

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

design to meet a particular standard, especially if that standard has been drafted on statistics from a large amount of credible data.

In IEEE Standard C62.41-1991 (Reference [17]), the importance of location of the equipment is emphasized. Location Category C is defined as being outside the building and service entrance; Category B includes distribution panels, heavy appliance outlets with “short” connections to service entrances, etc.; and Category A includes outlets and branch circuits more than 10 meters from Category B locations and more than 20 meters from Category C locations.

Information on standard waveforms for voltage and current surges in an ac distribution system for varying exposure to system transients is shown in Tables 7.4-2 and 7.4-3. This information is based on IEEE Standard C62.41-1991. Exposure levels are categorized as low, medium or high. These categories are described as follows:

- (1) Low Exposure. Systems in geographical areas known for low lightning activity, with little load or capacitor switching activity.
- (2) Medium Exposure. Systems in geographical areas known for medium to high lightning activity, or with significant switching transients. Both or only one of these causes may be present, as it is difficult to separate them in reviewing the results of monitoring disturbances.
- (3) High Exposure. Those rare installations that have greater surge exposures than those defined by Low Exposure and Medium Exposure. The more severe conditions result from extensive exposure to lightning or unusually severe switching surges.

Location Category C is rarely of concern. In location Categories B and A the peak voltage excursion is considered to be limited to 6 kV by flashover in outlets and insulation. Location A is assumed to be controlled by reactances that filter the surge into an oscillatory waveform. The “effective impedance” of the surge is simply the ratio of the peak voltage and peak current; it has the dimension of ohms, but is not a pure resistance.

TABLE 7.4-2: 0.5 μ S - 100 KHZ RING WAVE

LOCATION CATEGORY	SYSTEM EXPOSURE	VOLTAGE KV	CURRENT A	EFFECTIVE IMPEDANCE
A	Low	2	70	30
	Medium	4	130	30
	High	6	200	30
B	Low	2	170	12
	Medium	4	330	12
	High	6	500	12

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.4-3: 8/20 μ S, 1.2/50 μ S COMBINATION WAVE

LOCATION CATEGORY	SYSTEM EXPOSURE	VOLTAGE KV	CURRENT A	EFFECTIVE IMPEDANCE
B	Low	2	1	2
	Medium	4	2	2
	High	6	3	2
C	Low	6	3	2
	Medium	10	5	2
	High	20	10	2

The philosophy of IEEE Standard C62.41-1991 is that it is unnecessary to duplicate field-measured surges, since these occurrences are dependent on the site, time of year, etc. Rather, a few representative waveforms should be selected that are realistic and readily reproducible, and will allow researchers to compare the vulnerability of various equipment. The 0.5 μ s - 100 kHz ring wave and the 1.2/50 ms waveform are intended to be open-circuit voltages to test insulation, whereas the 8/20 μ s waveform is a current surge into a short circuit. When a test generator is connected to an MOV the voltage and current are not the same as the open-circuit and short-circuit standard waveforms due to the loading by the MOV; the effective source impedance, the ratio of $V_{\text{peak}}/I_{\text{peak}}$, is given in Tables 7.4-2 and 7.4-3.

7.4.1.12 Protection With Diodes

PN junction diodes are commonly used for transient protection because of their fast turn-on time and low series resistance. Diodes intended for transient suppression are especially designed to have low resistance. With their small size, low capacitance, wide range of clamping voltage, and somewhat modest ratings they are especially suited for on-board protection of integrated circuits and other semiconductor devices.

Figure 7.4-6 illustrates how diodes would be used to protect a discrete bipolar transistor. In part (a) of the figure diode D_1 in conjunction with R_B limits the base voltage to the range of one diode drop negative to one reverse breakdown voltage positive. D_2 prevents the output line from going negative, while the capacitor filters noise from the power supply bus.

In part (b) of Figure 7.4-6 a more elaborate arrangement of diodes and resistors limits the positive excursion of the base to two forward diode drops.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

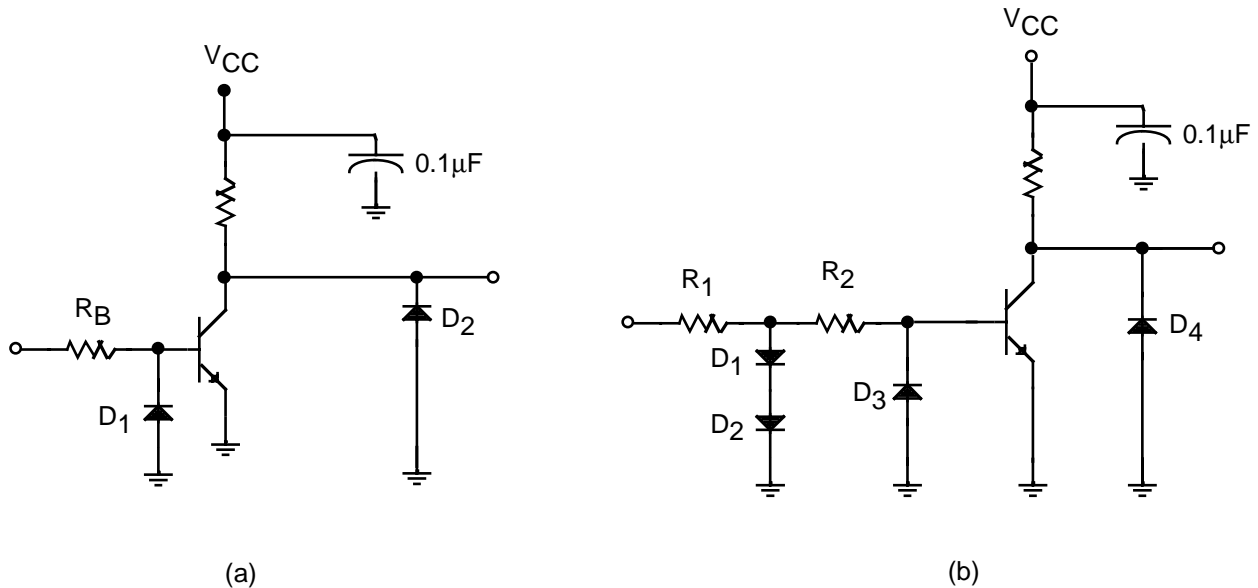


FIGURE 7.4-6: DIODE PROTECTION OF A BIPOLAR TRANSISTOR

Figure 7.4-7 shows the analogous protection scheme for a discrete MOSFET transistor. Some manufacturers suggest that D_2 be connected between the gate and drain, however the arrangement shown in the figure is preferred.

Large SCRs require transient protection for the gate circuit only. The peak inverse voltage rating should provide adequate protection for anode to cathode surges. Figure 7.4-8 shows two schemes for incorporating diode protection of the gate. Part (a) of the figure shows a simple resistor diode arrangement, whereas in part (b) the resistor and inductor form an integrating circuit to reduce the noise level at the gate.

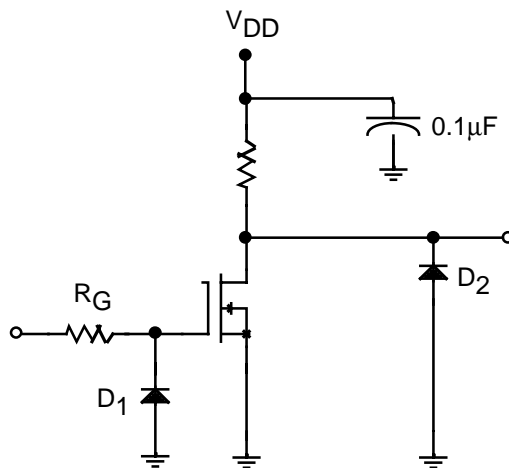


FIGURE 7.4-7: DIODE PROTECTION FOR A DISCRETE MOSFET TRANSISTOR

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

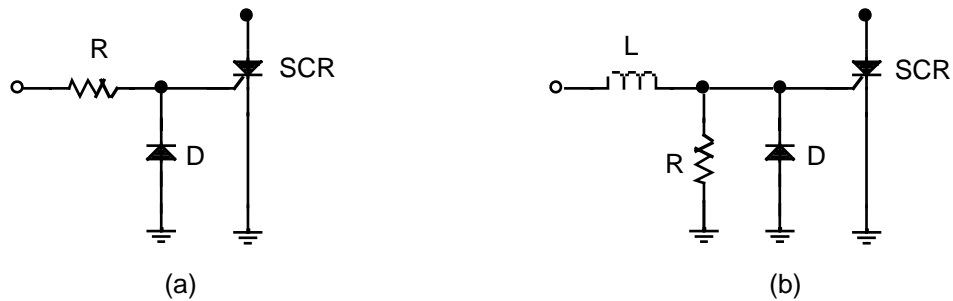


FIGURE 7.4-8: DIODE PROTECTION FOR SILICON CONTROLLED RECTIFIERS

Figure 7.4-9 illustrates diode protection for a TTL circuit. Diode D_1 clamps the negative transient to ground (using the output impedance of the driving circuit), and D_2 prevents the input from going more positive than V_{CC} . D_3 clips any negative surges on the output bus and the capacitor filters the V_{CC} bus.

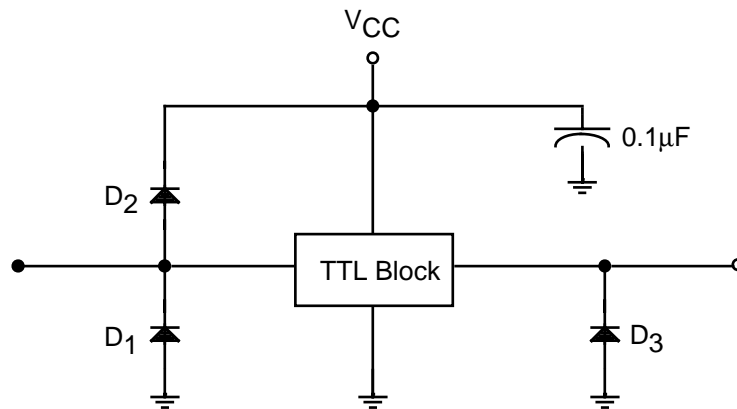


FIGURE 7.4-9: TRANSIENT PROTECTION FOR A TTL CIRCUIT USING DIODES

In Figure 7.4-10 a simple scheme for protecting CMOS circuits is shown. In part (a) the diode clamps positive pulses to V_{DD} and limits negative voltages to V_{DD} minus the diode reverse breakdown voltage. In part (b) the protection circuit is more elaborate, patterned after a commonly used on-chip protection scheme. D_1 is selected to have a larger reverse breakdown voltage than D_2 or D_3 . Resistor R_2 in conjunction with the on-chip protection network at the input of the CMOS circuit provides a third stage of protection. Each of the three stages would turn on sequentially as the input transient becomes larger and larger.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

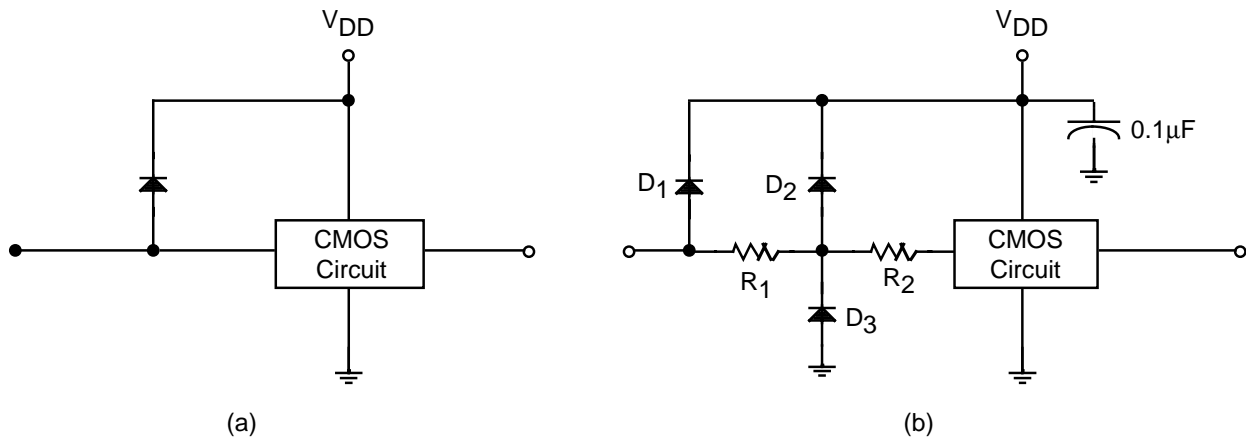


FIGURE 7.4-10: TRANSIENT PROTECTION FOR A CMOS CIRCUIT

Line transients are one of the causes of failures in switching mode power supplies. A major failure mode is shorting of the switching power transistors caused by power line surges. The inrush of current in conjunction with the equivalent series resistance and inductance of the filter capacitors produces an overstress of the power switches that leads to failure. The best remedy is to suppress the transients at the input to the power supply.

Figure 7.4-11 shows an effective method of suppressing line transients that uses a hybrid scheme employing both an MOV and clamping diodes. The MOV is a high energy absorbing device that provides the main protection. The clamping diodes provide a more precise limit to the voltage excursion. Suitable values of L and R are of the order of $100\mu\text{H}$ and 1 ohm , respectively.

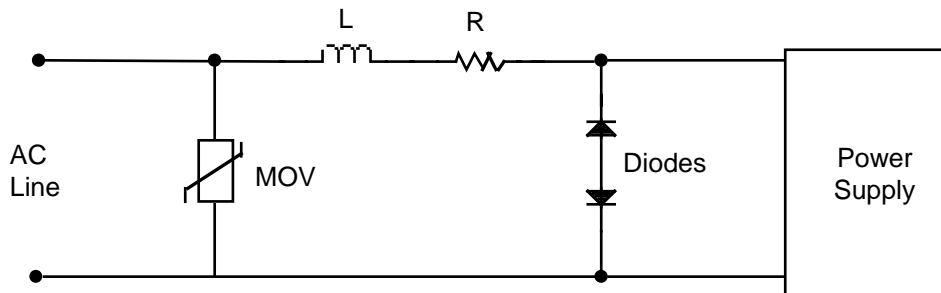


FIGURE 7.4-11: INPUT PROTECTION FOR POWER SUPPLIES

Diodes are compatible with on-board protection of components, and diode arrays can be effectively utilized to provide protection for data lines and power buses. Figure 7.4-12 shows an arrangement where the diode array is located adjacent to the edge connector. Some designers prefer to place the protection devices close to the components being protected; others try to avoid surge currents being propagated around the circuit board where they become sources of rf fields, and high voltage transients can cause arcs to nearby components or traces. For the latter case, the diodes are located at the connector as shown in the figure.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Transient voltage suppressor diodes usually fail short, but may also fail open. If they fail open there is no longer protection of susceptible components against subsequent transients. For the more common case of failing short, a significant surge current can occur unless limited by series impedances. This condition is much more serious for power buses than for data lines. The short-circuit current will eventually cause the protection diode to open-circuit. The relationship between the amplitude (squared) of the short-circuit current and the time to fail open is described fairly well by the classical Wunsch-Bell model; in other words the current is proportional to $t^{-1/4}$.

Figure 7.4-13 shows a fuse in a power bus protected by a diode. The fuse must be carefully selected to conduct the expected transient current, but to open when the diode fails short. These requirements are especially difficult to meet for low voltage diodes.

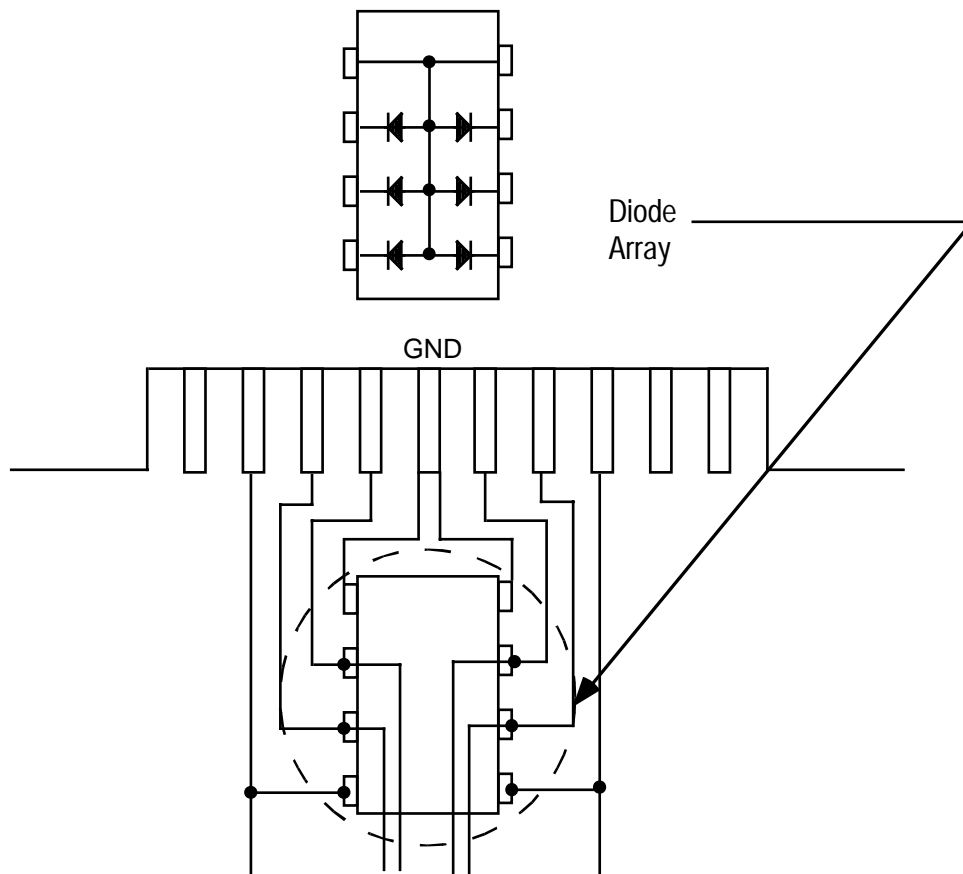


FIGURE 7.4-12: PROTECTION OF DATA LINES OR POWER BUSES USING A DIODE ARRAY

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

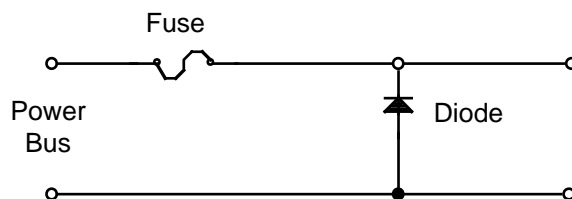


FIGURE 7.4-13: FUSE PROTECTION FOR A TRANSIENT VOLTAGE SUPPRESSOR DIODE

Since the threat from ESD comes mainly during handling of the boards, CRO-BAR[®] devices that connect all traces together at the edge connector pads would eliminate ESD pulses that are applied at the connector. CRO-BAR[®] devices automatically disengage when the board is inserted into a slot or when a cable is attached. CRO-BAR[®] devices on the cable itself also remove any static charges that may accumulate when the cable is left unconnected or unrolled from a spool.

Most of the techniques mentioned are common sense to those with some design experience in EMI, electromagnetic compatibility (EMC), ESD, or transient suppression. A few are still somewhat controversial. The importance of good design becomes increasingly relevant as electronic equipment and appliances proliferate and as devices become smaller and more sensitive. The battle is never finished, and as the electronics industry evolves, design engineers must realize that old remedies may no longer be applicable and new, innovative solutions must be thought of. Once a solution has been found, funding is often discontinued, those who make such decisions not realizing that like the mythical multiheaded dragon, new crises continually arise to frustrate those caught unawares.

7.4.2 Parameter Degradation and Circuit Tolerance Analysis

The values of part parameters, physical and electrical characteristics, are known to vary with time under the effects of aging and stress. Variations in part parameter values, if not considered in the design, can have undesirable effects on circuit performance and are a significant cause of system failure. Even when the variations in the value of a single parameter for a single part have no effect on system performance, the cumulative effect of such changes can degrade system performance to a point where it is no longer acceptable.

In addition to the variations caused by aging and stresses, the values of part parameters vary due to the manufacturing processes used in the manufacture of the parts. These variations can differ by manufacturing lot and can be affected by procedures in which parts are individually selected, using for example, “screens”. Whatever the causes, the variations in a given part parameter can be described by a statistical distribution. The expected value and standard deviation of this distribution represent the nominal or “average” value of the parameter and the variation around this nominal value, respectively. As already indicated, the nature of the distribution is a function of the manufacturing process, aging, and stress. Stress includes elements of the operating

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

environment, such as temperature, vibration, pressure, and so forth. Examples of part parameter variations are shown in Figures 7.4-14, 7.4-15, and 7.4-16. Figure 7.4-14 shows the average variation from the initial value and the standard deviation of the variation plotted over time for the resistance of a particular type of resistor and Figure 7.4-15 shows the same information for the capacitance of a particular type of capacitor. Figure 7.4-16 shows how the variability in the nominal resistance increases under a specified stress and temperature condition for a period of time, for two different levels of power dissipation.

In designing a system, these variations in the values of part parameters must be specifically addressed to ensure that the design is robust. A robust design is one in which substantial variations in the values of part parameters have little or no effect on system performance. In designing for robustness, designers must have a knowledge of the variations expected due to manufacturing, aging, and stress and the expected ranges of those variations. With this knowledge to guide them, designers can work to eliminate or mitigate the effects of variations in parameter values.

Two approaches that can be used to eliminate or mitigate the effects of variations in parameter values are:

- (1) Control the device and material parameter variations through process design and control to hold them within specified limits for a specified time under specified conditions. This will be referred to as Parts Control.
- (2) Design circuits and systems to be sufficiently tolerant of variations in device and material parameters so that anticipated variations over time and stress do not degrade system performance. This will be referred to as Design Control.

The first approach requires that the parameter value be controlled. Burn-in, preconditioning, and other screening methods, can be used to eliminate or reduce variation in a specific parameter. This screening results in parts having more stable parameters. Controlling the parameters of a part requires detailed testing and control of materials used in the parts. It requires strict control of manufacturing processes, the use of proven designs, and parts testing to collect data on parameter variation over time.

The second approach is to design circuits that are tolerant or insensitive to variations in parts parameters. Three different techniques for designing tolerant circuits are: (1) use feedback to electrically compensate for variations and thereby provide stable performance, (2) ensure that the circuitry provides the minimum required performance even under expected or worst case conditions (i.e., maximum variation), and (3) design the circuit to be insensitive to variations.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

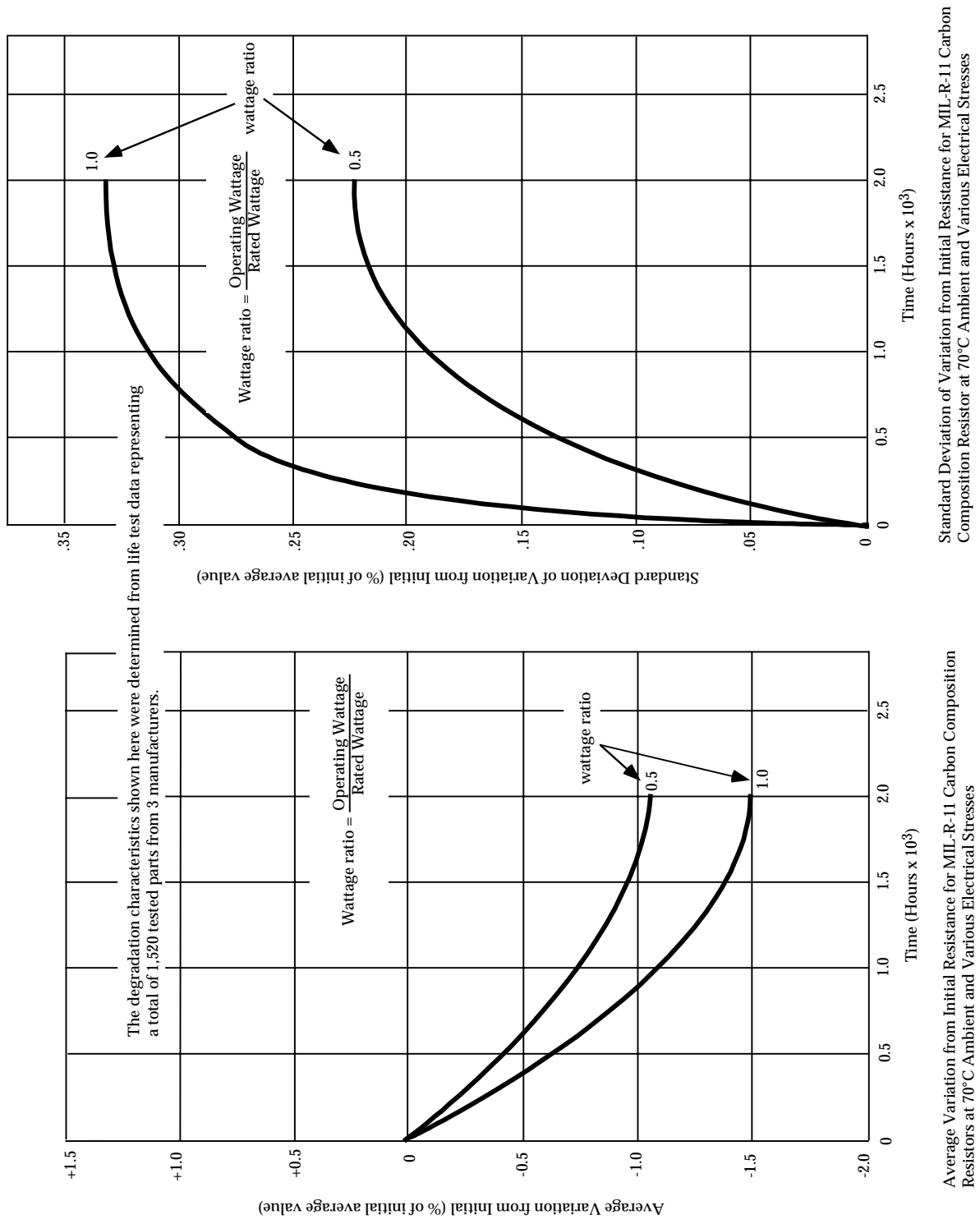


FIGURE 7.4-14: RESISTOR PARAMETER VARIATION WITH TIME (TYPICAL)

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

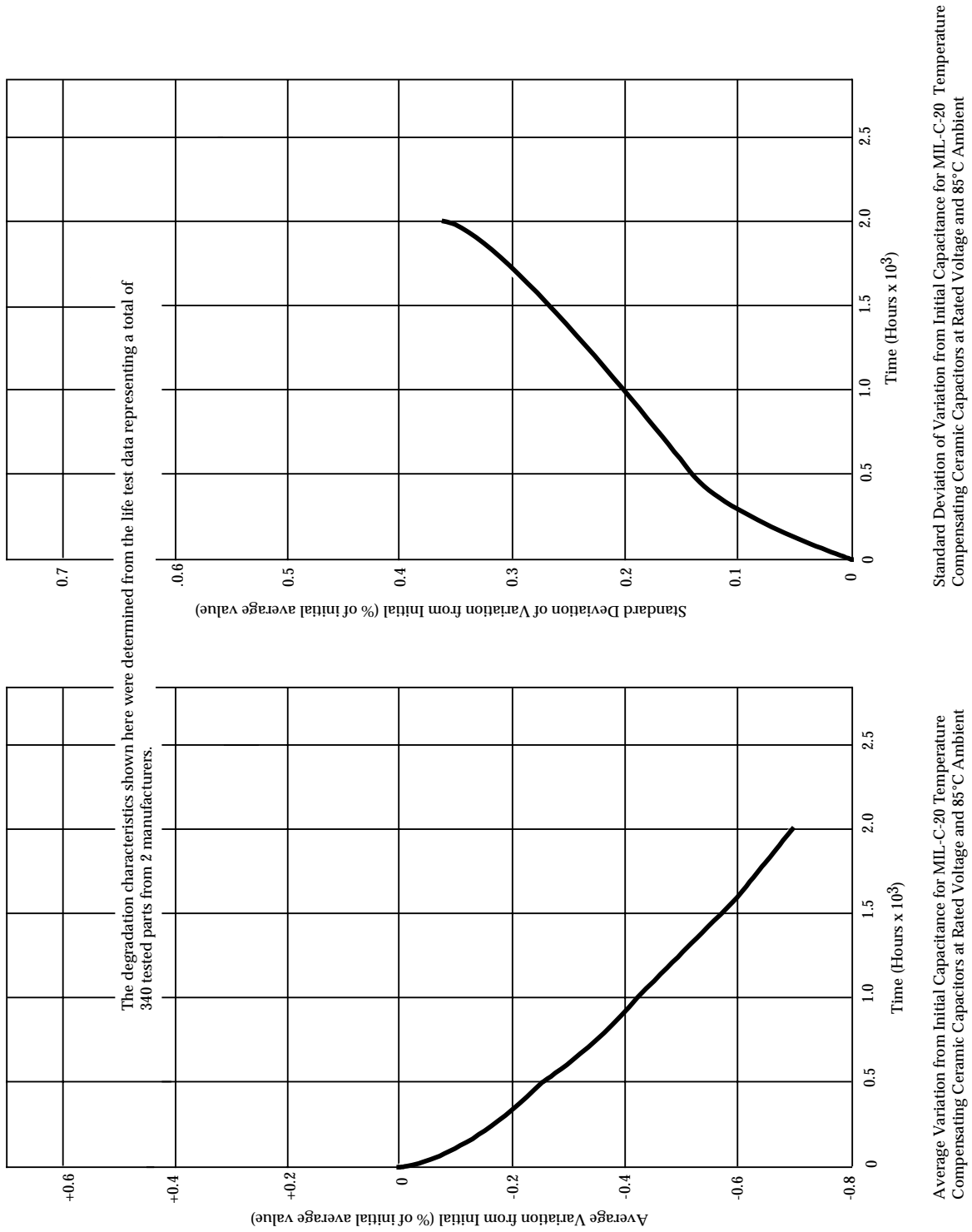
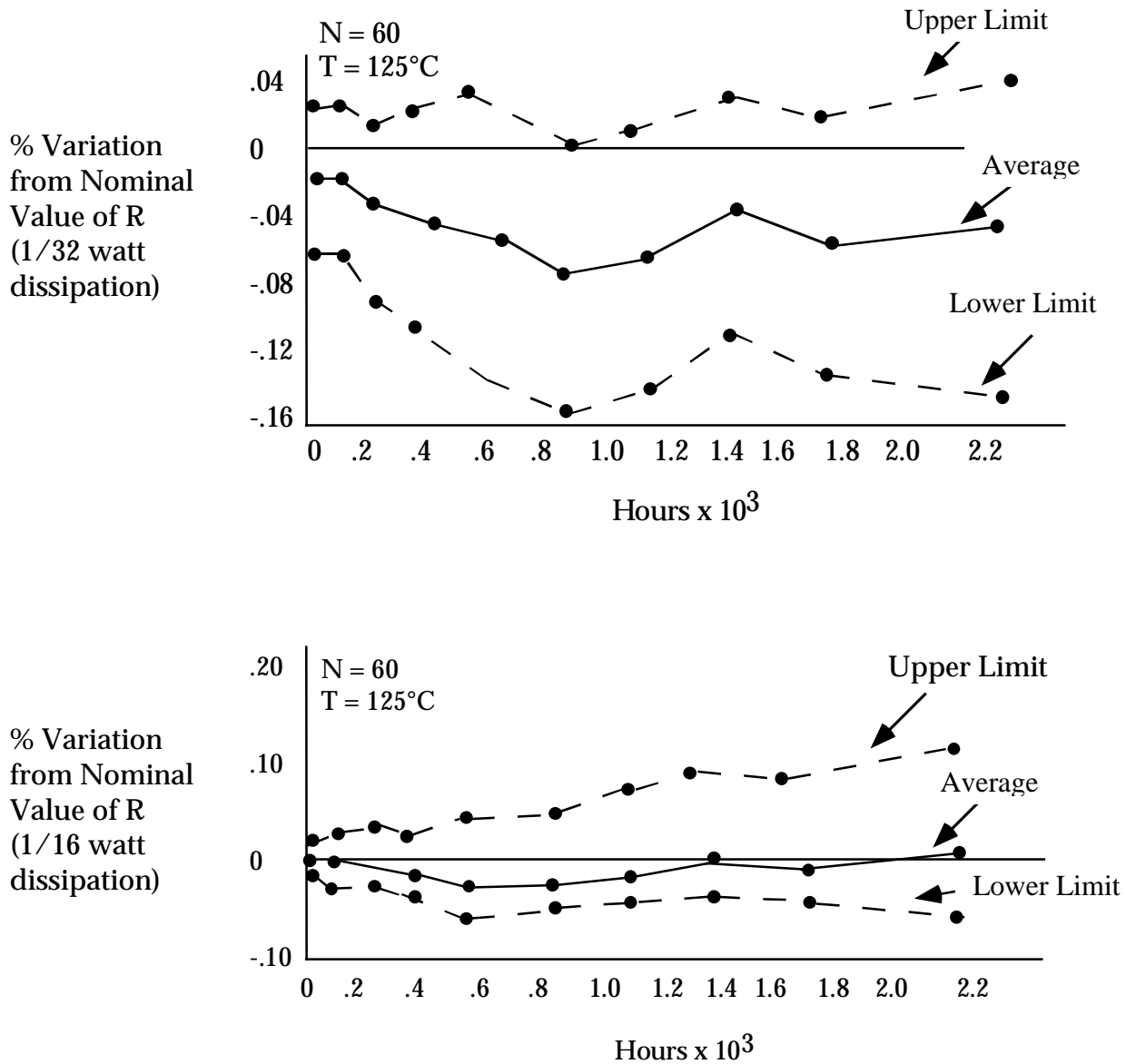


FIGURE 7.4-15: CAPACITOR PARAMETER VARIATION WITH TIME (TYPICAL)

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES



Data shown for 60 resistors of fixed metal film type rated at 1/8 watt during 2000 hours of operation at 125 degrees C and two different levels of power dissipation (stress levels).

FIGURE 7.4-16: RESISTOR PARAMETER CHANGE WITH STRESS AND TIME (TYPICAL)

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

In designing tolerant or insensitive circuits, the procedures for analyzing variability include:

- (1) Worst Case Circuit Analysis (WCCA)
- (2) Parameter Variation
- (3) Monte Carlo
- (4) Design of Experiments (DOE)
- (5) Taguchi robust design methodology

These methods are presented in Table 7.4-4 and are described in detail in References [18], [19], [20], and [21]. The ultimate objective of these analytical methods can be one of the following.

- (1) To select parts based on a determination of the allowable limits of variation for each part parameter and the anticipated operational environment. (Parts Control.)
- (2) To design the circuit to produce the minimum performance under worst case or statistically expected conditions of environment and parameter variation. (Design Control.)
- (3) To determine the parameter(s) most critical to proper operation of the part and then to design the circuit in such a way that variations in that parameter(s) do not affect performance. (Design Control.)

The first objective is to match the part to the application. It is seldom possible to find an exact match, so the parts usually have less parameter variability than could be tolerated. The second objective is to design the circuit to operate properly under the worst possible conditions. In so doing, the cost of the design could offset the advantages gained or make the design unaffordable. The last objective is to design a circuit in which the variation in critical part parameters is overcome by the nature of the design. Consider the following example from Reference [21].

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.4-4: COMPARISON OF VARIABILITY ANALYSIS METHODS

Analytical Method	Type of Analysis	Statistical?	Output	Objectives
WCCA	Mathematical	No	Worst-case values for inputs with all parameters at cumulative worst-case limits	Determine if failure is possible and, if so, under what conditions
Parameter Variation	Mathematical	No	Range of variability data for Schmoos plots	Establish realistic tolerance limits for parameters
Monte Carlo	Mathematical	Yes	Output histograms	Reliability estimates
DOE	Mathematical	No	Significant (critical) parameters and optimal values	Minimize number of experiments needed to establish relationship between parameters and performance
Robust design	Mathematical	Yes	Component values	Less variability (better quality)

A circuit is required to provide a specified output voltage, V_o , that is primarily determined by the gain of a transistor and the value of a resistor. As shown by the graphs of output voltage versus transistor gain for resistance values R_1 and R_2 in Figure 7.4-17, the transistor is a non-linear device. Assume the prototype circuit achieves the required voltage, indicated by the diamond, with resistance R_1 and transistor gain G_1 . The inherent variability in the gain of transistor 1 is depicted by the bell-shaped curve centered on G_1 . The amount of variability in R_1 causes a large variation in V_o as shown by the bell-shaped curve marked a .

Trying to reduce the variation in V_o by reducing the variability of G_1 may be very difficult or expensive. An alternative to selecting a higher quality (i.e., less variability) transistor is to develop a more robust design. We can do this in the following manner. First, operate the transistor at a higher gain, G_2 . Note that the variance of G_2 is now larger as indicated by the bell-shaped curve centered on G_2 . However, the non-linear relationship between gain and V_o results in a smaller variation of V_o as indicated by curve b . V_o , however, is now too large. By choosing resistance R_2 , we reduce the voltage to the proper level, as indicated by curve c . V_o is again equal to the target value but with a much smaller variability. Since transistor gain is somewhat affected by ambient temperature and V_o is now less sensitive to gain, an added benefit of this design is that V_o now is less sensitive to ambient temperature.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

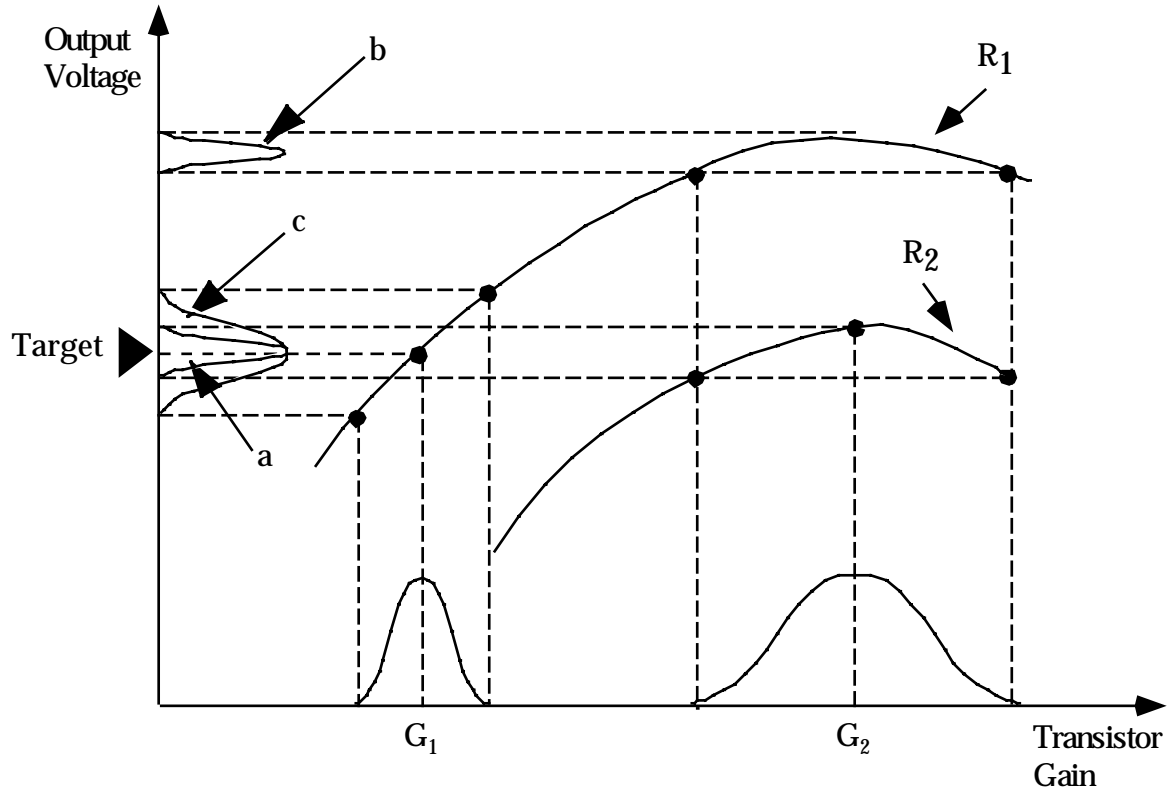


FIGURE 7.4-17: OUTPUT VOLTAGE VERSUS TRANSISTOR GAIN
BASED ON A FIGURE APPEARING IN TAGUCHI TECHNIQUES
FOR QUALITY ENGINEERING (REFERENCE [21])

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.4.3 Computer Aided Circuit Analysis

All of the following material in which computer analysis software packages are identified is presented for information only. The DoD does not endorse their specific use or attest to their quality.

Circuit Simulation: A Brief History

In the early 1960's military requirements led to the development of mathematical simulation of components (capacitors, semiconductors, etc.) to determine their response to pulsed x-ray and gamma radiation. These simulation studies were subsequently extended to small circuits to study their response to the same radiation conditions. This work resulted in the early circuit analysis programs (ECAP, SCEPTRE, CIRCUS, etc.).

Later program capabilities included AC, DC and transient performance simulation - with and without radiation effects. RF and microwave circuit simulation capabilities, sensitivity analysis, Monte Carlo, worst-case analysis and optimization analysis capabilities were also eventually added.

Early simulations were run overnight, in batch mode, on large mainframe computers; it was cumbersome to input the data and the graphics outputs were poor.

These simulation programs quickly migrated to engineering workstations and their capabilities were significantly enhanced by such features as simulation integration and schematic capture. They became more user friendly, included high resolution graphics and gave quick turn-around. These circuit analysis and simulation tools eventually became available for the ubiquitous PCs.

Hardware design and analysis is typically performed on workstations today. At the same time, however, the capabilities of PCs continue to improve. Thus, even the distinctions between PCs and workstations continues to blur with improvements in the state-of-the-art.

The current trends in design and in analysis software are toward portability and standardization, especially the increased use of higher level languages. The trend is to a fully integrated design-analysis environment including:

- (1) Schematic Capture
- (2) Circuit Simulation
- (3) Manufacturing Considerations
- (4) Test Vector Generation
- (5) Configuration Control

At present, analog circuit analysis and digital circuit analysis usually require different software packages. However, efforts are underway to unify analog and digital simulation software. Several commercial packages are available with mixed analog/ digital simulation capability.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.4.3.1 Advantages of Computer Aided Circuit Analysis/Simulation

Computer-aided analysis is the standard for large (multi-node), sophisticated circuits, those requiring special analysis techniques (transient, Monte Carlo, etc.) and iterative type analyses (e.g., frequency response). It is very cost effective for programs where the schedule imposes significant time restraints and where an insufficient number of skilled circuit analysts are available for the task. Computer-aided analysis is the only way to handle highly complex circuits accurately.

Computer simulation of circuit performance is a universally accepted technique. Its features are relatively easy to learn, including the ability to adjust (i.e., "tweak") parameter values for re-analysis (temperature changes, BOL (Beginning-of-Life) vs. EOL (End-of-Life) values, etc.). Furthermore, it can provide automatic documentation of the analytical results including: topology listings; calculations of voltage, current, and power; and plots of the variables.

7.4.3.2 Limitations of Computer-Aided Circuit Analysis/Simulation Programs

In general, a single computer program does not provide performance simulation of all classes or types of circuits, i.e., RF and microwave, analog (AC, DC, and transient analysis) and digital (logic and timing analyses). Also, because of the variety of computer platforms, computer programs are typically prepared for use by only one (or a few) computer families.

The accuracy of the circuit simulation results is no better than the accuracy of the model representing the circuit. This, of course, is also true for manual analysis. For each circuit type, special data are required. The accuracy of these data can also affect simulation results. In cases of extreme complexity, even the task of generating the circuit models needed for the computer analysis may be difficult to deal with.

7.4.3.3 The Personal Computer (PC) as a Circuit Analysis Tool

The PC has emerged as a powerful, economical engineering tool with a wealth of application software, particularly for MS-DOS/Windows-based systems. PC software packages typically used in circuit analysis include:

- (1) Spreadsheets
- (2) Data Base Management Programs
- (3) Mathematics packages
- (4) Circuit analysis and simulation programs

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Spreadsheets

Spreadsheet programs are useful for performing stress analysis and simple calculations. Various different spreadsheets are available. User interfaces for most spreadsheets are similar, thus making it relatively easy to switch between different spreadsheet packages.

Data Base Management Programs

Data base management programs are very helpful for dealing with large parts data bases. These software packages usually include a built-in command language to facilitate data manipulation and report generation.

Mathematical Software Packages

A variety of general purpose mathematical software packages are currently available. Typical package capabilities include:

- (1) Simultaneous equations
- (2) Complex variables
- (3) Derivatives and integrals
- (4) Iterations
- (5) Trigonometric and exponential functions
- (6) Equations entered in their normal form can generate output plots
- (7) Statistical functions
- (8) Cubic spline curve fitting
- (9) Fast Fourier transforms and inverse vectors and matrices
- (10) User-definable functions,
- (11) 3-dimensional plotting.

Additional features might include:

- (1) A scientific word processor, complete with mathematical function symbols.
- (2) Ability to solve both linear/non-linear simultaneous equations with constraints and conditions.
- (3) A "root" function which can solve for the zeros of linear and non-linear functions and combinations thereof.
- (4) Support for complex arithmetic and matrix data.
- (5) Ability to read and write scalar and matrix/vector data to standard ASCII files; or formatted files for matrix or vector data.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

- (6) Matrix operators: addition, subtraction, multiplication, inversion and powers, (where negative powers of the matrix are powers of the inverse), determinant, transpose, and complex conjugate along with numerous matrix functions.
- (7) Vector operators including: scalar multiplication, dot product, scalar division, addition, subtraction, scalar subtraction, magnitude, and complex conjugate along with numerous other vector functions.
- (8) Support for various mathematical functions including; trigonometric, hyperbolic, log, exponential, Bessel, complex variables, interpolation, statistical, linear regression and Fourier transform.

Circuit Analysis and Simulation Programs**Analog Circuit Simulation**

The different analog simulation programs available typically perform similar circuit analysis functions and program enhancements are implemented regularly. Typical features include :

- (1) DC (bias point) and AC (frequency response) steady state analysis
- (2) AC and DC Transient (time response) analysis
- (3) Noise Analysis
- (4) AC and Transient analyses at fixed temperatures
- (5) FOURIER Analysis
- (6) Worst-Case Analysis
- (7) MONTE CARLO Analysis
- (8) Component sweeps
- (9) Initial condition documentation
- (10) MACRO Models
- (11) Continuous and piece-wise nonlinearities
- (12) Graphic plot or tabular output

A MONTE CARLO analysis option allows multiple repetitive runs to be performed with a random selection of part values (within the tolerance band) for each run. This option can usually be applied to all types of circuit analyses. Data reduction capability then allows deviations from the nominal to be determined and tabulated to determine the probability of proper circuit performance.

Schematic capture interfaces may be included or they are available for most popular packages. Using one of these packages then allows you to go directly from the schematic to the circuit simulation.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Device Models and Parts Data

Device model libraries are usually supplied with the simulation program. Typically they might include: Diodes and Rectifiers, Bipolar Transistors, Power MOSFETs (with Enhanced Curttice and Raytheon models), GaAs MESFETS, Operational Amplifiers, Transformers and Power Inductors (with Jiles-Atherton nonlinear ferromagnetic equations), Voltage Comparators, Switches and miscellaneous parts such as; Voltage-controlled - capacitance, - inductance, - resistance, - conductance. More extensive integrated circuit libraries are also frequently available when needed from the part manufacturers themselves.

Semi-automated processes for creating model libraries may also be included. The parameters are typically estimated from the manufacturers' data sheet parameters. The process is interactive, prompts are provided for the input data, device curves can be presented for verification and the results can be saved in a library file.

Once they are developed, the circuit model libraries provide a repeatable, accurate, basis for analysis. Upon completion of the analysis, the results can easily be integrated into a final report.

Digital Circuit Simulation

Typical program features include:

- (1) Schematic capture interface
- (2) Extensive model libraries for specific ICs
- (3) Logic simulation
- (4) Multi-state simulator
- (5) Timing analysis
- (6) Nominal and worst-case timing
- (7) Race, spike, hazard and pulse width analyses
- (8) Fault simulation
- (9) Grading of test vectors
- (10) ATE tester interfaces are available
- (11) Ethernet link to workstations and/or mainframes

Digital circuit simulators are very convenient for performing critical timing analyses. Graphic display of the circuit nodes simplifies the analysis of timing relationships. Advanced program features, such as load-dependent delays improve the accuracy of the analysis and eliminate overly conservative delay estimates.

7.4.4 Fundamental Design Limitations

Probably the first and prime step in the establishment of reliability criteria is the establishment of the boundaries which represent the limitations on the controlled characteristics for the component or device in question. Some of the limitations are commonly known: breakdown voltage, power

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

dissipation limitation, current density limitations, and similar factors. Many, however, are either poorly known, or possibly not known at all. Often it is these factor which cause difficulties in circuits.

If one examines the behavior of components in systems, one finds that there normally is a region of operation in which failures are rare or unlikely, but when operating conditions reach a possibly undefinable level, the probability of failure rises substantially. Conversely, with any given configuration, improvements in reliability as a result of redesign may be easy to obtain to a certain level of improvement, and then become progressively more difficult to obtain.

Improvement of reliability in terms of these criteria generally makes more sense than either attempting to attain an excessively high value for all components or being satisfied with an excessively small value based on the poor reliability of the few components. Limiting the collector supply voltage to the minimum provides a very economical way of improving the reliability of a given circuit.

The optimization of the reliability of a system on a circuit-by-circuit basis might appear to be an excessively time consuming and difficult problem. Actually, however, such need not be the case, since it is entirely practical to test at the design state (on paper) the effects of voltage reduction on circuit performance. Since it is necessary to limit voltage gain for reasons of circuit stability, proceeding in this manner might lead to an occasional additional amplifier circuit but it should at the same time lead to substantially reduced power consumption and substantially reduced cooling problems. Both of these are important criteria for reliability.

The following paragraphs discuss some fundamental design limitations which are important to designers of military electronic equipment.

7.4.4.1 The Voltage Gain Limitation

The development of radar brought with it the need to be able to amplify very weak signals in the presence of strong ones, and for the first time made the question of stability and freedom from ringing a prime consideration in tuned amplifiers. These tuned amplifiers frequently were required to have voltage amplifications as great as a million overall, with no change in operating frequency permitted.

The basic criterion which must be satisfied, both for each individual amplifier stage and for the amplifier as a whole, is that the loop amplification of individual elements as well as of the assembled groups of elements must be rigidly limited to assure that stability will not be impaired. This stability problem is essentially a phase-sum problem. If an input voltage is applied to the amplifier or stage in question, then the voltage returned through feedback to be summed into the input voltage is the product of this voltage by the amplification "around the loop" from input back to input

$$K_L = K_v \cdot K_f \tag{7.3}$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

where K_v is the forward voltage amplification to the output, and K_f is the feedback "amplification" from the output back to the input on an open-loop basis.

The modified forward amplification, K'_v , then takes the form:

$$K'_v = K_v / (1 - K_v K_f) \quad (7.4)$$

and the phasor term $(1 - K_v K_f)$ determines both the variation of the signal amplitude and the signal phase.

Clearly, one of the requirements of any amplifier to which Eq. (7.3) applies is that $|K_v K_f|$ must be small compared to unity, or a potentially unstable situation can develop. In addition, significant phase shift in the output circuit compared to the input can occur even with relatively small values of $|K_v K_f|$ values as small as 0.1 or 0.2, for example. In such a situation, as much as 5 to 10 degree phase discrepancy per stage can be encountered.

Where phase stability is of prime importance, it is evident that values of $|K_v K_f|$ should be less than 0.01 if at all possible, as then there is reasonable chance that the cumulative phase angle discrepancy in a system may be limited to a fraction of a radian. The design of an amplifier meeting this limitation can be both difficult and painstaking, and the mechanical realization of the calculated design can be even more difficult. The design techniques described in Reference [35] offer possibly one of the best ways of achieving the required results.

Early radar experience quickly showed that the limit on per stage gain K_v for achieving amplitude and phase stability with minimum to modest ringing proved to be approximately 10. (It is possible to get device gains of 100 with common grid or common base circuits, but the required impedance transformation required to match the input circuit for the succeeding amplifier typically reduces the overall stage gain back to approximately 10.) This means that the maximum permitted value for K_f is approximately 0.01 to 0.02, for a power isolation possibly as much as 40 dB. Where phase stability is of primary importance, the maximum permitted value for K_f is nearer 0.001 than 0.01.

It is very important to control and restrain the circulation of carrier frequency currents throughout any multistage amplifier, since if five stages overall are involved, the isolation from output back to input must be about 0.01^5 or 10^{-10} . This is the reason that radar IF amplifiers were designed to receive power in the vicinity of the middle stage, and R-C decoupling was used in both directions for supply voltages, and L-C decoupling for heater currents. All voltage feed points were in addition individually bypassed, and grounds grouped within the channel in such a way as to prevent circulation of carrier frequency currents in the channel.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Clearly, there is really nothing magic about the value of K_v of 10. The magic number, if one exists, is in fact the "invariant" $K_v \cdot K_f$ whose value must be sufficiently small to limit the phase and amplitude excursions in the signal. This is the basic stability criterion. But there definitely is an upper limit on the value of K_v , at least in a practical way, since there is a lower practical limit on how small K_f can be made successfully in production type equipment. The internal stage voltage gain from input to output on control separation amplifiers can be significantly higher, since the input admittances for these devices are sufficiently high that the return feedback gain is severely reduced.

This limitation on voltage gain has very interesting consequences, particularly in design for reliable operation. The voltage gain of a bipolar transistor is given by Eq. (7.5).

$$K_v = \kappa \Lambda I_C Z_L \quad (7.5)$$

where:

K_v	=	forward voltage amplification
I_C	=	collector current
Z_L	=	load impedance
κ	=	efficiency factor $\cong 1$
Λ	=	$q/kT = 40V^{-1}$ at $25^\circ C$
q	=	electron charge
k	=	Boltzmann's constant
T	=	absolute temperature

In this equation, it is evident that $I_C Z_L$ is the maximum signal voltage for Class A operation.

It is possible to relate the voltage $I_C Z_L$ to the minimum possible supply voltage V_{CC} , which can be used with the ideal device in question to produce the required operating characteristics. The minimum supply voltage may then be defined in terms of the equation

$$I_C Z_L = \kappa_\eta (V_{CC} - V_{SAT}) \quad (7.6)$$

where κ_η is a parameter which relates the output load voltage to the supply voltage and V_{SAT} is the maximum saturation voltage. κ_η usually has a value between 0.2 and 1.0. Substituting Eq. (7.6) in Eq. (7.5) gives the result:

$$K_v = \kappa \kappa_\eta \Lambda (V_{CC} - V_{SAT}) \quad (7.7)$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

This equation may be solved for the minimum supply voltage V_{CC} for a device in a circuit to give

$$|V_{CC}| = |K_{\nu}| (\kappa \kappa_{\eta} \Lambda)^{-1} + V_{SAT} \quad (7.8)$$

In Eq. (7.8), the value of κ_{ν} is about 10, typical values of $\kappa \kappa_{\eta}$ are less than unity, and V_{sat} is a few tenths of a volt. As a result, with $\kappa \kappa_{\eta} = .5$, for example, the minimum value of supply voltage required for a circuit can be expected to be roughly a twentieth of the voltage gain. This means that the range of required supply voltage is between 0.5 and 10V, the lower voltage limit applying to the common emitter configuration, and the higher to the common base configuration.

The significance of this relation cannot be overemphasized. The properties of the device and its associated circuitry are controlled largely by the current level selected for operation, and ***there is little point to selecting a supply voltage for the output circuit which is more than marginally greater than calculated by Eq. (7.8)***. Selection of a higher voltage leads either to excessive power dissipation, excessive gain with its inherent instability, or combinations of these conditions. In short, the selected supply voltage should be as small as possible consistent with the demands on the circuits.

This discussion should not be construed to mean that the base supply voltage provided for base bias current and voltage necessarily can be as small as that for the collector. Since crude stabilization of circuits is frequently obtained by controlling the base current in a transistor, the supply voltage provided for this function must be sufficiently large to assure that an adequate constancy of current level can be achieved. This and this alone is the justification for use of a large voltage, yet the current requirement for these circuits is sufficiently small that a substantial decrease in power dissipation and a substantial improvement in reliability could be achieved through the use of separate power sources for these two functions. In comparison, then, one source of high current and low voltage is required, and one of higher voltage but substantially smaller current also is required. Using a common source for both clearly leads to the worst failures of each! Also, use of two power sources allows a better matching of total power and current to the demand resulting in a smaller, lighter, and less expensive solution than with a single power supply.

7.4.4.2 Current Gain Limitation Considerations

The voltage gain limitation is electrostatic, or charge control, in nature. It is particularly important with transadmittance² devices, which tend to have a relatively high input impedance and tend to become regenerative by passing through a zero admittance (infinite impedance) condition.

² Transadmittance for a bipolar transistor is $y'_f = \Lambda I_C$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

The network dual of the voltage gain limitation is the current gain limitation. It is technically possible for this also to be critical, but at present its consequences are much less severe than its dual. Probably the principal reason for this is the rapidity of decay of magnetic fields associated with currents due to mutual cancellation of opposing components. Additional reasons are the dependence on rate-of-change of current (since only changing fields create voltage and currents), and the nonexistence of true transimpedance devices.

The control of magnetic fields proves to be one of control of fluctuating currents. The more that can be done to keep current fluctuations isolated and out of wires and shielding structures, the more freedom there is from coupling currents and fields. Size of loops carrying fluctuating currents should be kept to an absolute minimum unless the inductive properties of the loop are essential to the operation at hand. Even then the loop or coil should be so designed and so installed that it generates its field efficiently, so that an adequate quality factor, or Q , is obtained, and so that coupled fields and circulating currents induced and generated by the field are limited to regions where they are required and otherwise kept to a practical minimum.

7.4.4.3 Thermal Factors

One of the major problems in the use of transistor circuits is the stabilization of operating conditions so that the circuit can give the required performance over an adequate range of environmental conditions.

