimate application to stabilize their characteristics and identify early failures.

Defect. A characteristic that does not conform to applicable specification requirements and that adversely affects (or potentially could affect) the quality of a device.

Degradation. A gradual deterioration in performance as a function of time.

Derating. The intentional reduction of stress-strength ratio in the application of an item, usually for the purpose of reducing the occurrence of stress-related failures.

Downtime. The period of time during which an item is not in a condition to perform its intended function.

Effectiveness. The ability of the system or device to perform its function.

Engineering reliability. The science that takes into account those factors in the basic design that will assure a required level of reliability.

Failure. The inability (more precisely termination of the ability) of an item to perform its required function.

Failure analysis. The logical, systematic examination of an item or its diagram(s) to identify and analyze the probability, causes, and consequences of potential and real failures.

Failure, catastrophic. A failure that is both sudden and complete.

Failure mechanism. The physical, chemical, or other process resulting in a failure.

Failure mode. The effect by which a failure is observed, e.g., an open or short circuit.

Failure, random. A failure whose cause and/or mechanism makes its time of occurrence unpredictable but that is predictable in a probabilistic or statistical sense.

Failure rate. The number of failures of an item per unit measure of life (cycles, time, etc.); during the useful life period, the failure rate λ is considered constant.

Failure rate change ($\dot{\lambda}$). The change in failure rate of an item at a given point in its life; $\dot{\lambda}$ is zero for an exponential distribution (constant failure rate), but represents the slope of the failure rate curve for more complex reliability distributions.

Failure, wear-out. A failure that occurs as a result of deterioration processes or mechanical wear and whose probability of occurrence increases with time.

Hazard rate Z(t). At a given time, the rate of change of the number of items that have failed divided by the number of items surviving.

Maintainability. A characteristic of design and installation that is expressed as the probability that an item will be retained in, or restored to, a specified condition within a given time when the maintenance is performed in accordance with prescribed procedures and resources.

Mean maintenance time. The total preventive and corrective maintenance time divided by the number of preventive and corrective maintenance actions accomplished during the maintenance time.

Mean time between failures (MTBF). For a given interval, the total functioning life of a population of an item divided by the total number of failures in the population during the interval.

Mean time between maintenance (MTBM). The mean of the distribution of the time intervals between maintenance actions (preventive, corrective, or both).

Mean time to repair (MTTR). The total corrective-maintenance time divided by the total number of corrective-maintenance actions accomplished during the maintenance time.

Redundancy. In an item, the existence of more than one means of performing its function.

Redundancy, active. Redundancy in which all redundant items are operating simultaneously rather than being switched on when needed.

Redundancy, standby. Redundancy in which alternative means of performing the function are inoperative until needed and are switched on upon failure of the primary means of performing the function.

Reliability. The characteristic of an item expressed by the probability that it will perform a required function under stated conditions for a stated period of time.

Reliability, inherent. The potential reliability of an item present in its design.

Reliability, intrinsic. The probability that a device will perform its specified function, determined on the basis of a statistical analysis of the failure rates and other characteristics of the parts and components that constitute the device.

Screening. The process of performing 100 percent inspection on product lots and removing the defective units from the lots.

Screening test. A test or combination of tests intended to remove unsatisfactory items or those likely to exhibit early failures.

Step stress test. A test consisting of several stress levels applied sequentially for periods of equal duration to a sample. During each period, a stated stress level is applied, and the stress level is increased from one step the next.

Stress, component. The stresses on component parts during testing or use that affect the failure rate and hence the reliability of the parts. Voltage, power, temperature, and thermal environmental stress are included.

Test-to-failure. The practice of inducing increased electrical and mechanical stresses in order to determine the maximum capability. A device in conservative use will increase its life through the derating based on these tests.

Time, down (downtime). See downtime.

Time, mission. The part of uptime during which the item is performing its designated mission.

Time, up (uptime). The element of active time during which an item is alert, reacting, or performing a mission.

Uptime ratio. The quotient determined by dividing uptime by uptime plus downtime.

Wear-out. The process of attrition which results in an increased failure rate with increasing age (cycles, time, miles, events, and so forth, as applicable for the item).

RELIABILITY THEORY AND PRACTICE

Exponential Failure Model

The life-characteristic curve (Fig. 3.1.1) can be defined by three failure components that predominate during the three periods of an item's life. The shape of this curve suggests the usual term *bathtub curve.* The components are illustrated in terms of an *equipment failure rate.* The failure components include:

1. *Early failures* because of design and quality-related manufacturing, which have a decreasing failure rate.
2. *Stress-related failures* because of application stresses, which have a constant failure rate.
3. *Wear-out failures* because of aging and/or deterioration, which have an increasing failure rate.

From Fig. 3.1.1 three conclusions can be drawn: (1) that the *infant-mortality* period is characterized by a high but rapidly decreasing failure rate that comprises a high quality-failure component, a constant-stress-related failure component, and a low wear-out-failure component. (2) The *useful-life* period is characterized by a constant failure rate comprising a low (and decreasing) quality-failure component, a constant stress-related-failure component, and a low (but increasing) wear-out-failure component. The combination of these three components results in a nearly constant failure rate because the decreasing quality failures and increasing wear-out failures tend to offset each other and because the stress-related failures exhibit a relatively larger amplitude. (3) The *wear-out period* is characterized by an increasing failure rate comprising a negligible quality-failure component, a constant stress-related-failure component, and an initially low but rapidly increasing wear-out-failure component.