There are two principal thermal factors that affect the stability of transistor circuits. The first factor is the reverse leakage current of the collector base junction, the so-called I_{CO} , and the second factor is the variation of V_{BE} with temperature. The leakage current increases rapidly as the temperature of the transistor is increased. This effect limits the conditions under which the transistor can provide effective operation (Figure 7.4-18). This current, in conjunction with the current gain of the transistor, limits the minimum usable current through the common emitter amplifier, thereby restricting the available range of operation.

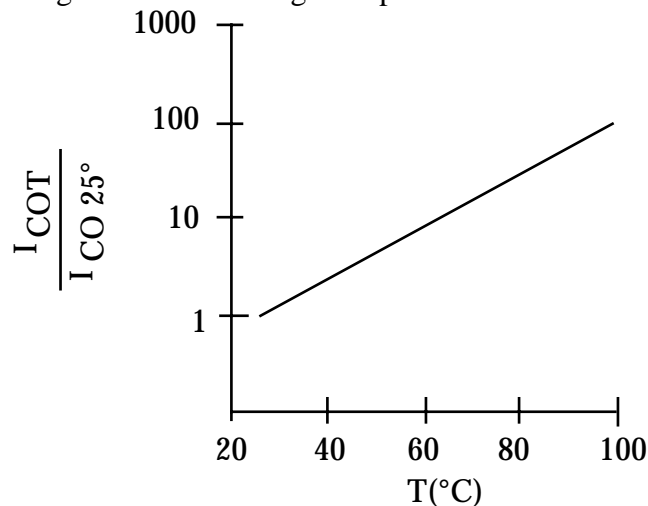


FIGURE 7.4-18: RATIO OF I_{CO} OVER TEMPERATURE T TO I_{CO} AT $T = 25^\circ\text{C}$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Even though it is possible to use the transistor in the common emitter circuit with very small values of currents, the nonlinearity of the device when the base current has a reverse polarity is so pronounced that it is not practical to attempt to do so.

The variation of the base-to-emitter voltage with temperature for fixed values of base and emitter current is the second important thermal property of a transistor requiring compensation. The voltage between base and emitter affects the static operation of the transistor, and it also affects the small signal operation. Because the static, or Q-point for the transistor varies rapidly with temperature if the base voltage is fixed, it is necessary to fix the Q-point in a way to assure that a full range of operating conditions is available over the required range of operating temperature. The static stability must be determined in terms of the practical circuit in use, and the circuit must be designed to provide the required stability.

Reference [6] provides detailed design procedures for thermal stabilization of circuits, as well as design procedures to prevent thermal runaway.

7.5 Fault Tolerant Design

Simply stated, fault tolerant design means providing a system with the ability to operate, perhaps at a degraded but acceptable level, in the presence of faults. The goal of fault tolerance is to intercept the propagation of faults so that failure does not occur, usually by substituting redundant functions affected by a particular fault. Depending on the system operational requirements, and the fault tolerant design techniques being implemented, a fault tolerant system may have to detect, diagnose, confine, mask, compensate and recover from faults. Systems are still being built today where real time reconfiguration, in the presence of a fault, is not required.

These system still need to have the capability to detect and isolate a failure, but may only require manual intervention to reconfigure the system to compensate. Other systems, such as those designed for space applications, may require built-in capabilities to detect, isolate, confine, mask, compensate and recover from faults in the system.

Each of the preceding concepts (i.e., fault detection, isolation, confinement, etc.) are typically related to what is known as redundancy management. Redundancy is typically necessary to achieve fault tolerance, but is not in itself sufficient for fault tolerance. For example, a system may contain redundant elements performing the same function such that in the presence of a fault, at least one of the outputs or results is correct. However, if the user must determine which result is correct, then only the user is performing the fault tolerant function. Only when the system is designed to determine which redundant result or output is correct for the user can we say that the system is fault tolerant. Using this example, redundancy management controls the non-faulty resources to provide the correct result. In this context then, each of the referenced concepts above can now be defined.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

- (1) Fault Detection: The process of determining that a fault has occurred.
- (2) Fault Isolation: The process of determining what caused the fault, or exactly which subsystem or component is faulty.
- (3) Fault Containment: The process that prevents the propagation of faults from their origin at one point in a system to a point where it can have an effect on the service to the user.
- (4) Fault Masking: The process of insuring that only correct values get passed to the system boundary in spite of a failed component.
- (5) Fault Compensation: If a fault occurs and is confined to a subsystem, it may be necessary for the system to provide a response to compensate for output of the faulty subsystem.

7.5.1 Redundancy Techniques

There are essentially two kinds of redundancy techniques employed in fault tolerant designs, space redundancy and time redundancy. Space redundancy provides separate physical copies of a resource, function, or data item. Time redundancy, used primarily in digital systems, involves the process of storing information to handle transients, or encoding information that is shifted in time to check for unwanted changes. Space, or hardware redundancy is the approach most commonly associated with fault tolerant design. Figure 7.5-1 provides a simplified tree-structure of hardware redundancy techniques that have been used or considered in the past.

A detailed discussion of each of the techniques can be found in Section 7.5.3 through 7.5.5.

7.5.1.1 Impact on Testability

As discussed previously, many of today's more sophisticated systems require the ability to not only detect faults, but to diagnose or isolate faults, and to reconfigure the system to avoid system failure. Automated fault detection and isolation has therefore become an essential means of obtaining highly fault tolerant systems. Because of this, the design of the diagnostic system, including any built-in-test (BIT) features and the overall testability of the design are important tradeoffs that need to be made as part of the fault tolerant design process. Table 7.5-1 presents a sample list of hardware fault tolerant design approaches and their impact on diagnostic approaches and BIT.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

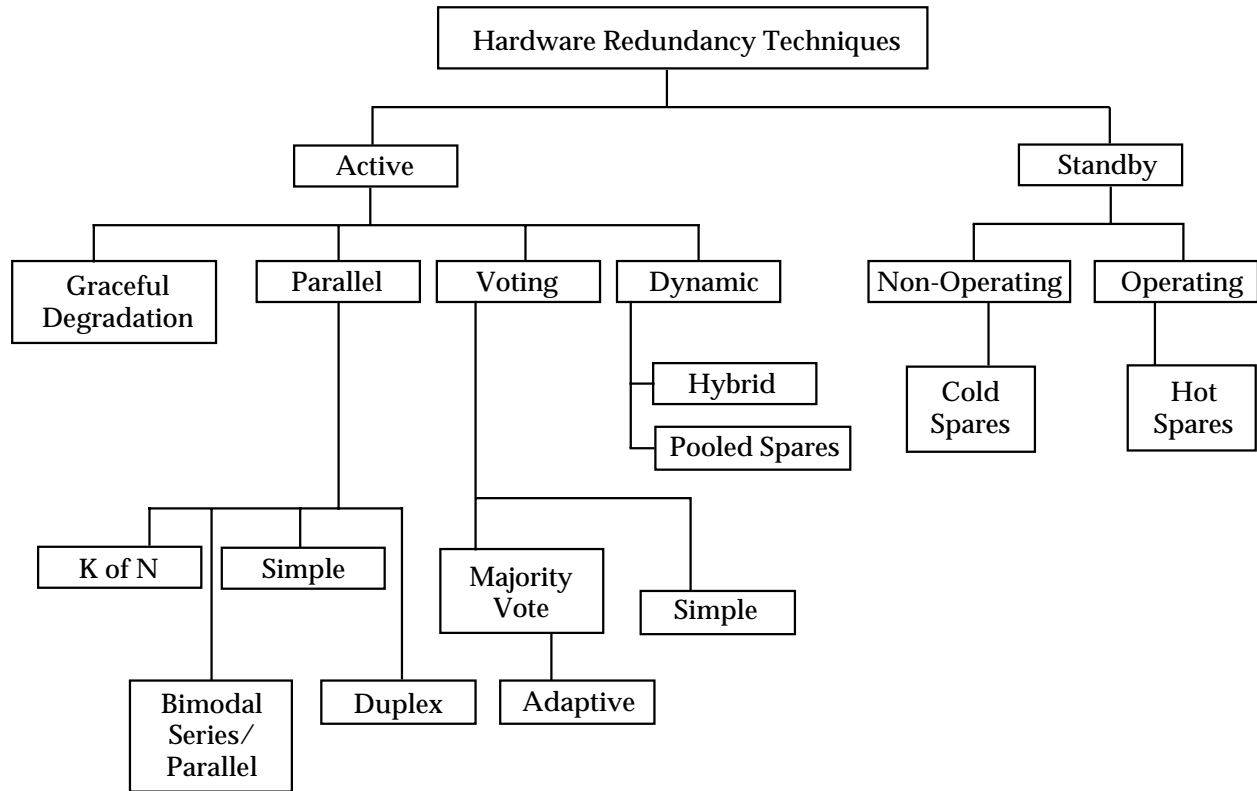


FIGURE 7.5-1: HARDWARE REDUNDANCY TECHNIQUES

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.5-1: DIAGNOSTIC IMPLICATIONS OF FAULT TOLERANT DESIGN APPROACHES

FAULT TOLERANT DESIGN TECHNIQUE	DIAGNOSTIC DESIGN IMPLICATIONS	BIT IMPLICATIONS
Active Redundancy	Hardware/Software is more readily available to perform multiple functions.	N/A
Active Redundancy with voting logic	Performance/status-monitoring function assures the operator that the equipment is working properly; failure is more easily isolated to the locked-out branch by the voting logic.	N/A
Stand-by Redundancy	Test capability and diagnostic functions must be designed into each redundant or substitute functional path (on-line AND off-line) to determine their status.	Passive, periodic, or initiated BIT.
Active Redundancy	N/A	Limited to passive BIT (i.e., continuous monitoring) supplemented with periodic BIT.

No matter what technique is chosen to implement fault tolerance in a design, the ability to achieve fault tolerance is increasingly dependent on the ability to detect, isolate, and repair malfunctions as they occur, or are anticipated to occur. This mandates that alternate maintainability diagnostic concepts be carefully reviewed for effectiveness before committing to a final design approach. In particular, BIT design has become very important to achieving a fault tolerant system. When using BIT in fault tolerant system design, the BIT system must:

- (1) Maintain a real-time status of the system's assets (both on-line and off-line equipment)
- (2) Provide the operator with the status of available system assets
- (3) Maintain a record of hardware faults and reconfiguration events required for system recovery during the mission for post-mission evaluation and corrective maintenance.

For fault tolerant systems, it is important that the design's inherent testability provisions include the ability to detect, identify, recover, and if necessary reconfigure, and report equipment malfunctions to operational personnel. Fault tolerant systems often are characterized by complex, non-serial reliability block diagrams, a multitude of backups with non-zero switch-over time, and imperfect fault detection, isolation, and recovery. Therefore it is imperative that effective testability provisions be incorporated in the system design concept. If not, the design, when fielded, will exhibit long troubleshooting times, high false alarm rates, and low levels of system readiness.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

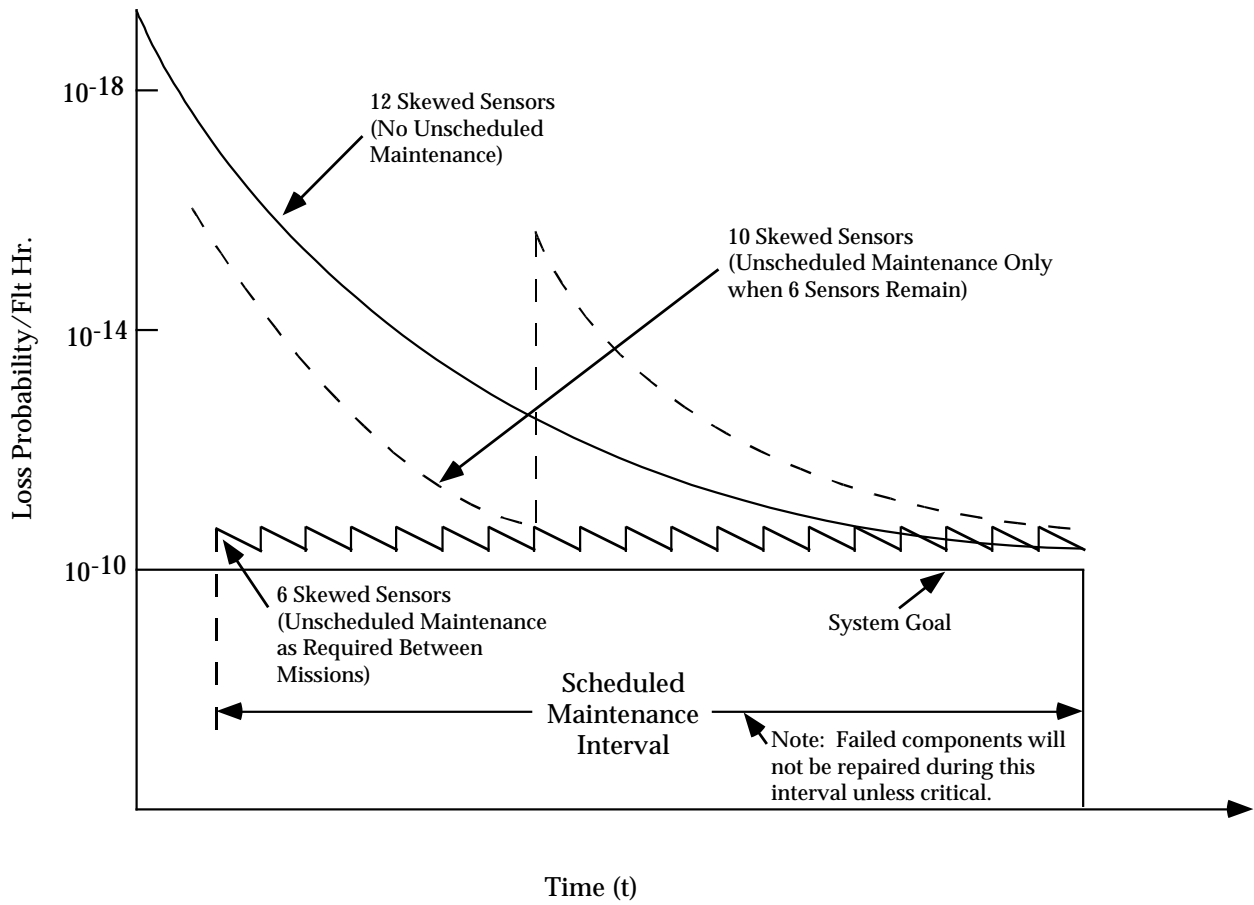
7.5.2 Reliability Role in the Fault Tolerant Design Process

The role of the reliability engineer in regards to fault tolerant design requirements is to assure that system reliability requirements are achievable for each of the fault tolerant design approaches being considered. Further, to properly design a fault tolerant system, including a diagnostic scheme, the designer needs to understand how the system can fail, and the effects of those faults. This requires that a failure mode and effects analysis (FMEA) be performed, as a minimum. The FMEA will identify which faults can lead to system failure and therefore must be detected, isolated and removed to maintain system integrity. In general, the reliability design manager must ask the following questions:

- (1) How do the system fault tolerance requirements impact the overall R/M/A requirements?
- (2) Where should fault tolerant design methods be applied?
 - (a) Which functions involve the most risk to mission success?
 - (b) What is the effect of the operating environment
 - (c) What maintenance strategy/policy needs to be considered?
- (3) What is the effect on Maintainability and Testability?
- (4) What are the constraints that affect fault tolerance ?
 - (a) cost
 - (b) size & weight
 - (c) power
 - (d) interface complexity
 - (e) diagnostic uncertainties

Each of the above questions, and others need to be considered as part of the overall fault tolerant design process. Other reliability tradeoffs to be considered involve analysis of the redundancy approaches being considered for the fault tolerant design. Section 7.5.3 - 7.5.6 provide details on methods of redundancy analysis. In addition to reliability concerns, fault tolerance also requires analysis of the impacts on maintainability and testability. As an example, consider Figure 7.5-2. This figure illustrates a design vs. corrective maintenance tradeoff analysis performed early in the product development phase. In particular, the figure shows the tradeoff of restoration frequency versus the number of sensors being used to meet requirements. This program requires a time period for allocating a scheduled maintenance activity and a probability of less than one in 10 billion per flight hour that a total loss of the skewed sensor function would occur. The tradeoff is made between the number of sensors and the cost of unscheduled maintenance activity associated with each approach. Other tradeoffs, such as cost, power, weight, etc. are also necessary. In general, as in any design analysis support function, the impacts on reliability, maintainability (including testability) and availability of a chosen fault tolerant design approach needs to be performed by the R/M/A professional.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES



Note: More Frequent Restoration of Redundancy Lowers Fault Tolerance Requirements, But Results in Higher Maintenance Manhours

FIGURE 7.5-2: EFFECT OF MAINTENANCE CONCEPT ON LEVEL OF FAULT TOLERANCE

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

As a final note on the role of the reliability engineer, consider the following reliability inputs to the development of the specification for a fault tolerant design

- (1) Critical mission definition
- (2) Quantitative mission reliability
- (3) Quantitative maintenance frequency reliability
- (4) Description of the storage, transportation, operation, and maintenance environments
- (5) Time measure or mission profile
- (6) Definition of satisfactory and acceptable degraded system performance
- (7) Tolerable failure policy (fail-safe, fail-operational, etc.)
- (8) Failure independence

These and other inputs are necessary to ensure that the system specifications are well defined and that they support the ability to clearly define the best approach that also meets R/M/A requirements.

7.5.2.1 Fault Tolerant Design Analysis

The FMEA is a primary reliability analysis, critical to the fault tolerant design process. The reliability engineer will also utilize additional techniques for analyzing the fault tolerant design to verify that it meets reliability requirements. However, many of the evaluation tools used in the past are no longer adequate to deal with more sophisticated fault tolerant designs that include more complex fault handling capabilities. Because fault handling methods include the use of fault detection and fault recovery approaches, any evaluation tool must include the ability to properly account for the effects of imperfect fault coverage (or fault detection) and fault recovery.

Monte Carlo simulation and Markov analysis techniques continue to be used as the primary means of analyzing highly sophisticated fault tolerant designs. These approaches have been modified to incorporate situations where the sequence of failure is important, where the failure is transient or intermittent, or where the response to failure (i.e., detection, isolation, recovery, reconfiguration) is imperfect. In these situations, Markov methods continue to lead the way in evaluation methods. Markov analysis is described in more detail in Section 7.5.6 and will not be discussed in detail here. In general, the Markov approach, which is used to define the specific states that a system can occupy, has been used to incorporate fault handling and recovery. A major limitation to the Markov approach is that the number of system states that must be defined to comprehensively describe a large system and model the behavior of complex fault

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

management schemes can become very large (approaching 10^5 for highly complex systems). A common solution to this problem is to partition the system into smaller systems, evaluate each partition separately, and then combine the results at the system level. However, such an approach is only exact when each partitioned subsystem's fault tolerant behavior is mutually independent of each other. If subsystem dependencies do exist, then an assumption of independence will result in only an approximate solution.

Other approaches that are now becoming more common involve decomposing the system into separate fault-occurrence and fault handling submodels. However, the inputs for this type of approach require knowledge of the distribution and parameter values of: detection, isolation, recovery, rates, etc. The following is a list of assumptions, limitations and sources of error found in existing reliability models:

- (1) Solving a fault-handling model in isolation and then reflecting its results in an aggregate model is, itself, an approximation technique. The assumptions necessary to determine a solution typically result in a lower bound (conservative) approximation of the system reliability.
- (2) Separate fault-handling models have been assumed to be independent of system state. This requires that the same fault-handling model and choice of parameters be used irrespective of the system's level of degradation. This ignores the fact that for many systems the recovery process is faster if the number of active units is smaller or that the recovery process may be different, depending on the sequence of events in different subsystems.
- (3) The common technique of partitioning the system into independent functional subgroups for computational ease is a potential source of error. The magnitude and direction of the error is a function of how truly independent/dependent the subgroups are of each other. If subgroups are assumed independent when in fact they are not, the effect is an overstatement of system reliability/availability. If subgroups are assumed completely dependent when some degree of independence exists, the effect is an understatement of the system's reliability/availability.
- (4) Some models assume a constant instantaneous fault-protection coverage factor in lieu of a separate fault handling model. These fail to recognize that during time spent in the intermediate fault-handling states to detect, isolate, and recover/reconfigure, a second item failure could result in system failure. Further, as with fault handling models, these times are generally not constant, but depend on the current state of the system.
- (5) Most models require the assumption that the system is perfect at the mission start. Therefore, they cannot evaluate the effects of latent defects (e.g., handling, manufacturing, transportation, prior mission), nor assist in determining the testability payoff or requirements for detection and removing them before the start of the mission.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Models with this limitation cannot be used to evaluate alternate maintenance concepts that include degradation between missions as an acceptable strategy.

- (6) Some models require that spares be treated exactly like active units, irrespective of their actual utilization in the system mechanization. This requires that spares are assumed to be “hot” and have the same failure rates and failure modes as the active units. This assumption will cause the model to understate the system reliability in those situations where spares are “cold” or in “stand-by” and/or where their failure rates may be less than those of the active units.
- (7) As indicated previously, some models require the assumption that item failure rates are constant throughout time. This will result in an overstatement of system reliability if the items have failure rates that increase with mission time. Some models remove this restriction and permit time-varying failure rates. However, the solution the algorithms employ requires the use of global time (as opposed to local time of entry into a state), thus precluding the use of the model for repairable systems and availability analysis.

7.5.3 Redundancy as a Design Technique

In reliability engineering, redundancy can be defined as the existence of more than one means for accomplishing a given task. In general, all means must fail before there is a system failure.

Thus, if we have a simple system consisting of two parallel elements as shown in Figure 7.5-3 with A_1 having a probability of failure q_1 and A_2 having a probability of failure q_2 , the probability of total system failure is

$$Q = q_1 q_2$$

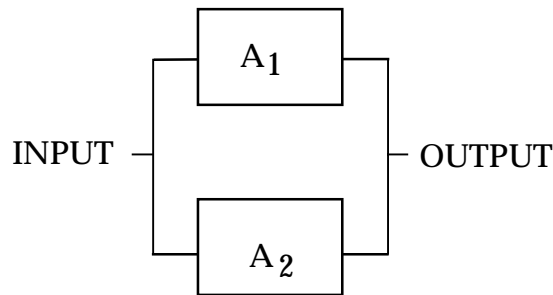


FIGURE 7.5-3: PARALLEL NETWORK

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Hence the reliability or probability of no failure is

$$R = 1 - Q = 1 - q_1 q_2$$

For example, assume that A_1 has a reliability r_1 of 0.9 and A_2 a reliability r_2 of 0.8. Then their unreliabilities q_1 and q_2 would be

$$q_1 = 1 - r_1 = 0.1$$

$$q_2 = 1 - r_2 = 0.2$$

and the probability of system failure would be

$$Q = (0.1)(0.2) = 0.02$$

Hence the system reliability would be

$$R = 1 - Q = 0.98$$

which is a higher reliability than either of the elements acting singly. Parallel redundancy is therefore a design tool for increasing system reliability when other approaches have failed. It should be pointed out that while redundancy reduces mission failures, it increases logistics failures.

In general, with n elements in parallel, the overall probability of failure at time t is

$$Q(t) = q_1(t) \cdot q_2(t) \cdot \dots \cdot q_n(t) \quad (7.9)$$

and the probability of operating without failure is

$$R(t) = 1 - Q(t) = 1 - q_1(t) q_2(t) \dots q_m(t) \quad (7.10)$$

which, because $q_i(t) = 1 - r_i(t)$ for each component, can also be given as

$$R(t) = 1 - [1 - r_1(t)] [1 - r_2(t)] \dots [1 - r_m(t)] \quad (7.11)$$

When each of the component reliabilities is equal, the above equations reduce to

$$Q(t) = [q(t)]^m \quad (7.12)$$

$$R(t) = 1 - [q(t)]^m = 1 - [1 - r(t)]^m \quad (7.13)$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Figure 7.5-4 summarizes the characteristics of simple parallel active redundancy.

So far it has been assumed that parallel components do not interact and that they may be activated when required by ideal failure sensing and switching devices. Needless to say, the latter assumption, in particular, is difficult to meet in practice. Therefore, the potential benefits of redundancy cannot be realized fully. The reader is referred to the cited references, e.g., References [22] and [23], for detailed treatment of redundancy with sensing and switching devices which are most ideal.

Most cases of redundancy encountered will consist of various groupings of series and parallel elements. Figure 7.5-5 typifies such a network. The basic formulas previously given can be used to solve the overall network reliability R_{AC} .

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

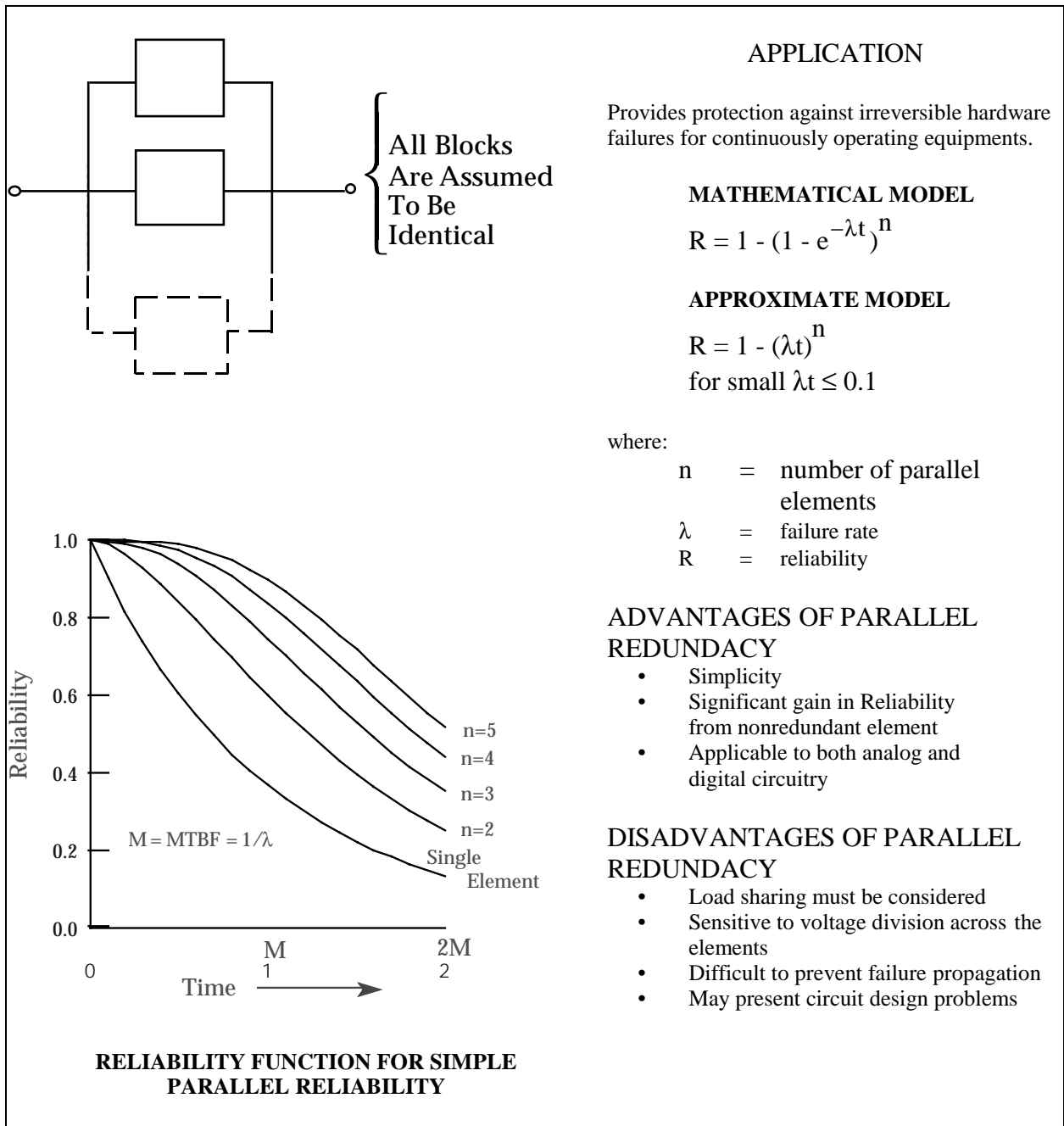


FIGURE 7.5-4: SIMPLE PARALLEL REDUNDANCY: SUMMARY

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

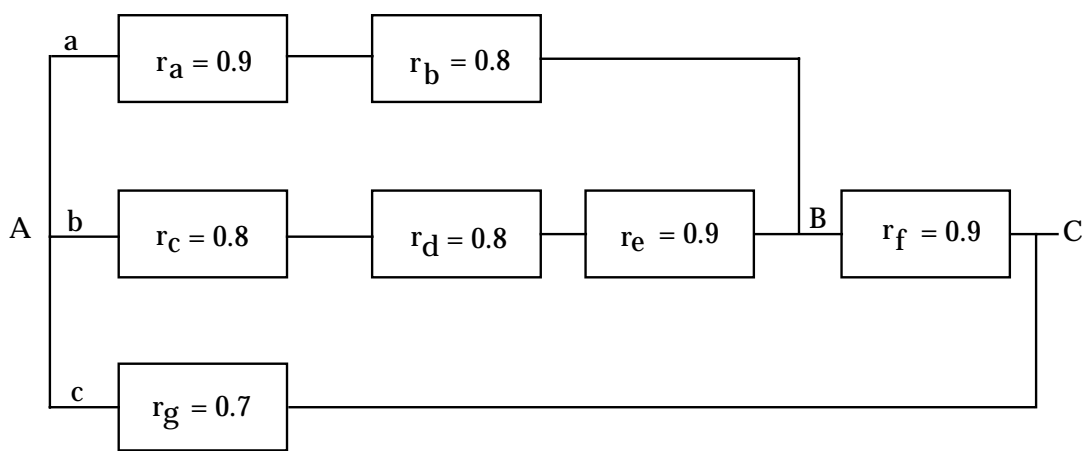


FIGURE 7.5-5: SERIES-PARALLEL REDUNDANCY NETWORK

7.5.3.1 Levels of Redundancy

Redundancy may be applied at the system level (essentially two systems in parallel) or at the subsystem, component, or part level within a system. Figure 7.5-6 is a simplified reliability block diagram drawn to illustrate the several levels at which redundancy can be applied. System D is shown with its redundant alternative D', at the system level. D' is in turn built up of redundant subsystems or components (C_1 and C_2) and redundant parts within components (b_1 and b_2 within Component B). From the reliability block diagram and a definition of block or system success, the paths which result in successful system operation can be determined. For example, the possible paths from Input to Output are:

- (1) A, a, b_1 , C_1
- (2) A, a, b_1 , C_2
- (3) A, a, b_2 , C_1
- (4) A, a, b_2 , C_2
- (5) D

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

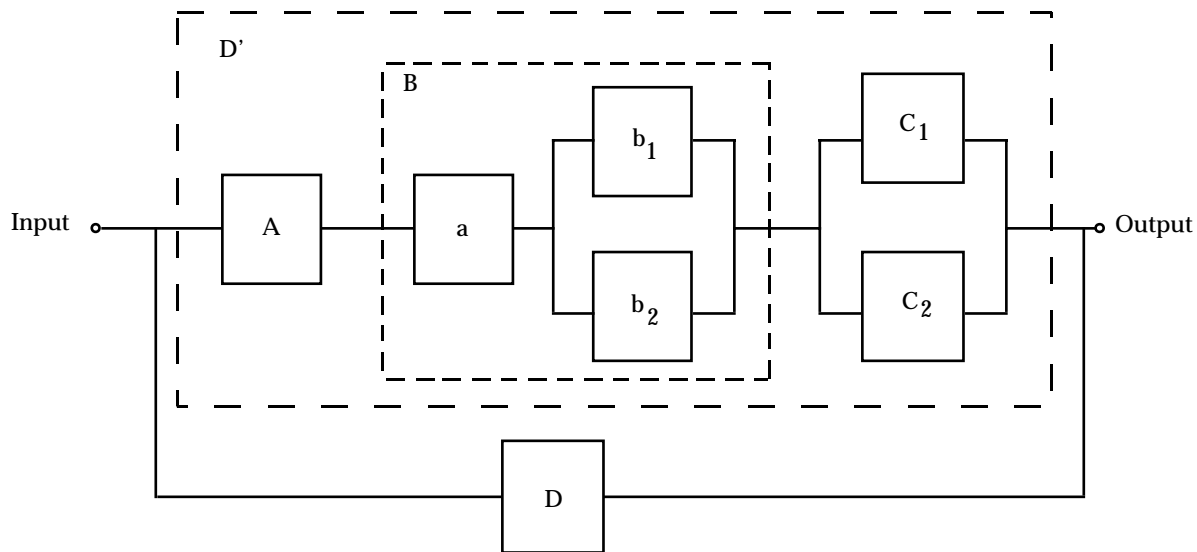


FIGURE 7.5-6: RELIABILITY BLOCK DIAGRAM DEPICTING REDUNDANCY AT THE SYSTEM, SUBSYSTEM, AND COMPONENT LEVELS

The success of each path may be computed by determining an assignable reliability value for each term and applying the multiplicative theorem. The computation of system success (all paths combined) requires a knowledge of the type of redundancy to be used in each case and an estimate of individual element reliability (or unreliability).

7.5.3.2 Probability Notation for Redundancy Computations

Reliability of redundancy combinations is expressed in probabilistic terms of success or failure -- for a given mission period, a given number of operating cycles, or a given number of time independent "events," as appropriate. The "MTBF" measure of reliability is not readily usable because of the nonexponentiality of the reliability function produced by redundancy. Reliability of redundancy combinations which are "time dependent" is therefore computed at a discrete point in time, as a probability of success for this discrete time period. The following notation is applicable to all cases and is used throughout this section:

R = probability of success or reliability of a unit or block

Q = \overline{R} = probability of failure or unreliability of a unit or block

p = probability of success or reliability of an element

q = probability of failure or unreliability of an element

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

For probability statements concerning an event:

$P(A)$ = probability that A occurs

$P(\bar{A})$ = probability that A does not occur

For the above probabilities:

$$R + Q = 1$$

$$p + q = 1$$

$$P(A) + P(\bar{A}) = 1$$

7.5.3.3 Redundancy Combinations

The method of handling redundancy combinations can be generalized as follows:

- (1) If the elements are in parallel and the units in series (Figure 7.5-7), first evaluate the redundant elements to get the unit reliability. Then find the product of all unit reliabilities to obtain the block reliability.
- (2) If the elements are in series and the units or paths are in parallel (Figure 7.5-8), first obtain the path reliability by calculating the product of the reliabilities of all elements in each path. Then consider each path as a redundant unit to obtain the block reliability.

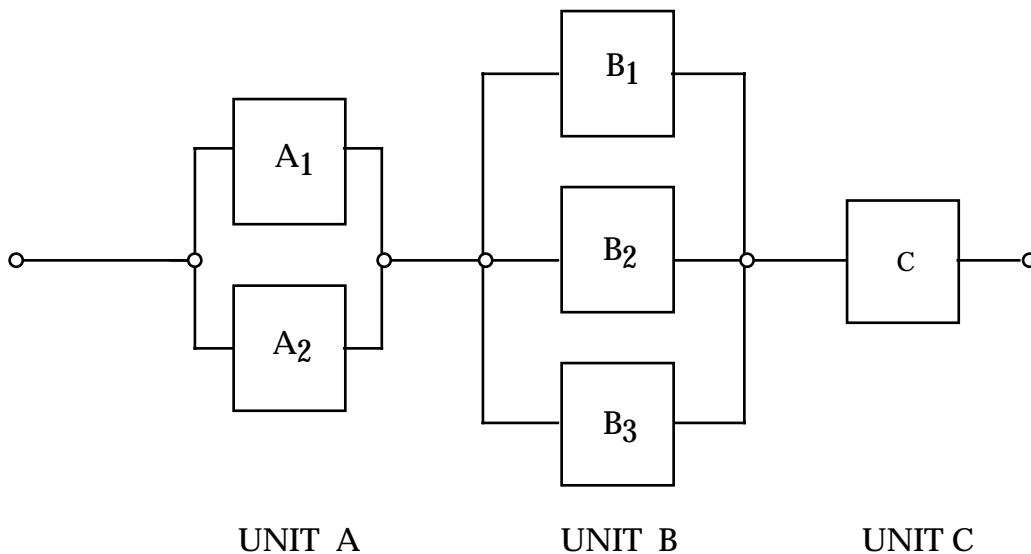


FIGURE 7.5-7: SERIES-PARALLEL CONFIGURATION

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

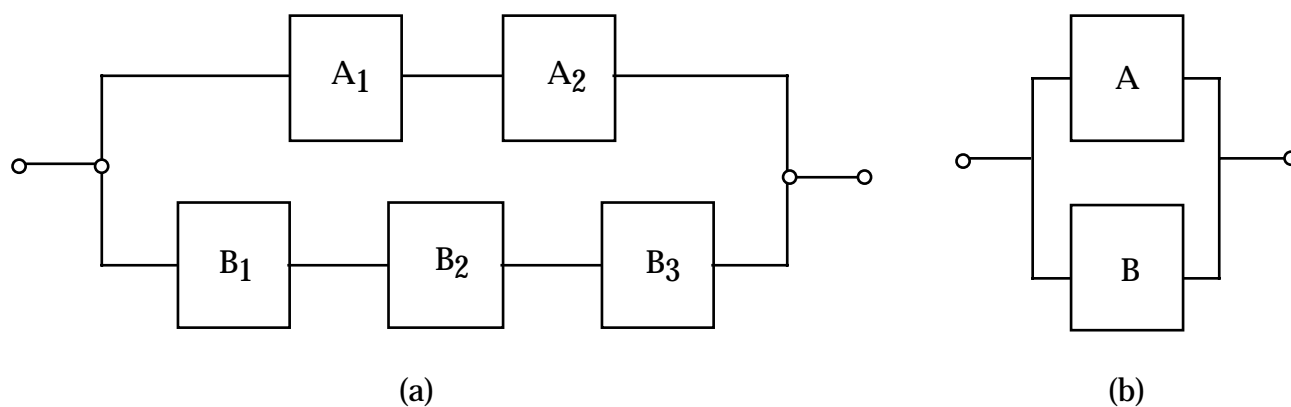


FIGURE 7.5-8: PARALLEL-SERIES CONFIGURATION

In the redundancy combination shown in Figure 7.5-7, Unit A has two parallel redundant elements, Unit B has three parallel redundant elements, and Unit C has only one element. Assume that all elements are independent. For Unit A to be successful, A_1 or A_2 must operate; for Unit B success, B_1 , B_2 or B_3 must operate; and C must always be operating for block success. Translated into probability terms, the reliability of Figure 7.5-7 becomes:

$$R = \left[1 - P(\overline{A}_1) \cdot P(\overline{A}_2) \right] \cdot [1 - P(\overline{B}_1) \cdot P(\overline{B}_2) \cdot P(\overline{B}_3)] \cdot P(C)$$

If the probability of success, p , is the same for each element in a unit,

$$\begin{aligned} R &= \left[1 - (1 - p_A)^2 \right] \cdot [1 - (1 - p_B)^3] \cdot p_C \\ &= (1 - q_A^2) \cdot (1 - q_B^3) \cdot p_C \end{aligned}$$

where:

$$q_i = 1 - p_i$$

Often there is a combination of series and parallel redundancy in a block as shown in Figure 7.5-8. This arrangement can be converted into the simple parallel form shown in Figure 7.5-8 by first evaluating the series reliability of each path:

$$p_A = p_{a_1} p_{a_2}$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

$$P_B = P_{b_1} P_{b_2} P_{b_3}$$

where the terms on the right hand side represent element reliability. Then block reliability can be found from:

$$\begin{aligned} R &= 1 - (1 - p_A) \cdot (1 - p_B) \\ &= 1 - q_A q_B \end{aligned}$$

7.5.4 Redundancy in Time Dependent Situations

The reliability of elements used in redundant configurations is usually time dependent. If the relation between element reliability and time is known, inclusion of the time factor does not change the basic notation and approach to redundancy computation outlined above. As an example, assume two active independent elements in parallel. System reliability is given by:

$$R = p_a + p_b - p_a p_b$$

This equation is applicable for one time interval. To express reliability over a segment of time, the reliability of each element must be expressed as a function of time.

Hence,

$$R(t) = p_a(t) + p_b(t) - p_a(t) p_b(t)$$

where:

$$R(t) = \text{system reliability for time } t, t > 0$$

and

$$p_a(t), p_b(t) = \text{element reliabilities for time } t$$

The failure pattern of most components is described by the exponential distribution, i.e.:

$$R(t) = e^{-\lambda t} = e^{-t/\theta}$$

where λ is the constant failure rate; t is the time interval over which reliability, R , is measured; and θ is the mean-time-between-failure.

For two elements in series with constant failure rates λ_a and λ_b , using the product rule of reliability gives:

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

$$\begin{aligned}
 R(t) &= p_a(t) p_b(t) \\
 &= e^{-\lambda_a t} e^{-\lambda_b t} = e^{-(\lambda_a + \lambda_b)t}
 \end{aligned}$$

The system reliability, $R(t)$, function is also exponential. With redundant elements present in the system, however, the system reliability function is not itself exponential. This is illustrated by two operative parallel elements whose failure rates are constant. From:

$$\begin{aligned}
 R(t) &= p_a + p_b - p_a p_b \\
 R(t) &= e^{-(\lambda_a)t} + e^{-(\lambda_b)t} - e^{-(\lambda_a + \lambda_b)t}
 \end{aligned}$$

which is not of the simple exponential form $e^{-\lambda t}$. Element failure rates cannot, therefore, be combined in the usual manner to obtain the system failure rate if considerable redundancy is inherent in the design.

Although a single failure rate cannot be used for redundant systems, the mean-time-to-failure of such systems can be evaluated. The mean life of a redundant "pair" whose failure rates are λ_a and λ_b , respectively, can be determined from:

$$\text{MTBF} = \int_0^{\infty} R(t) dt = \frac{1}{\lambda_a} + \frac{1}{\lambda_b} - \frac{1}{\lambda_a + \lambda_b}$$

If the failure rates of both elements are equal, then,

$$R(t) = 2e^{-\lambda t} - e^{-2\lambda t}$$

and

$$\text{MTBF} = \frac{3}{2\lambda} = \frac{3}{2} \theta$$

For three independent elements in parallel, the reliability function is:

$$R(t) = 1 - \left[(1 - e^{-\lambda_a t})(1 - e^{-\lambda_b t})(1 - e^{-\lambda_c t}) \right]$$

and

$$\text{MTBF} = \frac{1}{\lambda_a} + \frac{1}{\lambda_b} + \frac{1}{\lambda_c} - \frac{1}{\lambda_a + \lambda_b} - \frac{1}{\lambda_a + \lambda_c} - \frac{1}{\lambda_b + \lambda_c} + \frac{1}{\lambda_a + \lambda_b + \lambda_c}$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

If

$$\lambda_a = \lambda_b = \lambda_c = \lambda$$

then

$$R(t) = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}$$

and

$$MTBF = \frac{3}{\lambda} - \frac{3}{2\lambda} + \frac{1}{3\lambda} = \frac{1}{\lambda} + \frac{1}{2\lambda} + \frac{1}{3\lambda} = \frac{11}{6\lambda} = \frac{11}{6} \theta$$

In general, for n active parallel elements, each element having the same constant failure rate, λ ,

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

and

$$MTBF = \sum_{i=1}^n \frac{1}{i\lambda} = \sum_{i=1}^n \frac{\theta}{i}$$

7.5.5 Redundancy Considerations in Design

The two basic types of redundancy are:

- (1) Active Redundancy: External components are not required to perform the function of detection, decision and switching when an element or path in the structure fails. The redundant units are always operating and automatically pick up the load for a failed unit. An example is a multi-engined aircraft. The aircraft can continue to fly with one or more engines out of operation.
- (2) Standby Redundancy: External elements are required to detect, make a decision and switch to another element or path as a replacement for a failed element or path. Standby units can be operating (e.g., a redundant radar transmitter feeding a dummy load is switched into the antenna when the main transmitter fails) or inactive (e.g., a spare radio is turned on when the primary radio fails).

Table 7.5-2 summarizes a variety of redundancy techniques. The most important of these are discussed further later in this section.

The application of redundancy is not without penalties. It will increase weight, space requirements, complexity, cost, and time to design. The increase in complexity results in an increase in unscheduled maintenance. Thus, safety and mission reliability is gained at the expense of adding an item(s) in the unscheduled maintenance chain. The increase in

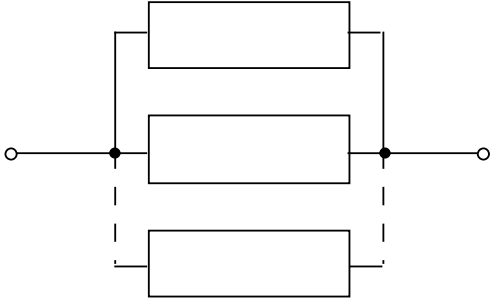
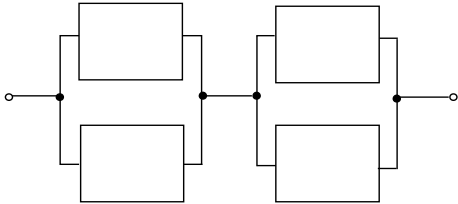
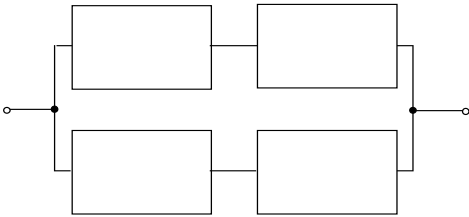
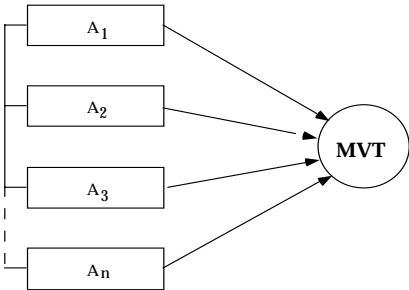
SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

unscheduled maintenance may be counteracted by reliability improvement techniques such as design simplification, derating, and the use of more reliable components, as discussed elsewhere in this Handbook.

The decision to use redundant design techniques must be based on analysis of the tradeoffs involved. Redundancy may prove to be the only available method, when other techniques of improving reliability, e.g., derating, simplification, better components, have been exhausted, or when methods of item improvement are shown to be more costly than duplications. When preventive maintenance is planned, the use of redundant equipment can allow for repair with no system downtime. Occasionally, situations exist in which equipments cannot be maintained, e.g., satellites; then redundant elements may be the best way to significantly prolong operating time.

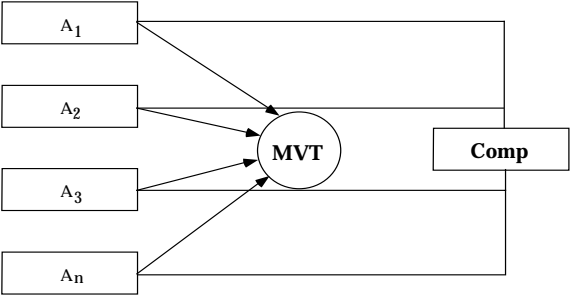
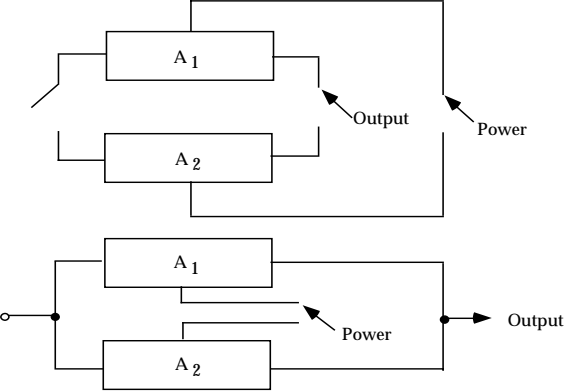
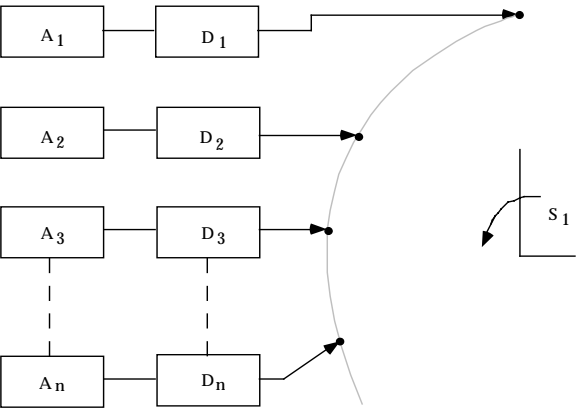
SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.5-2: REDUNDANCY TECHNIQUES

<p><u>Simple Parallel Redundancy (Active Redundancy)</u></p>  <p>(a) Bimodal Parallel/Series Redundancy</p>  <p>(b) Bimodal Series/Parallel Redundancy</p> 	<p>In its simplest form, redundancy consists of a simple parallel combination of elements. If any element fails open, identical paths exist through parallel redundant elements.</p> <p>A series connection of parallel redundant elements provides protection against shorts and opens. Direct short across the network due to a single element shorting is prevented by a redundant element in series. An open across the network is prevented by the parallel element. Network (a) is useful when the primary element failure mode is open. Network (b) is useful when the primary element failure mode is short.</p>
<p><u>Majority Voting Redundancy</u></p> 	<p>Decision can be built into the basic parallel redundant model by inputting signals from parallel elements into a voter to compare each element's signal with the signals of the other elements. Valid decisions are made only if the number of useful elements exceeds the failed elements.</p>

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.5-2: REDUNDANCY TECHNIQUES (CONT'D)

<p><u>Adaptive Majority Logic</u></p> 	<p>This technique exemplifies the majority logic configuration discussed previously with a comparator and switching network to switch out or inhibit failed redundant elements.</p>
<p><u>Standby Redundancy</u></p> 	<p>A particular redundant element of a parallel configuration can be switched into an active circuit by connecting outputs of each element to switch poles. Two switching configurations are possible.</p> <ol style="list-style-type: none"> 1) The elements may be isolated by the switch until switching is completed and power applied to the element in the switching operation. 2) All redundant elements are continuously connected to the circuit and a single redundant element activated by switching power to it.
<p><u>Operating Standby Redundancy</u></p> 	<p>In this application, all redundant units operate simultaneously. A sensor on each unit detects failures. When a unit fails, a switch at the output transfers to the next unit and remains there until failure.</p>

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

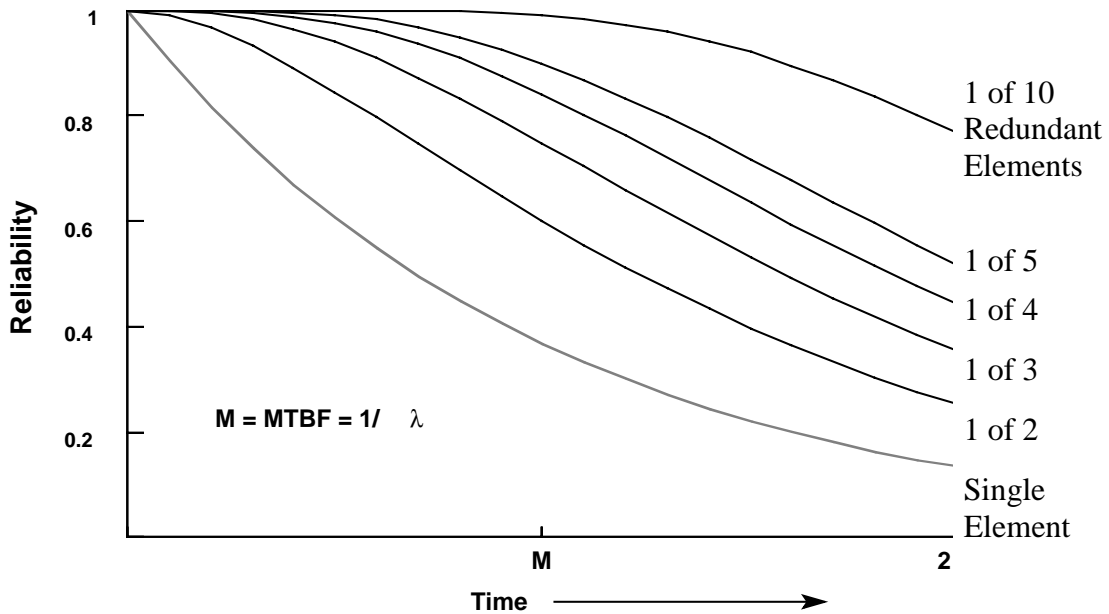
In general, the reliability gain for additional redundant elements decreases rapidly for additions beyond a few parallel elements. As illustrated by Figure 7.5-9 for simple parallel redundancy, there is a diminishing gain in reliability and MTBF as the number of redundant elements is increased. As shown for the simple parallel case, the greatest gain achieved through addition of the first redundant element is equivalent to a 50% increase in the system MTBF. Optimization of the number of parallel elements is discussed in Section 7.5.5.5.

In addition to maintenance cost increases due to repair of the additional elements, reliability of certain redundant configurations may actually be less than that of a single element. This is due to the serial reliability of switching or other peripheral devices needed to implement the particular redundancy configuration. Care must be exercised to insure that reliability gains are not offset by increased failure rates due to switching devices, error detectors and other peripheral devices needed to implement the redundancy configurations. One case where the reliability of switching devices must be considered is that of switching redundancy. This occurs when redundant elements are energized but do not become part of the circuit until switched in after the primary element fails. See Section 7.5.5.2.6 for further discussion.

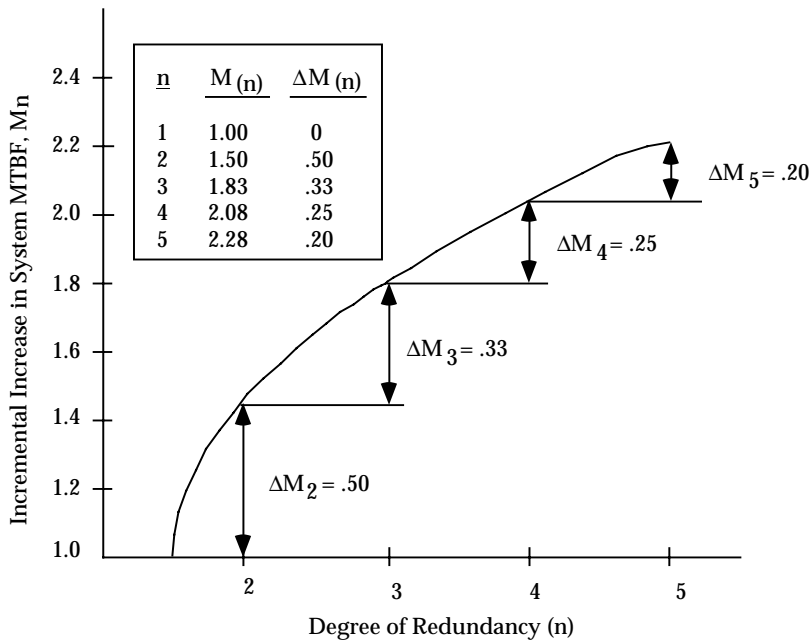
The effectiveness of certain redundancy techniques (especially standby) can be enhanced by repair. Standby redundancy allows repair of the failed unit (while operation of the good unit continues uninterrupted) by virtue of the switching function built into the standby redundant configuration. Through continuous or interval monitoring, the switchover function can provide an indication that failure has occurred and operation is continuing on the alternate channel. With a positive failure indication, delays in repair are minimized. A further advantage of switching is related to built-in test (BIT) objectives. Built-in test can be readily incorporated into a sensing and switchover network for ease of maintenance purposes.

An illustration of the enhancement of redundancy with repair is shown in Figure 7.5-10. The increased reliability brought about by incorporation of redundancy is dependent on effective isolation of redundant elements. Isolation is necessary to prevent failure effects from adversely affecting other parts of the redundant network. In some cases, fuses or circuit breakers, overload relays, etc., may be used to protect the redundant configuration. These items protect a configuration from secondary effects of an item's failure so that system operation continues after the element failure. The susceptibility of a particular redundant design to failure propagation may be assessed by application of failure mode and effects analysis as discussed in Section 7.8. The particular techniques addressed there offer an effective method of identifying likely fault propagation paths.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES



(a) Simple Active Redundancy for One of n Element Required



(b) Incremental Increase in System MTBF for n Active Elements

FIGURE 7.5-9: DECREASING GAIN IN RELIABILITY AS NUMBER OF ACTIVE ELEMENTS INCREASES

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

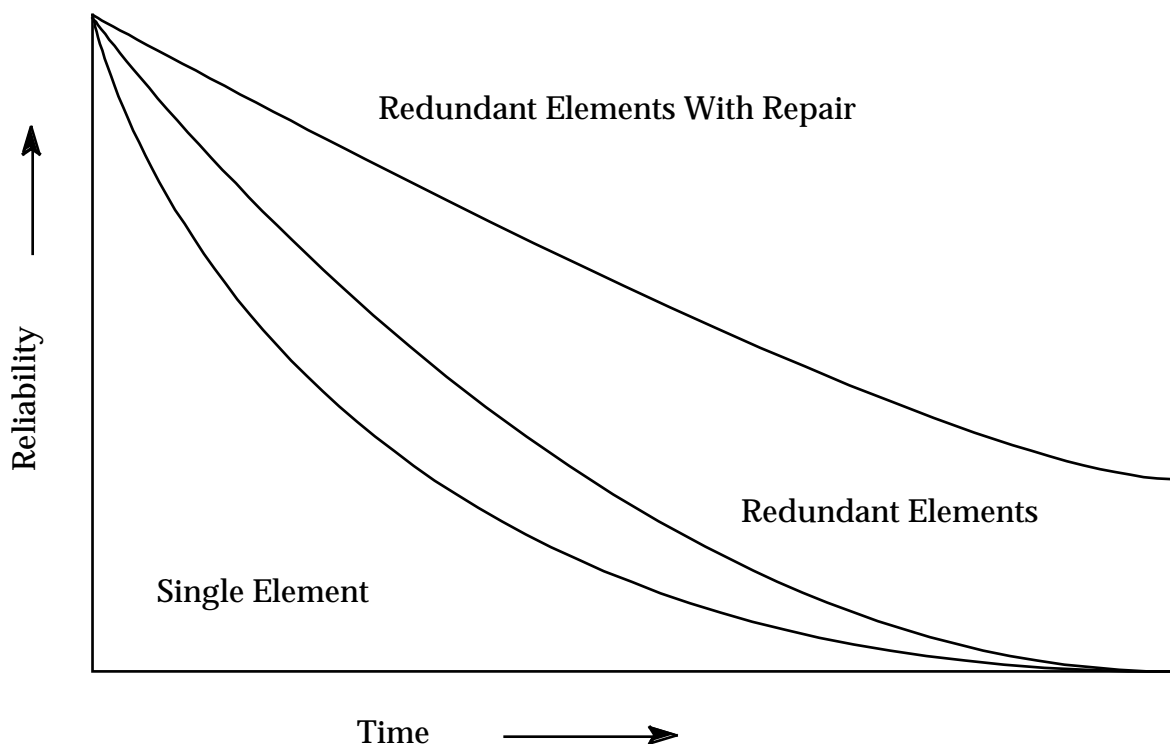


FIGURE 7.5-10: RELIABILITY GAIN FOR REPAIR OF SIMPLE PARALLEL ELEMENT AT FAILURE

Redundancy may be incorporated into protective circuits³ as well as the functional circuit which it protects. Operative redundancy configurations of protection devices (e.g., fuse, circuit breaker) can be used to reduce the possibility that the "protected" circuit is not completely disabled should the protective circuit device open prematurely or fail to open due to overcurrent.

The incorporation of redundancy into a design must take into account "checkability." Some items may not be checkable prior to mission start. Such items must then be assumed to be functional at the beginning of the mission. In reality, pre-mission failures of redundant items could be masked. If it is not known that redundant elements are operational prior to mission start, then the purpose of redundancy can be defeated because the possibility exists of starting a mission without the designed redundancy (a reliability loss). The designer must take this into account for built-in test planning, inclusion of test points, packaging, etc., when redundancy is used in system design.

³ It should be noted that the need for or usefulness of modeling reliability at the circuit level is not universally accepted. In particular, many engineers question the value of such modeling for modern technologies. Discussion of circuit-level modeling is included here since it may be of value in some instances.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.5.5.1 Partial Redundancy

Instances in which the system is successful if at least one of n parallel paths is successful has been discussed. In other instances, at least k out of n elements must be successful. In such cases, the reliability of the redundant group (each with the same Probability of Success, p) is given by a series of additive binomial terms in the form of

$$P(k, n | p) = \binom{n}{k} p^k (1 - p)^{n-k}$$

Two examples of partial redundancy follow.

Example 1:

A receiver has three channels. The receiver will operate if at least two channels are successful, that is, if $k = 2$ or $k = 3$. The probability of each channel being successful is equal to p ; then

$$\begin{aligned} R &= P(2, 3 | p) + P(3, 3 | p) \\ R &= \binom{3}{2} p^2 (1 - p) + \binom{3}{3} p^3 (1 - p)^0 \\ R &= 3p^2 (1 - p) + p^3 \\ R &= 3p^2 - 2p^3 \end{aligned}$$

Use of the binomial formula becomes impractical for hand calculation in multi-element partial redundant configurations when the values of n and k become large.⁴ In these cases, the normal approximation to the binomial may be used. The approach can be best illustrated by an example.

Example 2:

A new transmitting array is to be designed using 1000 RF elements to achieve design goal performance for power output and beam width. A design margin has been provided, however, to permit a 10% loss of RF elements before system performance becomes degraded below the acceptable minimum level. Each element is known to have a failure rate of 1000×10^{-6} failures per hour. The proposed design is illustrated in Figure 7.5-11, where the total number of elements is $n = 1000$; the number of elements required for system success is $k = 900$; and, the number of element failures permitted is $r = 100$. It is desired to compute and plot the reliability function for the array.

⁴ See any good textbook on probability and statistics.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

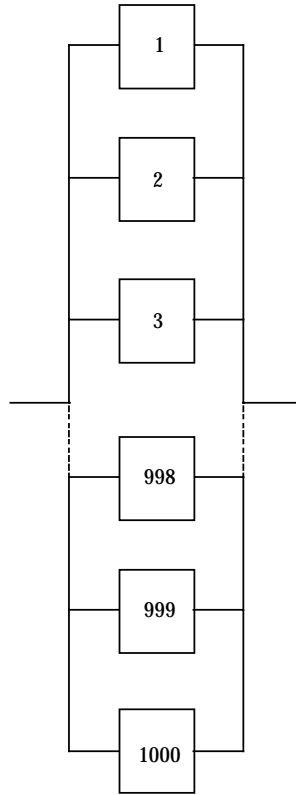


FIGURE 7.5-11: PARTIAL REDUNDANT ARRAY

For each discrete point of time, t , the system reliability function, $R_S(t)$ is given by the binomial summation as:

$$\begin{aligned}
 R_S(t) &= \sum_{x=0}^r \binom{n}{x} p^{n-x} q^x \\
 &= \sum_{x=0}^{100} \binom{1000}{x} (e^{-\lambda t})^{n-x} (1 - e^{-\lambda t})^x
 \end{aligned}$$

where:

$$\begin{aligned}
 q &= 1 - e^{-\lambda t} \\
 p &= e^{-\lambda t} \\
 x &= \text{number of failures} \\
 \lambda &= \text{element failure rate}
 \end{aligned}$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

This binomial summation can be approximated by the standard normal distribution function using Table 7.5-3 to compute reliability for the normalized statistic z .

TABLE 7.5-3: RELIABILITY CALCULATIONS FOR EXAMPLE 2

Time, t	z	$F(z) = R_s(t)$
90	1.57	.942
95	.989	.8389
105	0.0	.500
110	-.42	.337
120	-1.30	.097
130	-2.03	.021

Note that $R_s(t) = F(z)$

where:

$$z = \frac{x - \mu}{\sigma} = \frac{x - nq}{\sqrt{npq}} = \frac{x - n(1 - e^{-\lambda t})}{\sqrt{n(1 - e^{-\lambda t})e^{-\lambda t}}}$$

By observation, it can be reasoned that system MTBF will be approximately 100 hours, since 100 element failures are permitted and one element fails each hour of system operation. A preliminary selection of discrete points at which to compute reliability might then fall in the 80- to 100-hour bracket.

At 80 hours:

$$q = 1 - e^{-\lambda t} = 1 - e^{-(1000 \cdot 10^{-6} \cdot 80)} = .077$$

$$p = e^{-1000 \cdot 10^{-6} \cdot 80} = .923$$

$$\mu = nq = 1000 (1 - e^{-1000 \cdot 10^{-6} \cdot 80}) = 77$$

$$\sigma = \sqrt{npq} = \sqrt{1000 (.077) (.923)} = \sqrt{71.07} = 8.4$$

$$x = 100$$

$$z_{80} = \frac{100 - 77}{8.4} = 2.74$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

$$R_s(80) = F(z_{80}) = F(+2.74) = .997, \text{ from standard normal tables}$$

At 100 hours:

$$\mu = np = 1000 \left(1 - e^{-1000 \cdot 10^{-6} \cdot 100} \right) = 95$$

$$p = e^{-1000 \cdot 10^{-6} \cdot 100} = .905$$

$$\sigma = \sqrt{npq} = \sqrt{86} = 9.3$$

$$x = 100$$

$$z_{100} = \frac{100 - 95}{9.3} = 0.54$$

$$R_s(100) = F(z_{100}) = F(+.54) = .705$$

These points are then used to plot the reliability function for the array, shown in Figure 7.5-12. Also shown in the figure are curves for $r=0$, 50, and 150.

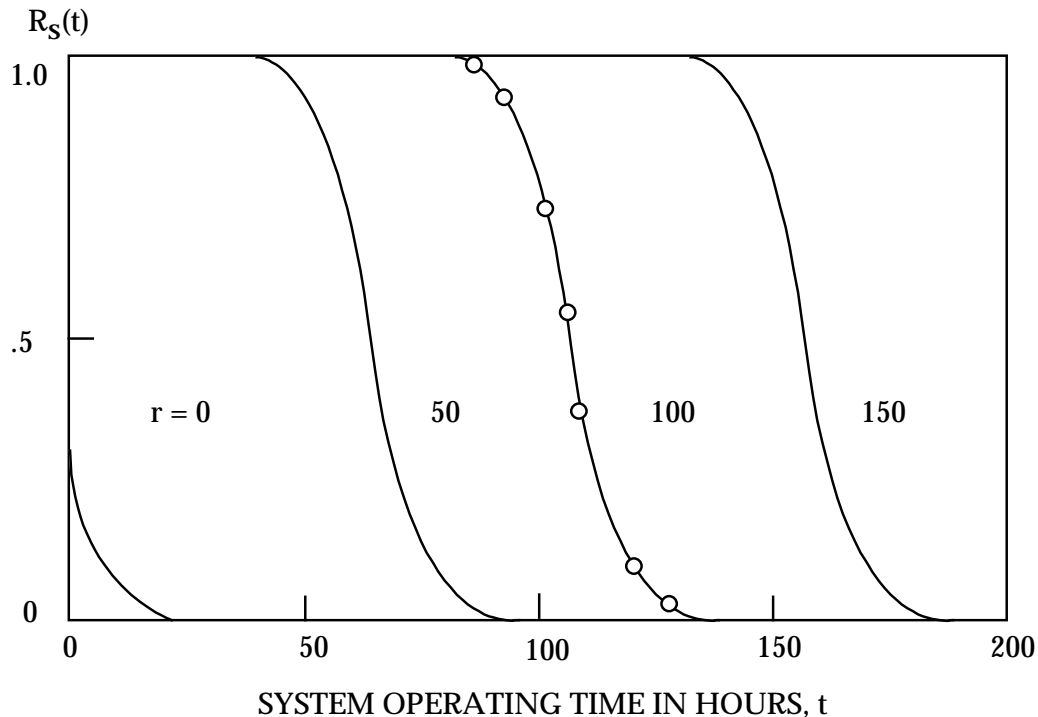


FIGURE 7.5-12: RELIABILITY FUNCTIONS FOR PARTIAL REDUNDANT ARRAY OF FIGURE 7.5-11

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.5.5.2 Operating Standby Redundancy

Until now we have dealt with circuits where it was assumed that switching devices were either absent or failure free. We now deal with circuits whose redundant elements are continuously energized but do not become part of the circuit until switched in after a primary element fails. We will consider two modes of failure that can be associated with the switching mechanism:

- a. Type (1). The switch may fail to operate when it is supposed to.
- b. Type (2). The switch may operate without command (prematurely).

In the following discussion

q_s = probability of a Type (1) failure

q'_s = probability of a Type (2) failure

7.5.5.2.1 Two Parallel Elements

Consider the system in Figure 7.5-13. There are three possible states that could lead to system failure:

- a. A succeeds, B fails, switch fails (Type 2).
- b. A fails, B succeeds, switch fails (Type 1).
- c. A fails, B fails.

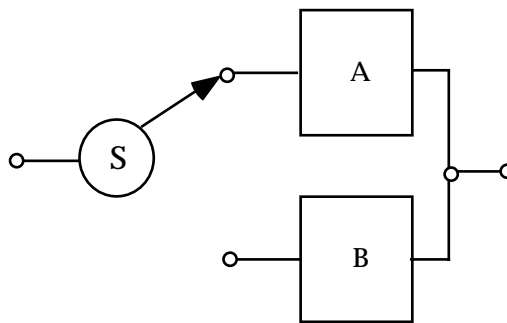


FIGURE 7.5-13: REDUNDANCY WITH SWITCHING

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

The unreliability of the system, Q , is found from

$$Q = p_a q_b q'_s + q_a p_b q_s + q_a q_b$$

As an example, assume

$$q_a = q_b = 0.2$$

and

$$q_s = q'_s = 0.1$$

Then

$$\begin{aligned} Q &= p_a q_b q'_s + q_a p_b q_s + q_a q_b \\ &= (0.8)(0.2)(0.1) + (0.2)(0.8)(0.1) + (0.2)(0.2) \\ &= 0.072 \end{aligned}$$

$$\begin{aligned} R &= 1 - Q \\ &= 1 - 0.072 \\ &= 0.928 \end{aligned}$$

If we are not concerned with Type (2) failures,

$$q'_s = 0$$

and the unreliability is

$$\begin{aligned} Q &= q_a p_b q_s + q_a q_b \\ &= (0.2)(0.8)(0.1) + (0.2)(0.2) \\ &= 0.056 \\ R &= 1 - 0.056 = 0.944 \end{aligned}$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.5.5.2.2 Three Parallel Elements

Figure 7.5-14 illustrates this type circuit. It operates as follows: If A fails, S switches to B. If B then fails, S switches to C. Enumerating all possible switching failures shows two kinds of Type (1) failure and four kinds of Type (2) failure:

a. Type (1) Switching Failures:

1. q_{s1} - A fails, S does not switch to B.
2. q_{s2} - A fails, S switches to B, B fails, S fails to switch to C.

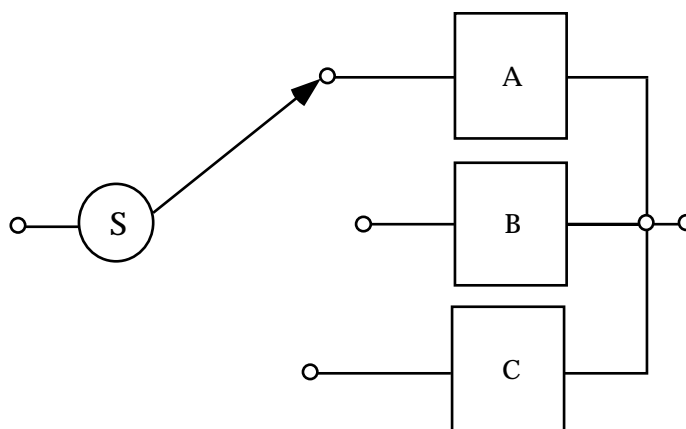


FIGURE 7.5-14: THREE-ELEMENT REDUNDANT CONFIGURATIONS WITH SWITCHING

b. Type (2) Switching Failures:

1. q'_{s3} - A succeeds, but S switches to B.
2. q'_{s4} - A succeeds, S switches to B, B fails, S does not switch to C.
3. q'_{s5} - A succeeds, S switches to B, B succeeds, S switches to C.
4. q'_{s6} - A fails, S switches to B, B succeeds, S switches to C.

The probability of switching failures must be considered in modeling redundancy with switching. The consideration of such failures can be complex. If the switching reliability is high in comparison with element reliability (i.e., switch failure rate is one-tenth that of the element failure rate), it is often possible to simplify the model with an acceptable loss of accuracy by

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

ignoring switch failures. For more detailed information, the reader is referred to textbooks on the subject and Refs. [22] and [24].

7.5.5.2.3 Voting Redundancy

Figure 7.5-15 shows three elements, A, B, and C, and the associated switching and comparator circuit which make up a voting redundant system. The circuit function will always be performed by an element whose output agrees with the output of at least one of the other elements. At least two good elements are required for successful operation of the circuit. Two switches are provided so that a comparison of any two outputs of the three elements can be made. A comparator circuit is required that will operate the two switches so that a position is located where the outputs again agree after one element fails.

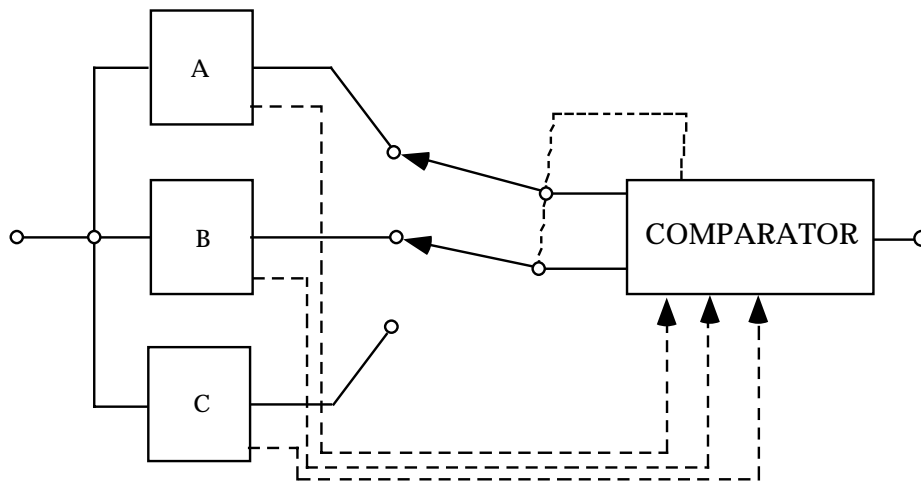


FIGURE 7.5-15: THREE-ELEMENT VOTING REDUNDANCY

If comparison and switching are failure free, the system will be successful as long as two or three elements are successful. In this case,

$$R = p_a p_b + p_a p_c + p_b p_c - 2p_a p_b p_c$$

If failure free switching cannot be assumed, conditional probabilities of switching operation have to be considered. To simplify the discussion, consider the probability of the comparator and switches failing in such a manner that the switches remain in their original positions. If this probability is q_s , then

$$R = p_a p_b + (p_a p_c + p_b p_c - 2p_a p_b p_c)(1 - q_s)$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Example of a Voting Redundant System

Let all three elements have the same probability of success, 0.9, i.e., $p_a = p_b = p_c = 0.9$. Assume that the comparator switch has a probability of failing (q_s) of 0.01:

$$R = .9^2 + \left[.9^2 + .9^2 - 2(.9)^3 \right] [1 - .01]$$

$$R = .970$$

Information and expressions for the general majority voting case are given in Figure 7.5-16.

7.5.5.3 Inactive Standby Redundancy

In a system with redundant elements on an inactive standby basis (not energized), no time is accumulated on a secondary element until a primary element fails. For a two-element system (see Figure 7.5-13) the reliability function can be found directly as follows. The system will be successful at time t if either of the following two conditions hold (let A be the primary element):

- a. A is successful up to time t .
- b. A fails at time $t_1 < t$, and B operates from t_1 to t .

For the exponential case where the element failure rates are λ_a and λ_b , reliability of the standby pair is given by

$$R(t) = \frac{\lambda_b}{\lambda_b - \lambda_a} e^{-\lambda_a t} - \frac{\lambda_a}{\lambda_b - \lambda_a} e^{-\lambda_b t}$$

This is a form of the mixed exponential and it does not matter whether the more reliable element is used as the primary or as the standby element.

The mean-time-to-failure of the system is

$$\begin{aligned} \text{MTBF} &= \frac{\lambda_a + \lambda_b}{\lambda_a \lambda_b} \\ &= \theta_a + \theta_b \\ &= 2\theta \text{ when } \theta_a = \theta_b = \theta \end{aligned}$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

For n elements of equal reliability, it can be shown that,

$$R(t) = e^{-\lambda t} \sum_{r=0}^{n-1} \frac{(\lambda t)^r}{r!}$$

where:

r is the number of failures

$$MTBF = \frac{n}{\lambda} = n\theta$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

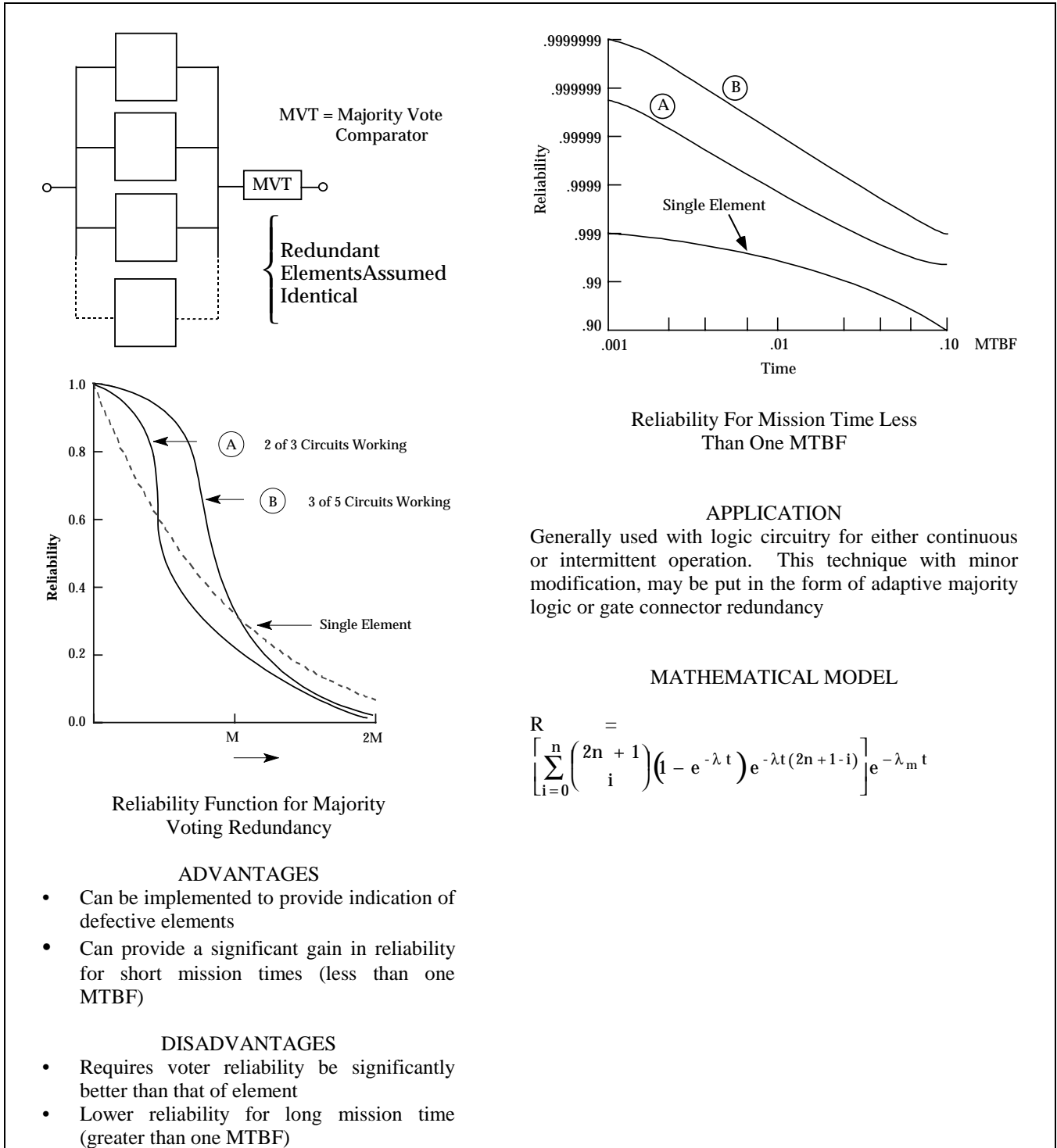


FIGURE 7.5-16: MAJORITY VOTING REDUNDANCY

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Figure 7.5-17 is a chart relating system reliability to the reliability of individual operating standby redundant parallel elements as a function of mission time, t/θ . By entering the chart at the time period of interest and proceeding vertically to the allocated reliability requirement, the required number of standby elements can be determined.

Example of Inactive Standby Redundancy

A critical element within a system has a demonstrated MTBF, $\theta = 100$ hours. A design requirement has been allocated to the function performed by this element of $R_s = .98$ at 100 hours. This corresponds to a 30-to-1 reduction in unreliability compared with that which can be achieved by a single element. In this case, $n = 4$ will satisfy the design requirement at $t/\theta = 1$. In other words, a four-element standby redundant configuration would satisfy the requirement. Failure rates of switching devices must next be taken into account.

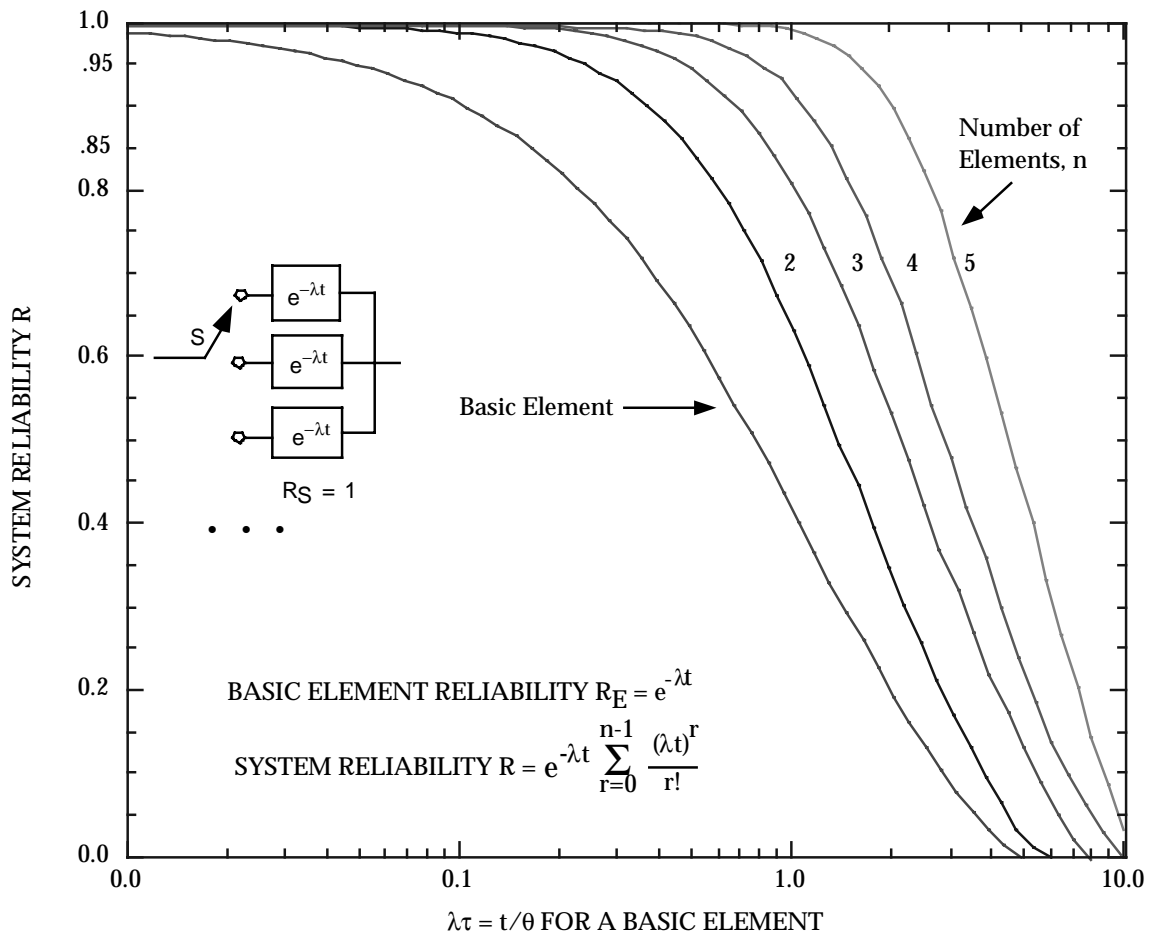


FIGURE 7.5-17: SYSTEM RELIABILITY FOR n STANDBY REDUNDANT ELEMENTS

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.5.5.4 Dependent Failure Probabilities

Up to this point, it has been assumed that the failure of an operative redundant element has no effect on the failure rates of the remaining elements. Dependent failures might occur, for example, with a system having two elements in parallel where both elements share the full load.

An example of conditional or dependent events is illustrated by Figure 7.5-18. Assume elements A and B are both fully energized, and normally share or carry half the load, $L/2$. If either A or B fails, the survivor must carry the full load, L . Hence, the probability that one fails is dependent on the state of the other, if failure probability is related to load or stress. The system is operating satisfactorily at time t if either A or B or both are operating successfully.

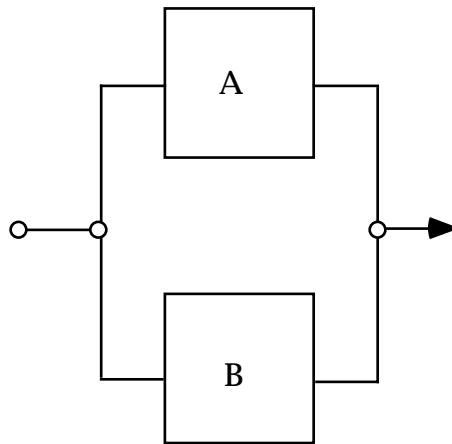


FIGURE 7.5-18: LOAD SHARING REDUNDANT CONFIGURATION

Figure 7.5-19 illustrates the three possible ways the system can be successful. The bar above a letter represents a failure of that element. A primed letter represents operation of that element under full load; absence of a prime represents operation under half load. If the elements' failure times are exponentially distributed and each has a mean life of θ under load $L/2$ and $\theta' = \theta/k$ under load L where $k \geq 0$, block reliability is given below without derivation:

$$R(t) = \frac{2\theta'}{2\theta' - \theta} e^{-t/\theta'} - \frac{\theta}{2\theta' - \theta} e^{-2t/\theta}$$

System mean life is equal to

$$\theta_s = \theta/k + \theta/2$$

When $k = 1$, the system is one in which load sharing is not present or an increased load does not affect the element failure probability. Thus, for this case, θ_s is equal to $3\theta/2$.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

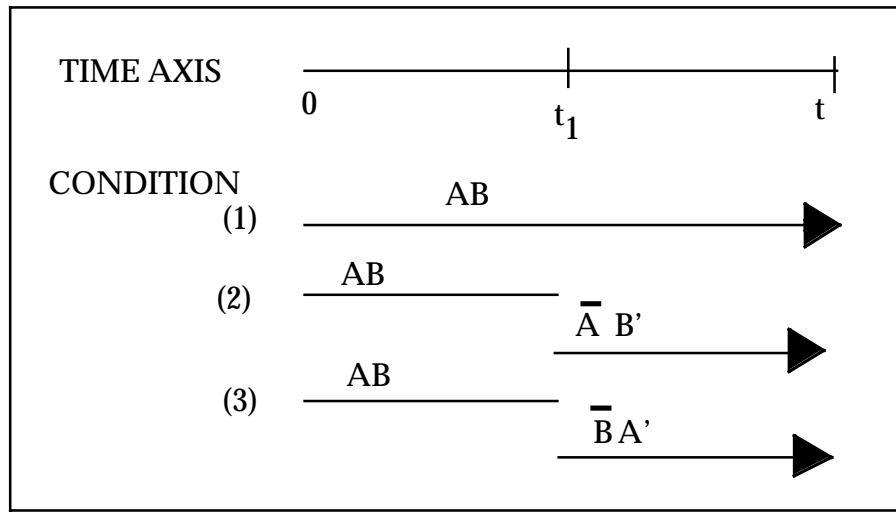


FIGURE 7.5-19: SUCCESS COMBINATIONS IN TWO-ELEMENT LOAD-SHARING CASE

7.5.5.5 Optimum Allocation of Redundancy

Decision and switching devices may fail to switch when required or may operate inadvertently. However, these devices are usually necessary for redundancy, and increasing the number of redundant elements increases the number of switching devices. If such devices are completely reliable, redundancy is most effective at lower system levels. If switching devices are not failure free, the problem of increasing system reliability through redundancy becomes one of choosing an optimum level at which to replicate elements.

Since cost, weight, and complexity factors are always involved, the minimum amount of redundancy that will produce the desired reliability should be used. Thus efforts should be concentrated on those parts of the system which are the major causes of system unreliability.

As an example, assume that we have two elements, A and B, with reliabilities over a certain time period of 0.95 and 0.50, respectively. If A and B are joined to form a series nonredundant circuit, its reliability is

$$R = (0.95)(0.50) = 0.475$$

If we duplicate each element, as in Figure 7.5-20a,

$$R_1 = [1 - (0.50)^2] [1 - (0.05)^2] = 0.748$$

 SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Duplicating Element B only, as in Figure 7.5-20b,

$$R_2 = 0.95 [1 - (0.50)^2] = 0.712$$

Obviously, duplicating Element A contributes little to increasing reliability.

Triplication of B gives the configuration shown in Figure 7.5-20c and

$$R_3 = 0.95 [1 - (0.5)^3] = 0.831$$

R_3 gives a 75% increase in original circuit reliability as compared to the 58% increase of R_1 .

If complexity is the limiting factor, duplicating systems is generally preferred to duplicating elements, especially if switching devices are necessary. If another series path is added in parallel, we have the configuration in Figure 7.5-20d, and

$$R_4 = 1 - (1 - .475)^2 = 0.724$$

R_4 is only slightly less than R_1 . If switches are necessary for each redundant element, R_4 may be the best configuration. A careful analysis of the effect of each element and switch on system reliability is a necessary prerequisite for proper redundancy application.

7.5.6 Reliability Analysis Using Markov Modeling

7.5.6.1 Introduction

Markov Modeling is a reliability analysis tool which in the past few years has become the most prominent method of computing the reliability (or unreliability) of fault tolerant systems. It is an extremely flexible tool which can be used to predict the reliability of in-flight critical digital electronic systems. It has been used on a number of digital electronic engine controls to compute the probability of events such as aircraft loss due to control system failures, mission aborts, in-flight shut-down of engines, overspeeding of engines and inadvertent thrust reversal. Markov modeling offers many advantages over other reliability modeling techniques, some of which are:

- (1) Simplistic modeling approach: The models are simple to generate although they require a more complicated mathematical approach. This is not a problem, however, because the mathematics are well suited for the digital computer.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

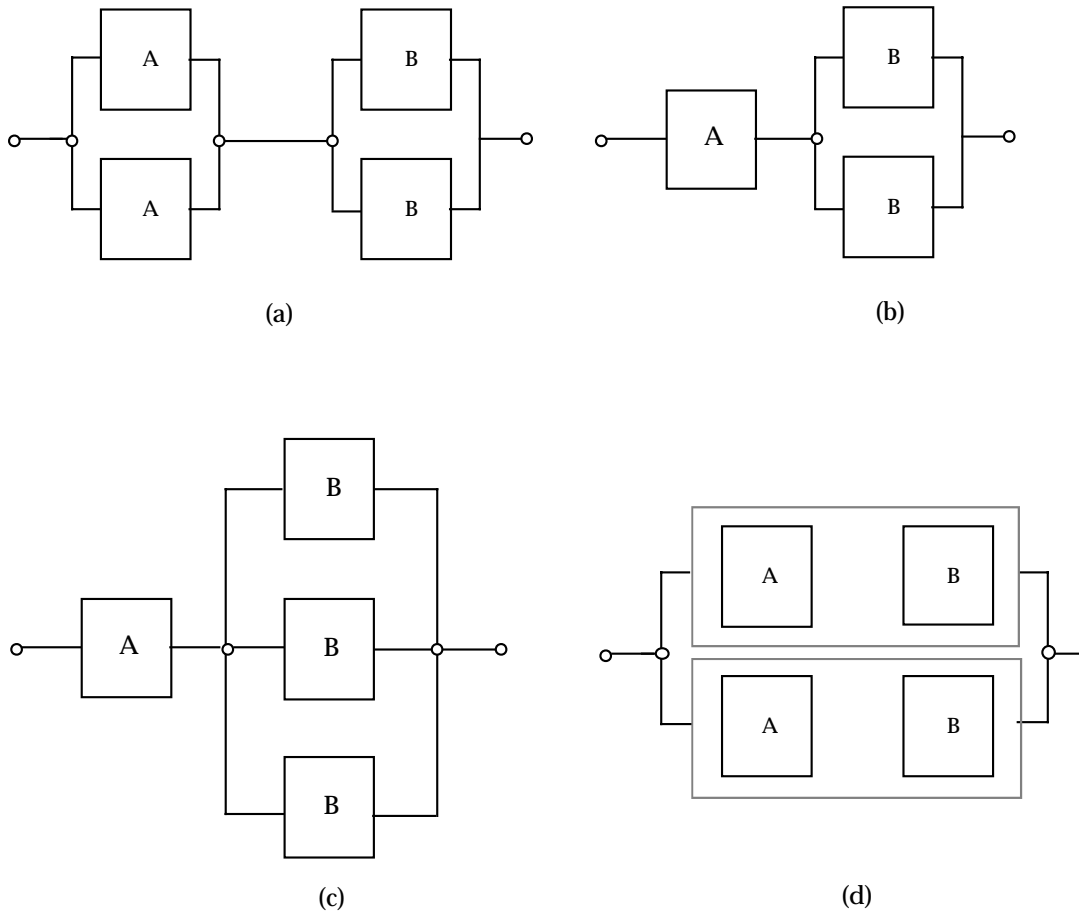


FIGURE 7.5-20: POSSIBLE REDUNDANT CONFIGURATIONS RESULTING FROM ALLOCATION STUDY

- (2) Redundancy management techniques: System reconfiguration required by failures is easily incorporated in the model.
- (3) Coverage: Covered and uncovered failures of components are mutually exclusive event. These are not easily modeled using classical techniques, but are readily handled by the Markov mathematics.
- (4) Complex systems: Many simplifying techniques exist which allow the modeling of complex systems.
- (5) Sequenced events: Many times the analyst is interested in computing the probability of an event which is the result of a certain sequence of sub-events. As an example, the probability of an engine overspeed might be desired. This is usually the result of two events, these being loss of overspeed protection and an uncommanded high fuel flow. These must necessarily occur in that order. For if the uncommanded high fuel flow

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

precedes the overspeed protection failure, an engine shutdown occurs rather than an overspeed. While these types of problems do not lend themselves well to classical techniques, they are easily handled using Markov modeling.

7.5.6.2 Markov Theory

Markov modeling can be applied to systems which vary discretely or continuously with respect to time and space. In reliability we are generally concerned with continuous time, discrete state models. These systems are characterized by randomly varying stochastic processes. Stochastic processes must have two important properties in order to model them with the Markov approach.⁵

These are:

- (1) The process must be memoryless
- (2) The process must be stationary

A memoryless system is characterized by the fact that the future state of the system depends only on its present state. A stationary system is one in which the probabilities which govern the transitions from state to state remain constant with time. In other words, the probability of transitioning from some state i to another state j is the same regardless of the point in time the transition occurs. The states of the model are defined by system element failures. The transitional probabilities between states are a function of the failure rates of the various system elements. A set of first-order differential equations are developed by describing the probability of being in each state in terms of the transitional probabilities from and to each state. The number of first-order differential equations will equal the number of states of the model. The mathematical problem becomes one of solving the following equation:

$$\dot{\underline{P}} = [A]\underline{P}$$

where $\dot{\underline{P}}$ and \underline{P} are $n \times 1$ column vectors, $[A]$ is an $n \times n$ matrix and n is the number of states in the system. The solution of this equation is:

$$\underline{P} = \exp[A]t \cdot \underline{P}(0)$$

where $\exp[A]t$ is an $n \times n$ matrix and $\underline{P}(0)$ is the initial probability vector describing the initial state of the system. Two methods which are particularly well suited for the digital computer for computing the matrix $\exp[A]t$ are the infinite series method and the eigenvalue/eigenvector method. Figure 7.5-21 presents a flow chart which illustrates the procedure used to develop a Markov model.

⁵ Extensions of the theory to other processes exist but are beyond the scope of this handbook.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

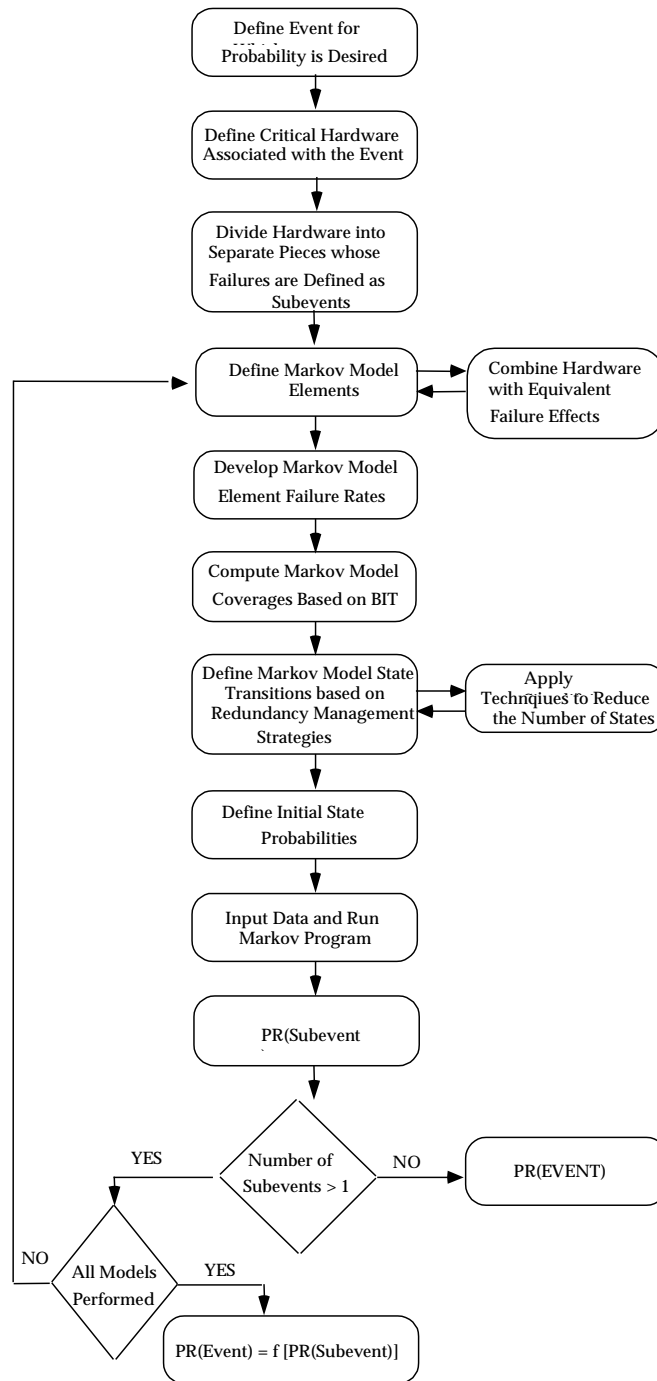


FIGURE 7.5-21: MARKOV MODELING PROCESS

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.5.6.3 Development of the Markov Model Equation

In order to illustrate how the Markov model equations are developed, assume we have a system which is made up of two elements. Each element has two mutually exclusive states - a good and failed. The states of the model are generated based on the elements being in one of these two states. The probabilities that cause transition from state to state are a function of the element failure rates. An element with constant failure rate (1) has a transitional probability which is approximated by $\lambda \cdot \Delta t$. The probability of more than one element failure in Δt is considered negligible. A flow diagram of the two element problem mentioned above is presented in Figure 7.5-22.

We develop the Markov differential equation by describing the probability of being in each of the states at time $t + \Delta t$ as a function of the state of the system at time t . The probability of being in state one at some time $t + \Delta t$ is equal to the probability of being in state one at time t and not transitioning out during Δt . This can be written as:

$$P1(t + \Delta t) = P1(t) \cdot [1 - (\lambda_1 + \lambda_2) \cdot \Delta t]$$

The probability of being in state two at time $t + \Delta t$ is equal to the probability of being in state one at time t and transitioning to state two in Δt plus the probability of being in state two at time t and **not** transitioning out during Δt . This can be written as:

$$P2(t + \Delta t) = P1(t) \cdot \lambda_1 \cdot \Delta t + P2(t)(1 - \lambda_2 \cdot \Delta t)$$

The other state probabilities are generated in the same manner resulting in the following equations:

$$P1(t + \Delta t) = P1(t) \cdot [1 - (\lambda_1 + \lambda_2) \cdot \Delta t]$$

$$P2(t + \Delta t) = P1(t) \cdot \lambda_1 \cdot \Delta t + P2(t)(1 - \lambda_2 \cdot \Delta t)$$

$$P3(t + \Delta t) = P1(t) \cdot \lambda_2 \cdot \Delta t + P3(t)(1 - \lambda_1 \cdot \Delta t)$$

$$P4(t + \Delta t) = P2(t) \cdot \lambda_2 \cdot \Delta t + P3(t) \cdot \lambda_1 \cdot \Delta t + P4(t)$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

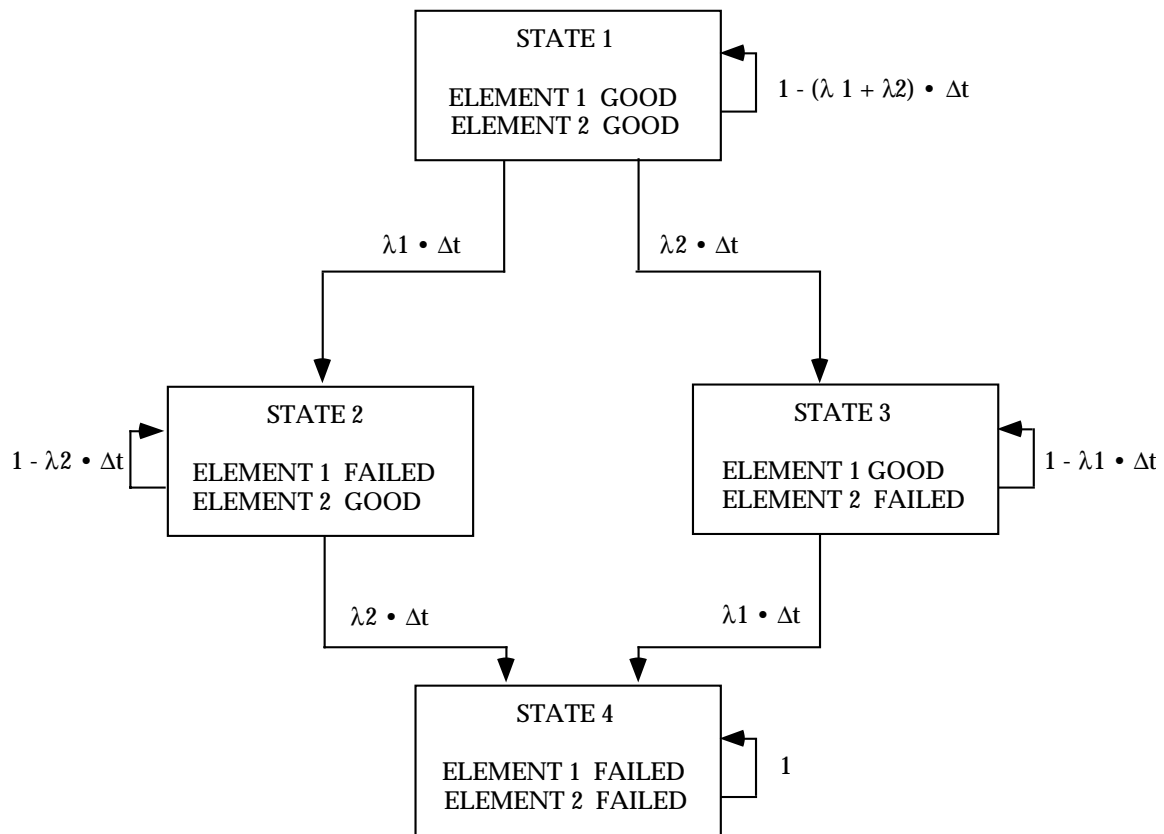


FIGURE 7.5-22: MARKOV FLOW DIAGRAM

Rearranging:

$$\begin{aligned}
 [P1(t + \Delta t) - P1(t)]/\Delta t &= -(\lambda_1 + \lambda_2) \cdot P1(t) \\
 [P2(t + \Delta t) - P2(t)]/\Delta t &= \lambda_1 \cdot P1(t) - \lambda_2 \cdot P2(t) \\
 [P3(t + \Delta t) - P3(t)]/\Delta t &= \lambda_2 \cdot P1(t) - \lambda_1 \cdot P3(t) \\
 [P4(t + \Delta t) - P4(t)]/\Delta t &= \lambda_2 \cdot P2(t) + \lambda_1 \cdot P3(t)
 \end{aligned}$$

Taking the limit as $\Delta t \rightarrow 0$:

$$\begin{aligned}
 dP1(t)/dt &= -(\lambda_1 + \lambda_2) \cdot P1(t) \\
 dP2(t)/dt &= \lambda_1 \cdot P1(t) - \lambda_2 \cdot P2(t) \\
 dP3(t)/dt &= \lambda_2 \cdot P1(t) - \lambda_1 \cdot P3(t) \\
 dP4(t)/dt &= \lambda_2 \cdot P2(t) + \lambda_1 \cdot P3(t)
 \end{aligned}$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

In matrix form this becomes:

$$\begin{pmatrix} dP1(t)/dt \\ dP2(t)/dt \\ dP3(t)/dt \\ dP4(t)/dt \end{pmatrix} = \begin{pmatrix} -(\lambda_1 + \lambda_2) & 0 & 0 & 0 \\ \lambda_1 & -\lambda_2 & 0 & 0 \\ \lambda_2 & 0 & -\lambda_1 & 0 \\ 0 & \lambda_2 & \lambda_1 & 0 \end{pmatrix} \cdot \begin{pmatrix} P1(t) \\ P2(t) \\ P3(t) \\ P4(t) \end{pmatrix}$$

or $\dot{\mathbf{P}} = [\mathbf{A}] \cdot \mathbf{P}$ where $[\mathbf{A}]$ is defined as the state transition matrix. The important thing to note here is that the analyst need only generate the states and the transitions between states as defined by the element failure rates. This information can then be inputted to the computer in a form which allows it to set up the state transition matrix and compute the state probabilities using matrix mathematics.

7.5.6.4 Markov Model Reduction Techniques

Since the Markov modeling approach can generate all the possible states of a system, the number of states can be extremely large even for a relatively small number of Markov elements. Therefore it become imperative for the analyst using the Markov modeling approach to become familiar with the reduction techniques that can be applied to reduce the number of states significantly while maintaining the accuracy of the model. As an example, if we assume a system contains 10 elements, each of which have two states (good and failed), the total number of possible states becomes:

$$\# \text{ STATES} = 2^N = 2^{10} = 1024$$

Furthermore, a system containing only 10 elements would be considered small when modeling digital electronic engine controls, for instance. Fortunately many simplification techniques exist which can be used alone, or in combination, to reduce the amount of states in the model.

One approach is to use the principle that states which represent multiple levels of failure contribute insignificantly to the overall probability of failure of the system. The model can be truncated at a certain failure level, combining all states below that level into one failed state. If for instance it is desired to truncate at the n^{th} level, all state transitions from $n-1$ level states would be directed to one n^{th} order failed state. Care should be taken, however, to make sure that this truncation does not have an overly conservative impact on the system.

Many elements have the same, or nearly the same, impact on system operation when failed. In this case the states which are the result of failure of these elements can be combined. As an example, assume we have a two channel engine control in dual active mode. By dual active mode we mean both channels are simultaneously in control. Let each channel have a failure rate λ . If one channel fails we have the ability to control with the other good channel. Because loss of either channel leads to the same effect (i.e., single channel control), the corresponding states

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

can be combined. Figure 7.5-23 shows the Markov model for this system using no reduction technique and the equivalent model by combining States 2 and 3. Because the system impact was the same independent of what channel failed first, and because the channel failure rates were the same, we are able to reduce the number of states with no loss of accuracy. If this is not the case, assumptions have to be made as to what element failure caused transition to the new state so that a conservative approximation to the transitions out of the state can be made.

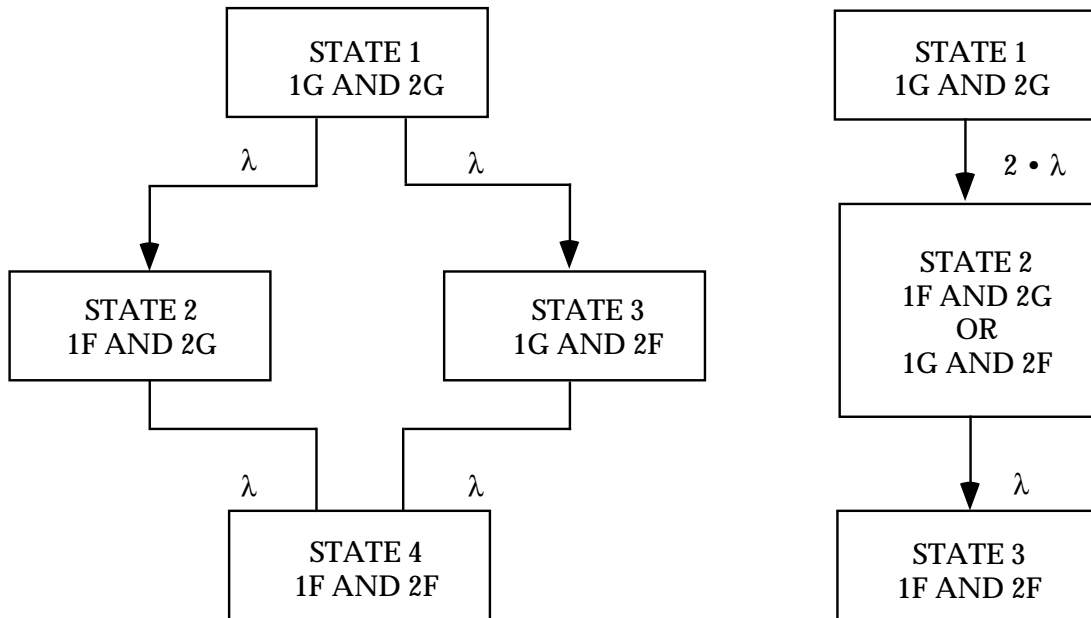


FIGURE 7.5-23: TWO CHANNEL EXAMPLE

Many times failure of a certain element causes loss of other elements in a system. An example would be loss of a power supply. In this case the analyst need not define transitions for the other lost element(s) because by definition they are also no longer part of the functioning system.

Another reduction technique involves dividing the top level event for which the probability of failure is desired into n sub-events, each of which is modeled separately. The probabilities for each sub-event are then combined to yield the probability of the top level event. If for instance the system being modeled has ten elements, we have a possible of 1024 total states. If the top level event containing these ten elements can be broken down into two sub-events, each containing five elements, the system can be described with two models each with a possible thirty-two states. If the top level event has probability P and the two sub-events have probabilities P_1 and P_2 respectively, the top level probability can be computed as $P = f(P_1, P_2)$.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.5.6.5 Application of Coverage to Markov Modeling

In redundant system modeling we generally consider three Markov element states - good, failed covered, and failed uncovered. Covered and uncovered markov element states are mutually exclusive meaning that an element cannot fail both covered and uncovered. System coverage is generally defined in terms of the conditional probability.

$$P[\text{detect, isolate, reconfigure} \mid \text{failure}]$$

When computing a coverage for Markov model elements we are concerned with that portion of the Markov element failure rate that is detectable and isolatable. Reconfiguration becomes a function of what resources are available at the time the failure occurs.

As an example of how coverage is used in the Markov model, we will return to the two channel dual active engineer control discussed previously. In this case if either channel fails **covered**, the other channel has the ability to take over full control. However, if either channel fails **uncovered**, system failure occurs. The Markov model for this example appears in Figure 7.5-24. Note that once state two is entered, no resources are available and both the covered and uncovered portions of the remaining channels failure rate are routed to system failure.

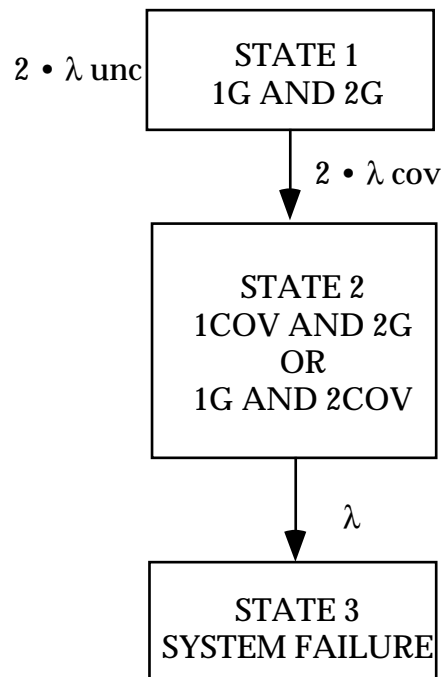


FIGURE 7.5-24: COVERAGE EXAMPLE

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.5.6.6 Markov Conclusions

Markov modeling is a powerful reliability analysis tool which allows the analyst to model complex fault tolerant systems that would otherwise be difficult to model with classical techniques. The Markov technique decreases the analysts task by reducing the problem from one of mathematical computation to one of state modeling. Many model reduction techniques exist which yield relatively simple models with insignificant impact on model accuracy.

An excellent resource document dealing with the Markov methodology is IEC 1165, Reference [25].

7.6 Environmental Design

7.6.1 Environmental Strength

A series of Engineering Design Handbooks deals explicitly, and in great detail, with environmental design problems (References [26] - [30]). Those handbooks should be consulted for specific information. This section will concentrate on some general environmental design considerations against specific environments. Many of the details on environmental prediction and specific design methods are in the previously mentioned documents.

To design inherently reliable equipment, the design engineer must take into account the environment in which the equipment is to operate, with relation to the ideal operating conditions for the elements which make up the equipment. Each item in a system has its own failure rate based upon the conditions under which it operates.

MIL-STD-210 (Climatic Extremes for Military Equipment) establishes climatic design criteria for material intended for worldwide usage. It provides design conditions for land, sea, and air in which equipment will be required to operate (or be stored). The standard breaks down climate extremes into three categories - ground, naval surface and air, and worldwide air. For these three categories, the climatic conditions for which values and factors are presented include temperature, humidity, precipitation, atmospheric pressure, and many others. MIL-STD-210 is the baseline document from which climatic environmental conditions can be derived. Operating conditions may vary considerably from climatic conditions due to changes caused by system operation, e.g., equipment heating. The designer may have to address climatic problems using special parts. Such parts may need to operate at low temperature, incorporate pre-heating arrangements, utilize temperature-tolerant lubricants, or incorporate other methods of adjusting for climatic conditions.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.6.2 Designing for the Environment

Since the reliability achieved in actual use depends on the operating conditions that are encountered during the entire life of the equipment, it is important that such conditions are accurately identified at the beginning of the design process. Environmental factors which exert a strong influence on equipment reliability are included in Table 7.6-1, which is a checklist for environmental coverage.