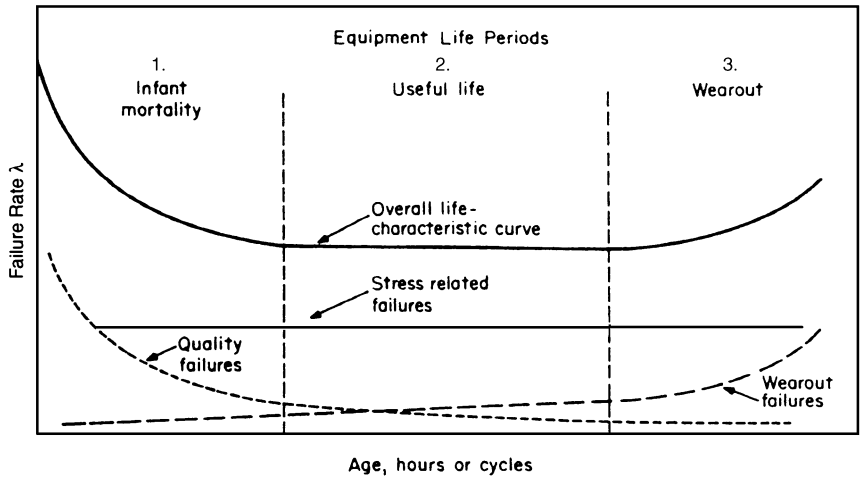


FIGURE 3.1.1 Life-characteristic curve, showing the three components of failure (when superimposed, the three failures provide the top curve).

The general approach to reliability for electronic systems is to minimize early failures by emphasizing factory test and inspection and to prevent wear-out failures by replacing short-lived parts before they fail. Consequently, the useful life period characterized by stress-related failures is the most important period and the one to which design attention is primarily addressed.

Figure 3.1.1 illustrates that during the useful life period the failure rate is constant. A constant failure rate is described by the exponential-failure distribution. Thus, the exponential-failure model reflects the fact that the item must represent a mature design whose failure rate, in general, is primarily because of stress-related failures. The magnitude of this failure rate is directly related to the stress-strength ratio of the item.

The validity of the exponential reliability function, Eq. (1), relates to the fact that the failure rate (or the conditional probability of failure in an interval given at the beginning of the interval) is independent of the accumulated life.

The use of this type of "failure law" for complex systems is judged appropriate because of the many forces that can act on the item and produce failure. The stress-strength relationship and varying environmental conditions result in effectively random failures. However, this "failure law" is not appropriate if parts are used in their wear-out phase (Phase 3 of Fig. 3.1.1).

The approach to randomness is aided by the mixture of part ages that results when failed elements in the system are replaced or repaired. Over time the system failure rate oscillates, but this cyclic movement diminishes in time and approaches a stable state with a constant failure rate.

Another argument for assuming the exponential distribution is that if the failure rate is essentially constant, the exponential represents a good approximation of the true distribution over a particular interval of time. However, if parts are used in their wear-out phase, then a more sophisticated failure distribution must be considered.

System Modeling

To evaluate the reliability of systems and equipment, a method is needed to reflect the *reliability connectivity* of the many part types having different stress-determined failure rates that would normally make up a complex equipment. This is accomplished by establishing a relationship between equipment reliability and individual part or item failure rates.

Before discussing these relationships, it is useful to discuss system reliability objectives. For many systems, reliability must be evaluated from the following three separate but related standpoints: reliability as it

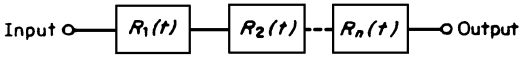


FIGURE 3.1.2 Serial connectivity.

affects personnel safety, reliability as it affects mission success, and reliability as it affects unscheduled maintenance or logistic factors. In all these aspects of the subject, the rules for reliability connectivity are applicable. These rules imply that failures are stress-related and that the exponential failure distribution is applicable.

Serial Connectivity. The serial equipment configuration can be represented by the block diagram, shown in Fig. 3.1.2. The reliability of the *series configuration* is the product of the reliabilities of the individual blocks

$$R_s(t) = R_1(t)R_2(t) \cdots R_i(t) \cdots R_n(t) \tag{2}$$

where $R_s(t)$ is the series reliability and $R_i(t)$ is the reliability of ith block for time t.

The concept of constant failure rate allows the computation of system reliability as a function of the reliability of parts and components:

$$R(t) = \prod_{i=1}^{n} e^{-\lambda_i t} = e^{-\lambda_1 t} e^{-\lambda_2 t} \cdots e^{-\lambda_n t} \tag{3}$$

This can be simplified to

$$R(t) = e^{-(\lambda_1 t + \lambda_2 t + \cdots + \lambda_n t)} = e^{-(\lambda_1 + \lambda_2 + \cdots + \lambda_n)t} \tag{4}$$

The general form of this expression can be written

$$R(t) = \exp\left[-t \sum_{t=1}^{n} \lambda_i\right] \tag{5}$$

Another important relationship is obtained by considering the jth subsystem failure rate λ_j to be equal to the sum of the individual failure rates of the n independent elements of the subsystems such that

$$\lambda_j = \sum_{i=1}^{n} \lambda_i \tag{6}$$

Revising the MTBF formulas to refer to the system rather than an individual element gives the *mean time between failures* of the system as

$$\text{MTBF} = \frac{1}{\lambda_j} = \frac{1}{\sum_{i=1}^{n} \lambda_i} \tag{7}$$

Successive estimates of the jth subsystem failure rate can be made by combining lower-level failure rates using

$$\lambda_j = \sum_{i=1}^{n} \lambda_{ij} \quad j = 1, \ldots, m \tag{8}$$

where λ_{ij} is the failure rate of the ith component in the jth-level subsystem and λ_j is the failure rate of the jth-level subsystem.

Parallel Connectivity. The more complex configuration consists of equipment items or parts operating both in series and parallel combinations, together with the various permutations. A parallel configuration accounts for the fact that alternate part or item configurations can be designed to ensure equipment success by redundancy.