TABLE 7.6-1: ENVIRONMENTAL COVERAGE CHECKLIST (TYPICAL)

NATURAL	INDUCED
Clouds	Acceleration
Fog	Electromagnetic, Laser
Freezing Rain	Electrostatic, Lightning
Frost	Explosion
Fungus	Icing
Geomagnetism	Radiation, Electromagnetic
Gravity, Low	Radiation, Nuclear
Temperature, High	Shock
Temperature, Low	Temperature, High, Aero. Heating
Humidity, High	Temperature, Low, Aero. Cooling
Humidity, Low	Turbulence
Ionized Gases	Vapor Trails
Lightning	Vibration, Mechanical
Meteoroids	Vibration, Acoustic
Pollution, Air	
Pressure, High	
Pressure, Low	
Radiation, Cosmic, Solar	
Radiation, Electromagnetic	
Rain	
Salt Spray	
Sand and Dust	
Sleet	
Snow	
Hail	
Ice	
Wind	

Concurrent (combined) environments are usually more detrimental to reliability than the effects of any single environment. Design and test criteria must consider both single and combined environments. Figure 7.6-1 illustrates the effects of combined environments (typical) in a matrix relationship. It shows the combinations where the total effect is more damaging than the cumulative effect of each environment acting independently. Concurrent environments may include a combination such as temperature, humidity, altitude, shock, and vibration. Table 7.6-2 provides reliability considerations for pairs of environmental factors.

The impact of each of the environmental factors anticipated during the life cycle of equipment on the operational and reliability characteristics of the materials and parts comprising the equipment being designed must be determined. Packaging techniques that afford the necessary protection against such degrading factors must also be identified.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

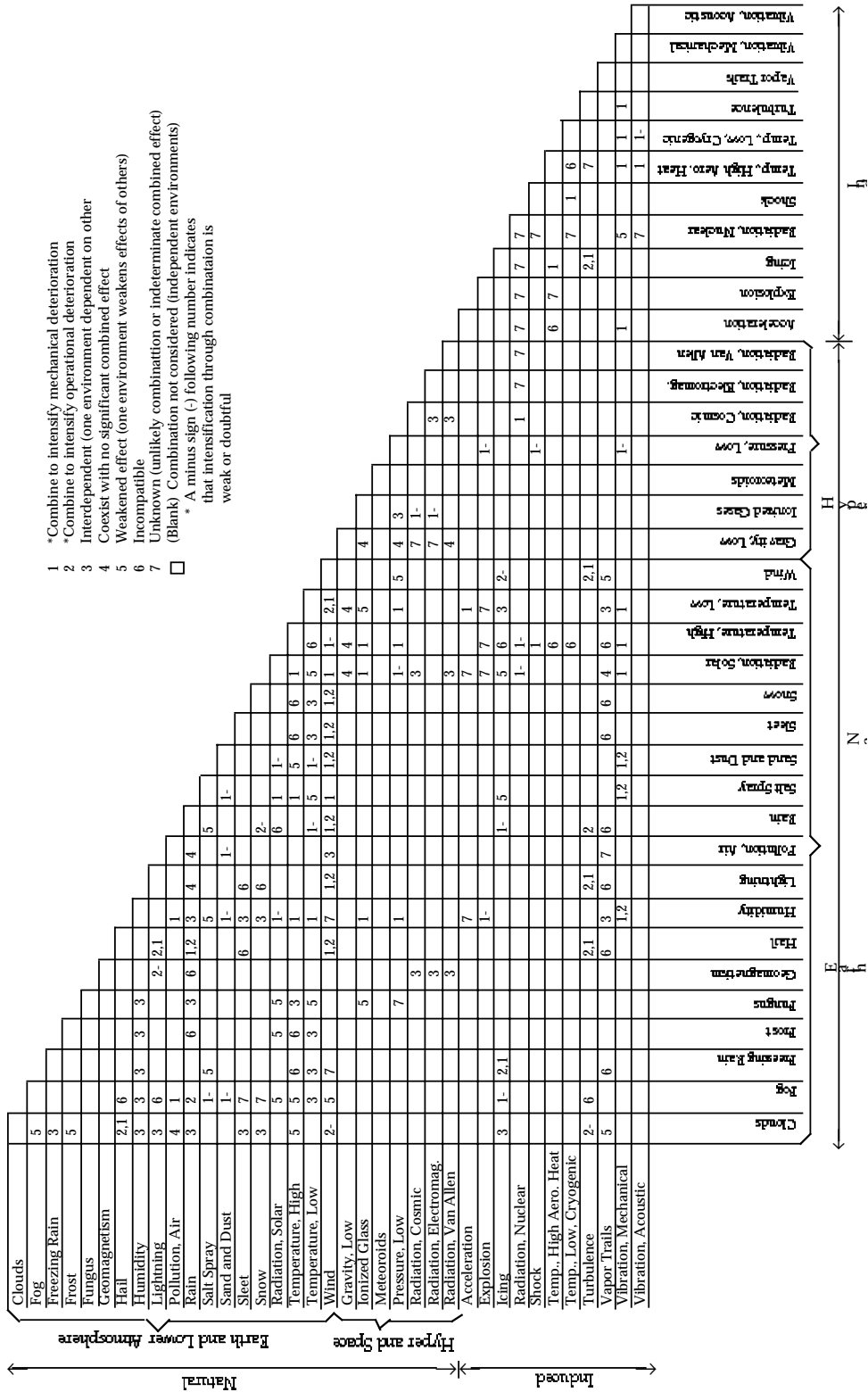


FIGURE 7.6-1: EFFECTS OF COMBINED ENVIRONMENTS

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-2: VARIOUS ENVIRONMENTAL PAIRS

HIGH TEMPERATURE AND HUMIDITY	HIGH TEMPERATURE AND LOW PRESSURE	HIGH TEMPERATURE AND SALT SPRAY
High temperature tends to increase the rate of moisture penetration. The general deterioration effects of humidity are increased by high temperatures.	Each of these environments depends on the other. For example, as pressure decreases, outgassing of constituents of materials increases, and as temperature increases, the rate of outgassing increases. Hence, each tends to intensify the effects of the other.	High temperature tends to increase the rate of corrosion caused by salt spray.
HIGH TEMPERATURE AND SOLAR RADIATION	HIGH TEMPERATURE AND FUNGUS	HIGH TEMPERATURE AND SAND AND DUST
This is a man-independent combination that causes increasing effects on organic materials.	A certain degree of high temperature is necessary to permit fungus and microorganisms to grow. But, above 160 ^o F (71 ^o C) fungus and micro-organisms cannot develop.	The erosion rate of sand may be accelerated by high temperature. However, high temperatures reduce sand and dust penetration.
HIGH TEMPERATURE AND SHOCK AND VIBRATION	HIGH TEMPERATURE AND ACCELERATION	HIGH TEMPERATURE AND EXPLOSIVE ATMOSPHERE
Both of these environments affect common material properties, and will intensify each other's effects. The degree of intensification depends on the magnitude of each environment in the combination. Plastics and polymers are more susceptible to this combination than metals, unless extremely high temperatures are involved.	This combination produces the same effect as high temperature and shock and vibration.	Temperature has little effect on the ignition of an explosive atmosphere, but it does affect the air-vapor ratio which is an important consideration.
LOW TEMPERATURE AND HUMIDITY	HIGH TEMPERATURE AND OZONE	
Humidity decreases with temperature, but low temperature induces moisture condensation, and, if the temperature is low enough, frost or ice.	Starting at about 300 ^o F (150 ^o C), temperature starts to reduce ozone. Above about 520 ^o F (270 ^o C) ozone cannot exist at pressures normally encountered.	
LOW TEMPERATURE AND SOLAR RADIATION	LOW TEMPERATURE AND LOW PRESSURE	LOW TEMPERATURE AND SALT SPRAY
Low temperature tends to reduce the effects of solar radiation, and vice versa.	This combination can accelerate leakage through seals, etc.	Low temperature reduces the corrosion rate of salt spray.
	Low temperature increases dust penetration.	Low temperature reduces fungus growth. At sub-zero temperatures, fungi remain in suspended animation.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-2: VARIOUS ENVIRONMENTAL PAIRS (CONT'D)

	LOW TEMPERATURE AND SAND AND DUST	LOW TEMPERATURE AND FUNGUS
LOW TEMPERATURE AND SHOCK AND VIBRATION	LOW TEMPERATURE AND ACCELERATION	LOW TEMPERATURE AND EXPLOSIVE ATMOSPHERE
Low temperature tends to intensify the effects of shock and vibration. It is, however, a consideration only at very low temperatures.	This combination produces the same effect as low temperature and shock and vibration.	Temperature has very little effect on the ignition of an explosive atmosphere. It does however, affect the air-vapor ratio which is an important consideration.
LOW TEMPERATURE AND OZONE	HUMIDITY AND LOW PRESSURE	HUMIDITY AND SALT SPRAY
Ozone effects are reduced at lower temperatures, but ozone concentration increases with lower temperatures.	Humidity increases the effects of low pressure, particularly in relation to electronic or electrical equipment. However, the actual effectiveness of this combination is determined largely by the temperature.	High humidity may dilute the salt concentration, but it has no bearing on the corrosive action of the salt.
HUMIDITY AND FUNGUS	HUMIDITY AND SAND AND DUST	HUMIDITY AND SOLAR RADIATION
Humidity helps the growth of fungus and microorganisms but adds nothing to their effects.	Sand and dust have a natural affinity for water and this combination increases deterioration.	Humidity intensifies the deteriorating effects of solar radiation on organic materials.
HUMIDITY AND VIBRATION	HUMIDITY AND SHOCK AND ACCELERATION	HUMIDITY AND EXPLOSIVE ATMOSPHERE
This combination tends to increase the rate of breakdown of electrical material.	The periods of shock and acceleration are considered too short for these environments to be affected by humidity.	Humidity has no effect on the ignition of an explosive atmosphere, but a high humidity will reduce the pressure of an explosion.
HUMIDITY AND OZONE	LOW PRESSURE AND SALT SPRAY	LOW PRESSURE AND SOLAR RADIATION
Ozone meets with moisture to form hydrogen peroxide, which has a greater deteriorating effect on plastics and elastomers than the additive effects of moisture and ozone.	This combination is not expected to occur.	This combination adds nothing to the overall effects.
	LOW PRESSURE AND FUNGUS	
	This combination adds nothing to the overall effects.	

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-2: VARIOUS ENVIRONMENTAL PAIRS (CONT'D)

LOW PRESSURE AND SAND AND DUST	LOW PRESSURE AND VIBRATION	LOW PRESSURE AND SHOCK OR ACCELERATION
This combination only occurs in extreme storms during which small dust particles are carried to high altitudes.	This combination intensifies effects in all equipment categories but mostly with electronic and electrical equipment.	These combinations only become important at the hyper-environmental levels, in combination with high temperature.
LOW PRESSURE AND EXPLOSIVE ATMOSPHERE	SALT SPRAY AND FUNGUS	SALT SPRAY AND DUST
At low pressures, an electrical discharge is easier to develop, but the explosive atmosphere is harder to ignite.	This is considered an incompatible combination.	This will have a more corrosive effect than humidity and sand and dust.
SALT SPRAY AND VIBRATION	SALT SPRAY AND SHOCK OR ACCELERATION	SALT SPRAY AND EXPLOSIVE ATMOSPHERE
This will have a more corrosive effect than humidity and vibration.	These combinations will produce no added effects.	This is considered an incompatible combination.
SALT SPRAY AND OZONE	SOLAR RADIATION AND FUNGUS	SOLAR RADIATION AND SAND AND DUST
These environments have a more corrosive effect than humidity and ozone.	Because of the resulting heat from solar radiation, this combination probably produces the same combined effect as high temperature and fungus. Further, the ultraviolet in unfiltered radiation is an effective fungicide.	It is suspected that this combination will produce high temperatures.
SOLAR RADIATION AND OZONE	FUNGUS AND OZONE	SOLAR RADIATION AND SHOCK OR ACCELERATION
This combination increases the rate of oxidation of materials.	Fungus is destroyed by ozone.	These combinations produce no additional effects.
SOLAR RADIATION AND VIBRATION		SAND AND DUST AND VIBRATION
Under vibration conditions, solar radiation deteriorates plastics, elastomers, oils, etc., at a higher rate.		Vibration might possibly increase the wearing effects of sand and dust.
SHOCK AND VIBRATION	VIBRATION AND ACCELERATION	
This combination produces no added effects.	This combination produces increased effects when encountered with high temperatures and low pressures in the hyper-environmental ranges.	
SOLAR RADIATION AND EXPLOSIVE ATMOSPHERE		
This combination produces no added effects.		

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

In the environmental stress identification process that precedes the selection of environmental strength techniques, it is essential that the environments associated with all life intervals of the equipment be considered. These include not only the operational and maintenance environments, but also the pre-operational environments, when stresses imposed on the parts during manufacturing assembly, inspection, testing, shipping, and installation may have a significant impact on the eventual reliability of the equipment. Stresses imposed during the pre-operational phase are often overlooked. They may, however, represent a particularly harsh environment which the equipment must withstand. Often, the environments to which a system is exposed during shipping and installation are more severe than those it will encounter under normal operating conditions. It is also probable that some of the environmental strength features of a system design address conditions that are encountered in the pre-operational phase, not in the operational phases.

Environmental stresses affect parts in different ways. Table 7.6-3 illustrates the principal effects of typical environments on system parts and materials.

High temperatures impose a severe stress on most electronic items since they can cause not only catastrophic failure (such as melting of solder joints and burnout of solid-state devices), but also slow, progressive deterioration of performance levels due primarily to chemical degradation effects. It is often stated that excessive temperature is the primary cause of poor reliability in electronic equipment.

In electronic systems design, great emphasis is placed on small size and high part densities. This design philosophy generally requires a cooling system to provide a path of low thermal resistance from heat-producing elements to an ultimate heat sink of reasonably low temperature.

Solid-state parts are generally rated in terms of maximum junction temperatures. The thermal resistance from a junction to either the case or to free air is usually specified. The specification of maximum ambient temperature for which a part is suitable is generally not a sufficient method for part selection, since the surface temperatures of a particular part can be greatly influenced by heat radiation or heat conduction effects from nearby parts. These effects can lead to overheating, even though an ambient temperature rating appears not to be exceeded. It is preferable to specify thermal environment ratings such as equipment surface temperatures, thermal resistance paths associated with conduction, convection and radiation effects, and cooling provisions such as air temperature, pressure and velocity. In this manner, the true thermal state of the temperature-sensitive internal elements can be determined. Reliability improvement techniques for high temperature stress include the use of heat dissipation devices, cooling systems, thermal insulation, and heat withstanding materials.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-3: ENVIRONMENTAL EFFECTS

ENVIRONMENT	PRINCIPAL EFFECTS	TYPICAL FAILURES INDUCED
High temperature	Thermal aging: Oxidation Structural change Chemical reaction Softening, melting, and sublimation Viscosity reduction and evaporation Physical expansion	Insulation failure; Alteration of electrical properties Loss of lubrication properties. Structural failure; Increased mechanical stress; Increased wear on moving parts
Low temperature	Increased viscosity and solidification Ice formation Embrittlement Physical Contraction	Loss of lubrication properties. Alteration of electrical properties. Loss of mechanical strength; cracking, fracture structural failure; increased wear on moving parts.
High relative humidity	Moisture absorption Chemical reaction Corrosion Electrolysis	Swelling, rupture of container; physical breakdown; loss of electrical strength. 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.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-3: ENVIRONMENTAL EFFECTS (CONT'D)

ENVIRONMENT	PRINCIPAL EFFECTS	TYPICAL FAILURES INDUCED
Low pressure	Expansion Outgassing Reduced dielectric strength of air	Fracture of container; Explosive expansion. Alteration of electrical properties; Loss of mechanical strength. 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 Electrolysis	Increased wear. Loss of mechanical strength; Alteration of electrical properties; Interference with function. Surface deterioration; Structural weakening; Increased conductivity.
Wind	Force application Deposition of materials Heat loss (low velocity) Heat gain (high velocity)	Structural collapse; Interference with function; Loss of mechanical strength; Mechanical interference and clogging; Abrasion accelerated. Accelerates low-temperature effects. Accelerates high temperature effects.
Rain	Physical stress Water absorption and immersion Erosion Corrosion	Structural collapse. Increase in weight; Aids heat removal; Electrical failure; Structural weakening. Removes protective coatings; Structural weakening; Surface deterioration. Enhances chemical reactions.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-3: ENVIRONMENTAL EFFECTS (CONT'D)

ENVIRONMENT	PRINCIPAL EFFECTS	TYPICAL FAILURES INDUCED
Temperature Shock	Mechanical stress	Structural collapse or weakening; Seal damage
High-speed particles (nuclear irradiation)	Heating Transmutation and ionization	Thermal aging; Oxidation. Alteration of chemical physical, and electrical properties; Production of gases and secondary particles.
Zero gravity	Mechanical stress Absence of convection cooling	Interruption of gravity-dependent functions. Aggravation of high-temperature effects.
Ozone	Chemical reactions: Crazing, cracking Embrittlement Granulation Reduced dielectric strength of air	Rapid oxidation; Alteration of electrical properties; Loss of mechanical strength; Interference with function. Insulation breakdown and arc-over.
Explosive decompression	Severe mechanical stress	Rupture and cracking; Structural collapse.
Dissociated gases	Chemical reactions: Contamination Reduced dielectric strength	Alteration of physical and electrical properties. Insulation breakdown and arc-over.
Acceleration	Mechanical stress	Structural collapse.
Vibration	Mechanical stress Fatigue	Loss of mechanical strength; Interference with function; Increased wear. Structural collapse.
Magnetic fields	Induced magnetization	Interference with function; Alteration of electrical properties; Induced heating.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Low temperatures experienced by electronic equipment can also cause reliability problems. These problems are usually associated with mechanical elements of the system. They include mechanical stresses produced by differences in the coefficients of expansion (contraction) of metallic and nonmetallic materials, embrittlement of nonmetallic components, mechanical forces caused by freezing of entrapped moisture, stiffening of liquid constituents, etc. Typical examples include cracking of seams, binding of mechanical linkages, and excessive viscosity of lubricants. Reliability improvement techniques for low temperature stress include the use of heating devices, thermal insulation and cold-withstanding materials.

Additional stresses are produced when electronic equipment is exposed to sudden changes of temperature or rapidly changing temperature cycling conditions. These conditions generate large internal mechanical stresses in structural elements, particularly when dissimilar materials are involved. Effects of the thermal shock-induced stresses include cracking of seams, delamination, loss of hermeticity, leakage of fill gases, separation of encapsulating components from components and enclosure surface leading to the creation of voids, and distortion of support members.

A thermal shock test is generally specified to determine the integrity of solder joints since such a test creates large internal forces due to differential expansion effects. Such a test has also been found to be instrumental in creating segregation effects in solder alloys leading to the formulation of lead-rich zones which are susceptible to cracking effects.

Electronic equipment is often subjected to environmental shock and vibration both during normal use and testing. Such environments can cause physical damage to parts and structural members when resulting deflections produce mechanical stresses which exceed the allowable working stress of the constituent parts.

The natural frequencies of items are important parameters which must be considered in the design process since a resonant condition can be produced if a natural frequency is within the vibration frequency range. The resonance condition will greatly amplify the deflection of the next higher level of assembly and may increase stresses beyond the safe limit.

The vibration environment can be particularly severe for electrical connectors, since it may cause relative motion between members of the connector. This motion, in combination with other environmental stresses, can produce fret corrosion. This generates wear debris and causes large variations in contact resistance. Reliability improvement techniques for vibration stress include the use of stiffening, control of resonance, and reduced freedom of movement.

Humidity and salt-air environments degrade equipment performance since they promote corrosion effects in metallic components. They can also foster the creation of galvanic cells, particularly when dissimilar metals are in contact. Another deleterious effect of humidity and salt air atmospheres is the formation of surface films on nonmetallic parts. These films cause leakage paths and degrade the insulation and dielectric properties of these materials. Absorption of moisture by insulating materials can also cause a significant increase in volume conductivity

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

and the dissipation factor of materials so affected. Reliability improvement techniques for humidity and salt environments include the usage of hermetic sealing, moisture-resistant material, dehumidifiers, protective coatings, protective covers, and reduced use of dissimilar metals.

Electromagnetic and nuclear radiation can disrupt performance and, in some cases, cause permanent damage to exposed equipment. It is important, therefore, that such effects be considered in determining the required environmental strength required to achieve a specified reliability goal.

Electromagnetic radiation often produces interference and noise effects within electronic circuitry which can impair the functional performance of the system. Sources of these effects include corona discharges, lightning discharges, sparking, and arcing phenomena. These may be associated with high voltage transmission lines, ignition systems, brush-type motors, and even the equipment itself. Generally, the reduction of interference effects requires incorporation of filtering and shielding features, or the specification of less susceptible components and circuitry.

Nuclear radiation can cause permanent damage by alteration of the atomic or molecular structure of dielectric and semiconductor materials. High energy radiation can also cause ionization effects which degrade the insulation levels of dielectric materials. The mitigation of nuclear radiation effects typically involves the use of materials and parts possessing a higher degree of radiation resistance, and the incorporation of shielding and hardening techniques.

Each of the environmental factors experienced by an item during its life cycle must be considered in the design process. This ensures that the design will have adequate environmental strength.

Equipment failures have three convenient classifications:

- (1) Poor design or incorrect choice of materials or components.
- (2) Inadequate quality control which permits deviations from design specifications.
- (3) Deterioration caused by environmental effects or influences.

Obviously, the first and third classes are related. Specifically, the careful selection of design and materials can extend item reliability by reducing or eliminating adverse environmental effects. The environment is neither forgiving nor understanding; it methodically surrounds and attacks every component of a system, and when a weak point exists, equipment reliability suffers. Design and reliability engineers, therefore, must understand the environment and its potential effects, and then must select designs or materials that counteract these effects or must provide methods to alter or control the environment within acceptable limits. Selecting designs or materials that withstand the environment has the advantage of not requiring extra components that also require environmental protection and add weight and cost.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

In addition to the obvious environments of temperature, humidity, shock, and vibration, the design engineer will create environments by his choice of designs and materials. A gasket or seal, for example, under elevated temperatures or reduced pressures may release corrosive or degrading volatiles into the system. Teflon may release fluorine, and polyvinylchloride (PVC) may release chlorine. Certain solid rocket fuels are degraded into a jelly-like mass when exposed to aldehydes or ammonia, either of which come from a phenolic nozzle cone. These examples illustrate that internal environments designed into the system can seriously affect reliability.

7.6.3 Temperature Protection

Heat and cold are powerful agents of chemical and physical deterioration for two very simple, basic reasons

- (1) The physical properties of almost all known materials are greatly modified by changes in temperature.
- (2) The rate of almost all chemical reactions is markedly influenced by the temperature of the reactants. A familiar rule-of-thumb for chemical reactions (Reference [31]) is that the rate of many reactions doubles for every rise in temperature of 10°C; this is equivalent to an activation energy of about 0.6 eV.

High temperature degradation can be minimized by passive or active techniques. Passive techniques use natural heat sinks to remove heat, while active techniques use devices such as heat pumps or refrigeration units to create heat sinks. Such design measures as compartmentation, insulation of compartment walls, and intercompartment and intrawall air flow can be applied independently or in combination. Every system component should be studied from two viewpoints:

- (1) Is a substitute available that will generate less heat?
- (2) Can the component be located and positioned so that its heat has minimum effect on other components?

For a steady temperature, heat must be removed at the same rate at which it is generated. Thermal systems such as conduction cooling, forced convection, blowers, direct or indirect liquid cooling, direct vaporization or evaporation cooling, and radiation cooling must be capable of handling natural and induced heat sources. Passive sinks require some means of progressive heat transfer from intermediate sinks to ultimate sinks until the desired heat extraction has been achieved. Thus, when heat sources have been identified, and heat removal elements selected, they must be integrated into an overall heat removal system, so that heat is not merely redistributed within the system. Efficiently integrated heat removal techniques can significantly improve item reliability.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Besides the out-gassing of corrosive volatiles when subjected to heat, almost all known materials will expand or contract when their temperature is changed. This expansion and contraction causes problems with fit and sealing, and produces internal stresses. Local stress concentrations due to nonuniform temperature are especially damaging, because they can be so high. A familiar example is a hot water glass that shatters when immersed in cold water. Metal structures, when subjected to cyclic heating and cooling, may ultimately collapse due to the induced stresses and fatigue caused by flexing. The thermocouple effect between the junction of two dissimilar metals causes an electric current that may induce electrolytic corrosion. Plastics, natural fibers, leather, and both natural and synthetic rubber are all particularly sensitive to temperature extremes as evidenced by their brittleness at low temperatures and high degradation rates at high temperatures. Table 7.6-4 summarizes some of the basic precautions for achieving reliability at low temperatures. An always-present danger is that in compensating for one failure mode, the change will aggravate another failure mode.

The preferred method for evaluating the thermal performance of electronic equipment (with respect to reliability) is a parts stress analysis method. It can be used to determine the maximum safe temperatures for constituent parts. The parts stress analysis method for evaluating system thermal performance is based on a determination of the maximum allowable temperature for each part. This determination is to be consistent with the equipment reliability and the failure rate allocated to that part.

A reduction in the operating temperature of components is a primary method for improving reliability. Reduction in temperature generally can be achieved by providing a thermal design which reduces heat input to minimally achievable levels and provides low thermal resistance paths from heat producing elements to an ultimate heat sink of reasonably low temperature. The thermal design is often as important as the circuit design in obtaining the necessary performance and reliability characteristics of electronic equipment. Adequate thermal design maintains equipment and parts within their permissible operating temperature limits under operating conditions. Thermal design is an engineering discipline in itself, and will not be addressed in this section. An excellent document on thermal design is MIL-HDBK-251. It provides a very comprehensive review of the aspects of thermal design. Also, Chapter 9 of Reference [32] discusses the subject in some detail.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-4: LOW TEMPERATURE PROTECTION METHODS

EFFECT	PREVENTIVE MEASURES
Differential contraction	Careful selection of materials Provision of proper clearance between moving parts Use of spring tensioners and deeper pulleys for control cables Use of heavier material for skins
Lubrication stiffening	Proper choice of lubricants: <ul style="list-style-type: none"> • Use greases compounded from silicones, diesters or silicone diesters thickened with lithium stearate • Eliminate liquid lubricants wherever possible
Leaks in hydraulic systems	Use of low temperature sealing and packing compounds, such as silicone rubbers
Stiffening of hydraulic system	Use of proper low temperature hydraulic fluids
Ice Damage caused by freezing of collected water	Elimination of moisture by: <ul style="list-style-type: none"> • Provision of vents • Ample draining facilities • Eliminating moisture pockets • Suitable heating • Sealing • Desiccation of air
Degradation of material properties and component reliability	Careful selection of materials and components with satisfactory low temperature capabilities

7.6.4 Shock and Vibration Protection

Protection against mechanical abuse is generally achieved by using suitable packaging, mounting, and structural techniques. The reliability impact of mechanical protection techniques is generally singular in that these measures do or do not afford the required protection against the identified mechanical abuse stresses. In most cases, tradeoff situations between the level of protection and reliability improvements are not as pronounced as in the case of thermal protection. The one exception may be the case of fatigue damage, where the level of protection would have a significant impact on reliability if, in fact, fatigue were a primary failure mechanism in the normal life of the equipment.

Basic structural design techniques, such as proper component location and selection of suitable materials, can aid in protecting an item against failure caused by severe environmental stresses from shock or vibration.

There are two approaches that may be taken when shock or vibration are present; either isolate the equipment or build it to withstand the shock or vibration. The problem with isolation is that effective, simultaneous control of both shock and vibration is difficult. When only one or the

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

other is present, special mountings are often used. Protective measures against shock and vibration stresses are generally determined by an analysis of the deflections and mechanical stresses produced by these environment factors. This generally involves the determination of natural frequencies and evaluation of the mechanical stresses within component and materials produced by the shock and vibration environment. If the mechanical stresses so produced are below the allowable safe working stress of the materials involved, no direct protection methods are required. If, on the other hand, the stresses exceed the safe levels, corrective measures such as stiffening, reduction of inertia and bending moment effects, and incorporation of further support members are indicated. If such approaches do not reduce the stresses below the safe levels, further reduction is usually possible by the use of shock absorbing mounts.

One factor, however, which is not often considered, is that the vibration of two adjacent components, or separately insulated subsystems, can cause a collision between them if maximum excursions and sympathetically induced vibrations are not evaluated by the designer. Another failure mode, fatigue (the tendency for a metal to break under cyclic stressing loads considerably below its tensile strength) is an area of reliability concern due to shock or vibration. Fatigue includes low cycle fatigue, acoustic fatigue, and fatigue under combined stresses. The interaction between multiaxial fatigue and other environmental factors such as temperature extremes, temperature fluctuations, and corrosion requires careful study. Stress-strength analysis of components and parameter variation analysis are particularly suited to these effects. Destruction testing methods are also very useful in this area. For one shot devices, several efficient nondestructive evaluation (NDE) methods are available - such as X-ray, neutron radiography, and dye penetrant - which can be used to locate fatigue cracks. Developing a simple design that is reliable is much better than elaborate fixes and subsequent testing to redesign for reliability.

In some cases, even though an item is properly isolated against shock and vibration damage, repetitive forces may loosen the fastening devices. Obviously, if the fastening devices loosen enough to permit additional movement, the device will be subjected to increased forces and may fail. Many specialized self-locking fasteners are commercially available, and fastener manufacturers usually will provide valuable assistance in selecting the best fastening methods.

An isolation system can be used at the source of the shock or vibration, in addition to isolating the protected component. The best results are obtained by using both methods. Damping devices are used to reduce peak oscillations, and special stabilizers employed when unstable configurations are involved. Typical examples of dampeners are viscous hysteresis, friction, and air damping. Vibration isolators commonly are identified by their construction and material used for the resilient elements (rubber, coil spring, woven metal mesh, etc.). Shock isolators differ from vibration isolators in that shock requires stiffer springs and a higher natural frequency for the resilient element. Some of the types of isolation mounting systems are underneath, over-and-under, and inclined isolators.

A specific component may initially appear to be sufficiently durable to withstand the anticipated shock or vibration forces without requiring isolation or insulation. However, this observation can be misleading since the attitude in which a part is mounted, its location relative to other

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

parts, its position within the system, and the possibility of its fasteners or another component fasteners coming loose can alter significantly the imposed forces. Another component, for example, could come loose and strike it, or alter the forces acting on it to the extent that failure results.

The following basic considerations must be included in designing for shock and vibration:

- (1) The location of the component relative to the supporting structure (i.e., at the edge, corner, or center of the supporting structure).
- (2) The orientation of the part with respect to the anticipated direction of the shock or vibration forces.
- (3) The method used to mount the part.

7.6.5 Moisture Protection

Moisture is a chemical (H₂O plus impurities) and, considering its abundance and availability in almost all environments, is probably the most important chemical deteriorative factor of all. It is the impurities in moisture that cause many of chemical problems. In addition to its chemical effects, such as the corrosion of many metals, condensed moisture also acts as a physical agent. An example of the physical effects of moisture is the damage done in the locking together of mating parts when moisture condenses on them and then freezes. Similarly, many materials that are normally pliable at low temperatures will become hard and perhaps brittle if moisture has been absorbed and subsequently freezes. Condensed moisture acts as a medium for the interaction between many otherwise-relatively-inert materials. Most gases readily dissolve in moisture. The chlorine released by PVC plastic, for example, forms hydrochloric acid when combined with moisture.

While the presence of moisture may cause deterioration, the absence of moisture also may cause reliability problems. The useful properties of many nonmetallic materials, for example, depend upon an optimum level of moisture. Leather and paper become brittle and crack when they are very dry. Similarly, fabrics wear out at an increasing rate as moisture levels are lowered and fibers become dry and brittle. Dust is encountered in environments and can cause increased wear, friction, and clogged filters due to lack of moisture.

Moisture, in conjunction with other environmental factors, creates difficulties that may not be characteristic of the factors acting alone. For example, abrasive dust and grit, which would otherwise escape, are trapped by moisture. The permeability (to water vapor) of some plastics (PVC, polystyrene, polyethylene, etc.) is related directly to their temperature. The growth of fungus is enhanced by moisture, as is the galvanic corrosion between dissimilar metals.

Some design techniques that can be used singly or combined to counteract the effects of moisture are: (1) eliminating moisture traps by providing drainage or air circulation; (2) using desiccant devices to remove moisture when air circulation or drainage is not possible; (3) applying

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

protective coatings; (4) providing rounded edges to allow uniform coating of protective material; (5) using materials resistant to moisture effects, fungus, corrosion, etc.; (6) hermetically sealing components, gaskets and other sealing devices; (7) impregnating or encapsulating materials with moisture resistant waxes, plastics, or varnishes; and (8) separating dissimilar metals, or materials that might combine or react in the presence of moisture, or of components that might damage protective coatings. The designer also must consider possible adverse effects caused by specific methods of protection. Hermetic sealing, gaskets, protective coatings, etc., may, for example, aggravate moisture difficulties by sealing moisture inside or contributing to condensation. The gasket materials must be evaluated carefully for out-gassing of corrosive volatiles or for incompatibility with adjoining surfaces or protective coatings.

MIL-HDBK-454 provides common requirements for electronic equipment related to corrosion protection (Guideline 15), dissimilar metals (Guideline 16), and moisture pockets (Guideline 31).

7.6.6 Sand and Dust Protection

Sand and dust primarily degrade equipment by:

- (1) Abrasion leading to increased wear.
- (2) Friction causing both increased wear and heat.
- (3) Clogging of filters, small apertures, and delicate equipment.

Thus, equipment having moving parts requires particular care when designing for sand and dust protection. Sand and dust will abrade optical surfaces, either by impact when being carried by air, or by physical abrasion when the surfaces are improperly wiped during cleaning. Dust accumulations have an affinity for moisture and, when combined, may lead to corrosion or the growth of fungus.

In relatively dry regions, such as deserts, fine particles of dust and sand are readily agitated into suspension in the air, where they may persist for many hours, sometimes reaching heights of several thousand feet. Thus, even though there is virtually no wind present, the speeds of vehicles or vehicle-transported equipment through these dust clouds can cause surface abrasion by impact, in addition to the other adverse effects of the sand or dust.

Although dust commonly is considered to be fine, dry particles of earth, it also may include minute particles of metals, combustion products, solid chemical contaminants, etc. These other forms may provide direct corrosion or fungicidal effects on equipment, since this dust may be alkaline, acidic, or microbiological.

Since most equipment requires air circulation for cooling, removing moisture, or simply functioning, the question is not whether to allow dust to enter, but, rather, how much or what size dust can be tolerated. The problem becomes one of filtering the air to remove dust particles

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

above a specific nominal size. The nature of filters, however, is such that (for a given working filter area), as the ability of the filter to stop increasingly smaller dust particles is increased, the flow of air or other fluid through the filter is decreased. Therefore, the filter surface area either must be increased, the flow of fluid through the filter decreased, or the allowable particle size increased. Interestingly enough, a study by R.V. Pavia (Reference [33]) showed that, for aircraft engines, the amount of wear was proportional to the weight of ingested dust, but that the wear produced by 100m dust is approximately half that caused by 15m dust. The 15m dust was the most destructive of all sizes tried.

Sand and dust protection, therefore, must be planned in conjunction with protective measures against other environmental factors. It is not practical, for example, to specify a protective coating against moisture if sand and dust will be present, unless the coating is carefully chosen to resist abrasion and erosion, or is self-healing.

7.6.7 Explosion Proofing

Protection against explosion is both a safety and reliability problem. An item that randomly exhibits explosive tendencies is one that has undesirable design characteristics and spectacular failure modes. Preventing this type of functional termination, therefore, requires extreme care in design and reliability analyses.

Explosion protection planning must be directed to three categories (not necessarily mutually exclusive) of equipment:

- (1) Items containing materials susceptible to explosion.
- (2) Components located near enough to cause the explosive items to explode.
- (3) Equipment that might be damaged or rendered temporarily inoperative by overpressure, flying debris, or heat from an explosion.

The first category includes devices containing flammable gases or liquids, suspensions of dust in the air, hypergolic materials, compounds which spontaneously decompose in certain environments, equipment containing or subjected to high or low extremes of pressure (includes implosions), or any other systems capable of creating an explosive reaction. The second category is fairly obvious and includes many variations on methods for providing an energy pulse, a catalyst, or a specific condition that might trigger an explosion. A nonexplosive component, for example, could create a corrosive atmosphere, mechanical puncture, or frictional wear on the side of a vessel containing high pressure air and thereby cause the air container to explode. The third category encompasses practically everything, including items in the first two categories, since a potentially explosive device (such as a high pressure air tank) can be damaged or made to explode by the overpressure from another explosion. Thus, some reasoning must be applied when considering devices not defined by the first two categories. From a practical standpoint, explosion protection for items in the third category ought to be directed to equipment that might

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

possibly be near explosions. The sides of an electronic maintenance van, for example, will be subjected to overpressures from exploding enemy artillery rounds. If designed for protection against anything but a direct hit, the van would be extremely difficult to transport. Thus, mobility (and size) and protections against blast are traded off. On the other end of the compromise scale, however, is the bad effect on the reliability of internal equipment when explosion protection is minimal or nonexistent.

The possibility of an explosive atmosphere leaking or circulating into other equipment compartments must be recognized. Lead acid batteries, for example, create hydrogen gas that, if confined or leaked into a small enclosure, could be exploded by electrical arcing from motor brushes, by sparks from metallic impacts, or by exhaust gases. Explosive environments, such as dust-laden air, might be circulated by air distribution systems.

Explosion protection and safety are very important for design and reliability evaluations, and must be closely coordinated and controlled. Just as safe equipment is not necessarily reliable, neither is reliable equipment necessarily safe.

7.6.8 Electromagnetic Radiation Protection

The electromagnetic spectrum is divided conveniently into several categories ranging from gamma rays at the short wavelength end through X-rays, ultraviolet, visible, infrared, and radio, to the long wavelength radiation from power lines. Solar radiation is the principal reliability concern. Damage near the surface of the earth is caused by the electromagnetic radiation in the wavelength range from approximately 0.15 to 5m. This range includes the longer ultraviolet rays, visible light, and up to about midpoint in the infrared band. Visible light accounts for roughly one-third of the solar energy falling on the earth, with the rest being in the invisible ultraviolet and infrared ranges. The solar constant (the quantity of radiant solar heat received normally at the outer layer of the atmosphere of the earth) is, very roughly, about 1 kilowatt per square meter. In some parts of the world, almost this much can fall on a horizontal surface on the ground at noon.

Solar radiation principally causes physical or chemical deterioration of materials. Examples are the effects due to the increased temperature and deterioration of natural and synthetic rubber. These are mechanical effects. Radiation also can cause functional effects, such as the temporary electrical breakdown of semiconductor devices exposed to ionizing radiation. Considerations to include in a radiation protection analysis are the type of irradiated material and its characteristics of absorption and sensitivity to specific wavelengths and energy levels, ambient temperature, and proximity of reactive substances such as moisture, ozone, and oxygen. Some specific protection techniques are shielding, exterior surface finishes that will absorb less heat and are less reactive to radiation effects of deterioration, minimizing exposure time to radiation, and removing possibly reactive materials by circulation of air or other fluids or by careful location of system components. More extensive information is given in Reference [27].

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Another form of natural electromagnetic radiation is that associated with lightning. It is estimated that lightning strikes the earth about 100 times each second, each stroke releasing large bursts of electromagnetic energy which encircle the globe. Most of this energy is concentrated at the low frequency end of the electromagnetic spectrum with the maximum power level being concentrated at about 3 kHz.

Man-made electromagnetic energy is second in importance only to solar energy. Artificial electromagnetic radiators include those in power distribution systems, a multitude of uses in communications, and specialized detection and analytical applications. The development of lasers has introduced another intense source of electromagnetic radiation and, in military application, the electromagnetic pulse (EMP) associated with nuclear weapon detonations is of considerable importance.

The EMP spectrum is similar to that created by lightning with a maximum energy appearing at about 10 kHz but distributed with smaller amplitudes throughout a broad region of the frequency spectrum. EMP energy is of considerably greater magnitude than that observed in lightning and extends over a much larger area of the earth. Despite the similarities among EMP and lightning and other strong sources of electromagnetic energy, it cannot be assumed that protective measures consistent with these other electromagnetic radiation sources will protect material from the effects of EMP. The rapid rise time of the pulse associated with a nuclear detonation and the strength of the resulting pulse are unique.

A variety of effects of electromagnetic radiation on material are known, probably a number of effects are still unrecognized, and some of the effects on humans are poorly understood. Of course, one of the most important effects of electromagnetic radiation in the environment is the electromagnetic interference (EMI) it produces in the electromagnetic spectrum. Well known examples are called radio interference and radar clutter. Another important effect in the military is the interaction of electromagnetic radiation with electroexplosive devices used as detonators. Military as well as civilian explosives are provided with detonators that often depend on heating a small bridge wire to initiate the explosion. Absorbed electromagnetic radiation can accidentally activate such fuzes.

Protection against the effects of electromagnetic radiation has become a sophisticated engineering field of electromagnetic compatibility (EMC) design. The most direct approach to protection is, in most cases, to avoid the limited region in which high radiation levels are found. When exposure cannot be avoided, shielding and filtering are important protective measures. In other cases material design changes or operating procedural changes must be instituted in order to provide protection.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.6.9 Nuclear Radiation

Although a natural background level of nuclear radiation exists, the only nuclear radiation that is of interest to design engineers is that associated with manmade sources such as reactors, isotope power sources, and nuclear weapons. The most important of these sources is nuclear weapons, the effects of which can produce both transient and permanent damaging effects in a variety of material.

X-rays, gamma rays, and neutrons are the types of nuclear radiation of most concern. As opposed to charged nuclear particles, which also emanate from nuclear reactions, those forms of radiation listed have long ranges in the atmosphere; thus, they can irradiate and damage a variety of military material.

Among the nuclear effects that are of most concern are those called "transient radiation effects on electronics," often referred to as TREE. These transient effects are due primarily to the non-equilibrium free charged condition induced in material primarily by the ionization effects of gamma rays and X-rays. The separation of transient and permanent effects is made on the basis of the primary importance of the radiation effects. For example, a large current pulse may be produced by ionizing radiation, and this current pulse may result in permanent damage to a device by overheating. This effect is considered transient because the permanent damage results from overheating due to excess current rather than to direct radiation-induced material property change.

It is impossible to completely protect material items from nuclear radiation. The variety of effects produced by nuclear radiation for different materials and components makes protective design difficult. The procedure employed is to define a radiation hardness level in a given material item and to design and test the item to that level.

Nuclear radiation hardening is a large and complex field with a variety of specialists required to deal with different aspects of the problem. This subject is treated extensively in the Design Engineers' Nuclear Effects Manual (References [34] - [37]).

Table 7.6-5 represents a summary of environmental effects and design techniques to overcome them.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-5: ENVIRONMENTAL STRESSES IMPROVEMENT TECHNIQUES IN ELECTRONIC EQUIPMENT

ENVIRONMENTAL STRESS	EFFECTS	RELIABILITY IMPROVEMENT TECHNIQUES
High Temperature	Parameters of resistance, inductance, capacitance, power factor, dielectric constant, etc. will vary; insulation may soften; moving parts may jam due to expansion; finishes may blister; devices suffer thermal aging; oxidation and other chemical reactions are enhanced; viscosity reduction and evaporation of lubricants are problems; structural overloads may occur due to physical expansions.	Heat dissipation devices, cooling systems, thermal insulation, heat-withstanding materials.
Low Temperature	Plastics and rubber lose flexibility and become brittle; electrical constants vary; ice formation occurs when moisture is present; lubricants gel and increase viscosity; high heat losses; finishes may crack; structures may be overloaded due to physical contraction.	Heating devices, thermal insulation, cold-withstanding materials.
Thermal Shock	Materials may be instantaneously overstressed causing cracks and mechanical failure; electrical properties may be permanently altered. <i>Crazing, delamination, ruptured seals.</i>	Combination of techniques for high and low temperatures.
Shock	Mechanical structures may be overloaded causing weakening or collapse; items may be ripped from their mounts; mechanical functions may be impaired.	Strengthened members, reduced inertia and moments, shock absorbing mounts.
Vibration	Mechanical strength may deteriorate due to fatigue or overstress; electrical signals may be mechanically and erroneously modulated; materials and structures may be cracked, displaced, or shaken loose from mounts; mechanical functions may be impaired; finishes may be scoured by other surfaces; wear may be increased.	Stiffening, control of resonance.
Humidity	Penetrates porous substances and causes leakage paths between electrical conductors; causes oxidation which leads to corrosion; moisture causes swelling in materials such as gaskets; excessive loss of humidity causes embrittlement and granulation.	Hermetic sealing, moisture-resistant material, dehumidifiers, protective coatings.
Salt Atmosphere and Spray	Salt combined with water is a good conductor which can lower insulation resistance; causes galvanic corrosion of metals; chemical corrosion of metals is accelerated.	Nonmetal protective covers, reduced use of dissimilar metals in contact, hermetic sealing, dehumidifiers.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-5: ENVIRONMENTAL STRESSES IMPROVEMENT TECHNIQUES IN ELECTRONIC EQUIPMENT (CONT'D)

ENVIRONMENTAL STRESS	EFFECTS	RELIABILITY IMPROVEMENT TECHNIQUES
Electromagnetic Radiation	Causes spurious and erroneous signals from electrical and electronic equipment and components; may cause complete disruption of normal electrical and electronic equipment such as communication and measuring systems.	Shielding, material selection, part type selection.
Nuclear/Cosmic Radiation	Causes heating and thermal aging; can alter chemical, physical and electrical properties of materials; can produce gases and secondary radiation; can cause oxidation and discoloration of surfaces; damages electrical and electronic components especially semiconductors.	Shielding, component selection, nuclear hardening.
Sand and Dust	Finely finished surfaces are scratched and abraded; friction between surfaces may be increased; lubricants can be contaminated; clogging of orifices, etc.; materials may be worn, cracked, or chipped; abrasion, contaminates insulations, corona paths.	Air-filtering, hermetic sealing.
Low Pressure (High Altitude)	Structures such as containers, tanks, etc. are overstressed and can be exploded or fractured; seals may leak; air bubbles in materials may explode causing damage; internal heating may increase due to lack of cooling medium; insulations may suffer arcing and breakdown; ozone may be formed, outgasing is more likely.	Increased mechanical strength of containers, pressurization, alternate liquids (low volatility), improved insulation, improved heat transfer methods.

7.6.10 Avionics Integrity Program (AVIP)

Attention is increasingly being given to potential wear-out mechanisms associated with electronic equipments used in modern aircraft. Fatigue induced failures are recognized as a major portion of complex aircraft electronics system failures. Both vibration and temperature cycling are major contributors to the fatigue phenomenon. Of these two factors, temperature cycling by itself usually makes the more significant contribution, but the combined effect of the two factors acting in concert can be much greater than either one in isolation. Many of the metals and plastics used in complex avionics electronic systems have a high thermal coefficient of expansion (TCE) and also a high modulus of elasticity.

This combination of TCE mismatch and high modulus of elasticity can lead to high localized stress within various circuit elements which is exacerbated by any vibration contribution as the equipment is exposed to the full range of operational temperatures, and the shock and vibration effects incident to high performance aircraft operation. Some of the greatest thermal-expansion problem areas are in the electronic-component lead wires, solder joints, and printed-circuit-board materials. A great deal of attention is also being focused on the field of leadless chip carrier components and other surface-mounted devices with respect to preventing thermal-creep strain in

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

the solder joints. A large number of different materials, with various different TCE's, are involved in the manufacture and assembly of these types of devices.

The Air Force Avionics Integrity Program (AVIP) as detailed in MIL-HDBK-87244, "Avionics Integrity Program," is specifically designed to address these types of problems. MIL-HDBK-87244 is a guidance handbook that emphasizes reliability by design including linkages to related systems engineering areas and experience from recent programs, program studies, related initiatives, and the latest concepts in integrated product development (IPD). AVIP is a logical and disciplined systems engineering approach to requirements definition, development, and production of avionics and other electronics products. It defines life, usage, environment and supportability requirements and process tasks to achieve required performance over the life of the electronics. AVIP employs basic physics, chemistry, and engineering principles to ensure an understanding of the influence of the usage and environments on materials and parts. It focuses on key production and process characteristics and control of variability of materials, parts and processes.

Incorporation of the AVIP philosophy into an integrated engineering and manufacturing process supports the following:

- a. Understanding and defining:
 - product life requirements
 - how and where the equipment will be operated and maintained and the associated environments
 - user supportability and constraints
- b. Understanding:
 - materials, processes and technologies to include properties, life limits and variabilities
 - the stresses imposed by the life cycle usage and environments
- c. Establishing product and process design criteria tailored for the specific application
- d. Identifying key product characteristics, design parameters, and production process characteristics and controlling their impact on cost, performance and supportability
- e. Performing iterative analyses, simulations and trade studies to facilitate a balanced design solution
- f. Conducting incremental developmental and qualification testing to verify analyses and design solutions

While all TCE and vibration induced stress concentrations cannot be eliminated in a typical electronic box, they can be minimized by the proper selection of parts and materials, and by the optimization of fabrication techniques, and geometrics. It is virtually impossible to analyze every

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

material interface, every notch, hole, rivet, bend and screw in every section of an electronic box. Time and money will usually permit the examination and analysis of only major structural members in the system. Therefore, it is necessary to recognize and identify the most probable primary and secondary stress points during the preliminary design phase and to adequately address at least these concerns before the design effort culminates in the final manufactured product.

Each event and situation in the life cycle of an item can be related to environmental factors. These events and situations in the pre-operational, operational, and maintenance environments can be related to stresses, which the equipment must withstand to perform reliably.

7.6.10.1 MIL-STD-1670: Environmental Criteria and Guidelines for Air Launched Weapons

This standard:

- (1) provides guidelines for determining the environmental conditions to which air-launched weapons will be subjected during the factory-to-target sequence (acceptance-to-end-of-useful-life profile).
- (2) describes the tasks involved in applying the essential environmental design criteria in all phases of weapon development.
- (3) provides the developer with background data on which to base environmental design and test requirements.

Table 7.6-6 provides a checklist for typical system use conditions. This checklist helps the designer or analyst to determine if environments have been adequately considered in the design for events and situations of an item's life cycle.

Table 7.6-7 shows some effects of natural and induced environments during the various phases of the lifetime of an item. Table 7.6-8 rates the importance of the environmental factors for the various regions of the environment.

Starting with program initiation, the standard defines the requirements necessary for the development of information leading to full-scale development. Usage information needed for delineation and examination of all probable environments that could affect reliability or operational capability of an air-launched weapon includes the aircraft profile (launch-to-landing subphases), combat use tactics, store mix, etc., of the same nature as items shown in Table 7.6-6. For reference, Figure 1 through 28 of MIL-STD-1670 demonstrate a method of presenting

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-6: SYSTEM USE CONDITIONS CHECKLIST (TYPICAL)

HANDLING/TRANSFER	TRANSPORTATION
<ul style="list-style-type: none"> - CONUS - Oversea Global Locality - Shore Station - NWS - Depot - Commercial Rework - Truck Transport - Rail Transport - Air Transport - Marine Transport - Carrier Onboard Delivery (COD) <ul style="list-style-type: none"> Aviation spares airlift - Underway Replenishment (UNREP) <ul style="list-style-type: none"> Vertical (Rotary Wing Aircraft) Cargo aircraft Ram tensioned highline (RTHL) High line transfer UNREP Ship - Launch Platform <ul style="list-style-type: none"> Aircraft carrier Expeditionary airlift Short Airfield for Tactical Support (SATS) Non-aviation ship (AGC, AK, CA, DE, DLGN,...) - Operational <ul style="list-style-type: none"> A/C handling, weapons handling Shipboard tie-down Land based tie-down Land based apron tie down Towing, Spotting Handling equipment Maintenance test Maintenance shop Avionics maintenance van A/C elevator vertical transit A/C cyclic turnaround Hangar/flight deck Mobile maintenance facility Flight deck-to-storage, storage-to-flight deck 	<ul style="list-style-type: none"> - CONUS - Oversea Global Locality - Truck Transport <ul style="list-style-type: none"> Flatbed truck, exposed Van, Truck Trailer Containerized - Rail Transport <ul style="list-style-type: none"> Boxcar Flatcar Containerized - Air Transport <ul style="list-style-type: none"> Turboprop Propeller Jet - Marine Transport <ul style="list-style-type: none"> Ammunition Ship (AE) Fast Combat Support Ship (AOE) Cargo Ship (AK) Other auxiliary ship (AKL,...) Ship Hold Ship deck exposure - NWS - Shore station - Depot - Commercial rework - Packaging

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-6: SYSTEM USE CONDITIONS CHECKLIST (TYPICAL) (CONT'D)

STORAGE	OPERATIONAL
<ul style="list-style-type: none"> - CONUS - Oversea global locality - Shore station - NWS - Depot - Commercial rework - Igloo magazine - Uninsulated building - Roofed Structure - no sidewalls - Dump storage, exposed - Dump storage, revetment - Railroad siding - Store item - Weapons item - Explosives item - Aircraft carrier - Expeditionary airfield - SATS - Non-aviation ship - Long term - Short term - Interim - Maintenance shop - Avionics maintenance van - Mobile maintenance facility - Containerization - Packaging 	<ul style="list-style-type: none"> - Natural environment - Induced environment - Combined environment - Catapult launch - Arrested landing - Store separation - Weapon release - Weapon delivery - Weapon exhaust impingement - Weapon to weapon - Weapon to A/C - A/C to weapon - A/C taxi - Jet exhaust backflow - Helicopter in-flight refueling (HIFR) - Probe/drogue refueling - Buddy tanker - Jet blast (other aircraft) - Jet blast (VTOL) - Mission mix - Store mix - Combat tactics - Operational deployment - A/C/Weapons maneuvers - Equipment location - Flight line operations - Chance of environment encounter - Launch platform

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-7: ENVIRONMENTAL ANALYSIS
(INDUCED ENVIRONMENT)

Mission Regime	Storage	Transportation	Standby (Idle)	Standby	Use	Maintenance
Acceleration	NA	NA	NA	⊗	⊗	NA
Acoustic Vibration	NA	NA	⊗	⊗	⊗	NA
Countermeasures	NA	NA	NA	NA	⊗	NA
Enemy Action	x	x	x	⊗	⊗	NA
Explosive Atmosphere	NA	NA	NA	NA	NA	NA
Flutter	NA	NA	NA	NA	⊗	NA
Ionized Gases	NA	NA	NA	NA	x	NA
Magnetic Fields	NA	NA	NA	o	o	o
Moisture	x	NA	x	⊗	⊗	⊗
Nuclear Radiation	NA	NA	NA	x	⊗	⊗
Pressure	NA	NA	NA	NA	⊗	NA
Shock	NA	x	NA	x	⊗	x
Temperature	NA	NA	⊗	⊗	⊗	NA
Temperature Shock	NA	NA	⊗	⊗	⊗	NA
Vibration	NA	x	NA	x	x	x

Effects	Operational Effects	Mechanical/Physical Effects
o - Operational x - Mechanical/Physical ⊗ - Either or both NA - Not Applicable	Function, mission, etc. influenced rather than direct physical alternation of item. Example: reduced visibility caused by fog	Direct physical alteration of item. Examples: corrosion, fracture, puncture, melting

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-7: ENVIRONMENTAL ANALYSIS
(NATURAL ENVIRONMENT) (CONT'D)

Mission Regime	Storage	Transpor- tation	Standby (Idle)	Standby	Use	Mainten- ance
Aridity	x	x	x	x	x	x
Asteroids	NA	NA	NA	NA	NA	NA
Birds	o	NA	NA	NA	∅	∅
Clouds	NA	NA	NA	o	o	NA
Cosmic Radiation	NA	NA	NA	NA	x	NA
Density, Air	NA	NA	NA	NA	o	NA
Dust, Interplanetary	NA	NA	NA	NA	NA	NA
Dust, Lunar	NA	NA	NA	NA	NA	NA
Dust, Terrestrial	∅	x	x	o	NA	x
Electricity, Atmospheric	NA	NA	NA	NA	∅	NA
Fog	x	NA	x	o	NA	o
Frost	x	NA	x	o	NA	x
Fungi	x	NA	NA	NA	NA	x
Geomagnetism	NA	NA	NA	NA	o	NA
Gravity	NA	NA	NA	NA	o	NA
Heat	x	x	x	∅	∅	x
Humidity	x	x	x	∅	∅	x
Icing	x	x	∅	∅	∅	∅
Ionized Gases	NA	NA	NA	NA	∅	NA
Insects	∅	∅	∅	∅	∅	∅
Lightning	x	x	x	∅	∅	∅
Meteoroids	NA	NA	NA	NA	NA	NA
Ozone	NA	NA	NA	NA	x	NA
Pollution, Air	x	x	x	NA	∅	NA
Pressure, Air	NA	NA	NA	o	∅	o
Rain	x	x	x	x	x	x

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.6-8: ASSOCIATION OF FACTOR IMPORTANCE WITH REGION OF ENVIRONMENT

Region of the Environment	Environmental Factor																					
	Terrain	Temperature	Humidity	Pressure	Solar radiation	Rain	Solar precipitation	Fog	Wind	Salt	Ozone	Macrobiological organism	Microbiological organism	Atmospheric pollutants	Sand and Dust	Vibration	Shock	Acceleration	Acoustics	Electromagnetic radiation	Nuclear radiation	
Storage	O	A	A	C	O	O	O	O	C	C	C	B	B	C	C	C	B	O	O	O	O	O
Transportation	A	B	B	O	C	B	B	B	C	O	O	O	O	O	C	A	A	C	C	O	O	O
Highway	A	B	B	O	C	C	C	C	C	O	O	O	O	O	C	A	A	C	C	O	O	O
Rail	O	C	B	O	C	C	O	B	C	B	O	C	O	O	O	B	C	C	C	O	O	O
Ship	O	B	O	C	O	C	C	A	B	O	O	O	O	O	C	B	B	C	O	O	O	O
Air	O	B	O	C	O	C	C	A	B	O	O	O	O	O	C	B	B	B	O	O	O	O
Operational Use	A	A	A	O	B	A	A	B	B	C	O	C	O	C	C	B	B	O	C	B	C	C
Cold regions	A	A	A	C	B	A	O	O	B	B	O	C	A	O	O	B	B	O	C	B	C	C
Hot-wet	A	A	A	O	A	A	O	O	B	B	O	C	O	O	A	B	B	O	C	B	C	C
Hot-dry	A	A	A	O	A	A	B	B	B	B	C	C	B	C	B	B	B	O	C	B	O	O
Temperature	A	A	A	C	B	A	B	B	B	B	C	C	B	C	B	B	B	O	C	B	O	O
Indoor Use	O	B	B	O	O	O	O	O	O	O	O	C	C	C	B	C	C	O	O	B	B	O
Operational Storage	O	A	A	O	B	B	B	O	C	B	C	B	B	C	C	O	C	O	O	C	C	C

A - Major Importance B - Important C - Minor O - Absent

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

environmental criteria. The standard illustrates the major events, corresponding environments, and weapon status in a factory-to-target sequence. The air-launched weapon must perform as required in this sequence subsequent to, or while being subjected to, the established environments.

For more detailed information on environments, see References [26] - [30].

7.7 Human Performance Reliability

This section contains copyright-protected material for which permission has been granted for publication in this handbook.

7.7.1 Introduction

A short, but informative history of human performance reliability is given by Dougherty and Fragola [38]. Lee et. al. [39] developed an extensive, useful literature survey on the subject. The survey is sorted into the following categories:

- (1) Human-Operator Reliability Prediction
- (2) Human Reliability in Maintenance Work
- (3) Data on Human Reliability Estimates
- (4) Human-Machine System Effectiveness
- (5) Allocation of Human-Machine Reliability
- (6) Human Operator Models in Control Loop Systems
- (7) Literature Survey and Overview
- (8) Miscellany

The survey includes a convenient comparison of hardware and human reliability, see Table 7.7-1.

Another major comparative work is the survey of human reliability models performed by Meister [40]. Although somewhat dated now, the work provides excellent detailed narratives of the models extant in 1971 and, to a large extent, still applicable. Each of the many models are described and then evaluated with respect to comprehensiveness, applicability, and timing. Model characteristics are described in terms of objectivity and structure. Ten analytic methods for operability prediction, six simulation methods for operability prediction, and three maintainability prediction methods are described.

In a profile of the state of the art almost 20 years after Meister's work, Apostolakis et al. [41] reviewed human performance reliability analysis techniques, primarily with respect to those used in the nuclear power industry. Some of the evaluations tend to be pessimistic regarding the utility and validity of the available models. The reader certainly is advised to consider the views they provide when considering a specific prediction technique.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.7-1: COMPARISON BETWEEN HARDWARE AND HUMAN RELIABILITY [39]

	HARDWARE RELIABILITY	HUMAN RELIABILITY	HUMAN RELIABILITY
Function	Hardware Reliability	Discrete Task	Continuous Task
System Definition	A set of components which perform their intended functions.	A task which consists of several human behavioral units.	Continuous control task such as vigilance, tracking, and stabilizing
System Configuration	Functional relationships of components	Relationships of behavior units for a given task (task taxonomy)	Not necessary to define functional relationships between task units.
System failure analysis	Fault-tree analysis	Human error categorization; derivation of mutually exclusive and exhaustive set of human errors for a given task.	Binary error logic for continuous system response.
Nature of failure	<ul style="list-style-type: none"> - Mostly binary failure logic - Multi-dimensionality of failure - Common-cause failure 	<ul style="list-style-type: none"> - Sometimes hard to apply binary error logic to human action - Multi-dimensionality of error - Common cause error - Error correction 	Same as discrete task
Cause of failure	Most hardware failures are explained by the laws of physics and chemistry.	No well-codified laws which are generally accepted as explanations of human errors.	Same as discrete task
System reliability evaluation	<ul style="list-style-type: none"> - With probabilistic treatments of failure logic and statistical independence assumption between components, mathematical models are derived. - In cases of network reliability and phased mission reliability, which require statistical dependency between components, it is hard to evaluate exact system reliability. 	Very difficult because of problems in depicting the functional relationships between human behavioral units.	With probabilistic treatments of binary error logic for system response stochastic models are derived.
Data	The data for most types of machines is relatively large and robust compared to human reliability.	<ul style="list-style-type: none"> - No trustworthy and useful data base exists for human behavior units. - Largely depends on the judgment of experts. 	Same as discrete task.

A brief survey of current industrial practices was conducted by LaSala [42]. In the survey, aerospace industries were queried with regard to the techniques used in human reliability prediction, design approaches, design validation approaches, allocation approaches, and needed tools. The survey revealed that the greatest need was for front-end tools.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

The facts that up to 70% of operational failures, Reference [43], and 40% of in-plant rework are due to human error demand aggressive consideration of operator and maintainer reliability for operational systems and aggressive consideration of assembler and maintenance technician reliability in in-plant operations.

7.7.2 Reliability, Maintainability, and Availability Parameters for Human - Machine Systems

A careful analysis of human-machine systems recognizes that both humans and machine elements can fail, and that human errors can have varying effects on a system. In some cases, human errors result from an individual's action during operation, while others are a consequence of system design or manner of use. Some human errors cause system failure or increase the risk of such failure while others merely create delays in reaching objectives. Thus, as with other system elements, the human elements exert a strong influence on the design and ultimate reliability of all human-machine systems.

The human interacts in a complicated manner with the non-human portions of the system. A tendency that must be resisted is to segregate human and machine functions. Watson and Hebenstreit [44] effectively characterized the interplay of human and machine in complex systems, as shown in Figure 7.7-1. In reality, effective system design recognizes that the "human-in-the-loop" cannot be segregated from other system functions.

Human errors take many forms and are due to many causes. There are types of human errors that are not caused specifically by design, although good design practices can reduce the occurrence of these errors. These are Reference [45]:

- (1) Slips - attentional failures
 - (a) Intrusion
 - (b) Omission
 - (c) Reversal
 - (d) Misordering
 - (e) Mistiming
- (2) Lapses - memory failures
 - (a) Omission of planned items
 - (b) Place-losing
 - (c) Forgetting intentions

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

- (3) Mistakes - rule- and knowledge-based
 - (a) Misapplication of good rules
 - (b) Application of bad rules
 - (c) Many types of knowledge-based mistake

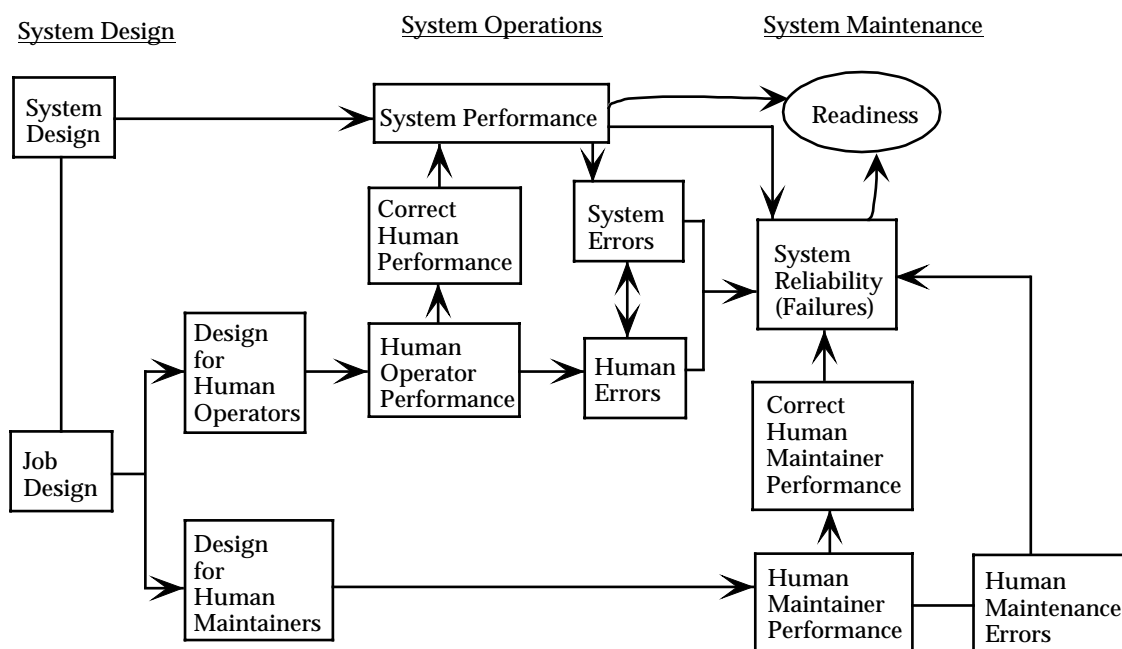
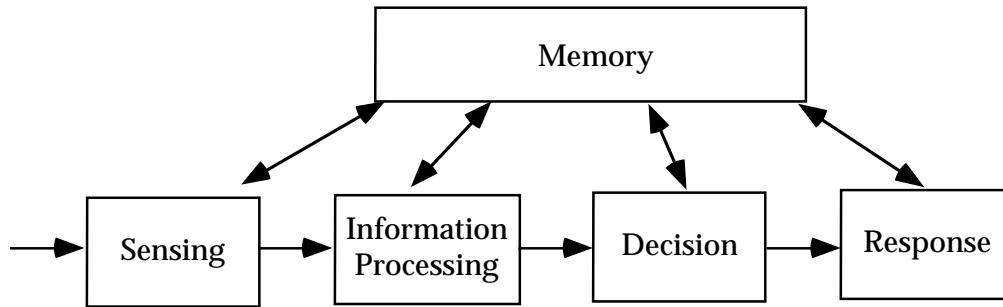


FIGURE 7.7-1: THE HUMAN IN SYSTEM RELIABILITY AND MAINTAINABILITY [44]

Closely related to the selection of reliability, maintainability, and availability models for human-machine systems is the subject of models of human performance. Although many models exist, for reliability purposes, the one that is most easily used is the “cognitive model” shown in Figure 7.7-2. The cognitive model considers a human function as four basic subfunctions, assisted by memory.

The reliability of the human function is affected by several types of factors as shown in Figure 7.7-3.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES



Examples: Radar operator, electric power monitor

FIGURE 7.7-2: THE COGNITIVE HUMAN MODEL

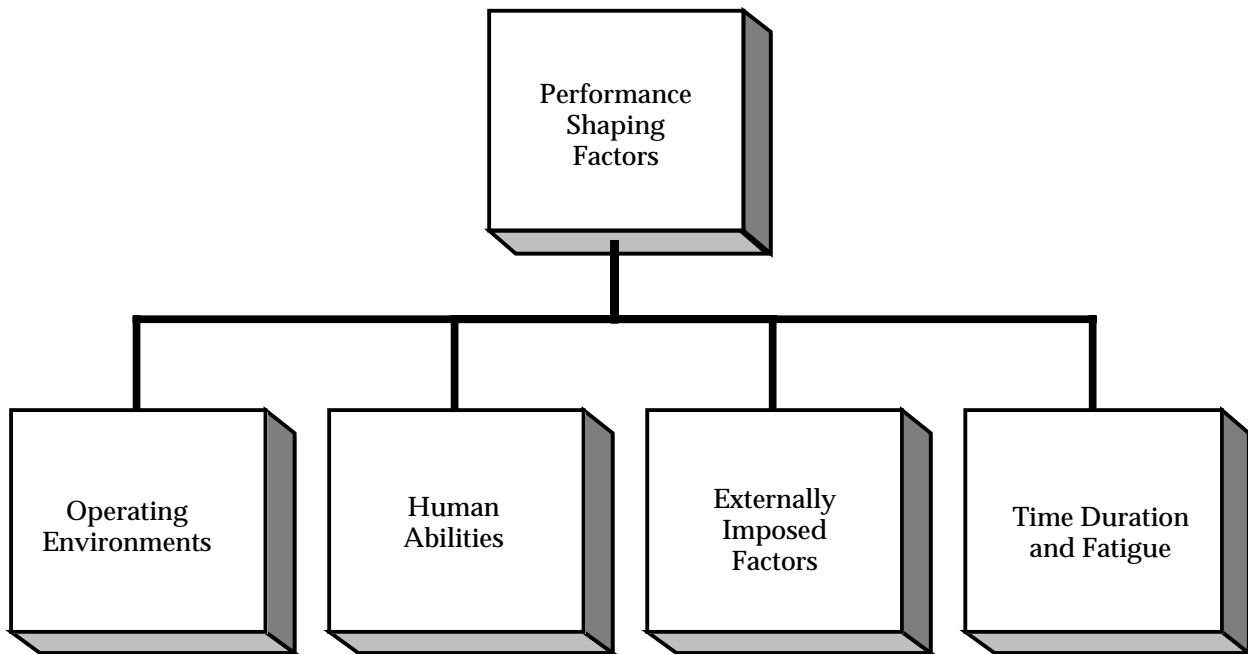


FIGURE 7.7-3: FACTORS THAT AFFECT HUMAN FUNCTION RELIABILITY

Of the factors shown in Figure 7.7-3, operating environments are, perhaps the easiest to understand. Some of the more commonly known environmental factors or combinations of factors are:

- (1) Temperature-humidity
- (2) Pressure-oxygen concentration
- (3) Longitudinal and transverse vibration
- (4) Ambient noise

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

For each of these, there is a region where human performance is not degraded, a region where human performance ceases, and a region of transition between the previous two (see Figure 7.7-4). Sources such as MIL-STD-1472E, "Human Engineering Design Criteria for Military Systems, Equipment, and Facilities" provide this information. Although specific reliability data have not been published for these regions, inferences can be made regarding the impact on the human performance reliability. In the case of ambient noise, message complexity, vocabulary content, distance between speaker and listener, and background noise levels and frequencies affect human performance reliability.

Human abilities pertain to the ability of the human to detect input signals, analyze their meaning, make decisions, and then perform the proper response. Typically, inputs consist of visual, sound, or touch-related signals. There are minimum levels for the detectability of each and levels at which damage is done to the human. There also are transition zones from the threshold of detection to physical damage.

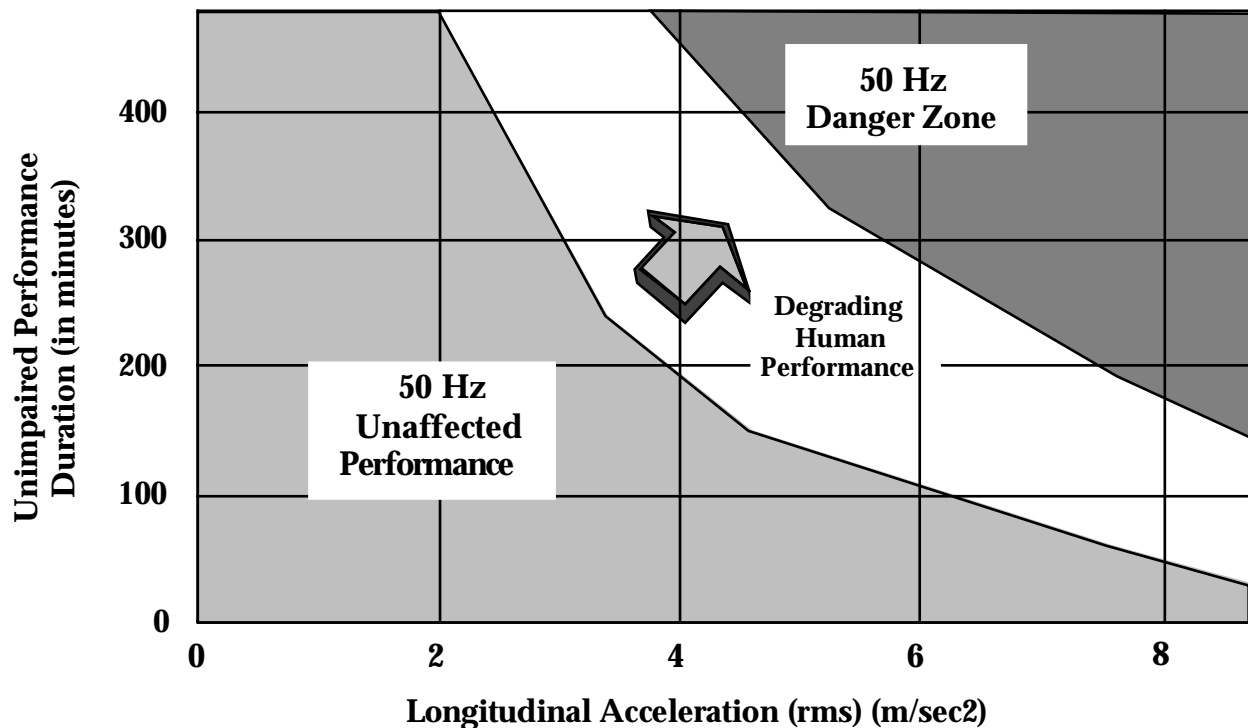


FIGURE 7.7-4: ZONES OF HUMAN PERFORMANCE FOR LONGITUDINAL VIBRATION (ADAPTED FROM MIL-STD-1472)

Externally imposed factors consist of workplace layout, assignments, group interactions and similar factors. Specific, reliability oriented data for these have not been tabulated, although studies have suggested changes in performance due to these factors.

Time duration and fatigue are important factors that frequently are neglected. For most tasks, performing 30 minutes without a break is the recommended limit because longer durations result

 SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

in degradation of human performance. Also, there must be a balance between the allowed time to perform a task and the actual time to perform the task, otherwise human errors will occur.

Much of the system development process depends on quantitative measures. Consequently, for human-machine systems, it is necessary to define a set of parameters that includes the human as well as the hardware. Fortunately, it is possible to construct a set of analogues to conventional reliability, maintainability, and availability measures [46]. Two examples follow.

$$\text{Human Performance Reliability} = \frac{\text{No. Human Task Success}}{\text{No. Human Task Attempt}}$$

$$\text{Human Availability} = 1 - \frac{\text{Unmanned Station Hours}}{\text{Total Hours}}$$

These parameters can be used in simulations and can be used in probability compounding models as well. Like all reliability and maintainability parameters, they should not be construed as ends in themselves but rather vehicles for obtaining good system designs.

7.7.3 Allocating System Reliability to Human Elements

The allocation of reliability and maintainability requirements is the first step in the man-machine system development process beyond the receipt of the customer requirements. This section discusses qualitative allocation and two forms of quantitative allocation: an application of the AGREE method and dynamic programming. Qualitative allocation pertains to the earliest stages of system functional analysis and the evaluation of potential design solutions. Although, in practice, quantitative allocation rarely is performed, the consequence of not performing a quantitative allocation is the inadequate design of human tasks and an increase in the likelihood of human error - in some cases to very significant and dangerous levels.

7.7.3.1 Qualitative Allocation

One of the early stages of system engineering is the identification and non-quantitative allocation of system functions. This step commonly is known as "functional analysis." "Functions" are discrete actions for the attainment of specific objectives. Generally, the products of functional analysis are functional flow diagrams that are structured in a hierarchical manner [47]. A simple example is shown in Figure 7.7-5.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

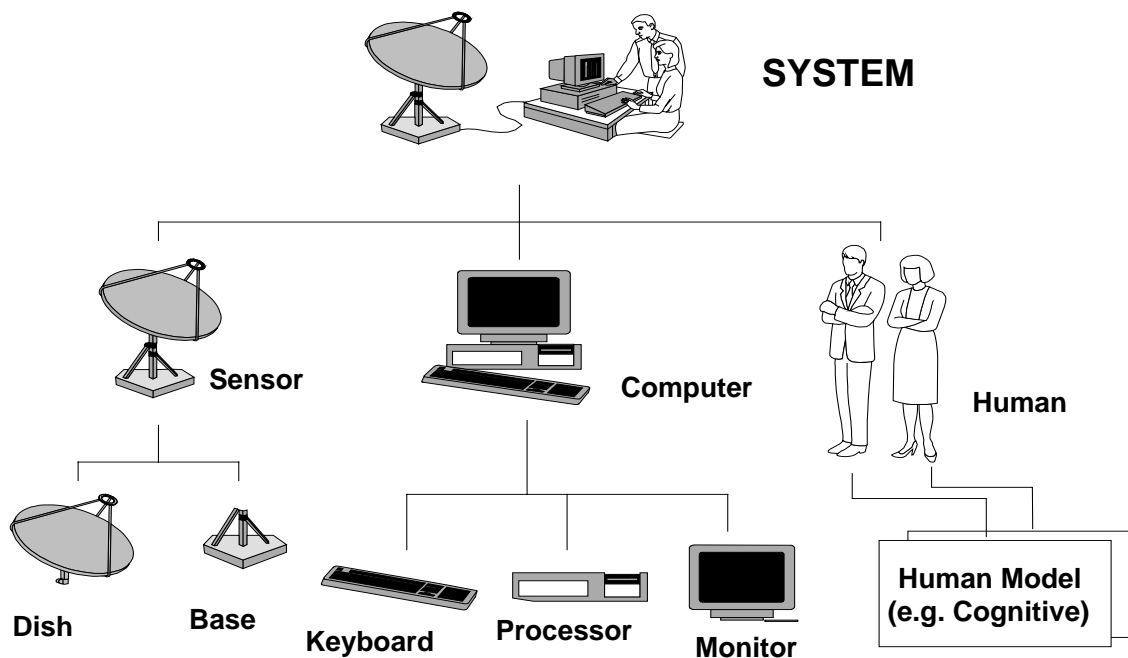


FIGURE 7.7-5: HIERARCHICAL STRUCTURE OF FUNCTIONAL ANALYSIS (EXAMPLE)

At an appropriate level in the functional analysis, it must be decided whether a function will be performed by human or machine. This can be a relatively high level, e.g. first tier, or at a detailed level such as the third or lower tier. For man-machine systems, the functional analysis can include operation and maintenance functions presented as separate flows or as a combined flow. Examples are given in reference [47].

Qualitative allocation is simply the selection of which functions are best performed by the human and which are best performed by the machine. Table 7.7-2 identifies the functions at which humans and machines excel. In general, the human is better at handling a variety of different information-processing tasks, adapting to new tasks and environments, devising new procedures, and resolving unexpected contingencies. The greatest limitations of the human are the rate of data processing and the amount of immediate retention.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.7-2: HUMAN-MACHINE COMPARATIVE CAPABILITIES

HUMAN SUPERIORITY	MACHINE SUPERIORITY
1. Originality (ability to arrive at new, different problem solutions)	1. Precise, repetitive operations
2. Reprogramming rapidly (as in acquiring new procedures)	2. Reacting with minimum lag (in microseconds, not milliseconds)
3. Recognizing certain types of impending failures quickly (by sensing changes in mechanical and acoustic vibrations)	3. Storing and recalling large amounts of data
4. Detecting signals (as radar scope returns) in high-noise environments	4. Being sensitive to stimuli (machines sense energy in bands beyond human's sensitivity spectrum)
5. Performing and operating though task-overloaded	5. Monitoring functions (even under stress conditions)
6. Providing a logical description of events (to amplify, clarify, negate other data)	6. Exerting large amounts of force
7. Reasoning inductively (in diagnosing a general condition from specific symptoms)	7. Reasoning deductively (in identifying a specific item as belonging to a larger class)
8. Handling unexpected occurrences (as in evaluating alternate risks and selecting the optimal alternate or corrective action)	—
9. Utilizing equipment beyond its limits as necessary (i.e. advantageously using equipment factors for safety)	—

From *An Introduction to the Assurance of Human Performance in Space Systems*, SP-6506, NASA, 1968.

7.7.3.2 Quantitative Allocation

The first of the quantitative methods, and the simplest, for allocating man-machine reliability is an adaptation of the AGREE allocation method. This method, described in Reference [48], was developed for electronic equipments and was based on unit complexity and importance.

Unit complexity is described in terms of modules, where a module is a single functional unit. Unit importance is defined as the probability that the system will fall if the unit fails. A importance value of one implies that the unit is essential for successful system operation. A value of zero means that the unit has no impact on system performance.

The AGREE allocation is expressed in terms of allocated reliability $R(t_j)$.

$$R(t_j) = 1 - \frac{1 - [R^*(T)]^{n_j / N}}{E_j}$$

where:

- $R^*(T)$ = system reliability requirement
- n_j = number of modules in unit j ,
- E_j = importance factor of unit j ,
- t_j = number of hours unit j will be required to operate in T system hours

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

N = total number of modules in the system.

Although the AGREE report discusses the allocation for redundant situations, the quality of the approximations for those cases is inadequate. Hence, serial system configurations should be considered the primary application of the AGREE allocation method.

To apply the AGREE method to man-machine systems, the system must be broken down into discrete functions and be depicted in a serial reliability block manner. The first order assignment of functions to man or machine can be made using the qualitative approach described in Section 7.7.3.1. In a similar manner to the machine portions, the human functions must be decomposed into discrete elements, e.g. the portions of the cognitive model. These elements determine function complexity. Function operating hours and importance then are determined. An example of a non-unity importance factor that is applicable to a man or a machine in a target (or malfunction) detection function might be that if the man or machine fails to perform properly, 25% of the targets (or malfunctions) may be lost. Hence E_j would be 0.25. The allocation formulas are used to determine the allocated failure rate or reliability as required.

In most practical situations, the problem is to design a man-machine system with the highest achievable reliability subject to practical considerations such as competing mission requirements, limitations on personnel, and limitations on cost. In an analytic sense, the problem is represented as a function (reliability) to be maximized subject to a set of constraints. Allocations with assigned constraints generally are solvable by means of dynamic programming because they become very complicated very quickly.

Dynamic programming is a mathematical technique for optimizing a sequence of decisions by breaking the sequence into a sequence of simpler problems. For each simpler problem, or stage, an optimal feasible solution is determined. The selected set of solutions is the optimal solution for the entire problem. It is used frequently in capital allocation and transportation problems. Blanchard and Fabricky [49] and Taha [50] have excellent treatments of the subject.

Mission reliability and operational readiness are common parameters for optimization. Other parameters could be used. For example, availability may be used in place of operational readiness depending on the planned use of the system. Bazovski [51] provided an excellent discussion for distinguishing between readiness and availability. The parameters provide a direct link between high level effectiveness requirements and component oriented design parameters such as MTBF, MTTR, and both numbers and skill levels of personnel.

To apply mission reliability and operational readiness to the allocation process, first identify critical functions and their reliability and maintainability design parameters and use the parameters to write expressions for the mission reliability and operational readiness of the man-machine system. One mission reliability constraint and one operational readiness equation must be written for each mission.

 SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Cost and personnel constraints must also be constructed. Personnel can be specified in many ways. The most convenient way is to specify numbers of men at a discrete skill level. Acquisition cost, support cost and life cycle cost can all be used as constraints. Regardless of the type of cost selected, the system cost must be defined in terms of human and hardware contributions and in terms of basic design parameters.

Example

A multi-mission equipment in which each mission, i , has a probability p_i of being required. The reliability function associated with each mission is r_i . The r functions are constructed to include the human element. For example, an operational sequence diagram, which is roughly equivalent to a reliability block diagram, can be merged with a functional reliability block diagram to provide a mission reliability function. Human functions are constructed in terms of reliability and maintainability parameters.

With the above preparation, the allocation problem can be written as the following optimization problem:

Maximize R_{op} (operational reliability):

$$R_{op} = \sum_{i=1}^n p_i r_i$$

subject to:

$$R_m \geq P_m$$

$$P_m \geq X_m$$

$$N \leq v$$

$$C \leq c$$

where:

R_m	=	mission reliability
P	=	availability
N	=	number of personnel
C	=	cost
m	=	a specific mission

There will be one set of constraint equations for each mission. This leads to exactly the form of optimization problem that is solved by dynamic programming. A simplified flow of dynamic programming is shown in Figure 7.7-6.

7.7.4 Sources of Human Performance Reliability Data

One of the major issues in man-machine reliability is the location and availability of human performance reliability data. The tabulated data take the form of time measurements, including

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

reaction time and task performance time, error and error frequency data. The most commonly used data are error data. Task performance data play an important role where task performance within a specified time is a criterion for mission success: e.g., restoration of full power within 30 minutes. Most of the data come from controlled laboratory studies; an increasing amount come from simulators; very little come from field use. The laboratory data have the liability of being derived from artificial situations that do not represent the real world. Consequently, although they have the requisite degree of precision, they have limited utility. Simulator data are better because they represent the real world more accurately, especially as simulators improve. However, they are collected generally for special applications and, hence, have limited application. Laboratory and simulator data vary from what would be expected in the real world because of the subjects' awareness that they are being tested. The most realistic data, field data, generally are not collected in a systematic way. Consequently, the physical and psychological environment in which the data were generated usually are not recorded or analyzed.

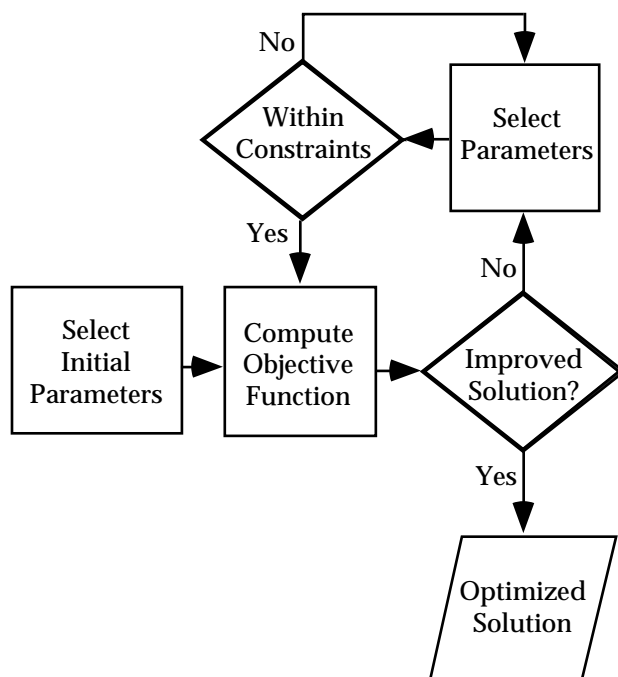


FIGURE 7.7-6: SIMPLIFIED DYNAMIC PROGRAMMING

An alternative to the use of "hard data" is the use of expert opinion. Techniques such as Delphi methods or paired comparison are used. The primary use of expert opinion occurs when hard data are modified special situations.

Early data sources consisted primarily of human factors data collections; e.g. Human Engineering Guide to Equipment Design [52], MIL-STD-1472E, "Human Engineering Design Criteria for Military System, Equipment, and Facilities." More recent data sources are the following: "Handbook Of Perception and Human Performance" [53], "Engineering Data Compendium:

 SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Human Perception and Performance” [54], the Compendium on a compact disc, and the Crew System Ergonomics Information Analysis Center.

The second vehicle for obtaining human performance reliability data is the "data bank." Table 7.7-3 shows the current major data banks [55]. Table 7.7-4 summarizes the data incorporated into each of the data banks.

Other sources of human performance reliability are described by references [56] and [57]. More detailed descriptions of many of the data sources and data banks described herein are given by Booher [55].

TABLE 7.7-3: DATA BANKS AND THEIR AFFILIATIONS [55]

	DATA BANK	ORGANIZATION
MICRO	Human Performance Evaluation System (HPES)	Nuclear Power
	Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR)	Nuclear Power
	Crew Station Ergonomics Information Analysis Center (CSERIAC)	Department of Defense
MACRO	Training and Performance Data Center (TPDC)	Department of Defense
	Materiel Readiness Support Activity (MRSA) MANPRINT Data Base	Department of the Army
	Project "A" Data Base	Department of the Army

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.7-4: DATA CATEGORIES OF NATIONAL DATA BANKS [55]

Data Categories	HPES	NUCLARR	CSERIAC	TPDC	MRSA MANPRINT	PROJECT "A"
Human Performance	X	X	X	X		X
Human Performance (Error)	X	X	X			
Hardware Reliability		X			X	
Human Factors Engineering			X			
Manpower			X	X	X	
Personnel			X	X	X	X
Training				X	X	X
System Safety			X		X	
Health Hazards			X		X	

There is a recognized need for a human performance data bank that applies to both the military and commercial sectors. Until a broadly supported effort such as this is implemented, there will be both considerable subjectivity and many limitations in the use of available human performance reliability data.

7.7.5 Tools for Designing Man-Machine Systems

This section explores the various tools that are used to design reliable man-machine systems. The tools are many and varied in their approaches. An overview of them is provided by Figure 7.7-7.

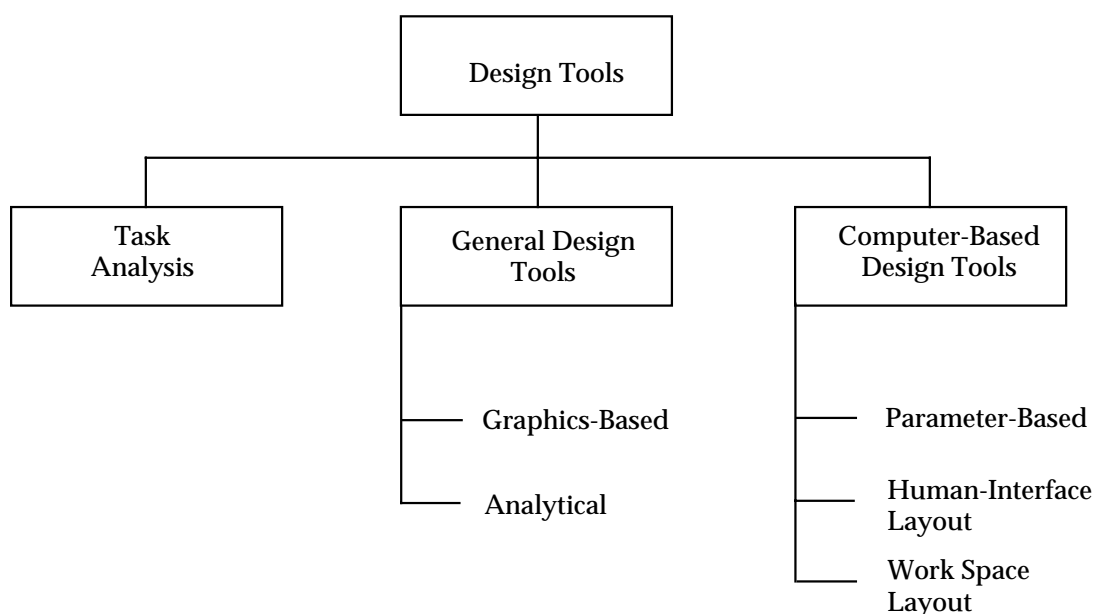


FIGURE 7.7-7: TOOLS FOR DESIGNING HUMAN-MACHINE SYSTEMS

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.7.5.1 Task Analysis

Task analysis is a critical part of a human factors program. However, it is usually not done as part of reliability program. Maintenance task analysis is usually done in a maintainability program. Task analysis focuses on the following:

- (1) Input information to human
- (2) Evaluation processes
- (3) Action to be taken
- (4) Environments and constraints
- (5) Tools and job aids
- (6) Manpower
- (7) Communications

7.7.5.2 General Design Tools

There are many general design tools that apply to the design of human-machine interfaces. One of the most useful is the Operational Sequence Diagram (OSD). The features of the OSD are:

- (1) Shows all participants
- (2) Displays functional flow - all functions
- (3) Represents types of operations with standard symbols
- (4) Represents approximate time line
- (5) Employs rules for representing flows
- (6) Represents a certain level of system or process indenture

Goal, success, and fault trees are other useful tools. The general format of these is shown in Figure 7.7-8. Operator action trees and event trees are horizontally-oriented trees that show possible branches in action and the consequences. The Failure Mode, Effects, and Criticality Analysis can be adapted for use in the analysis of human-machine reliability by incorporating human error modes and evaluating their consequences.

The treatment of the role of traditional human factors is brief. The brevity should not be construed as a reflection of the importance of the subject. Many excellent volumes, some of which are referenced, have been written on the subject and any attempt to replicate even portions of them here would serve little purpose. Human factors provides many of the basic design disciplines that enable reliable systems to be designed. Too often, this fact is not appreciated and the human factors experts are given a secondary priority in system development (unless safety is a critical factor). Human factors experts need to be involved in the earliest stages of system development, especially in the function allocations. The role of human factors in the achievement of system reliability often is clouded by the lack of sensitivity to the human by reliability engineers. The key to understanding that role is the recognition that functionally, human behavior can be modeled as stimulus-input chain: internal-response: output- response. Complex behavior is a combination of many of these chains. Human errors occur when:

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

- (1) A physical change in the environment is not perceived as a stimulus.
- (2) Several stimuli cannot be discriminated by an operator.
- (3) A stimulus is perceived, but its meaning is not understood.
- (4) The stimulus is correctly understood, but the correct output-response is unknown.
- (5) The correct output-response is known, but it is beyond the operator's physical capabilities.
- (6) The correct output-response is within the operator's capabilities, but the response is performed incorrectly or out of sequence.

The implications for equipment design are: in order for an operator to respond adequately, the stimulus must be perceivable and it must demand a response which the operator is capable of producing. Hence equipment and task characteristics must be tailored to the capabilities and limitations of the operator. To accomplish this, the design of equipment must take into account limitations on body size, body weight, and reaction times to environmental stimuli. The operator must receive some verification or feedback from his actions.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

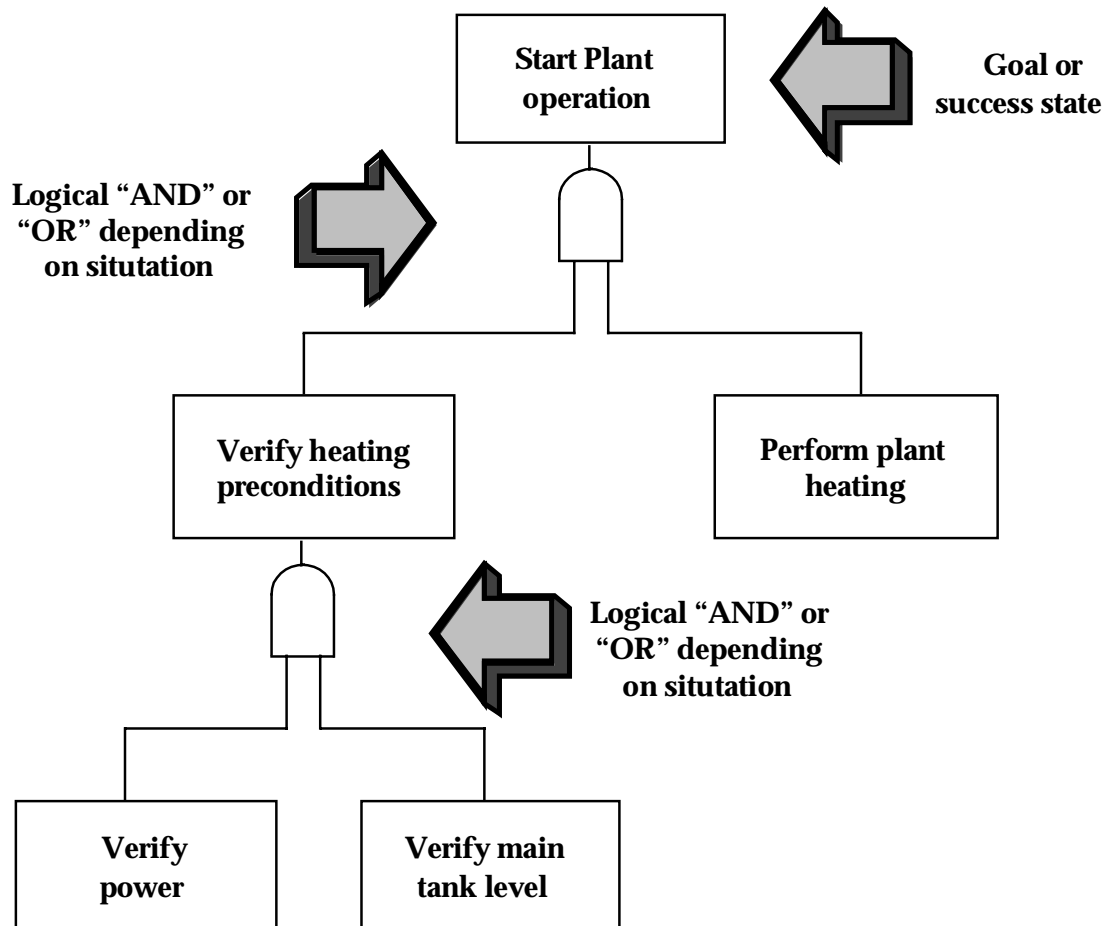


FIGURE 7.7-8: GOAL-SUCCESS TREE

7.7.5.3 Computer-Based Design Tools

There are many computer-based design tools and more are emerging rapidly. Some of the available ones are summarized in the following paragraphs. Almost all of the ones described here are proprietary. They are described here without either endorsement or criticism.

The computer-based design tools fall into three basic groups: parametric, interface design, and work space design. Some of the tools are:

- (1) Parametric design
 - (a) REHMS-D™
 - (b) GOMS
- (2) Interface design - VAPS™
 - (a) VAPS™

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

- (b) Computer Interface Toolkits (e.g. Visual Basic™)
- (3) Work space design
 - (a) SAMMIE™
 - (b) CREW CHIEF
 - (c) JACK™
 - (d) SAFEWORK™

7.7.5.3.1 Parametric Design Tools

REHMS-D uses reliability as a metric for selection of human interface and task parameters. It includes two levels of parameter sensitivity analysis, provides on-line help and safety warnings, and derives plans for testing human interfaces. REHMS-D is based on the cognitive model and offers options for configuring inputs to the human and responses by the human. It addresses the effects of the following environmental factors: illumination, atmospheric conditions, temperature-humidity, pressure-oxygen, ambient noise, and vibration. GOMS develops four aspects of human tasks: goals, operators, methods, and selection. The "goals" are a user defined set of things to do or obtain to achieve a task. The "operators" are the actions available to achieve the goals. The methods are the sequence of operations and subgoals for achieving the task - the "how to." Finally, the "selection" is a means for choosing a method when more than one method applies - usually rule-based. GOMS uses time-to-perform for its metric.

7.7.5.3.2 Interface Design Tools

VAPS is a work station-based tools that draws objects, specifies data-driven animation, connects objects to application data and specifies response behavior, and communicates with external sources to interact.

7.7.5.3.3 Work Space Design Tools

CREW CHIEF is a 3-dimensional modeling system developed by the US Air Force Human Resources Laboratory, Wright-Patterson AFB, OH. It is oriented toward the computer graphic simulation of an aircraft maintenance technician and interfaces readily with existing commercial CAD systems. CREW CHIEF reduces the incidence of design problems by allowing the designer to perform maintainability analyses and correct design defects while the system is in the early design stage. It does this by providing a 3-dimensional modeling system that creates a computerized man-model.

SAMMIE (System for Aiding Man/Machine Interaction Evaluation) is a human factors, 3-D design system that includes a sophisticated, computerized man-model with built-in reach and sight capabilities. The man-model is constructed from logically related links or joint. Virtually any size or shape person can be represented through specific dimensional changes or statistical profiles of population groups.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

SAFEWORK creates virtual humans of various percentiles. It contains access to population statistics. SAFEWORK mannequin movement includes fully articulated hand and spine models, virtual viewing, collision detection, and scene animation.

JACK includes 3D interactive environment for controlling articulated figures, a detailed human model, realistic behavior controls, anthropomorphic scaling, task animation and evaluation, view analysis, automatic reach and grasp, and collision detection and avoidance.

Design Evaluation for Personnel, Training, and Human Factors (DEPTH) analyzes maintenance activity using Transom Technologies Transom Jack™ human models; controls human model movements through standard mouse, body tracking equipment, or automatic simulation; handles a variety of populations, dress modes, and tools; and reports on accessibility, visibility, and strength.

7.7.6 Reliability Prediction for Human-Machine Systems

A great majority of the work published on human reliability has been concerned with human performance reliability prediction. Earlier work focused on probability compounding techniques. Some of these were linked with available data sources (never in really great abundance); other compounding techniques used specially collected data. With the proliferation of computers, digital simulation models were developed and used. More recently, stochastic models have been proposed. An excellent comparison of prediction techniques is given in reference [58]. Figure 7.7-9 shows the categories of the many human performance reliability prediction techniques that have been published.

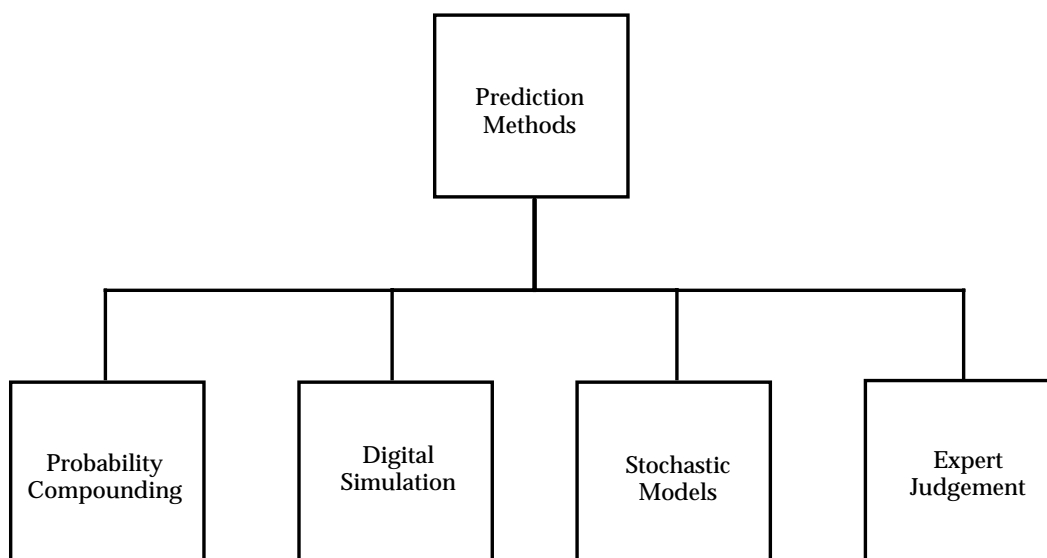


FIGURE 7.7-9: CATEGORIES OF HUMAN PERFORMANCE RELIABILITY PREDICTION METHODS

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Although there are a great many models for prediction - over 20 years worth of work - there is no consensus on human reliability prediction technology or a human reliability parameter database [59]. Dougherty [60] noted much the same situation. His expectation is that there will be a recognition that there is a need for a second generation of human reliability models.

Swain [61] notes the following inadequacies in human reliability analysis:

- (1) Inadequate data
- (2) Stop-gap models and expert judgment are used in place of "hard" data
- (3) Lack of agreement on expert judgment methods
- (4) Inadequate calibration of simulator data
- (5) Inadequate proof of accuracy in human reliability analyses

Increased use of higher mental functions is required by inadequate design of displays, controls, and their interactions.

The emphasis here is on the lack of data to support the human reliability analysis rather than the methodology itself. Swain does identify inadequate implementation of human factors disciplines as a root cause of the lack of data on favorable human performance situations.

7.7.6.1 Probability Compounding

There are a considerable number of probability compounding models for estimating human performance reliability in man-machine systems. Meister [40] provides excellent summaries of them. Selected techniques are summarized below.

Technique for Human Error Rate Prediction (THERP) [62], [63] has been the best known and most frequently applied technique for human reliability prediction. It is a method for predicting human error rates and for evaluating the degradation to a man-machine system likely to be caused by human errors in association with factors such as equipment reliability, procedures, and other factors. The THERP technique has been influenced strongly by hardware reliability techniques.

THERP involves five steps:

- (1) Define the system or subsystem failure which is to be evaluated. This involves describing the system goals and functions and the consequences of not achieving them. It also requires identifying mission, personnel, and hardware/software characteristics.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

- (2) Identify and list all the human operations performed and their relationships to the system tasks and functions. This requires an analysis of all operator and maintainer tasks.
- (3) Predict error rates for each human operation or group of operations. Errors likely to be made in each task or subtask must be identified. Errors that are not important in terms of system operation are ignored. This step includes estimating the likelihood of each error occurring and the likelihood of an error not being detected.
- (4) Determine the effect of human errors on the system, including the consequences of the error not being detected. This requires the development of event trees. The left limbs of the event trees are success paths; the right limbs are failure paths. Probabilities are assigned to each path. The tree reflects the effects of task dependence. The relative effects of performance-shaping factors, e.g. stress and experience, are estimated.
- (5) Recommend changes as necessary to reduce the system or subsystem failure rate as a consequence of the estimated effects of the recommended changes. The recommendations can be developed through the use of sensitivity analyses, in which factors and values are varied and effects monitored. THERP makes no assumptions about the dependence or independence of personnel behaviors. The data are taken from available sources.

One of the key aspects of THERP is the determination of the probability that an error or class of errors will result in a system failure. This probability is assigned a value F_i . Branching trees are constructed to determine the paths to system success and failure (Figure 7.7-10). The probability that an error will occur is given by P_i . $F_i P_i$ is the joint probability that an error will occur and that the error will lead to system failure. $1 - F_i P_i$ is the probability that an operation will be performed which does not lead to system failure. The probability that a class of errors will lead to system failure is given by:

$$Q_i = (1 - F_i P_i)^{n_i}$$

where n_i is the number of independent operations. The total system or subsystem failure rate is given by:

$$Q_T = 1 - \left[\prod_{k=1}^n (1 - Q_k) \right]$$

where Q_T is the probability that one or more failure conditions will result from errors in at least one of the n failure classes.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

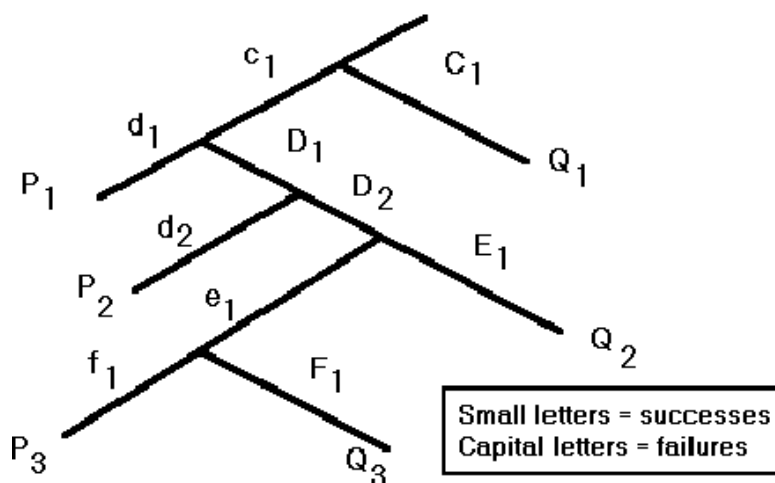


FIGURE 7.7-10: THERP PROBABILITY TREE [62]

THERP can be used for design analysis, manpower selection, prediction of system effectiveness, and determination of training requirements. For design analysis, it allows the comparison of alternative system configurations in terms of effect on operator capability. It also allows comparative analysis of initial system configuration options and reconfiguration if deficiencies are identified. For manpower selection, THERP allows the determination of the types, numbers, and skill levels of the personnel required to operate the system. For system effectiveness, THERP allows an assessment of whether quantitative requirements will be met. The determination of training requirements is more implicit than explicit. Unacceptable task performance error rates suggest the need for training to improve proficiency. Hence, THERP can suggest the need for training rather than specific training topics.

THERP can be applied to all types of equipments, tasks, and behaviors. With the aid of standard human engineering techniques, it can be used for design analysis. Finally, THERP can be applied to the early stages of system design as well as the later stages.

Constraints on its application are that it is applicable to situations where discrete task descriptions can be developed, error probability data must be available, the effects of performance-shaping factors must be known, and that time must be available to analyze and categorize all potential errors in a task. THERP is regarded as the standard tool for estimating human error probabilities in routine tasks. It uses performance shaping factors (PSFs) to make judgments about particular situations. However, experience has shown that in some cases, it was difficult to accommodate all of the PSFs that were considered important [64]. In many cases, THERP gave lower error probabilities than other methods. One evaluation of THERP [65] notes that THERP has the advantage of simplicity but does not account for the influence of time. Fragola [38] describes extensions to THERP, particularly with respect to nuclear power applications. Another evaluation [66] notes that when applied to severe accident applications, several problems were noted. In this case, the task information provided in NRC data forms typically is more detailed than required by THERP. Matching the NRC task data to THERP

 SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

operator actions was found to be subjective and a source of error. Also the THERP error data received criticism with respect to its being an adaptation of non-nuclear data to nuclear applications. Krois et. al. note that other data bases are available to be used in THERP and obviate this last criticism.

Dougherty and Fragola [38] have introduced the time-reliability correlation (TRC) system. This approach uses simulator training results to create a family of time-reliability correlations, which are adjusted with either the Success Likelihood Index or other expert judgment methods to account for special conditions. TRC is the relationship between human performance reliability and time. Data from simulators suggest that the lognormal distribution is sufficient for modeling TRCs. Interpolation between the s-confidence bounds can be accomplished through the use of a Success Likelihood Index (SLI). The SLI is derived in the following manner:

- (1) Choose the influences appropriate to the event and the situation.
- (2) Rank the influences as multiples of the least important for a given situation, which is set at "10."
- (3) Sum the rankings of all influences and normalize the rankings to this sum.
- (4) Assess the impact of each influence from best (1) to worst (10).
- (5) Compute the "dot product" of the ranking and the quality vectors. This is the SLI.
- (6) Apply the SLI. Mathematically, the SLI is expressed by:

$$SLI = \sum_1^N \left(\frac{I_i}{R} \right) q_i$$

where:

$$R = \sum_1^N r_i$$

and r_i is the rank of the influence i and q_i is the quality of the influence i .

Dougherty and Fragola focus on a lognormal TRC based on simulator data. This is in consonance with the modified Human Cognitive Reliability.

Human Cognitive Reliability (HCR) was developed by Hannaman et al. [67] for calculating the operator probability of non-response to a cognitive processing task as a function of time. The type of cognitive processing may be rule based, skill based, or knowledge based. For task j , the probability of non-response $P(t)$ is given by:

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

$$P(t) = \exp-(X_j)^{b_j}$$

where:

$$X_j = \frac{(t/T_{med}) - C_{gj}}{C_{nj}}$$

- and T_{med} = median time to perform the task corrected by a shaping factor K_j
- b_j = shape parameter
- C_{gj} = time delay factor as a fraction of T_{med} for type j cognitive processing
- C_{nj} = scale parameter as a fraction of T_{med} for type j cognitive processing

The dependency between tasks was not considered. The model was derived from a three parameter Weibull distribution. The model was used to develop normalized curves corresponding to rule based, skill based, and knowledge based cognitive processing. In applying the HCR approach to operator task analysis, a table records the following for each subtask:

- (1) Dominant human behavior
- (2) Stress level
- (3) Operator experience
- (4) Quality of operator/system interface
- (5) Median time assumed

The HCR approach has been modified [68] to use the log-normal distribution instead of the Weibull. The modified approach has the acronym HCR/ORE and is supported by simulator data. Guassardo [65] notes that the HCR must be used carefully because variations in applications can lead to very different results. The model does allow some accounting for time effects on error probability but is complicated by the fact that the correlation only can be used once when subtasks have the same influence parameters. In this case, there is an ambiguity regarding whether or not to cluster subtasks or to convolve individual subtask correlations. When examining consistency among teams using HCR, Poucet [64] noted that the results have greater variability than THERP methods. The method was very sensitive to assumptions about median time and the behavior type of the action. Very good median response time data must be available in order to apply HCR. Poucet also notes that some of the teams in his comparative study combined the use of THERP and HCR. THERP was used for manual or routine tasks; HCR was used for cognitive tasks.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.7.6.2 Stochastic Models

This approach to modeling the impact of the human in man-machine systems employs Markov models to analyze parallel, k-of-n, and standby redundant configurations with human errors and common failures. The human error is defined as a failure to perform a prescribed task (or the performance of a prohibited action), which could result in damage to equipment and property or disruption of scheduled operations. The errors are categorized as being "critical" or "non-critical." A critical error causes system failure. Common cause failures are cases where multiple units fail due to a single cause.

Five models are described by Dhillon [69] [70]. Each addresses a different redundant configuration. The models assume that:

- (1) Units fail independently
- (2) Failure rates for hardware, human error, and common cause failures are constant
- (3) Repair rates are constant
- (4) A repaired system is as good as new
- (5) Switchover mechanisms are perfect for standby configurations
- (6) System units are statistically identical

The first model represents a two independent and identical unit parallel system, which can fail because of human error or hardware failure. A Markov model is constructed and an expression for system availability A and mean-time-to-repair (MTTR) is obtained. An expression for mean-time-to-failure (MTTF) also is derived. All the expressions are complicated functions of the state transition probabilities (failure rates, error rates, and repair rates).

The second model is a special case of the first when the non-critical human error rate is zero. The non-critical human errors are omitted from the system transition diagram, which becomes much simplified. Expressions are derived for A , MTTR, MTTF, and variance of time to failure (TTF).

The third model represents a 2-out-of-3 unit system with critical human errors and common cause failures. All system units are identical. A system reliability function and an expression for MTTF are derived. It is noted that repair helps to increase MTTF and human errors decrease it, as expected.

The fourth model is a 3-out-of-four system with critical human errors and common cause failures. MTTF and TTF variance expressions are derived.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

The fifth model represents a standby system with critical human errors and common cause failures. Again, MTTF and TTF variance are calculated.

7.7.6.3 Digital Simulation

Digital simulation provides an inexpensive means for evaluating the impact of operator and maintainer performance in man-machine systems without the cost or complexity of physical experiments. It allows for the identification of problem areas before the actual system has been constructed. It can provide the answers to the following questions [71]:

- (1) What are the quantitative personnel requirements?
- (2) What are the qualitative personnel requirements? Where, during the system utilization, are the operators most overloaded? Underloaded?
- (3) How will cross-training improve system effectiveness?
- (4) Are the system operators able to complete all of their required tasks within the time allotted?
- (5) Where in the task sequence are operators or teams likely to fail most often? Least often?
- (6) In which states of the system is the human subsystem and its components least reliable and why?
- (7) How will task restructuring or task allocation affect system effectiveness?
- (8) How much will performance degrade when the systems operators are fatigued or stressed?
- (9) How will various environmental factors (e.g. heat, light, terrain) affect total man-machine system performance?
- (10) To what extent will system effectiveness improve or degrade if more or less proficient operators are assigned?
- (11) How do group factors such as morale and cohesion affect system performance?