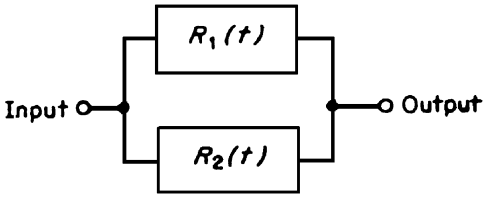


FIGURE 3.1.3 Parallel connectivity.

A two-element parallel reliability configuration is represented by the block diagram in Fig. 3.1.3. To evaluate the reliability of parallel configurations, consider, for the moment, that a reliability value (for any configuration) is synonymous with probability, i.e., probability of successful operation, and can take on values ranging between 0 and 1. If we represent the reliability by the symbol R and its complement $1 - R$, that is, unreliability, by the symbol Q, then from the fundamental notion of probability,

$$R + Q = 1 \quad \text{and} \quad R = 1 - Q \tag{9}$$

From Eq. (9) it can be seen that a probability can be associated with successful operation (reliability) as well as with failure (unreliability). For a single block (on the block diagram) the above relationship is valid. However, in the two-element parallel reliability configuration shown in Fig. 3.1.3, two paths for successful operation exist, and the above relationship becomes

$$(R_1 + Q_1)(R_2 + Q_2) = 1 \tag{10}$$

Assuming that $R_1 = R_2$ and $Q_1 = Q_2$, that is, the blocks are identical, this can be rewritten as

$$(R + Q)^2 = 1 \tag{11}$$

Upon expansion, this becomes

$$R^2 + 2RQ + Q^2 = 1 \tag{12}$$

We recall that reliability represents the probability of successful operation. This condition is represented by the first two terms of Eq. (12). Thus, the *reliability of the parallel configuration* can be represented by

$$R_p = R^2 + 2RQ \tag{13}$$

Note that either both branches are operating successfully (the R^2 term) or one has failed while the other operates successfully (the $2RQ$ term).

Substituting the value of $R = 1 - Q$ into the above expression, we obtain

$$R_p = (1 - Q)^2 + 2(1 - Q)Q = 1 - 2Q + Q^2 + 2Q - 2Q^2 = 1 - Q^2 \tag{14}$$

To obtain an expression in terms of reliability only, the substitution $Q = 1 - R$ can be made, which yields

$$R_p = 1 - (1 - R)(1 - R) \tag{15}$$

The more general case where $R_1 \neq R_2$ can be expressed

$$R_p = 1 - (1 - R_1)(1 - R_2) \tag{16}$$

By similar reasoning it can be shown that for n blocks connected in a parallel reliability configuration, the reliability of the configuration can be expressed by

$$R_p(t) = 1 - (1 - R_1)(1 - R_2) \cdots (1 - R_n) \tag{17}$$

The series and parallel reliability configurations (and combinations of them), as described above in Eqs. (5) and (17), are basic models involved in estimating the reliability of complex equipment.

Redundancy. The serial and parallel reliability models presented in the preceding paragraphs establish the mathematical framework for the reliability connectivity of various elements. Their application can be illustrated to show both the benefits and penalties of redundancy when considering safety, mission, and unscheduled maintenance reliability. Simplified equipment composed of three functional elements (Fig. 3.1.4) can be used to illustrate the technique.

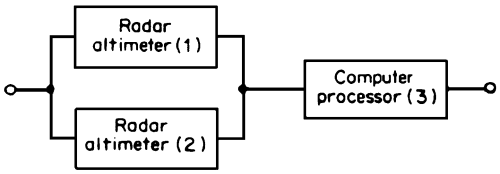


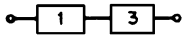
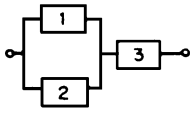
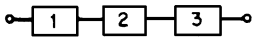
FIGURE 3.1.4 Serial and parallel connectivity.

Elements 1 and 2 are identical and represent one form of functional redundancy operating in series with element 3.

Reliability block diagrams can be defined corresponding to *nonredundant serial, safety, mission,* and *unscheduled maintenance* reliability. The block diagrams show only those functional elements that must operate properly to meet that particular reliability requirement. Figure 3.1.5 depicts the various block diagrams, reliability formulas, and typical values corresponding to these requirements. It indicates that the use of redundancy provides a significant increase in safety and mission reliability above that of a serial or nonredundant configuration; however, it imposes a penalty by adding an additional serial element in the scheduled maintenance chain.

Part-Failure Modeling

The basic concept that underlies reliability prediction and the calculation of reliability numerics is that system failure is a reflection of *part failure.* Therefore, a method for estimating part failure is needed. The most direct approach to estimating part-failure rates involves the use of large-scale data-collection efforts to obtain the relationships, i.e., models, between engineering and reliability variables. The approach uses controlled test

Reliability requirement	Reliability block diagram	Calculated values
1. Serial (nonredundant) reliability		$R = R_1 R_3 = 0.842$ MTBF = 575 hr
2. Safety (or mission) reliability		$R = \left[2R_1 - R_1^2\right] R_3$ $= 0.97$
3. Unscheduled maintenance reliability		$R = R_1 R_2 R_3 = 0.715$ MTBF = 298 hr

$$R_{\text{Serial}} = R_1 \cdot R_2 \cdots R_n$$

where

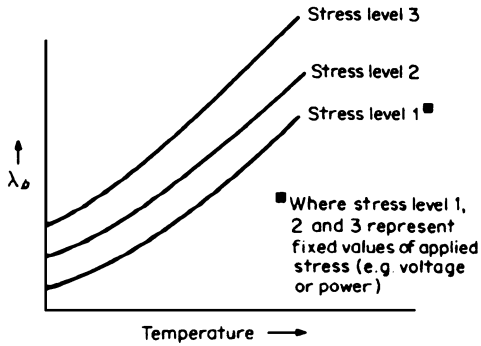
$$R_n = e^{-\lambda_n t}$$

$$\text{MTBF} = \frac{1}{\lambda_n}$$

$$R_{\text{Parallel}} = 1 - (1 - R)(1 - R) = 2R - R^2$$

$R_1 = 0.85$
$R_2 = 0.85$
$R_3 = 0.99$
$t = 100$ h

FIGURE 3.1.5 Calculations for system reliability.



Failure-rate adjustment factor	π_E	π_A	π_B	. . .	π_n
Value	x	y	. . .	. . .	. . .

$$\lambda_{part} = \lambda_b \pi_E \pi_A \pi_Q \cdots \pi_n$$

FIGURE 3.1.6 Conceptual part-failure model.

data to derive relationships between design and generic reliability factors and to develop factors for adjusting the reliability to estimate field reliability when considering application conditions.

These data have been reduced through *physics-of-failure techniques and empirical data* and are included in several different failure rate databases. Some of the more common failure rate databases are: MIL-HDBK-217, Telcordia/Bellcore SR-332, CNET's RDF 2000, British Telecom's database, Reliability Analysis Center's PRISM, and IEEE STD 493. All are suitable for estimating stress-related failure rates. Some even include thermal cycling, on/off switching, and dormant (shelf time) effects. This section will use MIL-HDBK-217 as an example, but all databases provide excellent guidance during design and allow individual part failure rates to be combined within a suitable system reliability model to arrive at an estimate of system reliability.

Although part-failure models (Fig. 3.1.6) vary with different part types, their general form is

$$\lambda_{\text{part}} = \lambda_b \pi_E \pi_A \pi_Q \cdots \pi_n \tag{18}$$

where λ_{part} = total part-failure rate
λ_b = base or generic failure rate
π's = adjustment factors

The value of λ_b is obtained from reduced part-test data for each generic part category, where the data are generally presented in the form of failure rate versus normalized stress and temperature factors. The part's primary-load stress factor and its factor of safety are reflected in this basic failure-rate value. As shown in Fig. 3.1.6, the value of λ_b is generally determined by the anticipated stress level, e.g., power and voltage, at the expected operating temperature. These values of applied stress (relative to the part's rated stress) represent the variables over which design control can be exercised and which influence the item's ultimate reliability.

π_E is the environmental adjustment factor which accounts for the influences of environments other than temperature; it is related to the operating conditions (vibration, humidity, and so forth) under which the item must perform. These environmental classes have been defined in MIL-HDBK-217. Table 3.1.1 defines each class in terms of its nominal environmental conditions. Depending on the specific part type and style, the value of π_E may vary from 0.2 to 120. The missile-launch environment is usually the most severe and generally dictates the highest value of π_E. Values of π_E for monolithic microelectronic devices have been added to Table 3.1.1 to characterize this range for a particular part type.

π_A is the application adjustment factor. It depends on the application of the part and takes into account secondary stress and application factors considered to be reliability-significant.

π_Q is the quality adjustment factor, used to account for the degree of manufacturing control with which the part was fabricated and tested before being shipped in the user. Many parts are covered by specifications that

TABLE 3.1.1 Environmental Symbols and Adjustment Factors

Environment	π_E symbol	Nominal environmental conditions	π_E value*
Ground, benign	G_B	Nearly zero environmental stress with optimum engineering operation and maintenance	0.5
Fixed	G_F	Conditions less than ideal to include installation in adequate racks with adequate cooling air, maintenance by military personnel and possible installation in unheated buildings	2.0
Mobile	G_M	Conditions more severe than those for G_I mostly for vibration and shock; cooling-air supply may also be more limited and maintenance less uniform	4.0
Naval, sheltered	N_S	Surface ship conditions similar to G_F but subject to occasional high shock and vibration	4.0
Unsheltered	N_U	Nominal suface shipborne conditions but with repetitive high levels of shock and vibration	6.0
Airborne, inhabited, cargo	A_IC	Typical conditions in cargo compartments and can be occupied by aircrew without environmental extremes of pressure, temperature, shock, and vibration and installed on long-mission aircraft such as transports and bombers	4.0
Fighter	A_{IF}	Same as A_{IC} but installed on high-performance aircraft such as fighters and interceptors	5.0
Uninhabited, cargo	A_{UC}	Bomb bay, equipment bay, tail, or wing installations where extreme pressure, vibration, and temperature cycling may be aggravated by contamination from oil, hydraulic fluid, and engine exhaust; installed on long-mission aircraft such as transports and bombers	5.0
Fighter	A_{UF}	Same as A_{UC} but installed on high-performance aircraft such as fighters and interceptors	8.0
Space, flight	S_F	Earth orbitral; approaches G_B conditions without access for maintenance; vehicle neither under powered flight nor in atmospheric reentry	0.5
Airborne, rotary winged	A_{RW}	Equipment installed on helicopters	8.0
Missile, flight	M_F	Conditions related to powered flight of air-breathing missiles, cruise missiles, and missiles in unpowered free flight	5.0
Cannon, launch	C_L	Extremely severe conditions related to cannon launching of 155 mm and 5 in guided projectiles; conditions also apply to projectile from launch to target impact	220.0
Missile, launch	M_L	Severe conditions of noise, vibration, and other environments related to missile launch and space-vehicle boost into orbit, vehicle reentry, and landing by parachute; conditions may also apply to installation near main rocket engines during launch operations	12.0

*Values for monolithic microelectronic devices.

have several quality levels. Several parts have multilevel quality specifications. Values of π_Q relate to both the generic part and its quality level.