Simulations can be used in the conceptual as well as developmental stages of system evolution. They provide vehicles for tradeoff analyses.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

At the time this section was written, the Maintenance Personnel Performance Simulation (MAPPS) [72] is the only supported member of the family of Siegel-Wolf simulation models. The basic features of the model are shown in Table 7.7-5.

TABLE 7.7-5: MAPPS SCOPE

FEATURE	MODEL LIMIT
Maximum number of tasks	200
Number of maintainers	2-8
Types of maintainers	5
Number of subtasks	100
Types of subtasks	28
Maximum task duration (days)	2
Number of shifts	1-10
Protective clothing types	3
Types of ability	2

The model establishes a team of up to eight members who begin a maintenance task at time $t=0$ under a set of initial conditions established by the user. For each maintenance task, subtasks are identified with data and shift termination information. Subtasks may be repeated because of inadequate performance, group decisions and looping back. MAPPS selects the maintainers to be assigned to each task or subtask and then processes the input data and current system state data to arrive at estimates of task performance. MAPPS is written in FORTRAN IV H (Enhanced) for the IBM 3033 system. MAPPS output can be characterized in terms of type of information and degree of detail. Output can be provided by subtask (the most detailed), by iteration, and by run. For a subtask, the model will provide results such as: degree of success; probability of success; start and end times; duration; time and communication stresses; effects of accessibility, fatigue and heat; and required ability.

The Cognitive Environment Simulation (CES) [73] is an artificial intelligence approach that simulates predictions about operator action by simulating the processes by which intentions are formed. It enables the analyst to represent of state of knowledge regarding a particular situation and then observe the consequences in terms of human intended actions. It is an application of the proprietary EAGOL artificial intelligence problem solving system developed by Seer Systems. EAGOL has the ability to reason in multiple fault situations and to reason in situations that evolve over time. The specific CES application of EAGOL is for emergency situations in nuclear power plants. Note that CES is not intended to be a "micro" view of human cognitive processing. Applying CES consists of matching CES resources to those of the power plant under study. Input data consists of a time series of plant state data that would be available to operator personnel. The data are processed into a virtual display board which reports the status of the plant, recognizes undesirable situations, and generates proposed rectifications to those situations. The output is a series of intentions to act and resolve the undesirable situation. CES contains three types of activities: monitoring, explanation building, and response management. The CES user can vary the demands placed on CES and the resources available to solve problems. CES is

 SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

used in association with the Cognitive Reliability Assessment Technique (CREATE) for use in the probabilistic risk analysis of nuclear power plants.

7.7.6.4 Expert Judgment Techniques

These are a collection of techniques that address the lack of "hard data" or firm interpretations of data through the use experts.

The Success-Likelihood Index Methodology (SLIM, SLIM-MAUD) [74] [75] examines performance shaping factors (PSFs) and establishes both ratings and weight for each PSF. SLIM-MAUD is a personal computer implementation of SLIM. The MAUD acronym refers to "Multi-Attribute Utility Decomposition." MAUD is a proprietary stand alone software package that aids the user in assessing alternatives. PSFs that can be considered are:

- (1) Situational characteristics
- (2) Job and task instructions
- (3) Task characteristics
- (4) Equipment characteristics
- (5) Psychological stressors
- (6) Physiological stressors
- (7) Internal factors (training, experience, skill)

SLIM ranks the most important PSFs. The products of the rating and the normalized weight for each task are added to obtain the SLI (described earlier). The SLI is related to the task success probability through the following calibration equation:

$$\ln P(\text{success}) = a * \text{SLI} + b$$

where a and b are empirical constants. Rosa et al. [76] notes that SLIM-MAUD requires that tasks be sorted into subsets of 4 to 10 tasks that are similarly affected by a proposed set of PSFs. The weighting and ranking of tasks is accomplished by a group of experts, usually four in number, who are led by a facilitator. Analysis is conducted with the aid of the MAUD computer program.

Rosa et al. noted many positive characteristics of SLIM-MAUD, including face validity, practicality, estimates with acceptable levels of reliability, ease of use and understanding, and ability to identify which PSFs have the most effect on the SLIs. Guassardo [65] notes that SLIM results are highly dependent on the boundary conditions used to find the calibration equation coefficients. Poucet [64] indicates that the SLIM results were highly dependent on the calibration reference points. The use of SLIM is recommended only if good reference data are available. Poucet also notes that SLIM does not address relationships among PSFs when such exist.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.7.7 Verification of Human Performance Reliability

For human-machine systems, the purposes of verification testing can be described as follows [77].

- (1) Demonstrate the conformance of the product to human engineering design criteria
- (2) Confirm compliance with specific performance requirements
- (3) Secure quantitative measures of human-machine performance characteristics that are functions of human-machine interaction
- (4) Determine whether or not undesirable characteristics have been introduced

The demonstration of human performance reliability (in maintenance situations) may overlap with maintainability demonstrations or testing. The same set of tasks may be considered but with different criteria. For example, in a maintainability demonstration, the principle concern is the time required to complete a task. If the same task is employed in a human performance reliability context, the important criteria are not only correct completion of the task but also completion of the task within a time constraint. The references provide additional details on structuring tests to estimate maintenance technician reliability.

For estimates of reliability in an operator type situation, data must be accumulated either by use of a simulator or by an expanded reliability demonstration that includes the operator as well as the equipment. In either case, the data will resemble actual field results only to the extent that the test scenario and the performance of the test subjects resemble the actual field conditions.

7.8 Failure Mode and Effects Analysis (FMEA)

7.8.1 Introduction

Failure Mode and Effects Analysis is a reliability procedure which documents all possible failures in a system design within specified ground rules. It determines, by failure mode analysis, the effect of each failure on system operation and identifies single failure points, that are critical to mission success or crew safety. It may also rank each failure according to the criticality category of failure effect and probability occurrence. This procedure is the result of two steps: the Failure Mode and Effect Analysis (FMEA) and the Criticality Analysis (CA).

In performing the analysis, each failure studied is considered to be the only failure in the system, i.e., a single failure analysis. The FMEA can be accomplished without a CA, but a CA requires that the FMEA has previously identified critical failure modes for items in the system design. When both steps are done, the total process is called a Failure Mode, Effects and Criticality Analysis (FMECA). The procedures for performing both the FMEA and the CA are found in Reference [78] and Reference [79]. At the time of this update Reference [78], MIL-STD-1629,

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

was scheduled to be cancelled and replaced by a non-government standard by June 1997. However, it is not known at this time what that new document will be.

FMEA utilizes inductive logic in a "bottoms up" approach. Beginning at the lowest level of the system hierarchy, (e.g., component part), and from a knowledge of the failure modes of each part, the analyst traces up through the system hierarchy to determine the effect that each failure mode will have on system performance. This differs from fault tree analysis (discussed in the next section) which utilizes deductive logic in a "top down" approach. In fault tree analysis, the analyst assumes a system failure and traces down through the system hierarchy to determine the event, or series of events, that could cause such a failure.

The FMEA provides:

- (1) A method of selecting a design with a high probability of operational success and crew safety.
- (2) A documented method of uniform style for assessing failure modes and their effect on operational success of the system.
- (3) Early visibility of system interface problems.
- (4) A list of possible failures which can be ranked according to their category of effect and probability of occurrence.
- (5) Identification of single failure points critical to mission success or to crew safety.
- (6) Early criteria for test planning.
- (7) Quantitative and uniformly formatted data input to the reliability prediction, assessment, and safety models.
- (8) A basis for design and location of performance monitoring and fault sensing devices and other built-in automatic test equipment.
- (9) A tool which serves as an aid in the evaluation of proposed design, operational, or procedural changes and their impact on mission success or crew safety.

Items (5) and (8) are the two most important functions performed by an FMEA.

The FMEA is normally accomplished before a reliability prediction is made to provide basic information. It should be initiated as an integral part of the early design process and should be periodically updated to reflect design changes. Admittedly, during the early stages, one usually does not have detailed knowledge of the component parts to be used in each equipment. However, one usually has knowledge of the "black boxes" which make up the system. Thus, at

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

this stage, an FMEA might start at the "black box" level and be expanded as more detailed knowledge becomes available. This analysis may also be used to provide a model for analyzing already-built systems. An FMEA is a major consideration in design reviews.

The principles of FMEA are straightforward and easy to grasp. The practice of FMEA is tedious, time consuming and very profitable. It is best done in conjunction with Cause-Consequence and Fault Tree Analysis. The bookkeeping aspects, namely, the keeping track of each item and its place in the hierarchy, are very important because mistakes are easily made.

The Cause-Consequence chart shows the logical relationships between causes (events which are analyzed in no more detail) and consequences (events which are of concern only in themselves, not as they in turn affect other events). The chart usually is represented with consequences at the top and causes at the bottom; and the words Top and Bottom have come into common use to describe those portions of the chart. A Failure Modes and Effects Analysis (FMEA) deals largely with the bottom part of the chart. A fault tree is a part of a Cause-Consequence chart. It consists of only one consequence and all its associated branches. The Cause-Consequence chart is created by superimposing the separately created fault trees. The Cause-Consequence chart can be used to organize one's knowledge about any set of causes and their consequences; its use is not limited to hardware oriented systems.

The FMEA consists of two phases which provide a documented analysis for all critical components of a system. First, however, definitions of failure at the system, subsystem, and sometimes even part level must be established.

Phase 1 is performed in parallel with the start of detailed design and updated periodically throughout the development program as dictated by design changes. Phase 2 is performed before, or concurrent with, the release of detail drawings.

The Phase 1 analysis consists of the following steps:

- (1) Constructing a symbolic logic block diagram, such as a reliability block diagram or a Cause-Consequence chart.
- (2) Performing a failure effect analysis, taking into account modes of failure such as:
 - (a) Open circuits
 - (b) Short circuits
 - (c) Dielectric breakdowns
 - (d) Wear
 - (e) Part-parameter shifts
- (3) Proper system and item identification.
- (4) Preparation of a critical items list.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

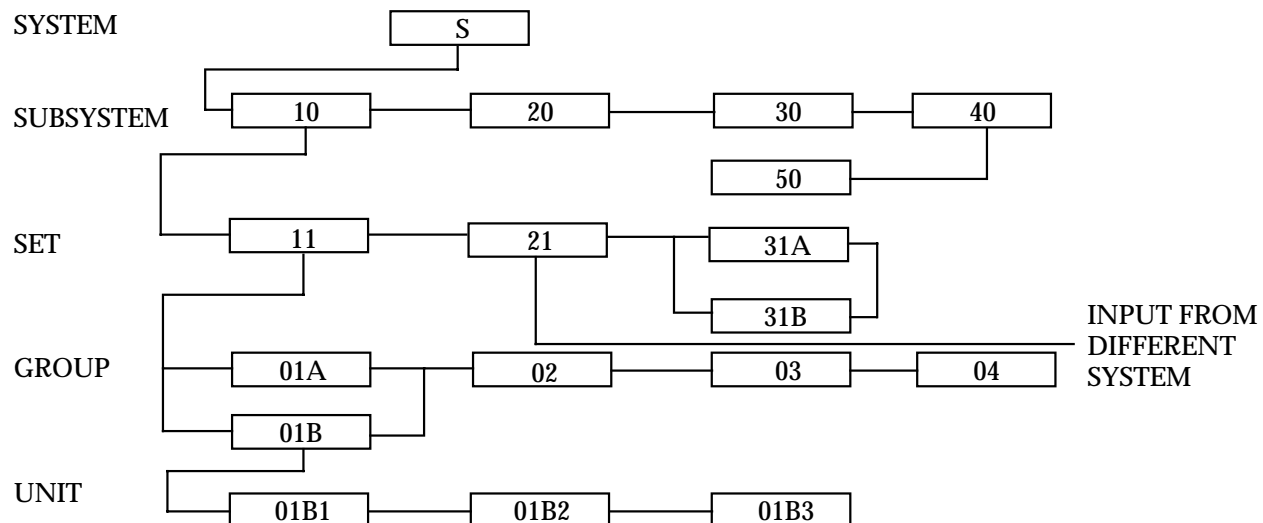
During Phase 2, the results of Phase 1 are revised and updated as required by design changes. In addition, all items in the system are analyzed to determine their criticality with respect to the system.

7.8.2 Phase 1

During this phase the following detailed steps are performed:

- (1) A Symbolic Logic Block Diagram is constructed. This diagram is developed for the entire system to indicate the functional dependencies among the elements of the system and to define and identify its subsystems. It is not a functional schematic or a signal flow diagram, but a model for use in the early analysis to point out weaknesses. Figures 7.8-1 and 7.8-2 show typical symbolic logic diagrams. Figure 7.8-1 illustrates the functional dependency among the subsystems, sets, groups, and units that make up the system. Figure 7.8-2 illustrates the functional dependencies among assemblies, subassemblies, and parts that make up one of the units in Figure 7.8-1.
- (2) A failure effect analysis is performed for each block in the symbolic logic block diagram, indicating the effect of each item failure on the performance of the next higher level on the block diagram. Table 7.8-1 shows a typical group of failure modes for various electronic and mechanical parts. The failure mode ratios are estimates and should be revised on the basis of the user's experience. However, they can be used as a guide in performing a detailed failure effect analysis.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

LEVEL

Notes:

- (1) The system depends on subsystems 10, 20, 30 and 40
- (2) Subsystem 10 depends on sets 11, 21, 31A, and 31B
- (3) Set 11 depends on groups 01A, 01B, 02, 03, and 04
- (4) Group 01B depends on units 01B1, 01B2, and 01B3
- (5) Sets 31A and 31B are redundant
- (6) Groups 01A and 01B are redundant
- (7) Subsystem 40 depends on subsystem 50
- (8) Set 21 depends upon an input from another system

FIGURE 7.8-1: TYPICAL SYSTEM SYMBOLIC LOGIC BLOCK DIAGRAM

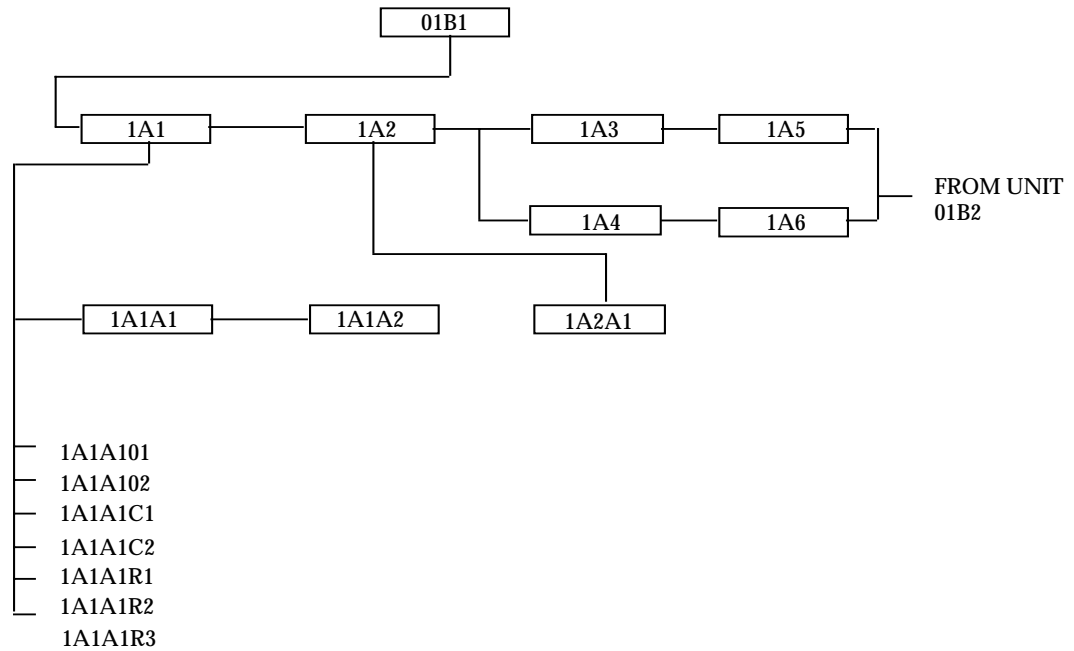
SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

LEVEL

UNIT

ASSEMBLY

SUBASSEMBLY



Notes:

- (1) Unit 01B1 depends on assemblies 1A1, 1A2 AND either '1A3 and 1A5' OR '1A4 and 1A6'
- (2) Assembly 1A1 depends on subassemblies 1A1A1 AND 1A1A2
- (3) Assembly 1A2 depends on subassembly 1A2A1
- (4) Subassembly 1A1A1 depends on all parts contained therein

FIGURE 7.8-2: TYPICAL UNIT SYMBOLIC LOGIC BLOCK DIAGRAM

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.8-1: FAILURE MODE DISTRIBUTION OF PARTS⁶

DEVICE TYPE	FAILURE MODE	MODE PROBABILITY (α)
Accumulator	Leaking	.47
	Seized	.23
	Worn	.20
	Contaminated	.10
Actuator	Spurious Position Change	.36
	Binding	.27
	Leaking	.22
	Seized	.15
Alarm	False Indication	.48
	Failure to Operate	.29
	Spurious Operation	.18
	Degraded Alarm	.05
Antenna	No Transmission	.54
	Signal Leakage	.21
	Spurious Transmission	.25
Battery, Lithium	Degraded Output	.78
	Startup Delay	.14
	Short	.06
	Open	.02
Battery, Lead Acid	Degraded Output	.70
	Short	.20
	Intermittent Output	.10
Battery, Ni-Cd	Degraded Output	.72
	No Output	.28
Bearing	Binding/Sticking	.50
	Excessive Play	.43
	Contaminated	.07
Belt	Excessive Wear	.75
	Broken	.25
Brake	Excessive Wear	.56
	Leaking	.23
	Scored	.11
	Corroded	.05
	Loose	.05
Bushing	Excessive Wear	.85
	Loose	.11
	Cracked	.04
Cable	Short	.45
	Excessive Wear	.36
	Open	.19
Capacitor, Aluminum, Electrolytic	Short	.53
	Open	.35
	Electrolyte Leak	.10
	Decrease in Capacitance	.02

⁶ Reliability Analysis Center, "Failure Mode/Mechanism Distributions" (FMD-91)

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.8-1: FAILURE MODE DISTRIBUTION OF PARTS (CONT'D)

DEVICE TYPE	FAILURE MODE	MODE PROBABILITY (α)
Capacitor, Ceramic	Short	.49
	Change in Value	.29
	Open	.22
Capacitor, Mica/Glass	Short	.72
	Change in Value	.15
	Open	.13
Capacitor, Paper	Short	.63
	Open	.37
Capacitor, Plastic	Open	.42
	Short	.40
	Change in Value	.18
Capacitor, Tantalum	Short	.57
	Open	.32
	Change in Value	.11
Capacitor, Tantalum, Electrolytic	Short	.69
	Open	.17
	Change in Value	.14
Capacitor, Variable, Piston	Change in Value	.60
	Short	.30
	Open	.10
Circuit Breaker	Opens Without Stimuli	.51
	Does Not Open	.49
Clutch	Binding/Sticking	.56
	Slippage	.24
	No Movement	.20
Coil	Short	.42
	Open	.42
	Change in Value	.16
Connector/Connection	Open	.61
	Poor Contact/Intermittent	.23
	Short	.16
Counter Assembly	Inaccurate Count	.91
	Seized	.09
Diode, General	Short	.49
	Open	.36
	Parameter Change	.15
Diode, Rectifier	Short	.51
	Open	.29
	Parameter Change	.20

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.8-1: FAILURE MODE DISTRIBUTION OF PARTS (CONT'D)

DEVICE TYPE	FAILURE MODE	MODE PROBABILITY (α)
Diode, SCR	Short	.98
	Open	.02
Diode, Small Signal	Parameter Change	.58
	Open	.24
	Short	.18
Diode, Thyristor	Failed Off	.45
	Short	.40
	Open	.10
	Failed On	.05
Diode, Triac	Failed Off	.90
	Failed On	.10
Diode, Zener, Voltage Reference	Parameter Change	.69
	Open	.18
	Short	.13
Diode, Zener, Voltage Regulator	Open	.45
	Parameter Change	.35
	Short	.20
Electric Motor, AC	Winding Failure	.31
	Bearing Failure	.28
	Fails to Run, After Start	.23
	Fails to Start	.18
Fuse	Fails to Open	.49
	Slow to Open	.43
	Premature Open	.08
Gear	Excessive Wear	.54
	Binding/Sticking	.46
Generator	Degraded Output	.60
	No Output	.22
	Fails to Run, After Start	.09
	Loss of Control	.09
Hybrid Device	Open Circuit	.51
	Degraded Output	.26
	Short Circuit	.17
	No Output	.06
Injector	Corroded	.87
	Deformed	.08
	Cracked/Fractured	.05

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.8-1: FAILURE MODE DISTRIBUTION OF PARTS (CONT'D)

DEVICE TYPE	FAILURE MODE	MODE PROBABILITY (α)
Keyboard Assembly	Spring Failure	.32
	Contact Failure	.30
	Connection Failure	.30
	Lock-up	.08
Lamp/Light	No Illumination	.67
	Loss of Illumination	.33
Liquid Crystal Display	Dim Rows	.39
	Blank Display	.22
	Flickering Rows	.20
	Missing Elements	.19
Mechanical Filter	Leaking	.67
	Clogged	.33
Meter	Faulty Indication	.51
	Unable to Adjust	.23
	Open	.14
	No Indication	.12
Microcircuit, Digital, Bipolar	Output Stuck High	.28
	Output Stuck Low	.28
	Input Open	.22
	Output Open	.22
Microcircuit, Digital, MOS	Input Open	.36
	Output Open	.36
	Supply Open	.12
	Output Stuck Low	.09
	Output Stuck High	.08
Microcircuit, Interface	Output Stuck Low	.58
	Output Open	.16
	Input Open	.16
	Supply Open	.10
Microcircuit, Linear	Improper Output	.77
	No Output	.23
Microcircuit, Memory, Bipolar	Slow Transfer of Data	.79
	Data Bit Loss	.21
Microcircuit, Memory, MOS	Data Bit Loss	.34
	Short	.26
	Open	.23
	Slow Transfer of Data	.17

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.8-1: FAILURE MODE DISTRIBUTION OF PARTS (CONT'D)

DEVICE TYPE	FAILURE MODE	MODE PROBABILITY (α)
Microwave Amplifier	No Output	.90
	Limited Voltage Gain	.10
Microwave, Connector	High Insertion Loss	.80
	Open	.20
Microwave Detector	Power Loss	.90
	No Output	.10
Microwave, Diode	Open	.60
	Parameter Change	.28
	Short	.12
Microwave Filter	Center Frequency Drift	.80
	No Output	.20
Microwave Mixer	Power Decrease	.90
	Loss of Intermediate Frequency	.10
Microwave Modulator	Power Loss	.90
	No Output	.10
Microwave Oscillator	No Output	.80
	Untuned Frequency	.10
	Reduced Power	.10
Microwave VCO	No Output	.80
	Untuned Frequency	.15
	Reduced Power	.05
Optoelectronic LED	Open	.70
	Short	.30
Optoelectronic Sensor	Short	.50
	Open	.50
Power Supply	No Output	.52
	Incorrect Output	.48
Printed Wiring Assembly	Open	.76
	Short	.24
Pump, Centrifugal	No Output	.67
	Degraded Output	.33
Pump, Hydraulic	Leaking	.82
	Improper Flow	.12
	No Flow	.06
Relay	Fails to Trip	.55
	Spurious Trip	.26
	Short	.19

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.8-1: FAILURE MODE DISTRIBUTION OF PARTS (CONT'D)

DEVICE TYPE	FAILURE MODE	MODE PROBABILITY (α)
Resistor, Composition	Parameter Change	.66
	Open	.31
	Short	.03
Resistor, Film	Open	.59
	Parameter Change	.36
	Short	.05
Resistor, Wirewound	Open	.65
	Parameter Change	.26
	Short	.09
Resistor, Network	Open	.92
	Short	.08
Resistor, Variable	Open	.53
	Erratic Output	.40
	Short	.07
Rotary Switch	Improper Output	.53
	Contact Failure	.47
Software	Design Changes	.46
	Design Errors	.41
	User Error	.07
	Documentation Error	.06
Solenoid	Short	.52
	Slow Movement	.43
	Open	.05
Switch, Push-button	Open	.60
	Sticking	.33
	Short	.07
Switch, Thermal	Parameter Change	.63
	Open	.27
	No Control	.08
	Short	.02
Switch, Toggle	Open	.65
	Sticking	.19
	Short	.16
Synchro	Winding Failure	.45
	Bearing Failure	.33
	Brush Failure	.22

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.8-1: FAILURE MODE DISTRIBUTION OF PARTS (CONT'D)

DEVICE TYPE	FAILURE MODE	MODE PROBABILITY (α)
Transducer	Out of Tolerance	.68
	False Response	.15
	Open	.12
	Short	.05
Transformer	Open	.42
	Short	.42
	Parameter Change	.16
Transistor, Bipolar	Short	.73
	Open	.27
Transistor, FET	Short	.51
	Output Low	.22
	Parameter Change	.17
	Open	.05
	Output High	.05
Transistor, GaAs FET	Open	.61
	Short	.26
	Parameter Change	.13
Transistor, R.F.	Parameter Change	.50
	Short	.40
	Open	.10
Tube, Traveling Wave	Reduced Output Power	.71
	High Helix Current	.11
	Gun Failure	.09
	Open Helix	.09
Valve, Hydraulic	Leaking	.77
	Stuck Closed	.12
	Stuck Open	.11
Valve, Pneumatic	Leaking	.28
	Stuck Open	.20
	Stuck Closed	.20
	Spurious Opening	.16
	Spurious Closing	.16
Valve, Relief	Premature Open	.77
	Leaking	.23

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

In order to accurately address the failure modes of a given LSI microcircuit each of these factors must be accounted for. As an example, if the IC chip is packaged in an hermetic cavity package there is a possibility that one wire may break and short to an adjacent wire. If this same chip were encapsulated in a plastic package, this short could not occur, since the wire is constrained by the potting material. However, the potting material can have other detrimental effects on an IC chip.

Figure 7.8-3 illustrates a useful form for conducting a failure effect analysis. (See also Figure 7.8-2 for an example of its use.) For each component in the system, appropriate information is entered in each column. Column descriptions are given in Table 7.8-2.

(1) ITEM	(2) CODE	(3) FUNCTION	(4) FAILURE MODE	(5) FAILURE EFFECT	(6) LOSS PROBABILITY, β

FIGURE 7.8-3: FAILURE EFFECTS ANALYSIS FORM

TABLE 7.8-2: COLUMN DESCRIPTIONS FOR FIGURE 7.8-3

COLUMN	NOMENCLATURE	DESCRIPTION
1	Item	Item name
2	Code	Item identification or circuit designation code
3	Function	Concise statement of the item's function
4	Failure Mode	Concise statement of the mode(s) of item failure
5	Failure Effect	Explanation of the effect of each failure mode on the performance of the next higher level in the symbolic logic block diagram
6	Loss Probability	Numerical value indicating the probability of system loss if the item fails in the mode indicated

 SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

A numerical reference for all items in the symbolic logic block diagram must be provided by using a standard coding system, such as that specified in MIL-STD-1629. All items below the set and group levels are identified using the scheme illustrated in Table 7.8-2. Items at and above the group and set levels are not subject to this standard nomenclature scheme. These items can be assigned a simple code such as that illustrated in Figure 7.8-1. In this illustration, the system is assigned a letter; and the subsystems, sets, and groups are assigned numbers in a specifically ordered sequence. As an example, the code S-23-01 designates the first group of the third set in the second subsystem of system S (Note, this code is limited to subsystems with less than 10 sets). The exact coding system used is not as important as making sure that each block in the diagram has its own number. Identical items (same drawing numbers) in different systems, or in the same system but used in different applications, should not be assigned the same code number.

- (1) During the failure effects analysis, a number of changes to the block diagrams may be required. Therefore, to minimize the number of changes in the coding system, it is recommended that the failure effects analysis be completed before assignment of code numbers is finalized.
- (2) Based on the failure effects analysis, a list of critical items should be prepared. This list will contain those items whose failure results in a possible loss, probable loss, or certain loss of the next higher level in the symbolic logic block diagram. All items that can cause system loss should be identified clearly in the list.

7.8.3 Phase 2

This phase is implemented by performing the following steps:

- (1) The symbolic logic block diagram, failure effects analysis, coding, and critical items list are reviewed and brought up- to-date.
- (2) Criticality is assigned, based on the item applicable failure mode, the system loss probability, the failure mode frequency ratio, and the item unreliability. The analysis of criticality is essentially quantitative, based on a qualitative failure effects analysis.

Criticality CR_{ij} defined by the equation

$$(CR)_{ij} = \alpha_{ij} \beta_{ij} \lambda_i \quad (7.21)$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

where:

α_{ij} = failure mode frequency ratio of item i for the failure mode j (see Table 7.8-1 for an example), i.e., the ratio of failures of the type being considered to all failures of the item.

β_{ij} = loss probability of item i for failure mode j (i.e., the probability of system failure if the item fails). A suggested scale is Certain Loss = 1.00, Probable Loss ranges from 0.1 to 1.0, Possible Loss ranges from 0 to 0.10, No Effect - 0.0

λ_i = failure rate of item i

$(CR)_{ij}$ = system failure rate due to item i 's failing in its mode j

The system criticality is given by Eq. (7.22)

$$(CR)_s = \sum_i \sum_j (CR)_{ij} \quad (7.22)$$

where:

$(CR)_s$ = system criticality (failure rate)

\sum_j = sum over all failure modes of item i

\sum_i = sum over all items

A form useful for conducting the criticality analysis is given in Figure 7.8-5. This form is a modification of Figure 7.8-3 to include the failure mode frequency ratio and the failure rate. The example in the next section and Figures 7.8-4 and 7.8-5 illustrate the procedure.

The CR value of the preamplifier unit is 5.739 per 10^6 hr. This number can be interpreted as the predicted total number of system failures per hour due to preamplifier failures, e.g., 5.739×10^{-6} . Whether or not this number is excessive, and thus calls for corrective action, depends upon the requirements for the system and the criticalities for other units in the system. If the number is excessive, it can be reduced by any of the following actions:

- (1) Lowering the failure rates of parts in the system by derating.
- (2) Decreasing the failure mode frequency ratio through selection of other parts.
- (3) Decreasing the loss probability by changing the system or preamplifier design.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

- (4) Redesign using various techniques such as redundancy, additional cooling, or switching.

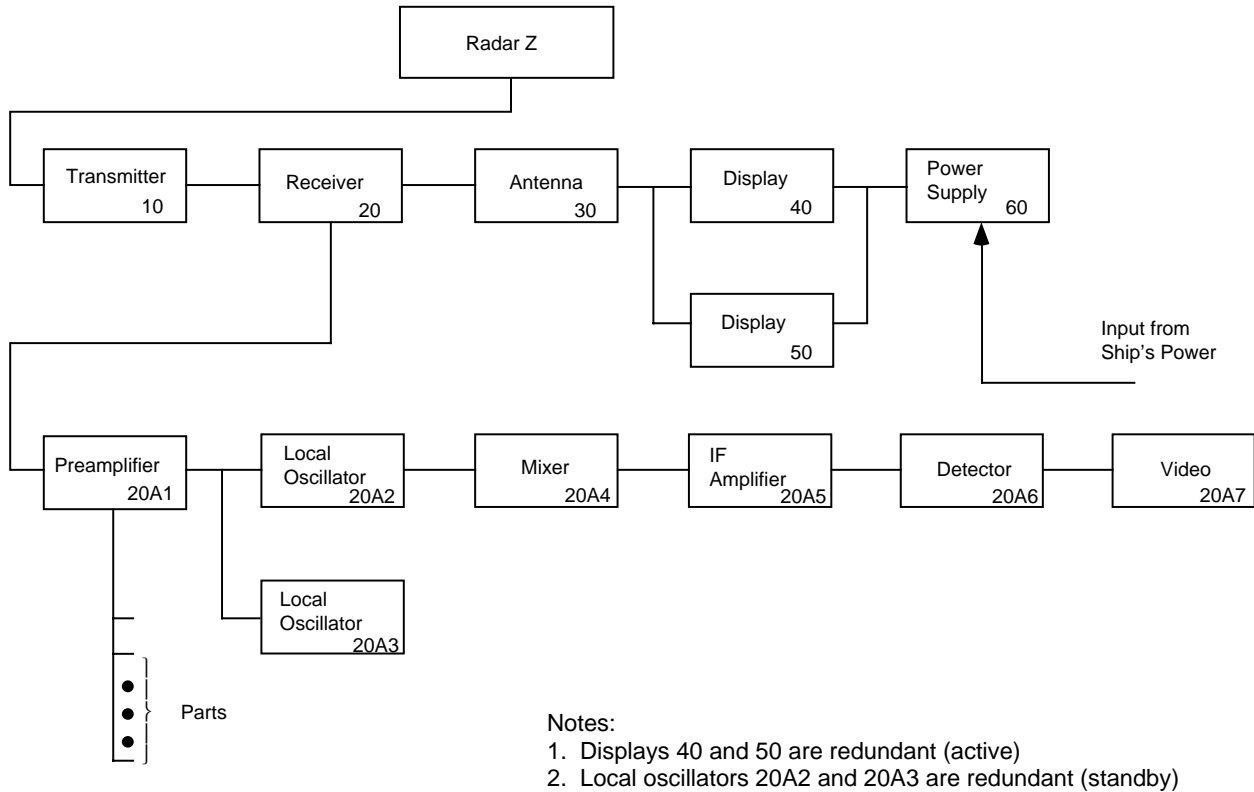


FIGURE 7.8-4: SYMBOLIC LOGIC DIAGRAM OF RADAR EXAMPLE

7.8.4 Example

The detail design of a radar system required the use of FMEA to determine the effect of item failures on the system. The FMEA analysis must be performed at this time prior to freezing the design. Perform an FMEA analysis as follows:

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

PROCEDURE	EXAMPLE
(1) Develop a symbolic logic block diagram of the radar system. The units making up the receiver subsystem are shown in detail. In an actual analysis, symbolic diagrams must be constructed for all other sub-systems.	See Figure 7.8-4
(2) Fill in the work sheets for all units in the receiver subsystem. Repeat this procedure for all subsystems.	See Figure 7.8-5
(3) Qualitatively estimate the values of loss probability for each part.	An analysis indicates that for this system the following values of β are applicable: 1.0, 0.1, and 0.0.
(4) Determine the failure mode frequency ratio for each failure mode of every part.	The resistor is fixed, film (Fig. 7.8-5); from Table 7.8-1, it has two failure modes: open = 0.59 and drift = 0.36.
(5) Tabulate failure rates for each component.	λ (20A1R1) = 1.5 per 10^6 hr.
(6) Compute the CR value for each failure mode of each part by Eq. (7.21).	$\text{CR}(\text{open}) = 0.59 \times 1.00 \times 1.5 \text{ per } 10^6 \text{ hr}$ $= 0.885 \text{ per } 10^6 \text{ hr}$
	$\text{CR}(\text{short}) = 0.05 \times 1.00 \times 1.5 \text{ per } 10^6 \text{ hr}$ $= 0.075 \text{ per } 10^6 \text{ hr}$
	$\text{CR}(\text{parameter change}) = 0.36 \times 10^6 \text{ hr}$ $\times 0.10 \times 1.5 \text{ per } 10^6 \text{ hr}$ $= 0.054 \text{ per } 10^6 \text{ hr}$
(7) Compute the total CR for the unit (CR), by Eq. (7.22).	The total CR for the preamplifier unit is 5.739 per 10^6 hr (See Figure 7.8-5).

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

CRITICALITY WORK SHEET		SYSTEM Radar (2)			SUBSYSTEM Receiver 20			UNIT Preamplifier 20A1			Parts	
(1) Item	(2) Code	(3) Function	(4) Failure Effect	(5) Failure Effect	(6) Loss Probability (β)	(7) Failure Mode Frequency Ratio (α)	(8) Failure Rate (Per Million Hours (λ))	(9) Criticality (CR)	(10) Comments			
Resistor	R1	Voltage Divider	Open	No Output	1.00	0.59	1.50	0.885	Film Resistor			
Resistor	R1	Voltage Divider	Short	No Output	1.00	0.05	1.50	0.075	Film Resistor			
Resistor	R1	Voltage Divider	Parameter Change	Wrong Output	0.10	0.36	1.50	0.054	Film Resistor			
Resistor	R2	Voltage Divider	Open	No Output	1.00	0.59	1.50	0.885	Film Resistor			
Resistor	R2	Voltage Divider	Short	No Output	1.00	0.05	1.50	0.075	Film Resistor			
Resistor	R2	Voltage Divider	Parameter Change	Wrong Output	0.10	0.36	1.50	0.054	Film Resistor			
Capacitor	C3	Decoupling	Open	No Effect	0.00	0.32	0.22	0.000	Tubular Tantalum			
Capacitor	C3	Decoupling	Short	No Output	1.00	0.57	0.22	0.125	Tubular Tantalum			
Capacitor	C3	Decoupling	Parameter Change	No Effect	0.00	0.11	0.22	0.000	Tubular Tantalum			
Diode	CR3	Voltage Divider	Open	No Output	1.00	0.24	1.00	0.240	Small Signal			
Diode	CR3	Voltage Divider	Short	No Output	1.00	0.18	1.00	0.180	Small Signal			
Diode	CR3	Voltage Divider	Parameter Change	Wrong Output	0.10	0.58	1.00	0.058	Small Signal			
Transistor	Q4	Amplifier	Open	No Output	1.00	0.10	3.00	0.300	R.F.			
Transistor	Q4	Amplifier	Short	No Output	1.00	0.40	3.00	1.200	R.F.			
Transistor	Q4	Amplifier	Parameter Change	Wrong Output	0.10	0.50	3.00	0.150	R.F.			
Transformer	T5	Coupling	Open	No Output	1.00	0.42	3.00	1.260				
Transformer	T5	Coupling	Shorted	Wrong Output	0.10	0.42	3.00	0.126				
Transformer	T5	Coupling	Parameter Change	Wrong Output	0.10	0.15	3.00	0.045				
Resistor	R6	Bias	Open	No Output	1.00	0.31	0.006	0.002	Composition			
Resistor	R6	Bias	Short	Wrong Output	0.10	0.03	0.006	0.000	Composition			
Resistor	R6	Bias	Parameter Change	No Effect	0.00	0.66	0.006	0.000	Composition			
Capacitor	C7	Bypass	Open	No Effect	0.00	0.35	0.48	0.000	Aluminum			
Capacitor	C7	Bypass	Short	Wrong Output	0.10	0.53	0.48	0.025	Electrolytic			
Capacitor	C7	Bypass	Parameter Change	No Effect	0.00	0.02	0.48	0.000	Capacitor			
Capacitor	C7	Bypass	Electrolyte Leakage	No Effect	0.00	0.10	0.48	0.000				
CRITICALITY TOTAL FOR UNIT 5.730												

FIGURE 7-8-5: DETERMINATION OF PREAMPLIFIER CRITICALITY

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.8.5 Risk Priority Number

An alternate evaluation approach to Criticality Analysis is that of the calculation of a Risk Priority Number (RPN). The risk priority number provides a qualitative numerical estimate of the design risk. This number is then used to rank order the various concerns and failure modes associated with a given design as previously identified in the FMEA. RPN is defined as the product of three independently assessed factors: Severity (S), Occurrence (O) and Detection (D).

$$\text{RPN} = (\text{S}) \times (\text{O}) \times (\text{D})$$

This technique was originally developed for use by the automotive industry, but it may also be effectively tailored to many other types of applications. A more detailed description of this technique may be found in Reference [80].

A description, and one detailed example, of each of these three independently assessed factors (S), (O), and (D) follows.

SEVERITY (S) is an assessment of the seriousness of the effect of the potential failure mode to the next higher component, subsystem, system or to the customer if it were to occur. Severity is typically estimated on a scale of “1” to “10”. One such method of ranking is illustrated in Table 7.8-3. This table could be appropriately tailored for other non-automotive applications. Severity applies only to the effect of the failure.

OCCURRENCE (O) is the likelihood that a specific cause/mechanism will occur. The likelihood of occurrence ranking number is an index number rather than a probability. Removing or controlling one or more of the causes/mechanisms of the failure mode through a design change is the only way a reduction in occurrence ranking can be effected.

The likelihood of occurrence of potential failure cause/mechanism is typically estimated on a scale of “1” to “10”. One such method of ranking is illustrated in Table 7.8-4.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.8-3: SEVERITY CLASSIFICATION

EFFECT	CRITERIA: SEVERITY OF EFFECT	RANKING
Hazardous - without warning	Very high severity ranking when a potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning.	10
Hazardous - with warning	Very high severity ranking when a potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning.	9
Very High	Vehicle / item inoperable, with loss of primary function.	8
High	Vehicle / item operable, but at reduced level of performance. Customer dissatisfied.	7
Moderate	Vehicle / item operable, but Comfort / Convenience item(s) inoperable. Customer experiences discomfort.	6
Low	Vehicle / item operable, but Comfort / Convenience item(s) operate at a reduced level of performance. Customer experiences some dissatisfaction.	5
Very Low	Fit & Finish / Squeak & Rattle item does not conform. Defect noticed by most customers.	4
Minor	Fit & Finish / Squeak & Rattle item does not conform. Defect noticed by average customer.	3
Very Minor	Fit & Finish / Squeak & Rattle item does not conform. Defect noticed by discriminating customer.	2
None	No Effect	1

TABLE 7.8-4: OCCURRENCE RANKING

PROBABILITY OF FAILURE	POSSIBLE FAILURE RATES	RANKING
Very High: Failure is almost inevitable	≥ 1 in 2	10
	1 in 3	9
High: Repeated failures	1 in 8	8
	1 in 20	7
Moderate: Occasional failures	1 in 80	6
	1 in 400	5
	1 in 2000	4
Low: Relatively few failures	1 in 15,000	3
	1 in 150,000	2
Remote: Failure is unlikely	≤ 1 in 1,500,000	1

In determining this estimate, questions such as the following should be considered:

- (1) What is the service history/field experience with similar components or subsystems?
- (2) Is this component carried over from, or similar to, a previously used component or subsystem?
- (3) How significant are the changes from a previously used component or subsystem?
- (4) Is the component radically different from a previously used component?

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

- (5) Is the component new?
- (6) Has the component application changed?
- (7) What, if any, are the environmental changes?
- (8) Has an engineering analysis been made to estimate the expected comparable occurrence rate for this application?

A consistent occurrence ranking system should be used to ensure continuity. The “Design Life Possible Failure Rates” shown in Table 7.8-4 are based upon the number of failures which are anticipated during the design life of the component, subsystem, or system. The occurrence ranking number is related to the rating scale and does not reflect the actual likelihood of occurrence.

CURRENT DESIGN CONTROLS: This is an additional parameter of concern beyond those previously addressed in the FMEA. Current Design Controls are defined as prevention, design verification/validation, or other activities which will assure the design adequacy for the failure mode and/or cause/mechanism under consideration. Current controls (e.g., road testing, design reviews, fail-safe analysis, mathematical studies, rig/lab testing, feasibility reviews, prototype tests, fleet testing etc.) are those that have been or are being used with the same or similar designs.

There are three types of Design Controls/Features to consider; those that: (1) Prevent the cause/mechanism or failure mode/effect from occurring, or reduce their rate of occurrence, (2) detect the cause/mechanism and lead to corrective actions, and (3) detect the failure mode.

The preferred approach is to first use type (1) controls if possible; second, use the type (2) controls; and third, use the type (3) controls. The initial detection ranking will be based upon the type (2) or type (3) current controls, provided the prototypes and models being used are representative of design intent.

DETECTION (D) is an assessment of the ability of the proposed type (2) current design controls, to detect a potential cause/mechanism (design weakness), or the ability of the proposed type (3) current design controls to detect the subsequent failure mode, before the component, subsystem, or system is released for production. In order to achieve a lower detection ranking, generally the planned design control (e.g. preventative, validation, and/or verification activities) has to be improved.

The detection of potential failure cause/mechanism is typically estimated on a scale of “1” to “10”. One such method of ranking is illustrated in Table 7.8-5.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.8-5: DETECTION RANKING

DETECTION	CRITERIA: LIKELIHOOD OF DETECTION BY DESIGN CONTROL	RANKING
Absolute Uncertainty	Design Control will not and/or can not detect a potential cause/ mechanism and subsequent failure mode; or there is no Design Control.	10
Very Remote	Very remote chance the Design Control will detect a potential cause/ mechanism and subsequent failure mode.	9
Remote	Remote chance the Design Control will detect a potential cause/ mechanism and subsequent failure mode.	8
Very Low	Very low chance the Design Control will detect a potential cause/ mechanism and subsequent failure mode.	7
Low	Low chance the Design Control will detect a potential cause/ mechanism and subsequent failure mode.	6
Moderate	Moderate chance the Design Control will detect a potential cause/ mechanism and subsequent failure mode.	5
Moderately High	Moderately high chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.	4
High	High chance the Design Control will detect a potential cause/ mechanism and subsequent failure mode.	3
Very High	Very high chance the Design Control will detect a potential cause/ mechanism and subsequent failure mode.	2
Almost Certain	Design Control will almost certainly detect a potential cause/ mechanism and subsequent failure mode.	1

7.8.5.1 Instituting Corrective Action

When the failure modes have been rank ordered by RPN (the product of S, O and D), corrective action should be first directed at the highest ranked concerns and critical items. The intent of any recommended action is to reduce any one or all of the occurrence, severity and/or detection rankings. An increase in design validation/verification actions will result in a reduction in the detection ranking only. A reduction in the occurrence ranking can be effected only by removing or controlling one or more of the causes/mechanisms of the failure mode through a design revision. Only a design revision can bring about a reduction in the severity ranking. Regardless of the resultant RPN, special attention should be given when severity is high.

After the corrective action(s) have been identified, estimate and record the resulting severity, occurrence, and detection rankings and recalculate the RPN.

7.8.6 Computer Aided FMEA

As with most other reliability analyses the computer can be quite helpful in performing an FMEA, since a large number of computations and a significant amount of record keeping are required for systems of reasonable size.

In the failure effects portion of the analysis the computer is very helpful for functional evaluation, using performance models. Given that the computer program contains the design equations relating system outputs to various design parameters, each item is allowed to fail in each of its modes, and the effect on the system is computed.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Several commercial programs are available for performing an FMECA in accordance with MIL-STD-1629A.

7.8.7 FMEA Summary

The FMEA does not replace the need for sound engineering judgment at the design level. This system analysis is, however, practical in determining many of the significant details which may not otherwise be determined by separate, individual studies. Like other design tools, the FMEA has limitations such as those discussed below.

- (1) It is not a substitute for good design. If used for its intended purpose it can be an aid to better design.
- (2) It will not solve item problems which may exist as a limitation to effective system design. It should define and focus attention on such problems and indicate the need for a design solution.
- (3) It will not, in itself, guarantee a system design. It is nothing more than a logical way of establishing "bookkeeping" which can be systematically analyzed for design reliability.

7.9 Fault Tree Analysis

The "fault tree" analysis (FTA) technique is a method for block diagramming constituent lower level elements. It determines, in a logical way, which failure modes at one level produce critical failures at a higher level in the system. The technique is useful in safety analysis where the discipline of block diagramming helps prevent an oversight in the basic FMEA discussed in the previous subsection.

As was previously mentioned, FMEA is considered a "bottoms up" analysis, whereas an FTA is considered a "top down" analysis. FMEAs and FTAs are compatible methods of risk analysis, with the choice of method dependent on the nature of the risk to be evaluated. There are some differences, however, because FTA is a top down analysis there is a higher probability of misinterpretation at the lowest level. On the other hand, FMEA starts at the lowest level, therefore will probably result in a better method of risk analysis (assuming lowest level data is available). Also, FMEA considers only single failures while FTA considers multiple failures. In general, FTA requires a greater skill level than FMEA.

Fault tree methods of analysis are particularly useful in functional paths of high complexity in which the outcome of one or more combinations of noncritical events may produce an undesirable critical event. Typical candidates for fault tree analysis are functional paths or interfaces which could have critical impact on flight safety, munitions handling safety, safety of operating and maintenance personnel, and probability of error free command in automated systems in which a multiplicity of redundant and overlapping outputs may be involved. The fault tree provides a concise and orderly description of the various combinations of possible

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

occurrences within the system which can result in a predetermined critical output event. However, performance of the fault tree analysis does require considerable engineering time and even then the quality of results is only as good as the validity of input data and accuracy of the fault tree logic.

Fault tree methods can be applied beginning in the early design phase, and progressively refined and updated to track the probability of an undesirable event as the design evolves. Initial fault tree diagrams might represent functional blocks (e.g., units, equipments, etc.), becoming more definitive at lower levels as the design materializes in the form of specific parts and materials. Results of the analysis are useful in the following applications:

- (1) Allocation of critical failure mode probabilities among lower levels of the system breakdown.
- (2) Comparison of alternative design configurations from a safety point of view.
- (3) Identification of critical fault paths and design weaknesses for corrective action.
- (4) Evaluation of alternative corrective action approaches.
- (5) Development of operational, test, and maintenance procedures to recognize and accommodate unavoidable critical failure modes.

Symbols commonly used in diagramming a fault tree analysis are shown in Figure 7.9-1. The basic relationships between functional reliability (success) block diagrams and the equivalent fault tree diagrams, using some of these symbols, are illustrated in Figures 7.9-2 and 7.9-3.

Success of the simple two element series system comprised of blocks A and B is given by $R = AB$; and the probability of system failure (i.e., unsuccessful or unsafe performance) is given by $\bar{R} = (1 - R) = 1 - AB$. When individual element unreliability (\bar{R}_i) is less than 0.1, the following approximations may be used to simplify computations in the fault tree logic diagram, with little (10%) error:

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

$$\begin{aligned}\overline{R} &= 1 - AB = 1 - (1 - \overline{A})(1 - \overline{B}) \\ &= \overline{A} + \overline{B} - \overline{AB} \approx \overline{A} + \overline{B}\end{aligned}$$

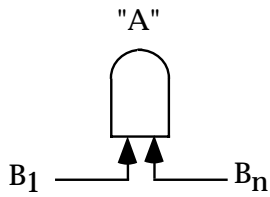
The two element block diagrams of Figure 7.9-2 is reconfigured as a simple parallel redundant system in Figure 7.9-3 to illustrate the treatment of parallel redundant elements in the fault tree logic diagram. Note that "AND" gates for the combination of successes (\overline{R}_s) become "OR" gates for the combination of failures (\overline{R}_f); and "OR" gates for R_s become "AND" gates for \overline{R}_f . This is illustrated in the series parallel network of Figure 7.9-3.

The fault tree analysis of critical failure modes should proceed as illustrated in the following steps.

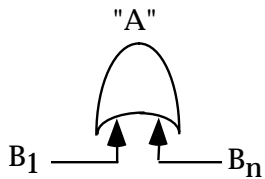
Step 1: Develop Function Reliability Block Diagram: Develop reliability block diagram for the system/equipment functional paths in which the critical failure mode is to be circumvented or eliminated. Define the critical failure mode in terms of the system level mal-performance symptom to be avoided. For example, the hypothetical firing circuit of Figure 7.9-4 is designed to ignite a proposed rocket motor in the following sequence:

- (1) Shorting switch S_1 is opened to enable launcher release and firing.
- (2) Firing switch S_2 is closed by the pilot to apply power to relay R_1 .
- (3) Relay R_1 activates the guidance and control (G&C) section.
- (4) Relay R_2 is activated by signal from the G&C section, closing the igniter firing circuit which starts the rocket motor.

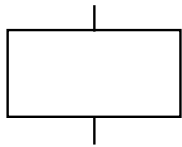
SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES



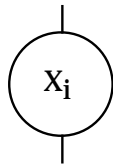
A logical "AND" gate - "A" exists if and only if all of B_1, B_2, \dots, B_n exist simultaneously.



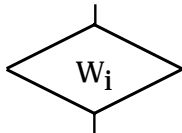
A logical inclusive "OR" gate - "A" exists if any B_1, B_2, \dots, B_n or any combination thereof



An event--usually the output of (or input to) and "AND" or an "OR" gate



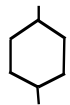
A failure rate of malfunction event-in terms of a specific circuit or component, represented by the symbol X with a numerical subscript



An event not developed further because of lack of information or because of lack of sufficient consequence. Represented by the symbol W with a numerical subscript



A connecting symbol to another part of the fault tree within the same major branch



An "inhibit" gate, used to describe the relationship between one fault and another. The input fault directly produces the output fault if the indicated conditions is satisfied

FIGURE 7.9-1: FAULT TREE ANALYSIS SYMBOLS

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

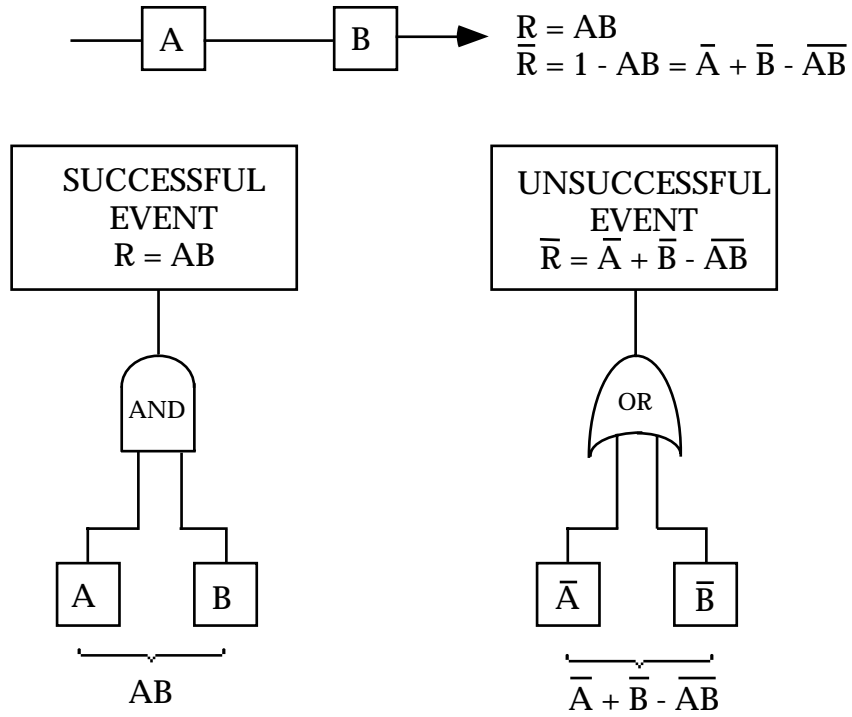


FIGURE 7.9-2: TRANSFORMATION OF TWO-ELEMENT SERIES RELIABILITY BLOCK DIAGRAM TO "FAULT TREE" LOGIC DIAGRAMS

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

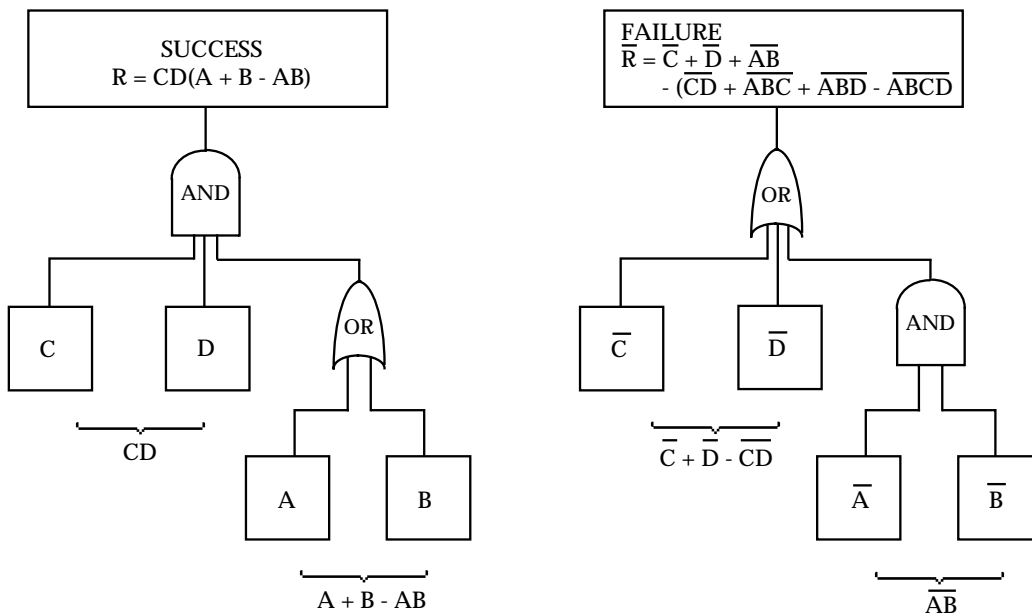
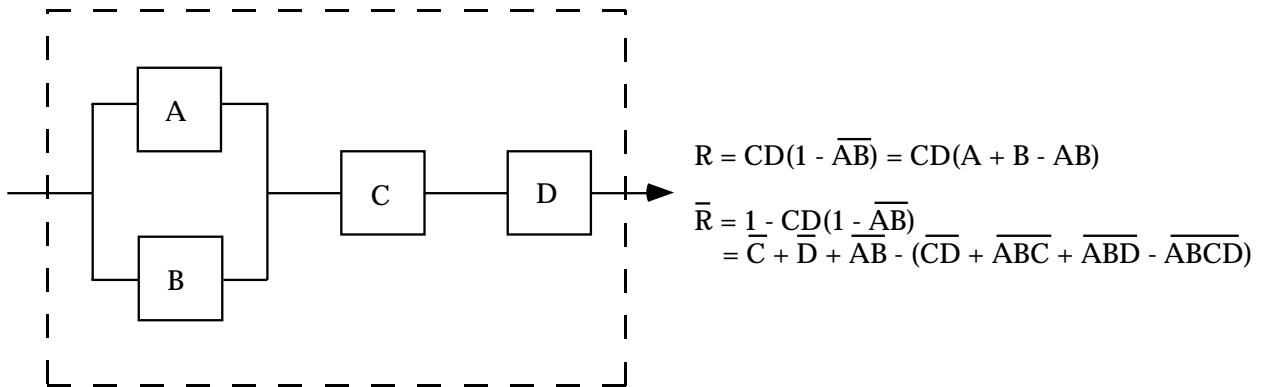


FIGURE 7.9-3: TRANSFORMATION OF SERIES/PARALLEL BLOCK DIAGRAM TO EQUIVALENT FAULT TREE LOGIC DIAGRAM

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

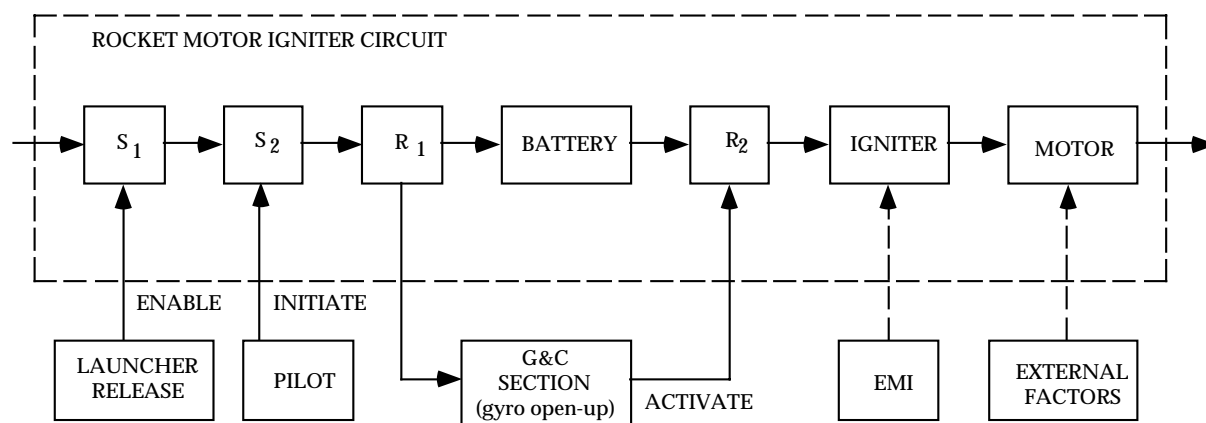


FIGURE 7.9-4: RELIABILITY BLOCK DIAGRAM OF HYPOTHETICAL ROCKET MOTOR FIRING CIRCUIT

The rocket motor can be inadvertently fired by premature ignition due to electronic failure, electromagnetic interference (EMI), or by external factors such as shock, elevated temperature, etc. These are the events to be studied in the fault tree analysis.