π_N is the symbol for a number of additional adjustment factors that account for cyclic effects, construction class, and other influences on failure rate.

The data used as the basis of MIL-HDBK-217 consisted of both controlled test data and field data. The controlled test data directly related stress-strength variables on a wide variety of parts and were suitable for establishing the base failure rates λ_b.

TABLE 3.1.2 Representative Part-Failure-Rate Calculations

	Model		
Value	Microcircuits, Gate/Logic Arrays and Microprocessors $\lambda_p = \pi_1 \pi_Q (C_1 \pi_T + C_2 \pi_E)$	Fixed resistor $\lambda_p = \lambda_b \pi_T \pi_P \pi_S \pi_Q \pi_E$	Fixed capacitor $\lambda_p = \lambda_b \pi_T \pi_C \pi_V \pi_{SR} \pi_Q \pi_E$
λ_b	. . . .	0.0017	0.00099
π_E	6.0	4.0	20.0
π_Q	2.0	3.0	1.0
π_L	1.0		
π_T	1.9	1.1	1.9
C_1	0.005		
C_2	0.002		
π_C	. . . .	. . . .	0.81
π_V	. . . .	. . . .	1.6
π_{SR}	. . . .	. . . .	1.0
π_S	. . . .	1.5	
π_P	. . . .	0.44	
$\lambda_p \times 10^{-6}$	0.043	0.015	0.049

MIL-HDBK-217 completely describes failure-rate models, failure-rate data, and adjustment factors to be used in estimating the failure rate for the individual generic part types. Table 3.1.2 presents a tabulation of several models, their base failure rates λ_b, associated π factors, and failure-rate values for several representative part types. The specific procedures for deriving the failure rates differ according to part class and type.

RELIABILITY EVALUATION

Summary

Reliability prediction, failure mode and effects analysis (FMEA), and reliability growth techniques represent prediction and design evaluation methods that provide a quantitative measure of how reliably a design will perform. These techniques help determine where the design can be improved. Since specified reliability goals are often contractual requirements that must be met along with functional performance requirements, these quantitative evaluations must be applied during the design stage to guarantee that the equipment will function as specified for a given duration under the operational and environmental conditions of intended use.

Prediction Techniques

Reliability prediction is the process of quantitatively assessing the reliability of a system or equipment during its development, before large-scale fabrication and field operations. During design and development, predictions serve as quantitative guides by which design alternatives can be judged for reliability. Reliability predictions also provide criteria for reliability growth and demonstration testing, logistics cost studies, and various other development efforts.

Thus, reliability prediction is a key to system development and allows reliability to become an integral part of the design process. To be effective, the prediction technique must relate engineering variables (the language of the designer) to reliability variables (the language of the reliability engineer).

A prediction of reliability is obtained by determining the reliability of the item at the lowest system level and proceeding through intermediate levels until an estimate of system reliability is obtained. The prediction

method depends on the availability of accurate *evaluation models* that reflect the reliability connectivity of lower-level items and substantial *failure data* that have been analyzed and reduced to a form suitable for application to low-level items.

Various formal prediction procedures are based on theoretical and statistical concepts that differ in the level data on which the prediction is based. The specific steps for implementing these procedures are described in detail in reliability handbooks. Among the procedures available are parts-count methods and stress-analysis techniques. Failure data for both models are available in most reliability data bases like MIL-HDBK-217.

Parts-Count Method. The parts-count method provides an estimate of reliability based on a count by part type (resistor, capacitor, integrated circuit, transistor, as so forth). This method is applicable during proposal and early design studies where the degree of design detail is limited. It involves counting the number of parts of each type, multiplying this number by a generic failure rate for each part type, and summing up the products to obtain the failure rate of each functional circuit, subassembly, assembly, and/or block depicted in the system block diagram.

The advantage of this method is that it allows rapid estimates of reliability to determine quickly the feasibility (from the reliability standpoint) of a given design approach. The technique uses information derived from available engineering information and does not require detailed part-by-part stress and design data.

Stress-Analysis Method. The stress-analysis technique involves the same basic steps as the parts-count technique but requires detailed part models plus calculation of circuit stress values for each part before determining its failure rate. Each part is evaluated in its electric-circuit and mechanical-assembly application based on an electrical and thermal stress analysis. Once part-failure rates have been established, a combined failure rate for each functional block in the reliability diagram can be determined.

To facilitate calculation of part-failure rates, worksheets based on part-failure-rate models are normally prepared to help in the evaluation. These worksheets are prepared for each functional circuit in the system. When completed, these sheets provide a tabulation of circuit part data, including part description, electrical stress factors, thermal stress factors, basic failure rates, the various multiplying or additive environmental and quality adjustment factors, and the final combined part-failure rates. The variation in part stress factors (both electrical and environmental) resulting from changes in circuits and packaging is the means by which reliability is controlled during design. Considerations for, and effects of, reduced stress levels (derating) that result in lower failure rates are treated in the chapter "Derating Factors and Application Guidelines."

Failure Analysis

Failure mode and effects analysis is an iterative documented process performed to identify basic faults at the part level and determine their effects at higher levels of assembly. The analysis can be performed with actual failure modes from field data or hypothesized failure modes derived from design analyses, reliability-prediction activities, and experience of how parts fail. In their most complete form, failure modes are identified at the part level, which is usually the lowest level of direct concern to the equipment designer. In addition to providing insight into failure cause-and-effect relationships, the FMEA provides the discipline method for proceeding part by part through the system to assess failure consequences.

Failure modes are analytically induced into each component, and failure effects are evaluated and noted, including severity and frequency (or probability) of occurrence. As the first mode is listed, the corresponding effect on performance at the next higher level of assembly is determined. The resulting failure effect becomes, in essence, the failure mode that affects the next higher level.