Step 2: Construct the Fault Tree: Develop the fault tree logic diagram relating all possible sequences of events whose occurrence would produce the undesired events identified in Step 1, e.g., inadvertent firing of the missile rocket motor. The fault tree should depict the paths that lead to each succeeding higher level in the functional configuration. Figure 7.9-5 illustrates the construction of one branch of the fault tree for the ignition circuit.

In constructing the fault tree for each functional path or interface within the reliability model, consideration must be given to the time sequencing of events and functions during the specified mission profile. Very often the operational sequence involves one or more changes in hardware configuration, functional paths, critical interfaces, or application stresses. When such conditions are found to apply, it is necessary to develop a separate fault tree for each operating mode, function, or mission event in the mission sequence.

Step 3: Develop Failure Probability Model: Develop the mathematical model of the fault tree for manual (or computer) computation of the probability of critical event occurrence on the basis of failure modes identified in the diagram. For example, the undesired system level critical failure mode identified in Figure 7.9-5 is "accidental rocket motor firing," given by the top level model as follows:

$$\overline{A} = \overline{B} + \overline{C} - \overline{BC}$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

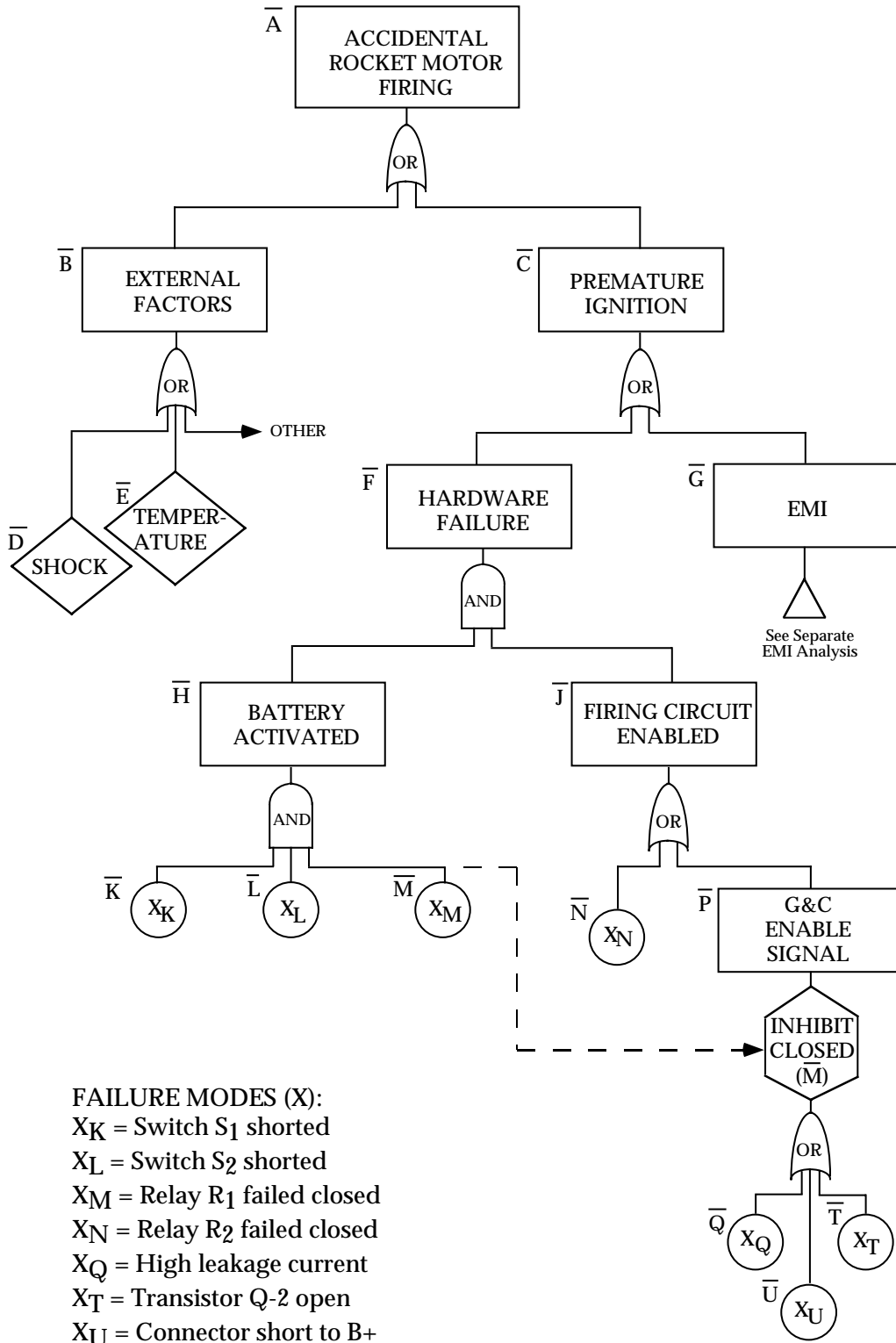


FIGURE 7.9-5: FAULT TREE FOR SIMPLIFIED ROCKET MOTOR FIRING CIRCUIT

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

As indicated in the figure, C represents the probability of accidental rocket motor firing due to premature ignition via the firing circuit either due to hardware failure (F) or electromagnetic interference (G), i.e.:

$$\overline{C} = \overline{F} + \overline{G} - \overline{FG}$$

Considering hardware failures only, the probability of premature ignition due to hardware failure is given by:

$$\overline{F} = \overline{HJ}$$

where:

$$\overline{H} = \overline{KLM}$$

$$\overline{J} = \overline{N} + \overline{P} - \overline{NP}$$

$$\overline{P} = \overline{Q} + \overline{T} + \overline{U} = (\overline{QT} + \overline{QU} + \overline{TU} - \overline{QTU})$$

Step 4: Determine Failure Probabilities or Identified Failure Modes: Determine probability of occurrence (i.e., probability of failure) in each event or failure mode identified in the model. Compute safety parameters at the system level by applying the failure data in the models derived in Step 3.

Assume, for example, the following failure probabilities in the premature ignition branch of the fault tree:

$$\overline{K} = 50 \times 10^{-3}$$

$$\overline{L} = 100 \times 10^{-3}$$

$$\overline{M} = 40 \times 10^{-3}$$

$$\overline{N} = 5 \times 10^{-3}$$

$$\overline{Q} = 2 \times 10^{-3}$$

$$\overline{T} = 1 \times 10^{-3}$$

$$\overline{U} = 0.5 \times 10^{-3}$$

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Using the bottom up approach, combine these data in the failure probability models developed in Step 3, and estimate the system level probability as follows:

$$\begin{aligned}\overline{P} &= \overline{Q} + \overline{T} + \overline{U} - (\overline{QT} + \overline{QU} + \overline{TU} - \overline{QTU}) \\ &= (2 + 1 + 0.5)10^{-3} - [(2 + 1 + 0.5)10^{-6} - (1)10^{-9}] \\ &\approx 3.5 \times 10^{-3}\end{aligned}$$

Higher order (product) terms in the model can be dropped in the P model since the values of individual terms are much less than 0.10.

Combining \overline{P} with \overline{N} to find \overline{J} yields:

$$\begin{aligned}\overline{J} &= \overline{N} + \overline{P} - \overline{NP} \\ &= 5 \times 10^{-3} + 3.5 \times 10^{-3} - 17.5 \times 10^{-6} \\ &\approx 8.5 \times 10^{-3}\end{aligned}$$

This is the probability of accidental firing circuit operation conditional on relay R₁ having failed in the closed position (i.e., M) in the battery branch of the fault tree. In the battery branch, the battery can be accidentally activated only if switches S₁ and S₂ fail in the short mode, and if relay R₁ fails in the closed position, given by:

$$\begin{aligned}\overline{H} &= \overline{KLM} \\ &= (50 \times 10^{-3}) (100 \times 10^{-3}) (40 \times 10^{-3}) \\ &= 200 \times 10^{-6}\end{aligned}$$

Probability of premature ignition because of hardware failure is then estimated from:

$$\begin{aligned}\overline{F} &= \overline{HJ} = (200 \times 10^{-6}) (8.5 \times 10^{-3}) \\ &= 1.70 \times 10^{-6}\end{aligned}$$

Assume that the EMI analysis discloses a probability of accidental ignition ($\overline{G} = 5 \times 10^{-6}$) due to exposure to specified level of RF radiation in the operating environment. The probability of premature ignition to either cause (hardware failure or EMI exposure) is given by:

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

$$\begin{aligned}
\overline{C} &= \overline{F} + \overline{G} - \overline{FG} \\
&\approx (1.70 \times 10^{-6}) + (5 \times 10^{-6}) - (1.70 \times 10^{-6})(5 \times 10^{-6}) \\
&\approx 6.70 \times 10^{-6}
\end{aligned}$$

Assume that failure data accrued during rocket motor qualification tests indicates $\overline{D} = 2.5 \times 10^{-6}$ and $\overline{E} = 12.5 \times 10^{-6}$ under specified conditions and levels of exposure. Under these circumstances,

$$\begin{aligned}
\overline{B} &= \overline{D} + \overline{E} - \overline{DE} \\
&= (2.5 \times 10^{-6}) + (12.5 \times 10^{-6}) - (2.5 \times 10^{-6})(12.5 \times 10^{-6}) \\
\overline{B} &= 15 \times 10^{-6}
\end{aligned}$$

Probability of accidental rocket motor firing during the handling and loading sequence is then:

$$\begin{aligned}
\overline{A} &= \overline{B} + \overline{C} - \overline{BC} \\
&\approx (15 \times 10^{-6}) + (6.70 \times 10^{-6}) - (15 \times 10^{-6})(6.75 \times 10^{-6}) \\
&\approx 21.7 \times 10^{-6}
\end{aligned}$$

That is, approximately 22 premature rocket motor firings per million missile load/launch attempts.

Failure rate values for most standard electronic and electromechanical parts are available in MIL-HDBK-217. The most recent document for failure rate values for mechanical parts is Reference [14]. Failure rate data for new parts and more recently developed "high reliability" parts may not be available in these sources, however. In such cases, it becomes necessary to draw on vendor certified data or special tests.

In the absence of complete and validated failure rate/failure mode data for all inputs, a preliminary fault tree analysis can be performed using conservative estimates of failure rates in the critical failure modes. This preliminary analysis will identify those input values which have little effect, as well as those having a critical effect on system performance. The latter can then be investigated in depth by testing.

Evaluation of the fault tree model may reveal that the conservatively estimated values are sufficient to satisfy the performance goal. Other values will warrant further study. In some cases, it may even be more expedient to change the design than to validate a data value.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Step 5: Identify Critical Fault Paths: When the probability of an unsafe failure mode at the system level exceeds specification tolerances, identify the critical paths which contribute most significantly to the problem. For example, both paths in the preceding analysis contribute about equally to the total problem because of environmental sensitivity - ignition circuit to EMI, and propellant insulation to high ambient temperature.

7.9.1 Discussions of FTA Methods

There are basically three methods for solving fault trees: (1) direct simulation (Reference [81]), (2) Monte Carlo (Reference [82]), and (3) direct analysis (Reference [83]).

Direct simulation basically uses Boolean logic hardware (similar to that in digital computers) in a one-to-one correspondence with the fault tree Boolean logic to form an analog circuit. This method usually is prohibitively expensive. A hybrid method obtains parts of the solution using the analog technique and parts from a digital calculation, in an effort to be cost competitive. Because of the expense involved, this method rarely is used.

Monte Carlo methods are perhaps the most simplest in principle but in practice can be expensive. Since Monte Carlo is not practical without the use of a digital computer, it is discussed in that framework. The most easily understood Monte Carlo technique is called "direct simulation." The term "simulation" frequently is used in conjunction with Monte Carlo methods, because Monte Carlo is a form of mathematical simulation. (This simulation should not be confused with direct analog simulation.) Probability data are provided as input, and the simulation program represents the fault tree on a computer to provide quantitative results. In this manner, thousands or millions of trials can be simulated. A typical simulation program involves the following steps.

- (1) Assign failure data to input fault events within the tree and, if desired, repair data.
- (2) Represent the fault tree on a computer to provide quantitative results for the overall system performance, subsystem performance, and the basic input event performance.
- (3) List the failure that leads to the undesired event and identify minimal cut sets contributing to the failure.
- (4) Compute and rank basic input failure and availability performance results.

In performing these steps, the computer program simulates the fault tree and, using the input data, randomly selects the various parameter data from assigned statistical distributions; and then tests whether or not the TOP event occurred within the specified time period. Each test is a trial, and a sufficient number of trials is run to obtain the desired quantitative resolution. Each time the TOP event occurs, the contributing effects of input events and the logical gates causing the specified TOP event are stored and listed as computer output. The output provides a detailed perspective of the system under simulated operating conditions and provides a quantitative basis to support objective decisions.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

A number of computer programs have been developed for fault tree analysis. References [83] - [85] provide additional information on fault tree analysis.

In practice, the methods used for fault tree analysis will depend on which ones are available for the computer being used. It will rarely, if ever, be worthwhile generating a computer program especially for a particular problem.

7.10 Sneak Circuit Analysis (SCA)

7.10.1 Definition of Sneak Circuit

A sneak circuit is an unexpected path or logic flow within a system which, under certain conditions, can initiate an undesired function or inhibit a desired function. The path may consist of hardware, software, operator actions, or combinations of these elements. Sneak circuits are not the result of hardware failure but are latent conditions, inadvertently designed into the system or coded into the software program, which can cause it to malfunction under certain conditions. Categories of sneak circuits are:

- (1) Sneak paths which cause current, energy, or logical sequence to flow along an unexpected path or in an unintended direction.
- (2) Sneak timing in which events occur in an unexpected or conflicting sequence.
- (3) Sneak indications which cause an ambiguous or false display of system operating conditions, and thus may result in an undesired action taken by an operator.
- (4) Sneak labels which incorrectly or imprecisely label system functions, e.g., system inputs, controls, displays, buses, etc., and thus may mislead an operator into applying an incorrect stimulus to the system.

Figure 7.10-1 depicts a simple sneak circuit example. With the ignition off, the radio turned to the on position, the brake pedal depressed, and the hazard switch engaged, the radio will power on with the flash of the brake lights.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

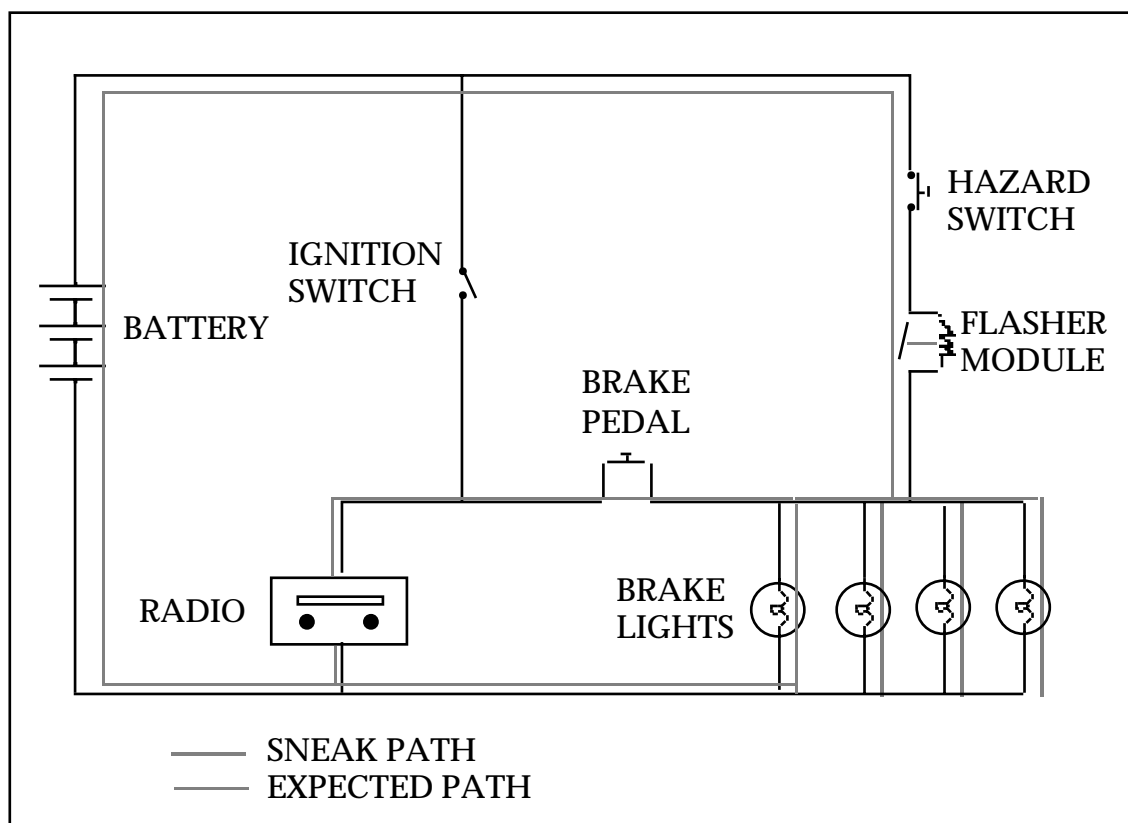


FIGURE 7.10-1: AUTOMOTIVE SNEAK CIRCUIT

7.10.2 SCA: Definition and Traditional Techniques

Sneak circuit analysis is the term that has been applied to a group of analytical techniques which are intended to methodically identify sneak circuits in systems. SCA techniques may be either manual or computer assisted, depending on system complexity. Current SCA techniques which have proven useful in identifying sneak circuits in systems include:

- (1) Sneak Path Analysis: A methodical investigation of all possible electrical paths in a hardware system. Sneak path analysis is a technique used for detecting sneak circuits in hardware systems, primarily power distribution, control, switching networks, and analog circuits. The technique is based on known topological similarities of sneak circuits in these types of hardware systems.
- (2) Digital Sneak Circuit Analysis: An analysis of digital hardware networks for sneak conditions, operating modes, timing races, logical errors, and inconsistencies. Depending on system complexity, digital SCA may involve the use of sneak path analysis techniques, manual or graphical analysis, computerized logic simulators or computer aided design (CAD) circuit analysis.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

- (3) Software Sneak Path Analysis: An adaptation of sneak path analysis to computer program logical flows. The technique is used to analyze software logical flows by comparing their topologies to those with known sneak path conditions in them.

7.10.3 New SCA Techniques

SCA is a powerful analytical tool. Historically, however, SCA has been expensive and performed late in the design cycle after all of the design documentation was virtually complete. Thus, any subsequent design changes resulting from the SCA were difficult to make and costly to implement. Therefore, the use of SCA was usually limited to only items and functions which were critical to safety or mission success or where other techniques were not proven to be effective.

This situation, however, has begun to change. Some Air Force publications shed considerable new light on SCA techniques. These publications are:

- (1) *Sneak Circuit Analysis for the Common Man*, RADC-TR-89-223, Reference [86]
- (2) *Integration of Sneak Circuit Analysis with Design*, RADC-TR-90-109, Reference [87]
- (3) *Automated Sneak Circuit Analysis Technique (SCAT)*, Reference [88]
- (4) *SCAT: Sneak Circuit Analysis Tool, Version 3.0, RL-TR-95-232*, Reference [89]

SCAT is an interactive "Expert System" design tool to assist the designer in identifying and eliminating both sneak circuits and design concerns early in the design phase. In contrast to normal sneak circuit analyses, SCAT analyses are performed at the assembly level, rather than at the system level. Thus SCAT is not considered to be a replacement for a complete Sneak Circuit Analysis. However, since SCAT is used much earlier in the design phase, it may result in the elimination of many (but not all) potential sneak circuits and decrease the later need for a complete sneak circuit analysis.

Specifically, the referenced publications identify some Sneak Circuit Design Rules, Functional Guidelines, and Device Guidelines that can be applied much earlier in the design phase. This new approach helps significantly to demystify the SCA techniques and enables the Sneak Circuit Analysis to become a much more cost effective reliability design tool.

Because the technology of hardware and software is rapidly evolving, new SCA techniques will undoubtedly evolve as well. SCA will also find applications in non-electrical/electronic systems where analogous situations of energy flow, logic timing, etc. are encountered.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.10.4 Examples of Categories of SNEAK Circuits

The broad categories of sneak circuits were described in section 7.10.1. Following are some specific examples of each of the categories.

Sneak Path. A sneak path is one which allows current or energy to flow along an unsuspected path or in an unintended direction. There are two distinct subsets of this category. They are:

Sneak Path, Enable occurs when the sneak path initiates an undesired function or result under certain conditions, but not all conditions. An example of this class is shown in Figure 7.10-2.

The electrical power regulator output circuits shown in Figure 7.10-2 represent a portion of the power distribution system in an air vehicle instrument. The sneak path is identified by the arrows along the connection between terminal E6 and pin A of connector J16. This sneak path connects the +4VDC output of regulator VR1 to the +12VDC output of regulator VR2. This path would permit excessive current to flow from the +12VDC output into the +4VDC loads. The result could be failure of either or both regulators (VR1, VR2) and possible catastrophic burnout of the +4VDC loads. Any of these failures would result in the loss of the instrument. If immediate failure did not occur, out-of-tolerance operation of the +4VDC loads would occur due to the 3-times normal voltage being applied. The recommended correction was to remove the wire connection between terminal E6 and pin A of connector J16.

Sneak Path, Inhibit occurs when the sneak path prevents a desired function or results under certain conditions, but not all conditions. An example of this is shown in Figure 7.10-3.

The circuit shown in Figure 7.10-3 was used in a satellite to provide isolation of the power circuits in a double redundant subsystem. The technique removes both power and power ground from the nonoperating backup circuit. The sneak paths which bypass the Q3 grounding switches are identified in Figure 7.10-3 by the arrows placed along each path. When the hardware was wired as shown, total isolation no longer existed and the design intent was violated. The recommended correction was to remove the wire in cable W62 connecting pin 27 of connector P12 to terminal E5 of the single point ground (SPG). When wired as recommended, the power ground switching can be performed by either channel's Q3 and the SPG at E4.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

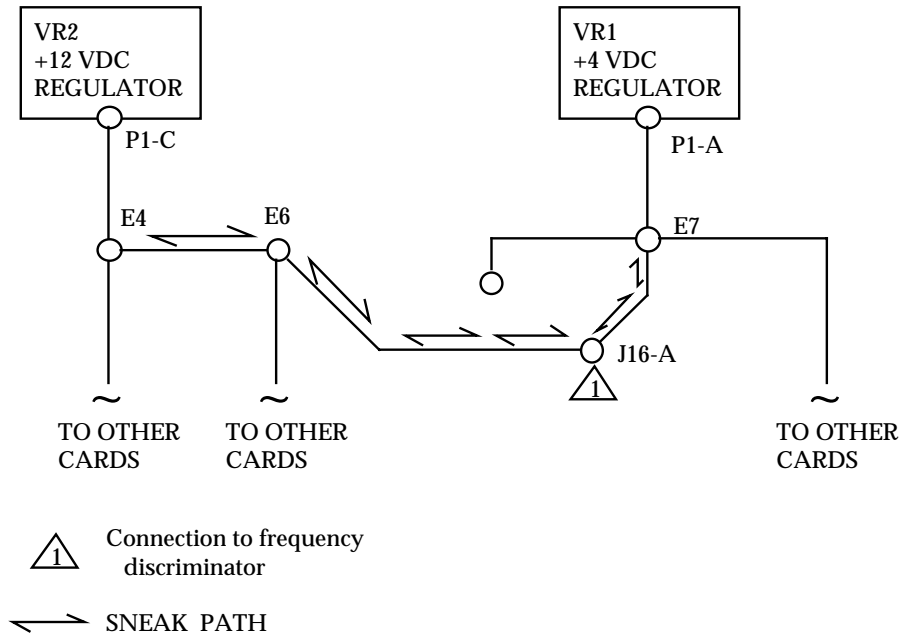


FIGURE 7.10-2: SNEAK PATH ENABLE

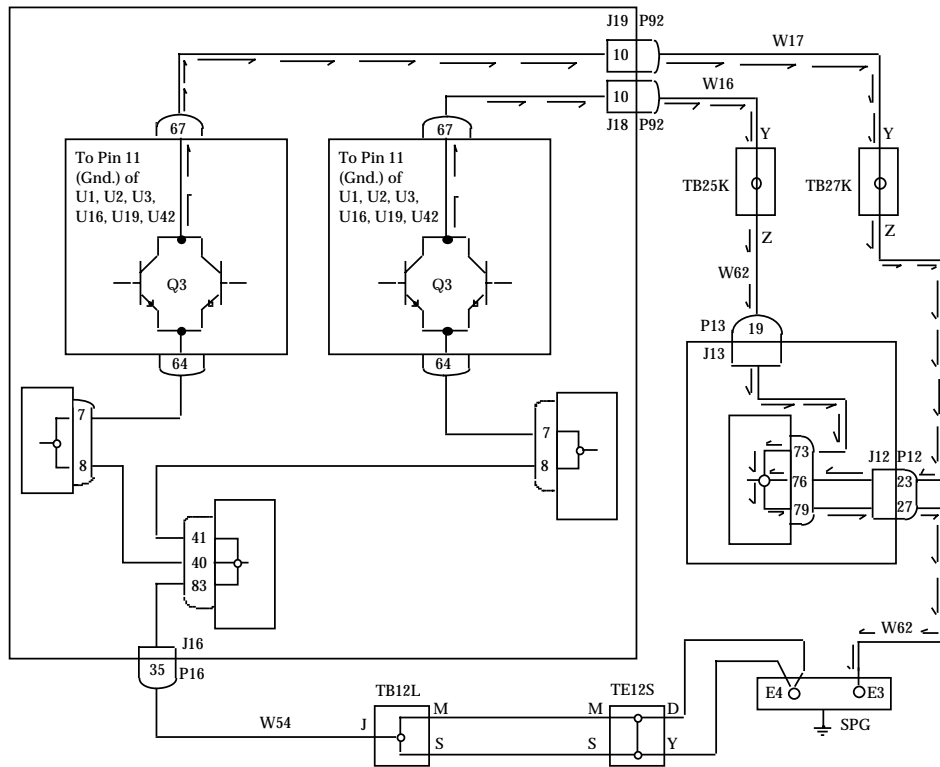


FIGURE 7.10-3: REDUNDANT CIRCUIT SWITCHED GROUND

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Sneak Timing: A sneak timing condition is one which causes functions to be inhibited or to occur at an unexpected or undesired time. The example in Figure 7.10-4a illustrates a sneak that occurred in the digital control circuitry of a mine. The enable logic for U4 and U5 allows them, briefly, to be enabled simultaneously. Being CMOS devices in a "wired or" configuration, this allows a potential power-to-ground short through the two devices, damaging or destroying them during operation.

Sneak Indication: An indication which causes ambiguous or incorrect displays. Figure 7.10-4c illustrates a sneak indication which occurred in a sonar power supply system. The MOP (Motor Operated Potentiometer) OFF and ON indicators do not, in fact, monitor the status of the MOP motor. Switch S3 could be in the position shown, providing an MOP ON indication even through switches S1 or S2 or relay contacts K1 or K2 could be open, inhibiting the motor.

Sneak Label: A label on a switch or control device which would cause incorrect actions to be taken by operators. The example in Figure 7.10-4b taken from an aircraft radar system, involves a circuit breaker which provides power to two disparate systems, only one of which is reflected in its label. An operator attempting to remove power from the liquid coolant pump would inadvertently deactivate the entire radar.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

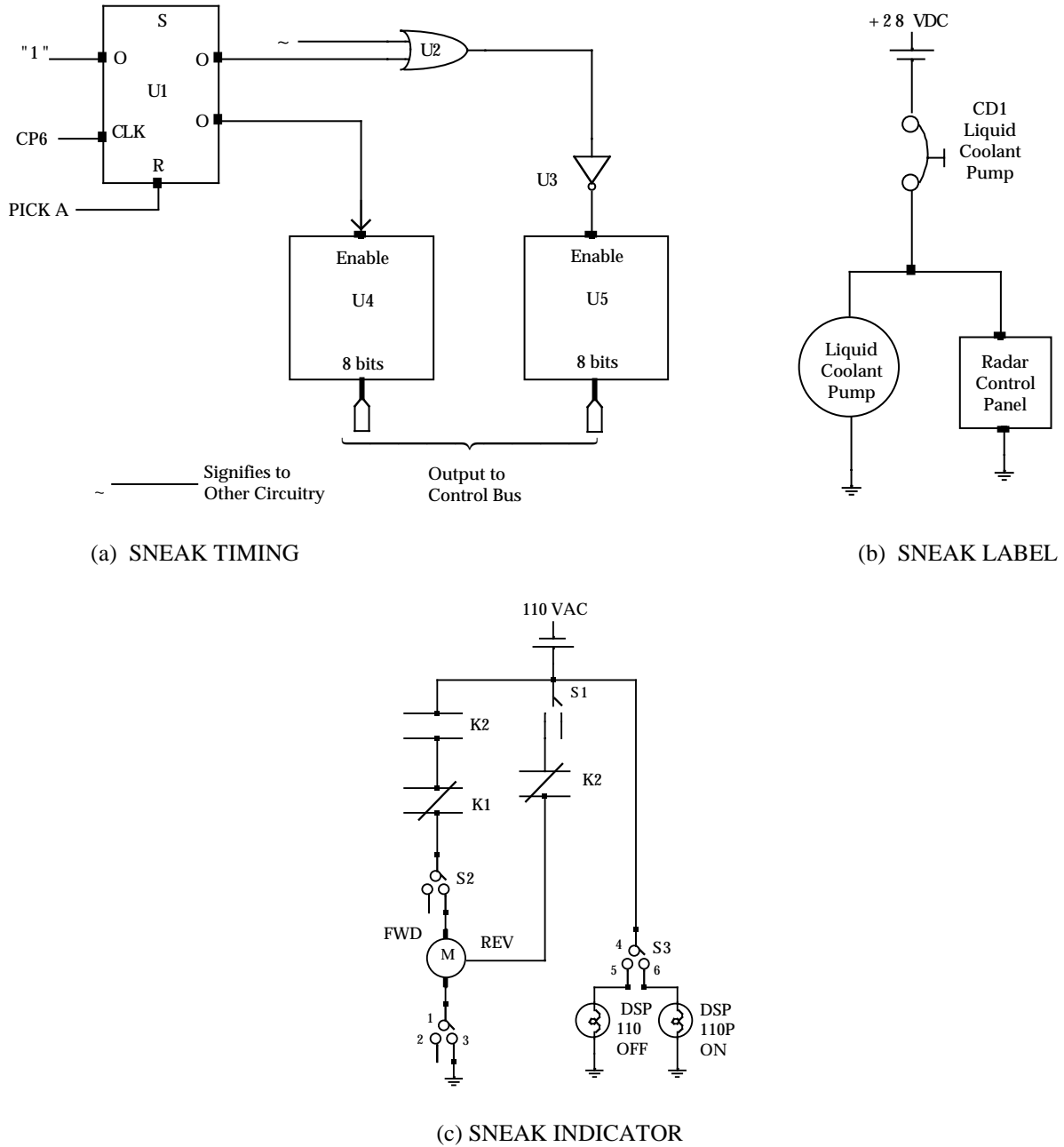


FIGURE 7.10-4: EXAMPLES OF CATEGORIES OF SNEAK CIRCUITS

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.10.5 SCA Methodology**7.10.5.1 Network Tree Production**

The first major consideration that must be satisfied to identify sneak circuit conditions is to ensure that the data being used for the analysis represent the actual "as built" circuitry of the system. Functional, integrated, and system level schematics do not always represent the actual constructed hardware. Detailed manufacturing and installation schematics must be used, because these drawings specify exactly what was built, contingent on quality control checks, tests, and inspection. However, manufacturing and installation schematics rarely show complete circuits. The schematics are laid out to facilitate hookup by technicians without regard to circuit or segment function. As a result, analysis from detail schematics is extremely difficult. So many details and unapparent continuities exist in these drawings that an analyst becomes entangled and lost in the maze. Yet, these schematics are the data that must be used if analytical results are to be based on true electrical continuity. The first task of the sneak analyst is, therefore, to convert this detailed, accurate information into a form usable for analytical work. The magnitude of data manipulation required for this conversion necessitates the use of computer automation in most cases.

Automation has been used in sneak circuit analysis since 1970 as the basic method for tree production from manufacturing detail data. Computer programs have been developed to allow encoding of simple continuities in discrete "from-to" segments extracted from detail schematics and wire lists. The encoding can be accomplished without knowledge of circuit function. The computer connects associated points into paths and collects the paths into node sets. The node sets represent interconnected nodes that make up each circuit. Plotter output of node sets and other reports are generated by the computer to enable the analyst to easily sketch accurate topological trees. The computer reports also provide complete indexing of every component and data point to its associated tree. This feature is especially useful in cross indexing functionally related or interdependent trees, in incorporating changes, and in troubleshooting during operational support.

7.10.5.2 Topological Pattern Identification

Once the network trees have been produced, the next task of the analyst is to identify the basic topological patterns that appear in each tree. Five basic patterns exist for hardware SCA: (1) single line (no-node) topograph, (2) ground dome, (3) power dome, (4) combination dome, and (5) "H" pattern. These patterns are illustrated in Figure 7.10-5. One of these patterns or several in combination will characterize the circuitry shown in any given network tree. Although, at first glance, a given circuit may appear more complex than these basic patterns, closer inspection reveals that the circuit is actually composed of these basic patterns in combination. In examining each node in the network tree, the sneak circuit analyst must identify the topographical pattern or patterns incorporating the node and apply the basic clues that have been found to typify sneak circuits involving that particular pattern.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

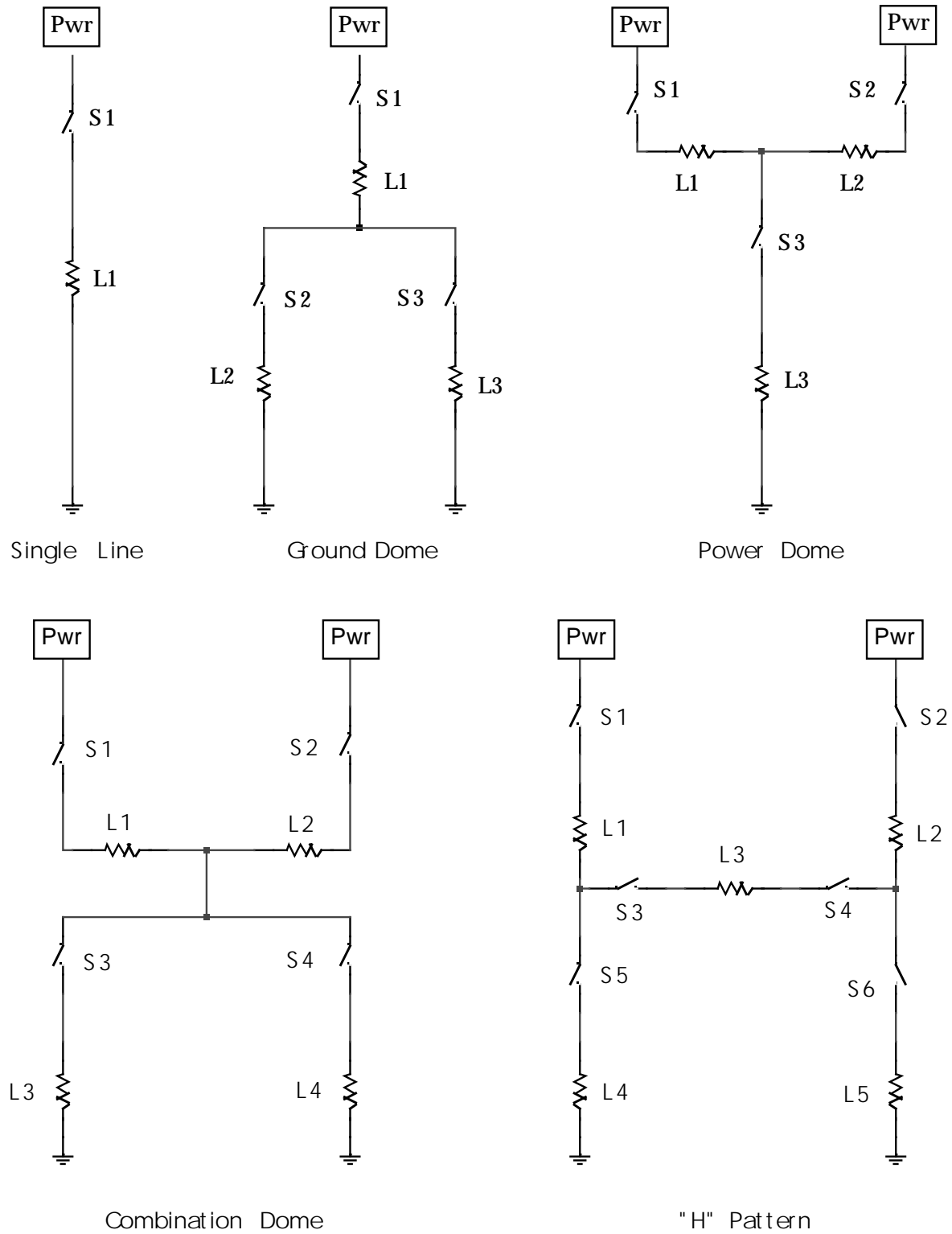


FIGURE 7.10-5: BASIC TOPOGRAPHS

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.10.5.3 Clue Application

Associated with each pattern is a list of clues to help the analyst identify sneak circuit conditions. These lists were first generated during the original study of historical sneak circuits. The lists were updated and revised during the first several years of applied sneak circuit analysis. Now, the list of clues provides a guide to all possible design flaws that can occur in a circuit containing one or more of the five basic topological configurations, subject to the addition of new clues associated with new technological developments. The lists consist of a series of questions that the analyst must answer about the circuit to ensure that it is sneak free.

As an example, the single line topograph (Figure 7.10-5) would have clues such as:

- (a) Is switch S open when load L is desired?
- (b) Is switch S closed when load L is not desired?

Obviously, sneak circuits are rarely encountered in this topograph because of its simplicity. Of course, this is an elementary example and is given primarily as the default case which covers circuitry not included by the other topographs.

With each successive topograph, the clue list becomes longer and more complicated. The clue list for the "H" pattern includes over 100 clues. This pattern, because of its complexity, is associated with more sneak circuits than any of the previous patterns. Almost half of the critical sneak circuits identified to date can be attributed to the "H" patterns. Such a design configuration should be avoided whenever possible. The possibility of current reversal through the "H" crossbar is the most commonly used clue associated with "H" pattern sneak circuits.

7.10.6 Software Sneak Analysis

In 1975, a feasibility study was performed resulting in the development of a formal technique, involving the use of mathematical graph theory, electrical sneak theory, and computerized search algorithms, to identify sneaks in software programs. A software sneak is defined as a logic control path which causes an unwanted operation to occur or which bypasses a desired operation, without regard to failures of the hardware system to respond as programmed.

The feasibility study concluded that:

- (1) Software Sneak Analysis is a viable means of identifying certain classes of software problems.
- (2) Software Sneak Analysis works equally well on different software languages.
- (3) Software Sneak Analysis does not require execution of the software to detect problems.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

The Software Sneak Analysis technique has evolved along lines very similar to hardware Sneak Circuit Analysis. Topological network trees are used with electrical symbology representing the software commands to allow easy cross analysis between hardware and software trees and to allow the use of a single standardized analysis procedure.

Since topological pattern recognition is the keystone of both Sneak Circuit Analysis and Software Sneak Analysis, the overall methodologies are quite similar. The software package to be analyzed must be encoded, processed, and reduced to a standardized topographical format, the basic topological patterns identified and the appropriate problem clues applied to each pattern. For software, it has been found that six basic patterns exist: the Single Line, the Return Dome, the Iteration/Loop Circuit, the Parallel Line, the Entry Dome, and the Trap Circuit, as shown in Figure 7.10-6.

Although at first glance, a given software tree may appear to be more complex than these basic patterns, closer inspection will reveal that the code is actually composed of these basic structures in combination. As each node in the tree is examined, the analyst must identify which pattern or patterns include that node. The analyst then applies the basic clues that have been found to typify the sneaks involved with that particular structure. These clues are in the form of questions that the analyst must answer about the use and interrelationships of the instructions that are elements of the structure. These questions are designed to aid in the identification of the sneak conditions in the instruction set which could produce undesired program outputs.

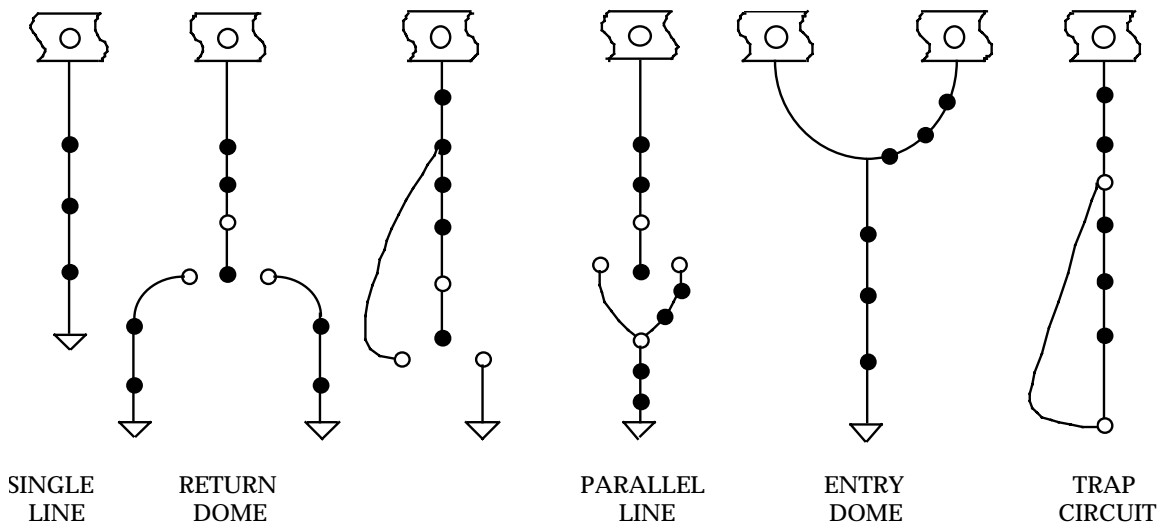


FIGURE 7.10-6: SOFTWARE TOPOGRAPHS

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Software sneaks are classified into four basic types:

- (1) Sneak Output: The occurrence of an undesired output.
- (2) Sneak Inhibit: The undesired inhibition of an output.
- (3) Sneak Timing: The occurrence of an undesired output by virtue of its timing or mismatched input timing
- (4) Sneak Message: The program message does not adequately reflect the condition.

Figure 7.10-7 illustrates a software sneak which occurred in the operating software of a military aircraft. Figure 7.10-7a illustrates the design intent of the section of software with the sneak. When the actual code was produced, however, the two tests were inadvertently interchanged. The network tree of the actual software code (see Figure 7.10-7b) makes the sneak readily apparent. This historical problem was uncovered only during the software system integrated testing when it was found that the instructions represented by LOAD 1 could never be executed.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

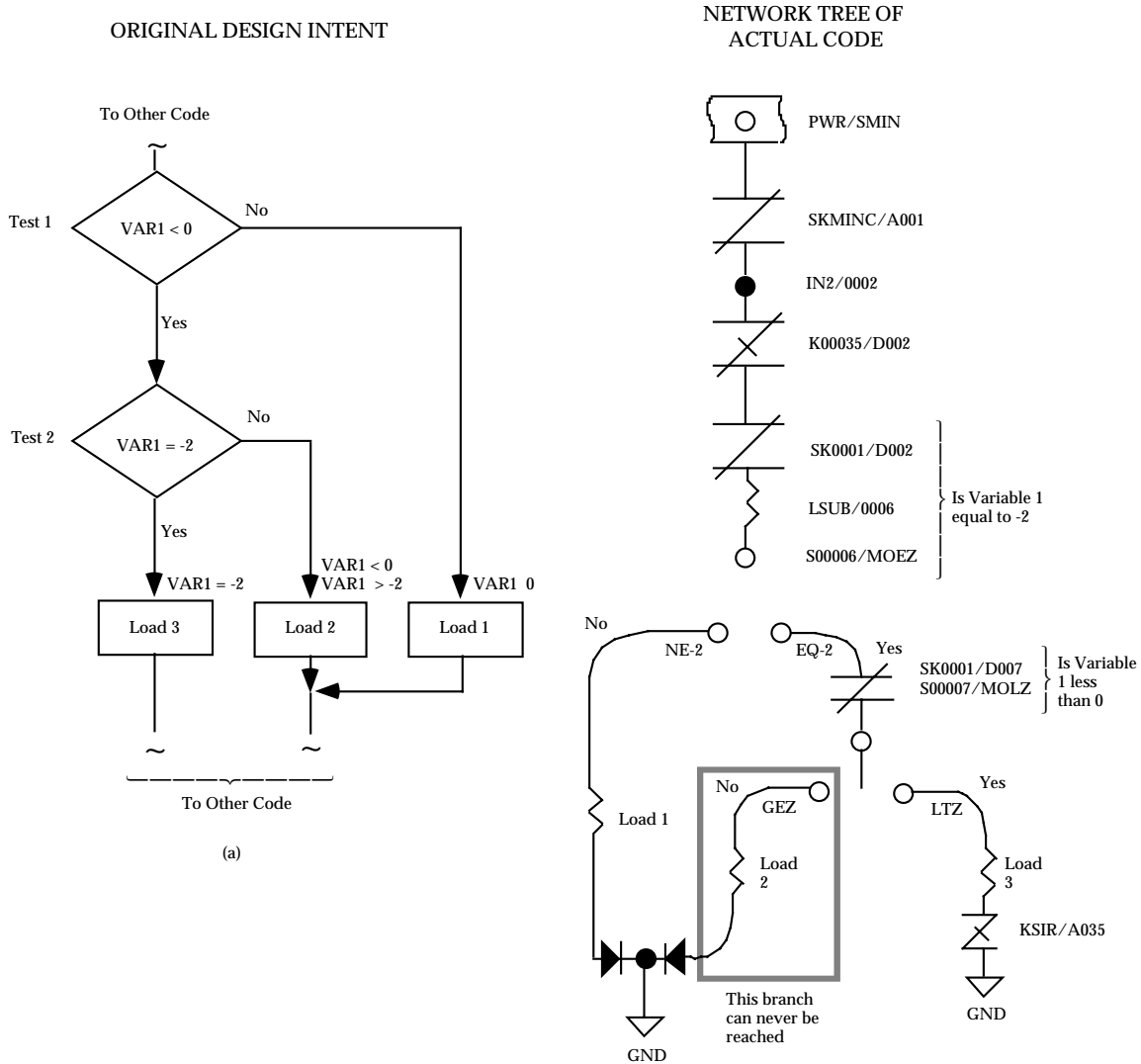


FIGURE 7.10-7: SOFTWARE SNEAK EXAMPLE

7.10.7 Integration of Hardware/Software Analysis

After a sneak circuit analysis and a software sneak analysis have been performed on a system, the interactions of the hardware and software can readily be determined. For this purpose, the analyst has diagrammatic representations of these two elements of the system in a single standardized format. The effect of a control operation that is initiated by some hardware element can be traced through the hardware trees until it impacts the system software. The logic flow can then be traced through the software trees to determine its ultimate impact on the system. Similarly, the logic sequence of a software initiated action can be followed through the software and electrical network trees until its eventual total system impact can be assessed.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

The joint analysis of a system's software and hardware circuitry previously described is simply called Sneak Analysis. Sneak Analysis helps provide visibility of the interactions of a system's hardware and software and hence will help reduce the difficulties involved in the proper integration of two such diverse, complex system designs. As hardware and software systems increase in complexity, the use of interface bridging analysis tools, such as Sneak Analysis, becomes imperative to help ensure the safety of the total system.

7.10.8 Summary

SCA is different from other analyses commonly performed in a reliability program in a number of important ways. SCA generally concentrates on the interconnections, interrelationships, and interactions of system components rather than on the components themselves. SCA concentrates more on what might go wrong in a system rather than on verifying that it works right under some set of test conditions. The SCA technique is based on a comparison with other systems which have "gone wrong", not because of part failures, but because of design oversight or because a human operator made a mistake. The consequence of this subtly different perspective may be very important, because it tends to concentrate on and find problems which may be hidden from the perspectives of other analytical techniques.

For example FMEA/FMECA differs from SCA in that it predicts and quantifies the response of a system to failures of individual parts or subsystems. An FMECA is an analysis of all expected failure modes and their effect on system performance. FMECA results are often used in maintainability predictions, in the preparation of maintenance dependency charts, and to establish sparing requirements. SCA, on the other hand, considers possible human error in providing system inputs while FMECA does not. In this regard the two types of analysis tend to complement one another.

Fault Tree Analysis is a deductive method in which a catastrophic, hazardous end result is postulated and the possible events, faults, and occurrences which might lead to that end event are determined. Thus, FTA overlaps SCA in purpose because the FTA is concerned with all possible faults, including component failures as well as operator errors.

Concerning the availability of SCA computer programs, the original SCA computer programs developed under government contract with (NASA), Johnson Spacecraft Center, Houston, Texas, on the Apollo program are available to all industry and government agencies. They can be purchased from Computer Software Management and Information Center (COSMIC), University of Georgia, 112 Barrow Hall, Athens, Georgia 30602. These programs may not be current. However, several companies have purchased these programs and updated them. The improved programs and the accompanying analysis techniques are considered proprietary by most companies.

References [86] - [93] provide more details on SCA.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.11 Design Reviews

7.11.1 Introduction and General Information

The purpose of a design review is to ensure that each design has been studied to identify possible problems, to improve the item where necessary, and to provide assurance that the most satisfactory design has been selected to meet the specified requirements. Design reviews are critical audits of all pertinent aspects of the design and are conducted at critical milestones in an acquisition program. They are essential to reliability engineering.

The formal review (depicted in Figure 7.11-1) of equipment design concepts and design documentation for both hardware and software is an essential activity in any development program. Standard procedures should be established to conduct a review of all drawings, specifications, and other design information by a supplier's technical groups such as engineering, reliability engineering, and manufacturing engineering. (Ideally, representatives of these and other key groups would comprise one or more integrated product development teams (IPDTs)). This review should be accomplished prior to the release of design information for manufacturing operations. Such a review is an integral part of the design-checking reviews. Responsible members of each reviewing department meet to consider all design documents, resolve any problem areas uncovered, and signify their acceptance of the design documentation by approving the documents for their departments.

Reliability engineering, ideally as part of an IPDT, should conduct an intensive review of the system during initial design. A design review, from a reliability perspective, includes the following major tasks:

- (1) Analysis of environment and specifications
- (2) Formal design review of engineering information
- (3) Reliability participation in all checking reviews

Prior to the formal review, the requirements defined in applicable specifications are reviewed. The expected environmental extremes of the system are studied to determine suspected detrimental effects on equipment performance. Checklists, based on these studies, are prepared to ensure that the objectives of formal design reviews are fulfilled.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

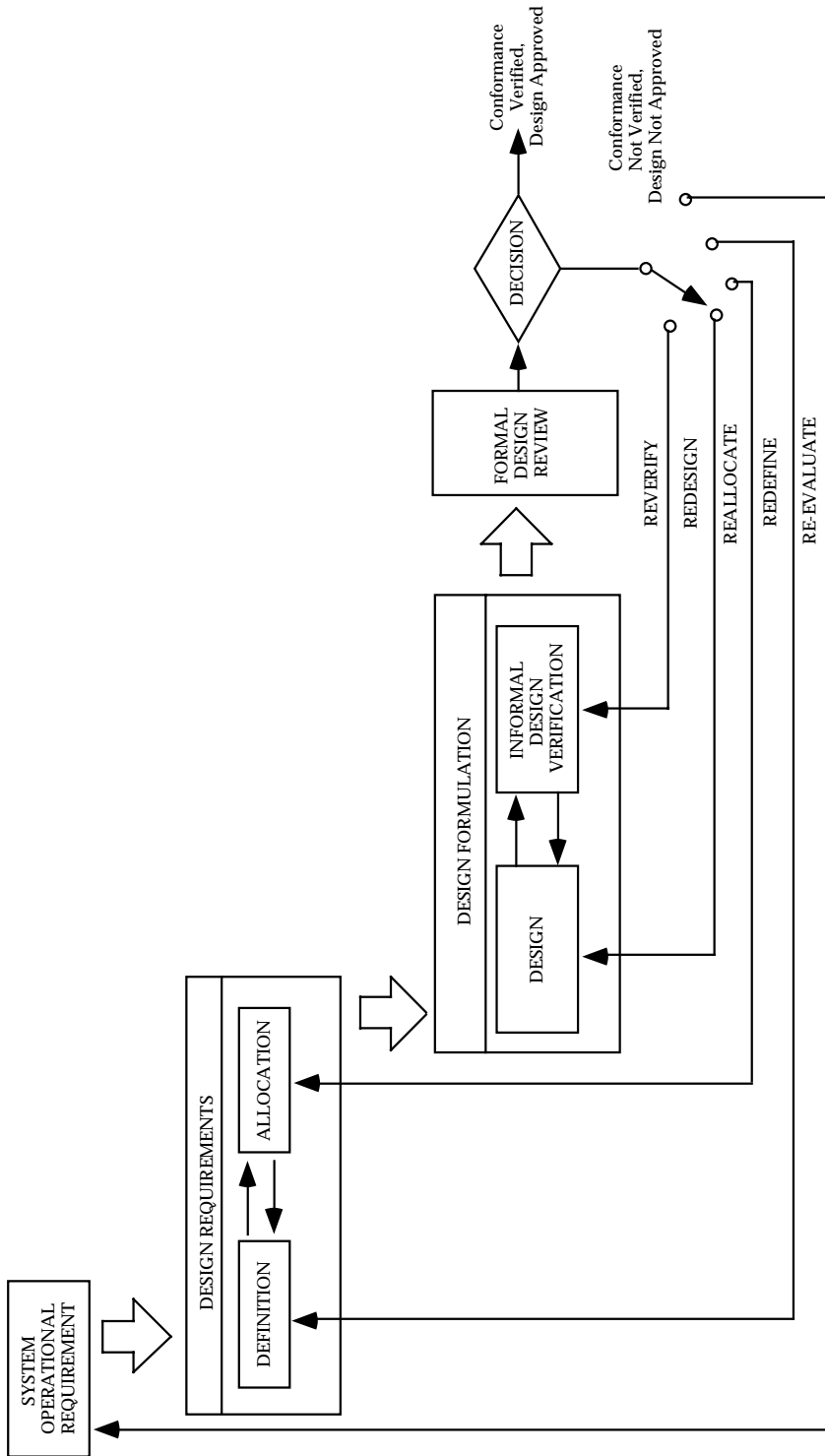


FIGURE 7.11-1: DESIGN REVIEW AS A CHECK VALVE IN THE SYSTEM ENGINEERING CYCLE

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

The formal design review, which is instituted prior to the release of drawings, is intended to do the following in regard to reliability:

- (1) Detect any conditions that could degrade equipment reliability
- (2) Provide assurance of equipment conformance to applicable specifications
- (3) Ensure the use of preferred or standard parts as far as practical
- (4) Ensure the use of preferred circuitry as far as possible
- (5) Evaluate the electrical, mechanical, and thermal aspects of the design
- (6) Review stress analysis to ensure adequate part derating
- (7) Ensure accessibility of all parts that are subject to adjustment
- (8) Ensure interchangeability of similar subsystems, circuits, modules, and subassemblies
- (9) Ensure that adequate attention is given to all human factors aspects of the design
- (10) Ensure that the quality control effort will be effective

Reviews should be made at appropriate stages of the design process. It may be necessary to conduct specific reviews to evaluate achievement of the reliability requirements on a timely basis. The reviews should include, to the extent applicable but not necessarily limited to: current reliability estimates and achievements for each mode of operation, as derived from reliability analyses or test(s); potential design or production (derived from reliability analyses) problem areas, and control measures necessary to preserve the inherent reliability; failure mode(s) and effect(s) and criticality analyses; corrective action on reliability critical items; effects of engineering decisions, changes and tradeoffs upon reliability achievements, potential and growth, within the functional model framework; status of supplier and vendor reliability programs; and status of previously-approved design review actions. The results of reliability reviews should be documented.