Iteration of this process results in establishing the ultimate effect at the system level. Once the analysis has been performed for all failure modes, each effect or symptom at the system level usually may be caused by several different failure modes at the lowest level. This relationship to the end effect provides the basis for grouping the lower-level failure modes.

Using this approach, probabilities of the occurrence of the system effect can be calculated, based on the probability of occurrence of the lower-level failure modes, i.e., modal failure rate times time. Based on these probabilities and a severity factor assigned to the various system effects, a *criticality number* can be calculated. Criticality numerics provide a method of ranking the system-level effects derived previously and the basis for corrective-action priorities, engineering-change proposals, or field retrofit actions.

Fault-Tree Analysis. Fault-tree analysis (FTA) is a tool that lends itself well to analyzing failure modes found during design, factory test, or field data returns. The fault-tree-analysis procedure can be characterized as an iterative documented process of a systematic nature performed to identify basic faults, determine their causes and effects, and establish their probabilities of occurrence.

The approach involves several steps, among which is the structuring of a highly detailed logic diagram that depicts basic faults and events that can lead to system failure and/or safety hazards. Then follows the collection of basic fault data and failure probabilities for use in computation. The next step is the use of computational techniques to analyze the basic faults, determine failure-mode probabilities, and establish criticalities. The final step involves formulating corrective suggestions that, when implemented, will eliminate or minimize faults considered critical. The steps involved, the diagrammatic elements and symbols, and methods of calculation are shown in Fig. 3.1.7.

This procedure can be applied at any time during a system's life cycle, but it is considered most effective when applied (1) during preliminary design, on the basis of design information and a laboratory or engineering test model, and (2) after final design, before full-scale production, on the basis of manufacturing drawings and an initial production model.

The first of these (in preliminary design) is performed to identify failure modes and formulate general corrective suggestions (primarily in the design area). The second is performed to show that the system, as manufactured, is acceptable with respect to reliability and safety. Corrective actions or measures, if any, resulting from the second analysis would emphasize controls and procedural actions that can be implemented with respect to the "as manufactured" design configuration.

The outputs of the analysis include:

1. A detailed logic diagram depicting all basic faults and conditions that must occur to result in the hazardous condition(s) under study.
2. A probability-of-occurrence numeric value for each hazardous condition under study.
3. A detailed fault matrix that provides a tabulation of all basic faults, their occurrence probabilities and criticalities, and the suggested change or corrective measures involving circuit design, component-part selection, inspection, quality control, and so forth, which, if implemented, would eliminate or minimize the hazardous effect of each basic fault.

Reliability Testing

Reliability Growth. Reliability growth is generally defined as the improvement process during which hardware reliability increases to an acceptable level. The measured reliability of newly fabricated hardware is much less than the potential reliability estimated during design, using standard handbook techniques. This definition encompasses not only the technique used to graph increases in reliability, i.e., "growth plots," but also the management-resource-allocation process that causes hardware reliability to increase.

The purpose of a growth process, especially a reliability-growth test, is to achieve acceptable reliability in field use. Achievement of acceptable reliability depends on the extent to which testing and other improvement techniques have been used during development to "force out" design and fabrication flaws and on the rigor with which these flaws have been analyzed and corrected.

A primary objective of growth testing is to provide methods by which hardware reliability development can be dimensioned, disciplined, and managed as an integral part of overall development. Reliability-growth testing also provides a technique for extrapolating the current reliability status (at any point during the test) to some future result. In addition, it provides methods for assessing the magnitude of the test-fix-retest effort before the start of development, thus making trade-off decisions possible. Many of the models for reliability growth represent the reliability of the system as it progresses during the overall development program. Also, it is commonly assumed that these curves are nondecreasing; i.e., once the system's reliability has reached a certain level, it will not drop below that level during the remainder of the development program. This assumes that any design or engineering changes made during the development program do not decrease the system's reliability.

For complex electronic and electromechanical avionic systems, a model traditionally used for reliability-growth processes, and in particular reliability-growth testing, is one originally published by Duane (1964). It

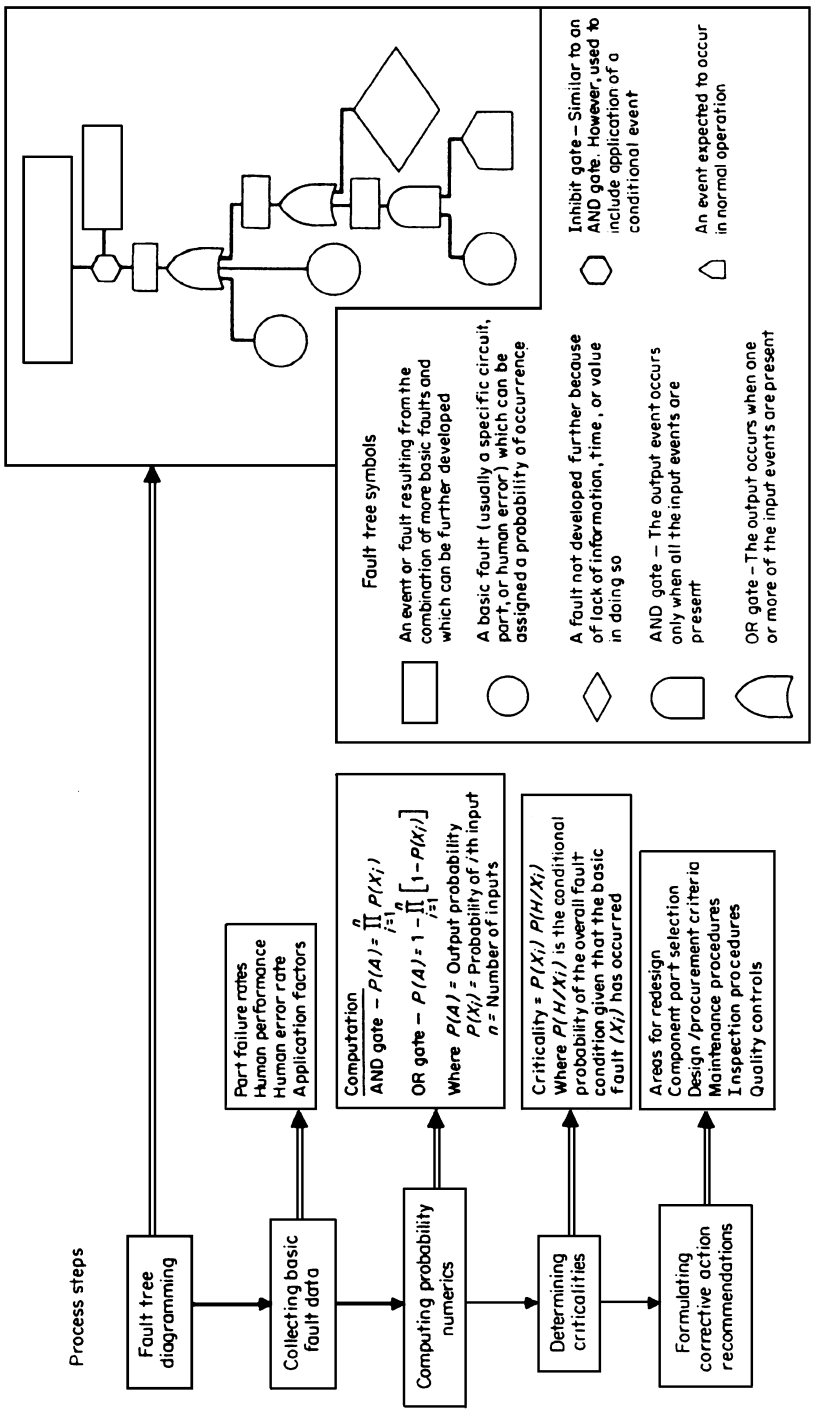


FIGURE 3.1.7 Fault-tree analysis.

provides a deterministic approach to reliability growth such that the system MTBF versus operating hours falls along a straight line when plotted on log-log paper. That is, the change in MTBF during development is proportional to T^d, where T is the cumulative operating time and d is the rate of growth corresponding to the rapidity with which faults are found and changes made to permanently eliminate the basic faults observed.

To structure a growth test program (based on the Duane model) for a newly designed system, a detailed test plan is necessary. This plan must describe the test-fix-retest concept and show how it will be applied to the system hardware under development. The plan requires the following:

1. Values for specified and predicted (inherent) reliabilities. Methods for predicting reliability (model, database, and so forth) must also be described.
2. Criteria for reliability starting points, i.e., criteria for estimating the reliability of initially fabricated hardware. For avionics systems, the initial reliability for newly fabricated systems has been found to vary between 10 and 30 percent of their predicted (inherent) values.
3. Reliability-growth rate (or rates). To support the selected growth rate, the rigor with which the test-fix-retest conditions are structured must be completely defined.
4. Calendar-time efficiency factors, which define the relationship of test time, corrective-action time, and repair time to calendar time.

Each of the factors listed above affects the total time (or resources) that must be scheduled to grow reliability to the specified value. Figure 3.1.8 illustrates these concepts and the four elements needed to structure and plan a growth test program.

1. *Inherent reliability* represents the value of design reliability estimated during prediction studies; it may be greater than that specified in procurement documents. Ordinarily, the contract specifies a value of reliability that is somewhat less than the inherent value. The relationship of the inherent (or specified) reliability to the starting point greatly influences the total test time.
2. *Starting point* represents an initial value of reliability for the newly manufactured hardware, usually falling within the range of 10 to 30 percent of the inherent or predicted reliability. Estimates of the starting point can be derived from previous experience or based on percentages of the estimated inherent reliability. Starting points must take into account the amount of reliability control exercised during the design program and the relationship of the system under development to the state of the art. Higher starting points minimize test time.

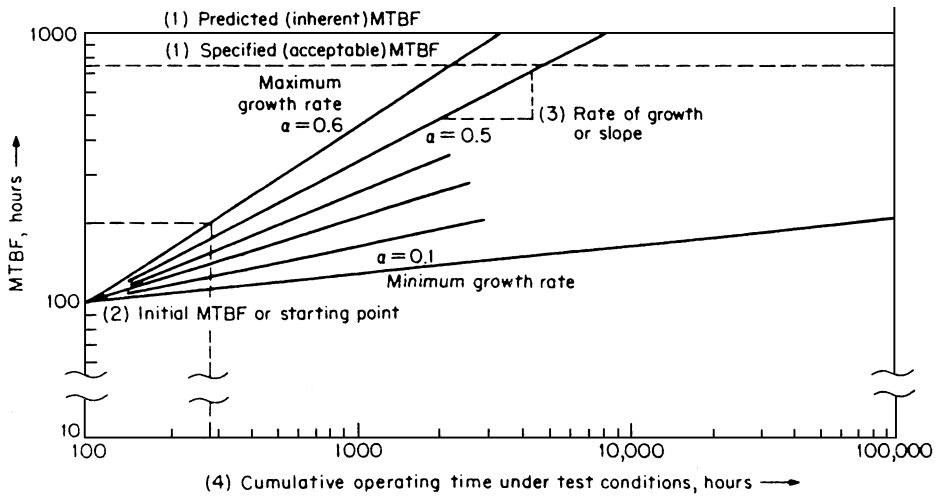


FIGURE 3.1.8 Reliability-growth plot.

3. *Rate of growth* is depicted by the slope of the growth curve, which is, in turn, governed by the amount of control, rigor, and efficiency by which failures are discovered, analyzed, and corrected through design and quality action. Rigorous test programs that foster the discovery of failures, coupled with management-supported analysis and timely corrective action, will result in a faster growth rate and consequently less total test time.
4. The ratio of *calendar time to test time* represents the efficiency factors associated with the growth test program. Efficiency factors include repair time and the ratio of operating and nonoperating time as they relate to calendar time. Lengthy delays for failure analysis, subsequent design changes, implementation of corrective action, or short operating periods will extend the growth test period.

Figure 3.1.8 shows that the value of the growth-rate parameter can vary between 0.1 and 0.6. A growth rate of 0.1 can be expected in programs where no specific consideration is given to reliability. In those cases, growth is largely because of solution of problems affecting production and corrective action taken as a result of user experience. A growth rate of 0.6 can be realized from an aggressive reliability program with strong management support. Such a program must include a formal stress-oriented test program designed to aggravate and force defects and vigorous corrective action.

Figure 3.1.8 also shows the requisite hours of operating and/or test time and continuous effort required for reliability growth. It shows the dramatic effect that the rate of growth α has on the cumulative operating time required to achieve a predetermined reliability level. For example, for a product whose MTBF potential is 1000 h it shows that 100,000 h of cumulative operating time is required to achieve an MTBF of 200 h when the growth rate is $\alpha = 0.1$. A rate of 0.1 is expected when no specific attention is paid to reliability growth. However, if the growth rate can be accelerated to 0.6, only 300 h of cumulative operating time is required to achieve an MTBF of 200 h.

Reliability Demonstration. Reliability-demonstration tests are designed to prove a specific reliability requirement with a stated statistical confidence, not specifically to detect problems or for reliability growth. The test takes place after the design is frozen and its configuration is not permitted to change. However, in practice, some reliability growth may occur because of the subsequent correction of failures observed during the test.

Reliability demonstration is specified in most military-system procurement contracts and often involves formal testing conducted per MIL-STD-781. This standard defines test plans, environmental exposure levels, cycle times, and documentation required to demonstrate formally that the specified MTBF requirements of the equipment have been achieved. Demonstration tests are normally conducted after growth tests in the development cycles using initial production hardware.

Reliability-demonstration testing carries with it a certain statistical confidence level; the more demonstration testing, the greater the confidence. The more reliability-growth testing performed, the higher the actual reliability. Depending on the program funding and other constraints, system testing may follow one of two options. The first option maximizes growth testing and minimizes demonstration testing, resulting in a high MTBF at a low confidence. The second option minimizes reliability growth testing with a resultant lower MTBF at higher confidence.

RELIABILITY DESIGN DATA

Data Sources

Reliability design data are available from a number of sources. Both the parts-count and stress-analysis methods of predicting reliability rely on part-failure-rate data. One source of such data is MIL-HDBK-217. Other sources may be sought, or estimating techniques using comparative evaluations may be used. Provided similarity exists, comparative evaluations involve the extrapolation of failure data from well-documented parts to those having little or no failure data.

Publications containing up-to-date experience data for a variety of parts, including digital and linear integrated circuits, hybrid circuits, and discrete semiconductor devices, are available through the Reliability Analysis Center, P.O. Box 4700, Rome, NY 13442-4700. The publications include malfunction through distributions, screening fallout, and experienced failure rates. They also publish the PRISM reliability design database.

Physics of Failure

The physical or chemical phenomena leading to the deterioration or failure of electron devices or components in storage under operating conditions is termed *physics of failure* or *reliability physics.* A major source of information on reliability-physics phenomena of electron devices is the *Annual Proceedings of the International Reliability Physics Symposium* (IRPS). This symposium is jointly sponsored by IEEE's Electron Devices Society and IEEE's Reliability Society and continues yearly.

Failure Modes. A knowledge of the physics of device failure is helpful in predicting and avoiding device failure. Prevalent failure modes are identified in a number of publications, besides the *IRPS Proceedings.* Other sources include MIL-HDBK-217F, and MIL-STD-1547(USAF).

Suspect Devices. In selecting parts for a particular application and in designing screens to identify potential early-life failures, it is helpful to be aware of failure-aspect device designs. A standard intended for the procurement of "space quality" piece parts for space missions, MIL-STD-1547(USAF), includes an identification of reliability-suspect items. Clearly the identification of such parts *does not suggest their inapplicability for all types of electronic systems.*

BIBLIOGRAPHY

Blischke, W. R., and D. N. Prabhakar Murthy (eds.), "Case Studies in Reliability and Maintenance," Wiley, 2002.

Blischke, W. R., and D. N. Prabhakar Murthy, "Reliability: Modeling, Prediction, and Optimization," Wiley, 2000.

Duane, J. T., "Learning curve approach to reliability monitoring," *IEEE Trans. Aerospace*, Vol. 11, 1964.

IEEE Proc. Annu. Reliability and Maintainability Symp.

IEEE Proc. Int. Reliability Phys. Symp.

Musa, J., A. Iannino, and K. Okumoto, "Software Reliability: Measurement, Prediction, Application," McGraw-Hill, 1987.

O'Connor, P. D. T., "Practical Reliability Engineering," Wiley, 2001.

Ohillon, B. S., "Design Reliability: Fundamentals and Applications," CRC Press, 1999.

Ramakumar, R., "Engineering Reliability: Fundamentals and Applications." Prentice Hall, 1993.

Reliability Standards and Data (some 600 publications on specific topics available from IEC).