In order to satisfy the objectives of the design review, the review team must have sufficient breadth to handle aspects of the items under review, such as performance, reliability, etc., and the interfaces and interactions with adjacent items. The ultimate objective of the team is to arrive at a balanced and reliable design.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.11.2 Informal Reliability Design Review

The informal reliability design review is conducted for the purpose of evaluating and guiding specified reliability characteristics and maintenance features "in process." That is, it is conducted while the design is in the evolutionary or formative stage and still amenable to major conceptual and configuration changes. Reviews are conducted on an unscheduled, "as required," informal basis. They are usually conducted at the request of the designer or the systems engineer to verify conformance throughout the team effort, to allocate requirements and design constraints, to verify the solution of problems identified in earlier design iterations, or to provide the basis for selection of design alternatives.

Even though the verification review is an informal working session, usually involving only a few selected reviewers, results of each review should be documented. The review may result in one of five alternatives being selected for further design iteration. These alternatives are:

- (1) **Reverify Design Adequacy** to provide additional analytical or empirical proof of design adequacy to facilitate design review approval decision with more confidence than current data will substantiate
- (2) **Redesign** to correct design discrepancies and marginal characteristics disclosed by the review
- (3) **Reallocate Design Requirements** to rectify allocation errors identified in the review, or reallocate subsystem requirements on the basis of updated estimates of design feasibility or changes in relative criticality disclosed during the review
- (4) **Redefine Design Requirements** to restudy previous requirements analyses and tradeoff studies, and redefine or refine baseline design and configuration requirements more nearly consistent with state-of-art and program constraints revealed during the design review.
- (5) **Re-evaluate System Operational Requirements** to provide the basis for choosing one of two alternatives: (a) redefine system operational requirements consistent with current design state-of-art and program constraints; or (b) redefine program constraints, such as delivery schedule and funds, to rectify earlier estimating errors.

The recommended design review team membership, and functions of each member, are briefly summarized in Table 7.11-1. For these informal design reviews, customer participation is usually optional. The IPDT is the current and preferred approach to forming the design team.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.11.3 Formal Design Reviews

Formal design reviews, when the customer is the government, are usually the subject of contractual agreement between the government and the supplier. Table 7.11-1 shows the recommended review team composition. Regardless of who the customer is, formal reviews normally include the following:

Preliminary Design Review (PDR): The PDR is conducted prior to the detail design process to evaluate the progress and technical adequacy of the selected design approach, determine its compatibility with the performance requirements of the specification; and establish the existence and the physical and functional interfaces between the item and other items of equipment or facilities. The basic design reliability tasks shown in Figure 7.11-3 should be accomplished for the PDR.

Eight suggested basic steps pertinent to the PDR are shown in Figure 7.11-2.

Critical Design Review: The CDR is conducted when detail design is essentially complete and fabrication drawings are ready for release. It is conducted to determine that the detail design satisfies the design requirements established in the specification, and establish the exact interface relationships between the item and other items of equipment and facilities.

Preproduction Reliability Design Review (PRDR): The PRDR is a formal technical review conducted to determine if the achieved reliability of a weapon system at a particular point in time is acceptable to justify commencement of production. For DoD acquisitions, details for the PRDR are usually provided in the individual Service documents or instructions, e.g., NAVAIR INST. 13070.5.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.11-1: DESIGN REVIEW GROUP, RESPONSIBILITIES
AND MEMBERSHIP SCHEDULE

Group Member	Responsibilities
Chairman	Calls, conducts meetings of group, and issues interim and final reports
Design Engineer(s) (of product)	Prepares and presents design and substantiates decisions with data from tests or calculations
*Reliability Manager or Engineer	Evaluates design for optimum reliability, consistent with goals
Quality Control Manager or Engineer	Ensures that the functions of inspection, control, and test can be efficiently carried out
Manufacturing Engineer	Ensures that the design is producible at minimum cost and schedule
Field Engineer	Ensures that installation, maintenance, and operator considerations were included in the design
Procurement Representative	Assures that acceptable parts and materials are available to meet cost and delivery schedules
Materials Engineer	Ensures that materials selected will perform as required
Tooling Engineer	Evaluates design in terms of the tooling costs required to satisfy tolerance and functional requirements
Packaging and Shipping Engineer	Assures that the product is capable of being handled without damage, etc.
Design Engineers (not associated with unit under review)	Constructively review adequacy of design to meet all requirements of customer
Customer Representative (optional)	Generally voices opinion to acceptability of design and may request further investigation on specific items

*May have other titles within some companies. Other specialties, such as maintainability, human factors, and value engineering are also represented.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

The PRDR is conducted just prior to production (and, for DoD programs, after completion of initial operational test and evaluation) to ensure the adequacy of the design from a reliability standpoint. The level of achieved reliability and adequacy of design will be evaluated primarily on initial technical and operational testing, e.g., test results, failure reports, failure analyses reports, reports of corrective action, and other documents which could be used as necessary for back-up or to provide a test history.

Suggested steps for a CDR are shown in Figure 7.11-4. The basic design reliability tasks shown in Figure 7.11-5 should be accomplished for the CDR.

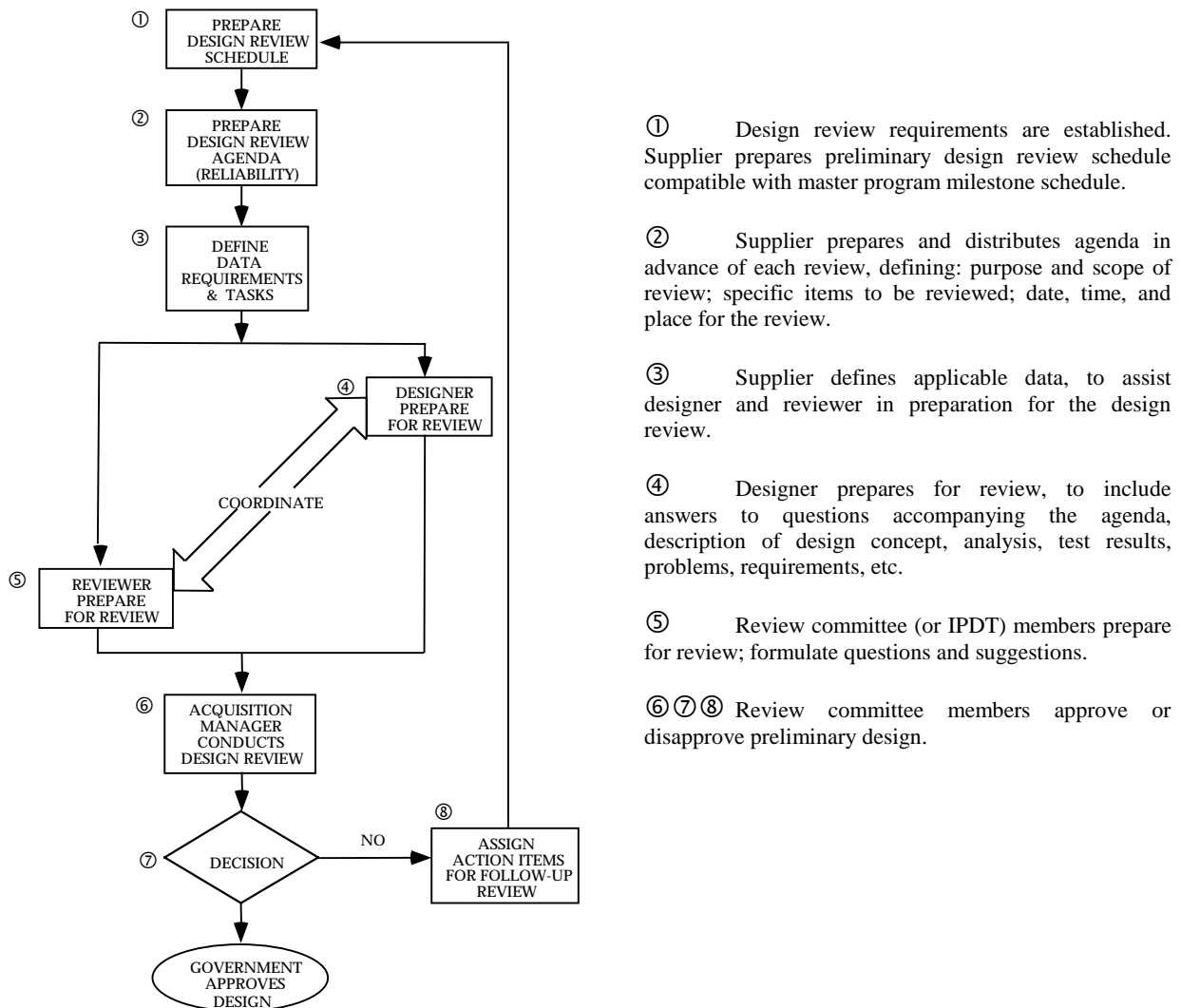


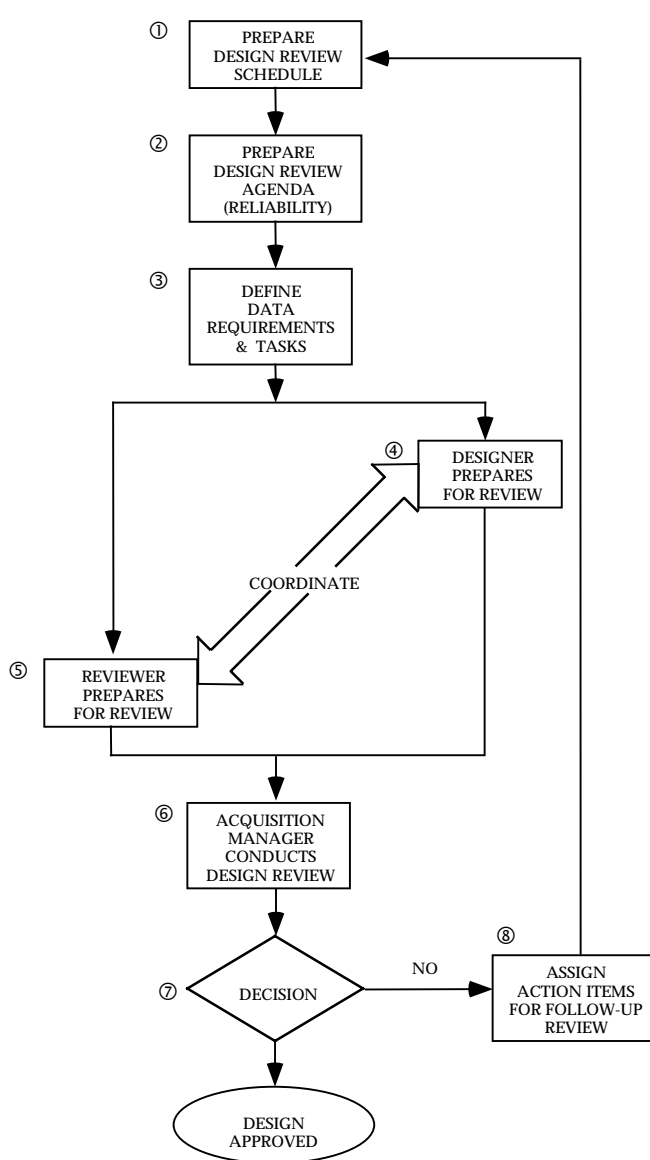
FIGURE 7.11-2: BASIC STEPS IN THE PRELIMINARY DESIGN REVIEW (PDR) CYCLE

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

1. Identify the quantitative reliability requirements and compare preliminary predictions with specified requirements.
2. Review failure rate sources, derating policies, and prediction methods.
3. Identify planned actions when predictions are less than specified requirements.
4. Identify and review parts or items which have a critical life or require special consideration, and general plan for handling.
5. Identify applications of redundant elements. Evaluate the basis for their use and provisions for redundancy with switching.
6. Review critical signal paths to determine that a fail-safe/fail-soft design has been provided.
7. Review margins of safety between functional requirements and design provisions for elements, such as: power supplies, transmitter modules, motors, and hydraulic pumps. Similarly, review structural elements, i.e., antenna pedestals, dishes, and radomes to determine that adequate margins of safety are provided between operational stresses and design strengths.
8. Review Reliability Design Guidelines to ensure that design reliability concepts shall be available and used by equipment designers. Reliability Design Guidelines should include, part application guidelines (electrical derating, thermal derating, part parameter tolerances), part selection order of preference, prohibited parts/materials, reliability allocations/predictions, and management procedures to ensure compliance with the guidelines.
9. Review preliminary reliability demonstration plan: failure counting ground rules, accept-reject criteria, number of test articles, test location and environment, planned starting date, and test duration.
10. Review elements of reliability program plan to determine that each task has been initiated toward achieving specified requirements.
11. Review vendor reliability controls.

FIGURE 7.11-3: DESIGN RELIABILITY TASKS FOR THE PDR

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES



①② Design review requirements are established. Supplier prepares and distributes agenda in advance of Critical Design Review (CDR) defining: purpose and scope of review; specific items to be reviewed; date, time and place for the review.

③ Supplier defines applicable data, to assist designer and reviewer in preparation for the design review.

④ Designer prepares for pre-critical design review, to include answers to questions accompanying the agenda, description of design concept, analyses, test results, problems, requirements, etc.

⑤ Review committee (or IPDT) members prepare for review; formulate questions and suggestions.

⑥ Acquisition Manager conducts the critical design review meeting.

⑦ Decisions made either to approve the design or to withhold approval pending correction of deficiencies.

⑧ Action items for correction of deficiencies assigned and schedule for follow-up review established.

FIGURE 7.11-4: BASIC STEPS IN THE CDR CYCLE

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

1. Review the most recent predictions or assessments of quantitative reliability and compare against specified requirements. Substantiate predictions by review of parts application stress data and substantiate assessments by reviewing any test data.
2. Review application of parts or items with minimum life, or those which require special consideration to insure their affect on system performance is minimized.
3. Review completed Reliability Design Review Checklist to insure principles have been satisfactorily reflected in the design.
4. Review applications of redundant elements to establish that expectations have materialized since the PDR.
5. Review detailed reliability demonstration plan for compatibility with specified test requirements. Review the number of test articles, schedules, location, test conditions, and personnel involved to insure a mutual understanding of the plan and to provide overall planning information to activities concerned.

FIGURE 7.11-5: DESIGN RELIABILITY TASKS FOR THE
CRITICAL DESIGN REVIEW (CDR)

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.11.4 Design Review Checklists

A design review checklist delineates specific areas to be considered for the item under review. In order to ensure that every consideration has been appropriately taken into account, a checklist for design should be prepared. Figure 7.11-6 is a typical list of areas to be considered in various stages of a design review (not to be considered all inclusive). Table 7.11-2 is a typical example of a Reliability Actions Checklist.

Technical checklists can be in question format to ensure that critical factors will not be overlooked. Figure 7.11-7 illustrates typical questions which could be asked at various stages of the design review.

1. System concept/alternative approaches
2. System performance and stability
3. Design documentation
4. Design changes
5. Tradeoff studies
6. Materials and Processes
7. Construction, Fabrication, Maintenance and Service
8. Analyses (Failure Mode, Effects and Criticality, Tolerance, etc.
9. Equipment compatibility
10. Environmental effects
11. Test data
12. Reliability allocation/prediction/assessment
13. Redundancy
14. Cost and procurement considerations
15. Life and controls
16. Interchangeability, spares and repair parts
17. Weight
18. Supplier design
19. Safety
20. Critical functions

FIGURE 7.11-6: TYPICAL AREAS TO BE COVERED IN A DESIGN REVIEW

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.11-2: RELIABILITY ACTIONS CHECKLIST

DESIGN TITLE		NUMBER		Notes & Comments
		Design	Reliability	
No.	Item	Completed		
1.	System Constraints		D	X
	a. Success Criteria		D	X
	b. Environmental Stresses		D	X
	c. Compatibility Factors		D	X
	d. User Skill Levels		D	X
2.	Feasibility Study		D	X
3.	Reliability Apportionment			R
4.	Preliminary Reliability Review		D	R
5.	Trade-Off Studies		D	X
6.	Functional Schematics		D	X
7.	Block Diagram		D	X
8.	Cause and Effect Analysis		D	X
9.	Worst Case Analysis		D	X
10.	Subsystem and Equipment Reliability Prediction			
	a. Part Failure Rate Method		D	X
	b. Safety Margin Method		D	X
	c. Drift Rate and Tolerance Method		D	X
11.	Intermediate Design Review		D	R
12.	Time/Cycle Recording Requirements		D	X
13.	Failure Reporting Requirements		D	X
14.	Serialization Requirements		D	X
15.	Procurement Specification Review			R
16.	Vendor Proposal Review			R

CODE

D - Prime Action by Designer - check off, sign and date as completed.

R - Prime Action by Reliability Engineer - check off, sign and date as completed.

X - Check by Reliability Engineer - initial and date.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.11-2: RELIABILITY ACTIONS CHECKLIST (CONT'D)

DESIGN TITLE	Completed	NUMBER		Notes & Comments
		Design	Responsibility Reliability	
No. Item				
17. Source Selection Review			R	
18. Parts Selection and Application Review		D	X	
19. Reliability Signoff - Top Assy. & Inst. Dwgs.			R	
20. Vendor Design Review			R	
21. Critical Design Review		D	R	
22. Process Controls		D	X	
23. Manufacturing Procedure Controls			X	
24. Qualification Test Review		D	X	
25. Acceptance Test Review		D	X	
26. Integration Test Review		D	X	
27. Reliability Demonstration Test Review		D	X	
28. System Test:				
a. Test Requirements Review		D	X	
b. Test Plans Review		D	X	
c. Reliability Tests			R	
29. Reliability Summary Sheet			R	

CODE

D - Prime Action by Designer - check off, sign and date as completed.

R - Prime Action by Reliability Engineer - check off, sign and date as completed.

X - Check by Reliability Engineer - initial and date.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

1. Is the design simple?
2. Does the design reflect an integrated system approach rather than an accumulation of parts?
3. Is the item compatible with the system in which it is used?
4. Are there adequate indicators to verify critical functions?
5. Has reliability of spares and repair parts been considered?
6. Are reliability requirements established for critical items? For each part?
7. Are there specific reliability design criteria for each item?
8. Have reliability tests been established?
9. Are appropriate parts being used properly?
10. Are unreliable parts identified?
11. Has the failure rate for each part or part class been established?
12. Have parts been selected to meet reliability requirements?
13. Has shelf life been determined?
14. Have limited-life parts been identified, and inspection, and replacement requirements specified?
15. Have critical parts which required special procurement, testing, and handling been identified?
16. Have stress analyses been accomplished?
17. Have derating factors been used in the application of parts?
18. Have safety factors and safety margin been used in the application of parts?
19. Are circuit safety margins ample?
20. Have standard and proven circuits been used?
21. Has the need for the selection of parts (matching) been eliminated?
22. Have circuit studies been made considering variability and degradation of electrical parameters of parts?
23. Is the reliability or MTBF of the item based on actual application of the parts?
 - a. Comparison made with reliability goal?
 - b. Provision for necessary design adjustments?

FIGURE 7.11-7: TYPICAL QUESTIONS CHECKLIST FOR THE DESIGN REVIEW

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

24. Are the best available methods for reducing the adverse effects of operational environments on critical parts being utilized?
25. Has provision been made for forecasting failures, including the use of marginal testing?
26. Is there a process for identifying improvements to eliminate design inadequacies observed in tests?
27. Have normal modes of failure and the magnitude of each mode for each item or critical part been identified?
28. Have the following effects been considered?
 - a. External effects on the next higher level in which the item is located.
 - b. Internal effects on the item.
 - c. Common effects, or direct effect of one item on another item, because of mechanical or electro-mechanical or electro-mechanical linkage.
30. Has redundancy been provided where needed to meet specified reliability?
31. Have failure mode and effects analyses been adequately conducted for the design?
32. Have the risks associated with critical item failures been identified? Accepted? Has design action been taken?
33. Does the design account for early failure, useful life and wear-out?

FIGURE 7.11-7: TYPICAL QUESTIONS CHECKLIST FOR THE DESIGN REVIEW

7.12 Design for Testability

Testability, an important subset of maintainability, is a product design characteristic reflecting the ability to determine the status (operable, inoperable or degraded) of an item, and to isolate faults within the item in a timely and efficient manner. Therefore, a great deal of attention must be paid to ensuring that all designs incorporate features that allow testing to occur without a great deal of effort. The design must be such that testing is efficient in terms of detecting and isolating only failed items, with no removal of good items. The removal of good items continues to be a problem in many industries, with obvious impacts on troubleshooting times and repair and logistics costs.

Design guides and analysis tools must be used rigorously to ensure a testable design. Not doing so leads to greater costs in the development of manufacturing and field tests, as well as in the development of test equipment. Trade-offs must be made up front on the use of built-in-test (BIT) versus other means of fault detection and isolation. Further, the expected percentage of faults that can be detected and isolated to a specified or desired level of ambiguity must be determined - it is an important input to the logistics analysis process. The consequences of poor testability are higher manufacturing costs, higher support costs, and lower customer satisfaction.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.12.1 Definition of Testability and Related Terms

Testability is a discipline that has many unique terms that may be unfamiliar to some readers. Many of these terms are defined in Section 3. Some additional terms are defined here to help in understanding the material that follows. Additional terms and definitions related to testability are provided (References [94] and [95]).

- Controllability: A design attribute that defines or describes the degree of test control that can be realized at internal nodes of interest.
- General Purpose Test Equipment (GPTE): Test equipment used to measure a range of parameters common to two or more systems of basically different design.
- Observability: A design attribute that describes the extent to which signals of interest can be observed.
- On-line Test: Testing of a UUT in its normal operating environment.
- Off-line Test: Testing of a UUT removed from its normal operating environment.
- Troubleshooting: A procedure for locating and diagnosing malfunctions or breakdowns in equipment using systematic checking or analysis.

7.12.2 Distinction between Testability and Diagnostics

Whereas testability is related to the physical design characteristics of a product, diagnostics are related to the means by which faults are detected and isolated. This includes the actual on-line and off-line tests themselves, as well as the means (BIT, BIT Equipment, GPTE, External Test Equipment, etc.) by which tests are performed. Achieving good diagnostics involves determining the diagnostic capability required in a product. A diagnostic capability can be defined as all capabilities associated with detecting, isolating, and reporting faults, including testing, technical information, personnel, and training. In comparing testability with diagnostics, we see that testability is an inherent design characteristic, while diagnostics involves factors other than those associated with the design itself. Attention paid to both in all design phases will impact not only the cost of producing a product, but certainly the cost and time associated with troubleshooting failures of the product once it has been fielded.

7.12.3 Designing for Testability

Although a subset of maintainability, testability has become recognized as a separate design discipline in its own right. Because of the impact of poor testability on production and maintenance costs, it will continue to be treated as a distinct discipline, at least in the foreseeable future. Therefore, it is important to develop a testability program plan as an integral part of the systems engineering process, and to elevate testability to the same level of importance accorded to other product assurance disciplines. Plans must be established that define the need to analyze

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

a design to assure it contains characteristics that allow efficient and effective fault detection and isolation.

Ensuring that a product is testable requires adherence to some basic testability design principles. A brief description of the most common testability design principles follows.

- Physical and functional partitioning - The ease or difficulty of fault isolation depends to a large extent upon the size and complexity of the units that are replaceable. Partitioning the design such that components are grouped by function (i.e., each function is implemented on a single replaceable unit), or by technology (e.g., analog, digital) whenever possible will enhance the ability to isolate failures.
- Electrical partitioning - Whenever possible, a block of circuitry being tested should be isolated from circuitry not being tested via blocking gates, tristate devices, relays, etc.
- Initialization - The design should allow an item to be initialized to a known state so it will respond in a consistent manner for multiple testing of a given failure.
- Controllability - The design should allow external control of internal component operation for the purpose of fault detection and isolation. Special attention should be given to independent control of clock signals, the ability to control and break up feedback loops, and tri-stating components for isolation.
- Observability - Sufficient access to test points, data paths and internal circuitry should be provided to allow the test system (machine or human) to gather sufficient signature data for fault detection and isolation.
- Test System Compatibility - Each item to be tested should be designed to be electrically and mechanically compatible with selected or available test equipment to eliminate or reduce the need for a large number of interface device (ID) designs.

In addition to the preceding principles, checklists of testability design practices have been developed that are specific to technologies, such as analog, digital, mechanical, and so forth. See 7.12.6.1.2 for one such checklist.

Determining the amount of testability necessary in a design will be driven by the requirements for fault *detection* and fault *isolation*. Fault detection requirements are typically stated as the percentage of faults that can be detected, using defined means (BIT, semi-automatic/automatic test, etc.), out of all possible faults. For instance, a system may have a requirement of 95% fault detection, indicating that 95% of all possible failures are to be detectable by the diagnostic capability of the system. Fault isolation requirements are typically stated as the percentage of time fault isolation is possible to a specified number of components. As an example, a system may have a requirement of 90% isolation to a single replaceable unit (RU), 95% isolation to an ambiguity group of 2 or fewer RUs and 100% isolation to an ambiguity group of 3 or fewer RUs.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Mathematically, fault detection and isolation are defined in the following equations for the fraction of faults detectable (FFD) and the fraction of faults isolatable (FFI).

$$\text{FFD} = \text{FD/FA}$$

where:

FA = total number of actual faults occurring over time

FD = no. of actual failures correctly identified using defined means

Equation 1 is used to calculate predicted fault resolution. To use the equation, data are required that correlate each detected failure with the signature, or “error syndrome”, that each failure produces during testing. The data are most conveniently ordered by signature and by failed module within each signature. The signature, then, is the observed test response when a particular failure occurs. This information typically is generated from an FMEA, or in the case of electronics design, especially digital, from a fault simulation program. The collection of test responses, or failure signatures, represents a fault dictionary. In many instances, several failures will produce the same observed (usually at the system output(s)) signature, creating ambiguity. The fault resolution predicted by equation 1 measures the amount of ambiguity that exists, for a given level of test capability. As noted, for each signature, a list of suspect modules is created, providing the input data needed to apply the following equation:

$$\text{FFI}_L = \left(\frac{100}{\lambda_d} \right) \sum_{i=1}^N X_i \sum_{j=1}^{M_i} \lambda_{ij}$$

where:

X_i = 1 if $M_i \leq L$; 0 otherwise

N = number of unique test responses

L = number of modules isolated to (i.e., ambiguity group size)

i = signature index

M_i = number of modules listed in signature i

j = module index within signature

λ_{ij} = failure rate for j th module for failures having signature i

$$\lambda_d = \text{overall failure rate of detected failures} = \sum_{i=1}^N \sum_{j=1}^{M_i} \lambda_{ij}$$

Additional quantitative measures of testability may include fault isolation time, which is derived from the Mean Time To Repair (MTTR).

Mean Fault isolation time = Mean [repair time - (operation time + disassembly time + interchange time + reassembly time + alignment time + verification time)]

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Note that the first two measures are interrelated in that before you can isolate a fault, you must first detect it. Therefore, a testability analysis program is designed to analyze the effectiveness of the *detection* scheme, and then to analyze the effectiveness of the *isolation* scheme. For complex designs, the analysis of testability often requires the use of testability design and analysis tools that provide information on fault detection and isolation, for a given diagnostic approach, or diagnostic capability.

False alarms (in which a failure is “detected” even though none occurred) is a problem related to both testability and a system's diagnostic design. Manifesting themselves in varying degrees in avionics and other types of equipment, false alarms are a drain on maintenance resources and reduce a system's mission readiness. The two most commonly reported symptoms of false alarms are CND and RTOK.

False alarms occur for many reasons, including external environmental factors (temperature, humidity, shock, etc.), design of diagnostics, equipment degradation due to age, design tolerance factors, maintenance-induced factors (e.g., connectors, wire handling, etc.), or combinations of these factors. External environmental factors may cause failures of avionics or other equipment that do not occur under ambient conditions and are believed to be a leading cause of false alarms. When the environmental condition is removed, the “failure” cannot be found. One solution to the problem is to use a stress measurement device to record the environmental stresses before, during, and after a system anomaly. Subsequent diagnosis can use this data to determine what occurred and whether any action (maintenance, modifications, etc.) is needed.

The Time Stress Measurement Device (TSMD) is a stress measurement device that has been developed over the past few years by the Air Force. TSMDs measure and record selected environmental parameters and fault signatures and record a time stamp, for use in subsequent failure correlation analysis. TSMD has been adapted to record an image of all of the environmental data prior to, during, and after a system anomaly. These recorded events can be used to identify environmental stress-related conditions that may be causing intermittent or hard failures. The TSMD data aids in reducing RTOK, and CND conditions by correlating the event with the conditions that existed when the anomaly was detected.

Several different models of TSMDs have been developed by different manufacturers. They feature both 8 bit (Ref. [96]) and 32 bit (Ref. [97]) internal microprocessors and RS-232 and RS-485 interfaces. Typically they are powered by 5 volts DC drawn from the host system and dissipate 1 watt or less. They may be powered by an external battery for operation under power-off conditions, e.g., shipping or storage, or when host system power is impractical or too costly to provide.

Many commercial stress measurement devices are also in use or under study. A RAC publication (Ref. [98]) provides a compendium of such commercially available devices, including their sensing and storing capabilities. This publication is part of an on-going market survey aimed at identifying sources of stand-alone environmental stress data collection systems.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.12.4 Developing a Diagnostic Capability

Defining and developing a product's diagnostic capability depends on factors such as:

- The product's performance and usage requirements
- Maintenance support requirements (e.g., levels of maintenance)
- Technology available to: improve diagnostics in terms of test effectiveness; reduce the need for test equipment, test manuals, personnel, training, and skill levels; and reduce cost
- The amount of testability designed into the product
- Previously known diagnostic problems on similar systems

Each of these factors will play a role in determining the approach to detecting and isolating faults. A typical approach to diagnostics includes the use of BIT. BIT is an integral capability of the mission equipment which provides an on-board, automated test capability. This capability consists of software or hardware (or both) components that detect, diagnose, or isolate product (system) failures. The fault detection and isolation capability is used for periodic or continuous monitoring of a system's operational health, and for observation and diagnosis as a prelude to maintenance action. BIT reduces the need for maintenance manpower and External Test Equipment. Other approaches may consider the use of automatic or semi-automatic test equipment, manual testing using benchtop test equipment, or visual inspection procedures. In all cases, tradeoffs are required among system performance, cost, and test effectiveness.

It must be remembered that the effectiveness of the diagnostic capability, and the cost of development, is greatly influenced by how well testability has been designed into the system. Should there be a lack of test points available to external test equipment, for example, then the ability to isolate failures to smaller ambiguity group sizes may be adversely affected. The result is higher costs to locate the failure to a single replaceable item. The cost of test development may also increase. BIT design should be supported by the results of a failure modes and effects analysis (FMEA). An FMEA should be used to define those failures that are critical to system performance, and to identify when the effects of a failure can be detected using BIT. Without such information, BIT tests will be developed based only on the test engineer's knowledge of how the system works, and not on whether a test needs to be developed for a particular fault.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.12.5 Designing BIT

Planning for BIT at all levels within the system design is becoming more important for several reasons. First, surface mount devices (SMDs) are increasingly being used in circuit cards. The use of SMDs, and devices with higher packaging density (including double-sided boards), decreases the accessibility required for guided-probe testing, while increasing the risks of such testing. Incorporating BIT in such designs therefore becomes critical to effective diagnostics. Second, many component vendors of integrated circuits (ICs), such as Application Specific ICs (ASICs) are incorporating some form of BIT into their designs. Higher-level designs (i.e., board, module, etc.) that use such devices must take advantage of this fact by planning to integrate lower-level BIT capabilities with higher-level BIT designs. Doing this will increase the vertical testability of an entire system, wherein factory-level test programs can be used in field operations as well as the factory. Further, tests performed using BIT at higher levels of support (e.g., depot or intermediate) can also be used at lower levels (i.e., intermediate and organizational). This characteristic of the diagnostic system will help to maintain consistency across maintenance levels and may reduce the high incidences of false alarms. False alarms are often reflected by such measures as Retests OK (RTOK) or Can Not Duplicates (CNDs). (Note that not all the military services either use these terms or define them the same way).

The most important factor in BIT design is early planning. Without planning for BIT early in the life cycle, it will be harder to maximize any advantages offered by the use of BIT while minimizing any negative impacts such as increased design cost, higher hardware overhead, and increased failure rate. In “Chip-To-System Testability” (Interim Report submitted to Rome Laboratory under Contract No. F30602-94-C0053, 1996, Research Triangle Institute and Self-Test Services), five axioms are given that will allow designers to capitalize on the use of BIT. These axioms are:

- Plan for BIT starting at the earliest stage (e.g., proposal stage) of the program
- Design BIT in conjunction with the functional design, not as an afterthought
- Use the same high degree of engineering cleverness and rigor for BIT that is used for the functional design
- Take advantage of computer aided design (CAD) tools for the BIT design process whenever possible
- Incorporate the subject of BIT into peer, design and program reviews

BIT must be a part of the product’s design to avoid the risks and consequences shown in Table 7.12-1.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.12-1: RISKS AND CONSEQUENCES OF NOT MAKING BIT PART OF PRODUCT DESIGN

Risks	Consequences
BIT is designed independently of the product	BIT fails to support operational and maintenance needs
BIT is designed after the fact	BIT's MTBF is less than that of the product
Production personnel are not consulted on BIT	BIT is not effective in the factory

7.12.6 Testability Analysis

Testability analysis is important at all levels of design and can be accomplished in a variety of ways. For instance, when designing complex integrated circuits (ICs), such as Application Specific ICs, or ASICs, it is important to develop test vectors that will detect a high percentage of 'stuck at' faults (i.e., signal stuck at logic '1' or '0'). This is almost always determined via logic simulation wherein a model of the design is developed in an appropriate fault simulation language. Once the model is compiled and ready to be simulated, a set of test vectors are applied to the model. The fault simulation program then produces a list of faults detected by the test vectors, as well as reporting the percentage (or fraction) of faults detected. Many such programs also identify specific signals that were not detected such that adjustments can be made either in the design or in the test vectors themselves in order to increase the fault detection percentage.

For non-digital electronics, fault detection efficiency is typically determined with the aid of an FMEA. The FMEA will identify those faults that result in an observable failure and can therefore be detected. The test engineer then must develop a test that will verify operation and detect any malfunctions identified in the FMEA. Fault detection percentages are determined by summing the number of faults identified in the FMEA that are detected versus the total number identified as being detectable. This process can occur at all levels of design. The fault grading methods described in the preceding paragraph are primarily applied at the IC and printed circuit card levels.

In addition to determining fault detection percentage, a testability analysis should be performed to determine the fault isolation effectiveness of designed tests. For digital electronics, many of the tools used to grade test vectors also provide statistics on fault isolation percentages. This is typically provided by creating a fault dictionary. During fault simulation, the response of the circuit is determined in the presence of faults. These responses collectively form the fault dictionary. Isolation is then performed by matching the actual response obtained from the circuit or test item with one of the previously computed responses stored in the fault dictionary. Fault simulation tools can determine from the fault dictionary the percentage of faults that are uniquely isolatable to an ambiguity group of size n ($n = 1, 2, 3, \dots$). These tools can be used to verify fault isolation goals or requirements via analysis, prior to actual testing. For non-digital circuits, hybrid circuits or even digital systems above the printed circuit card level, analysis of fault isolation capability can be performed with the aid of a diagnostic model and a software tool that analyzes that model. Examples are dependency modeling tools such as the Weapon System

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Testability Analyzer (WSTA), System Testability Analysis Tool (STAT) or the System Testability and Maintenance Program (STAMP)⁷. These tools, and others like them, can be used to determine the fault isolation capability of a design based on the design topology, order of test performance, and other factors such as device reliability. Statistics such as percentage of faults isolatable to an ambiguity of group size n are provided, as is the identification of which components or modules are in an ambiguity group for a given set of tests. Test effectiveness and model accuracy are the responsibility of the test designer, however.

7.12.6.1 Dependency Analysis

Assessing testability via dependency analysis has gained in popularity recently, and it is therefore prudent to provide some additional information on this technique. Dependency analysis starts with the creation of a dependency model of the item to be analyzed. The model is designed to capture the relationship between tests or test sites within a system, and those components and failure modes of components that can affect the test. As an example, consider the simple functional block diagram shown in Figure 7.12-1.

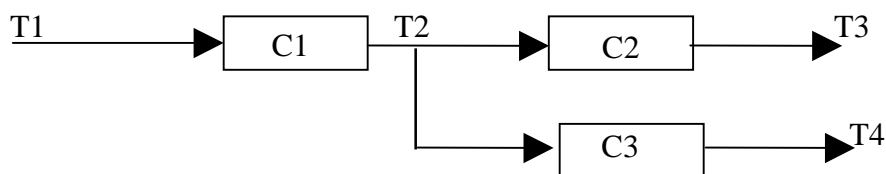


FIGURE 7.12-1: SIMPLE SYSTEM SHOWING TEST DEPENDENCIES

The dependency model for the system, in the form of a tabular list of tests and their dependencies is provided in Table 7.12-2.

TABLE 7.12-2: FIRST ORDER DEPENDENCY MODEL FOR SIMPLE SYSTEM

Test	First-Order Dependencies
T1	None
T2	C1, T1
T3	C2, T2
T4	C3, T2

Figure 7.12-1 has been labeled to identify each potential test site within the system, where in this example, exactly one test is being considered at each node. The dependency model shown in Table 7.12-2 is a list of “first-order dependencies” of each test. For example, the first order dependency of test T3 is C2 and T2. This would indicate that T3 *depends* upon the health of component C2 and any inputs to C2, which is T2 in this case. For this simple system, it is also

⁷ STAT is a registered trademark of DETEX Systems, Inc. and STAMP is a registered trademark of the ARINC Research Corporation. WSTA is a tool developed by the US Navy and available to most US Government contractors and US Government employees.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

obvious that T3 will also depend on C1 and T1, but these are considered higher-order dependencies. Each of the tools mentioned previously (i.e., STAT, STAMP and WSTA), determine all higher order dependencies based on a first order dependency input model.

Dependency modeling is attractive due to its applicability to any kind or level of system. Note in the example that neither the nature nor level of the system is required to process the model. Consequently, this methodology is applicable to most any type of system technology and any level (i.e., component to system).

Based on the input model, the analysis tools can determine the percentage of time isolation to an ambiguity group of n or fewer components will occur. In addition, each of the tools discussed will also identify which components or failures will be in the same ambiguity group with other components or failures. Furthermore, any test feedback loops that exist, including those components contained within the feedback loop, will also be identified. Note that the ambiguity group sizes and statistics are based on a binary test outcome (i.e., test is either good or bad), and in most cases the tools assume that the test is 100% effective. This means that if the model indicates that a particular test depends on a specified set of components, the tools assume that should the test pass, all components within the dependency set are good. Conversely, a failed test makes all of the components within the dependency set suspect. Therefore, the accuracy of the model, in terms of what components and component failure modes are actually covered by a particular test are the responsibility of the model developer. The coverage is very much dependent upon test design and knowledge of the system's functional behavior.

Even before intimate knowledge of what tests are to be performed is known, such as in the early stages of system development, a model can be created that assumes a test at every node, for instance. The system design can be evaluated as to where feedback loops reside, which components are likely to be in ambiguity, and where more visibility, in terms of additional test points, need to be added to improve the overall testability of the design. Once the design is more developed, and knowledge of each test becomes available, the dependency model can then be refined. Given that the analyst is satisfied with the model results, each of the tools discussed can be used to develop optimal test strategies based on system topology and one or more weighting factors such as test cost, test time, component failure rates, time to remove an enclosure to access a test point, etc.

One of the drawbacks in the past to dependency modeling has been the time it takes to create a model. However, translation tools exist and are continuously being developed that can translate a design captured in a CAD format, such as the Electronic Data Interchange Format (EDIF), into a dependency model compatible with the specific dependency analysis tool being used. The analyst is still responsible for verifying the accuracy of the model, however, as in some cases, not all dependencies will be 100% correctly translated. Despite this fact, the amount of time that can be saved in translation outweighs any additional time it may take to verify the model.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.12.6.1.1 Dependency Analysis Tools

The three tools mentioned, STAT, STAMP and WSTA, provide the same basic kinds of outputs as just discussed. Each tool has other features that may be attractive depending on the system being analyzed, CAD tools being used in the design process, etc. Therefore, more information should be gathered on these and other similar tools prior to making a final decision as to which one to acquire.

The key points to remember about any of these tools is that model accuracy is most important. Therefore, it is important to understand how the system behaves in the presence of a failure, and which tests can be developed to detect such behavior. Thus, to gain the most benefit from the model development process, experts in design and test should be involved.

7.12.6.2 Other Types of Testability Analyses

Other types of analyses that do not require the use of a software tool are ad hoc procedures, such as reviewing a design against a known set of testability design practices. Grumman, and later Raytheon, developed such a procedure for the US Air Force Rome Laboratory that rates a design based on the presence or absence of design features that increase or decrease ease of test. The result is a score that is subjectively evaluated as indicating the design is anywhere between untestable without redesign to very testable. Used in conjunction with a design guide, also developed as part of the process by the mentioned companies, this method can be very effective in making the test engineer's job easier and less costly. The report, RL-TR-92-12 (Ref. [99]), VOLUMES I & II - Testability Design Rating System: Testability Handbook (VOL. I) & Analytical Procedure (VOL. II), include testability design.

In addition to specific diagnostics testability and diagnostics guidelines, RL-TR-92-12 provides the following general guidance regarding testability.

Redundancy - Built-in-Test (BIT) can be implemented by repeating the functional circuitry (the redundancy) to be tested by BIT. The same functional signal(s) is input into the redundant element and Circuit Under Test (CUT). Therefore, the circuitry of the CUT exists twice in the design and the outputs can be compared. If the output values are different and their difference exceeds a limit (analog circuits), then a fault exists. Due to the expense of this technique, redundant BIT design is usually implemented only in critical functions

An example of a BIT design using redundancy is shown in Figure 7.12-2. In this example, an analog circuit is repeated and the difference between the output levels is compared. If the difference exceeds a predefined threshold, then a fault signal is generated and latched.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

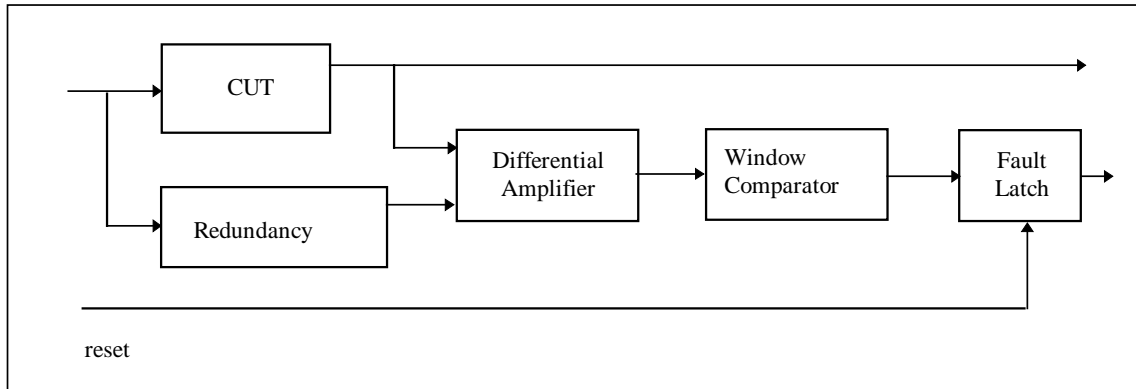


FIGURE 7.12-2: REDUNDANCY BIT (SOURCE: RADC-TR-89-209, VOL. II)

Wrap-around BIT - Wrap-around BIT requires and tests microprocessors and their input and output devices. During test, data leaving output devices is routed to input devices of the module. The BIT routine is stored in on-board read-only memory (ROM). Wrap-around can be done by directing output signals from the processor back to the input signals and verifying the input signal values. Wrap-around BIT can be applied to both digital and analog signals concurrently. An example of wrap-around BIT testing both analog and digital devices is shown in Figure 7.12-3. In this example, during normal operation processor outputs are converted from digital to analog outputs and analog inputs are converted to digital input signals. When the BIT is initiated, the analog outputs are connected to the analog inputs and the signals are verified by the processor.

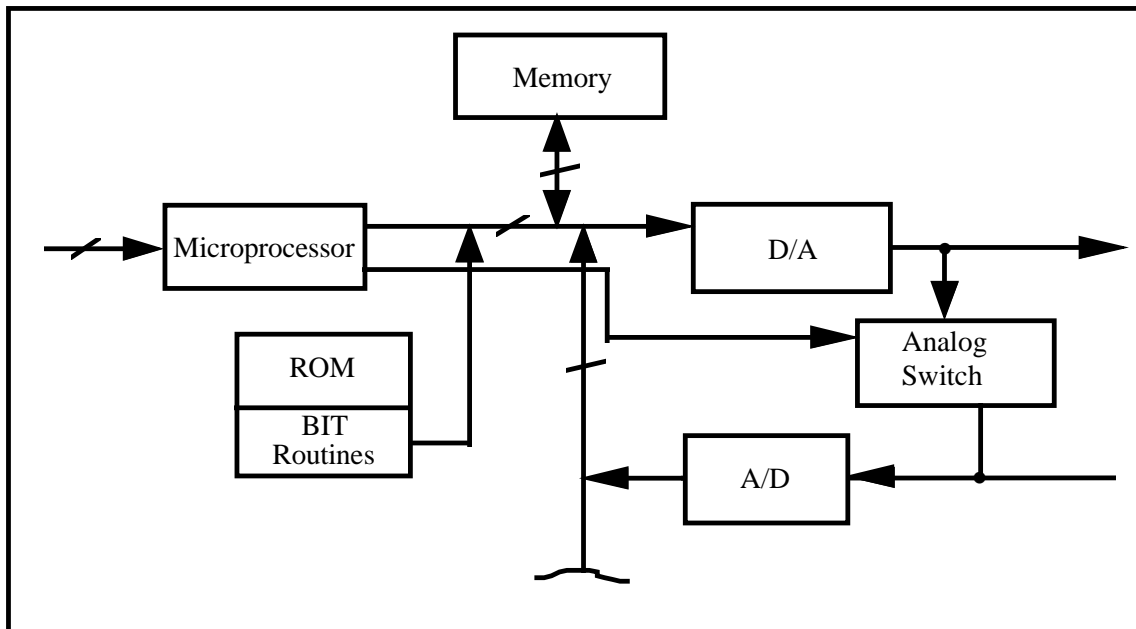


FIGURE 7.12-3: WRAP-AROUND BIT (SOURCE: RADC-TR-89-209, VOL II)

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

The remainder of RL-TR-92-12, VOL I, provides detailed guidance on testability design techniques and structured test techniques for various categories of part types and technologies.

In addition to the practical design guide information found in RL-TR-92-12, VOL I, Reference [100], provides an inherent testability checklist. It is reprinted here, in a slightly different format, as Table 7.12-3. Refer to Reference [100] for further guidance on testability program planning.

7.13 System Safety Program

7.13.1 Introduction

Reliability and safety are closely related subjects. Many of the analyses are complementary. For these reasons, a discussion of a system safety program is included here.

The principal objective of a system safety program is to ensure that safety, consistent with mission requirements, is designed into systems, subsystems, equipment and facilities, and their interfaces.

Within the DoD, MIL-STD-882, "System Safety Program Requirements," provides uniform guidelines for developing and implementing a system safety program of sufficient comprehensiveness to identify the hazards of a system and to impose design requirements and management controls to prevent mishaps by eliminating hazards or reducing the associated risk to a level acceptable to the managing activity.

Four different types of program elements are addressed: (a) Program Management and Control Elements, (b) Design and Integration Elements, (c) Design Evaluation Elements and (d) Compliance and Verification Elements.

- (a) Program Management and Control Elements are those relating primarily to management responsibilities dealing with the safety of the program and less to the technical details involved.
- (b) Design and Integration Elements focus on the identification, evaluation, prevention, detection, and correction or reduction of the associated risk of safety hazards by the use of specific technical procedures.
- (c) Design Evaluation Elements focus on risk assessment and the safety aspects of tests and evaluations of the system and the possible introduction of new safety hazards resulting from changes.
- (d) Compliance and Verification Elements are those directly related to the actual verification or demonstration that all legal and contractual safety requirements have been compiled with.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.12-3: INHERENT TESTABILITY CHECKLIST

Mechanical Design Checklist (for electronic designs)	
<ul style="list-style-type: none"> • Is a standard grid layout used on boards to facilitate identification of components? • Are the number of I/O pins in an edge connector or cable connector compatible with the I/O capabilities of the selected test equipment? • Are connector pins arranged such that the shorting of physically adjacent pins will cause minimum damage? • Is the design free of special set-up requirements (special cooling) which would slow testing? • Does the item warm up in a reasonable amount of time? • Has provision been made to incorporate a test-header connector into the design to enhance ATE testing of surface-mounted devices? 	<ul style="list-style-type: none"> • Is defeatable keying used on each board so as to reduce the number of unique interface adapters required? • Is each hardware component clearly labeled? • Are all components oriented in the same direction (pin 1 always in same position)? • Does the board layout support guided-probe testing techniques? • When possible, are power and ground included in the I/O connector or test connector? • Have test and repair requirements impacted decisions on conformal coating? • Is enough spacing provided between components to allow for clips and test probes?
Partitioning Checklist (for electronic functions)	
<ul style="list-style-type: none"> • Is each function to be tested placed wholly upon one board? • Within a function, is the size of each block of circuitry to be tested small enough for economical fault detection and isolation? • Is the number of power supplies required compatible with the test equipment? • If more than one function is placed on a board, can each be tested independently? 	<ul style="list-style-type: none"> • If required, are pull up resistors located on the same board as the driving component? • Is the number and type of stimuli required compatible with the test equipment? • Within a function, can complex digital and analog circuitry be tested independently? • Are analog circuits partitioned by frequency to ease tester compatibility? • Are elements which are included in an ambiguity group placed in the same package?
Test Control Checklist	
<ul style="list-style-type: none"> • Are connector pins not needed for operation used to provide test stimulus and control from the tester to internal nodes? • Is it possible to disable on-board oscillators and drive all logic using a tester clock? • Is circuitry provided to by-pass any (unavoidable) one-shot circuitry? • In microprocessor-based systems, does the tester have access to the data bus, address bus and important control lines? • Are active components, such as demultiplexers and shift registers, used to allow the tester to control necessary internal nodes using available input pins? • Can circuitry be quickly and easily driven to a known initial state? (master clear, less than N clocks for initialization sequence)? 	<ul style="list-style-type: none"> • Can long counter chains be broken into smaller segments in test mode with each segment under tester control? • Can feedback loops be broken under control of the tester? • Are test control points included at those nodes which have high fan-in (test bottlenecks)? • Are redundant elements in design capable of being independently tested? • Can the tester electrically partition the item into smaller independent, easy-to-test segments? (placing tri-state element in a high impedance state). • Have provisions been made to test the system bus as a stand-alone entity? • Are input buffers provided for those control point signals with high drive capability requirements?

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.12-3: INHERENT TESTABILITY CHECKLIST (CONT'D)

Parts Selection Checklist	
<ul style="list-style-type: none"> • Is the number of different part types the minimum possible? • Is a single logic family being used? If not, is a common signal level used for interconnections? 	<ul style="list-style-type: none"> • Have parts been selected which are well characterized in terms of failure modes? • Are the parts independent of refresh requirements? If not, are dynamic devices supported by sufficient clocking during testing?
Test Access	
<ul style="list-style-type: none"> • Are unused connector pins used to provide additional internal node data to the tester? • Are test access points placed at those nodes which have high fan-out? • Are active components, such as multiplexers and shift registers, used to make necessary internal node test data available to the tester over available output pins? • Are signal lines and test points designed to drive the capacitive loading represented by the test equipment? • Are buffers employed when the test point is a latch and susceptible to reflections? 	<ul style="list-style-type: none"> • Are all high voltages scaled down within the item prior to providing test point access so as to be consistent with tester capabilities? • Are test points provided such that the tester can monitor and synchronize to onboard clock circuits? • Are buffers or divider circuits employed to protect those test points which may be damaged by an inadvertent short circuit? • Is the measurement accuracy of the test equipment adequate compared to the tolerance requirement of the item being tested?
Analog Design Checklist	
<ul style="list-style-type: none"> • Is one test point per discrete active stage brought out to the connector? • Are circuits functionally complete without bias networks or loads on some other UUT? • Is a minimum number of complex modulation or unique timing patterns required? • Are response rise time or pulse width measurements compatible with test capabilities? • Does the design avoid or compensate for temperature sensitive components? • Is each test point adequately buffered or isolated from the main signal path? • Is a minimum number of multiple phase-related or timing-related stimuli required? 	<ul style="list-style-type: none"> • Are stimulus frequencies compatible with tester capabilities? • Are stimulus amplitude requirements within the capability of the test equipment? • Does the design allow testing without heat sinks? • Are multiple, interactive adjustments prohibited for production items? • Is a minimum number of phase or timing measurements required? • Do response measurements involve frequencies compatible with tester capabilities? • Does the design avoid external feedback loops? • Are standard types of connectors used?
Performance Monitoring Checklist	
<ul style="list-style-type: none"> • Have critical functions been identified (by FMECA) which require monitoring for the system operation and users? • Have interface standards been established that ensure the electronic transmission of data from monitored systems is compatible with centralized monitors? 	<ul style="list-style-type: none"> • Has the displayed output of the monitoring system received a human engineering analysis to ensure that the user is supplied with the required information in the best useable form?

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.12-3: INHERENT TESTABILITY CHECKLIST (CONT'D)

RF Design Checklist	
<ul style="list-style-type: none"> • Do transmitter outputs have directional couplers or similar signal sensing/attenuation techniques employed for BIT or off-line test monitoring purposes, or both? • Has provision been made in the off-line ATE to provide switching of all RF stimulus and response signals required to test the subject RF UUT? • Are the RF test input/output access ports of the UUT mechanically compatible with the off-line ATE I/O ports? • Have adequate testability (controllability/ observability) provisions for calibrating the UUT been provided? • If an RF transmitter is to be tested utilizing off-line ATE, has suitable test fixturing (anechoic chamber) been designed to safely test the subject item over its specified performance range of frequency and power? • Have all RF testing parameters and quantitative requirements for these parameters been explicitly stated at the RF UUT interface for each RF stimulus/ response signal to be tested? • Has the UUT/ATE RF interface been designed so that the system operator can quickly and easily connect and disconnect the UUT without special tooling? 	<ul style="list-style-type: none"> • Have RF compensation procedures and data bases been established to provide calibration of all stimulus signals to be applied and all response signals to be measured by BIT or off-line ATE to the RF UUT interface? • Have suitable termination devices been employed in the off-line ATE or BIT circuitry to accurately emulate the loading requirements for all RF signals to be tested? • Does the RF UUT employ signal frequencies or power levels in excess of the core ATE stimulus/ measurement capability? If so, are signal converters employed within the ATE to render the ATE/UUT compatible? • Has the RF UUT been designed so that repair or replacement of any assembly or subassembly can be accomplished without major disassembly of the unit? • Does the off-line ATE or BIT diagnostic software provide for compensation of UUT output power and adjustment of input power, so that RF switching and cable errors are compensated for in the measurement data?
Electro-optical (EO) Design Checklist	
<ul style="list-style-type: none"> • Have optical splitters/couplers been incorporated to provide signal accessibility without major disassembly? • Has temperature stability been incorporated into fixture/UUT design to assure consistent performance over a normal range of operating environments? • Have optical systems been functionally allocated so that they and associated drive electronics can be independently tested? • Are the ATE system, light sources, and monitoring systems of sufficient wave-length to allow operation over a wide range of UUTs? • Does the test fixturing intended for the off-line test present the required mechanical stability? • Is there sufficient mechanical stability and controllability to obtain accurate optical registration? • Can requirements for boresighting be automated or eliminated? 	<ul style="list-style-type: none"> • Do monitors possess sufficient sensitivity to accommodate a wide range of intensities? • Can optical elements be accessed without major disassembly or realignment? • Do they possess sufficient range of motion to meet a variety of test applications? • Has adequate filtering been incorporated to provide required light attenuation? • Can all modulation models be simulated, stimulated, and monitored? • Can targets be automatically controlled for focus and aperture presentation? • Do light sources provide enough dynamics over the operating range? • Do test routines and internal memories test pixels for shades of gray? • Are optical collimators adjustable over their range of motion via automation?

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.12-3: INHERENT TESTABILITY CHECKLIST (CONT'D)

Digital Design Checklist	
<ul style="list-style-type: none"> • Does the design contain only synchronous logic? • Does the design avoid resistance capacitance one-shots and dependence upon logic delays to generate timing pulses? • Is the design free of WIRED-ORs? • Will the selection of an unused address result in a well defined error state? • Are all clocks of differing phases and frequencies derived from a single master clock? • Is the number of fan-outs for each board output limited to a predetermined value? Are latches provided at the inputs to a board in those cases where tester input skew could be a problem? • For multilayer boards, is the layout of each major bus such that current probes or other techniques may be used for fault isolation beyond the node? 	<ul style="list-style-type: none"> • If the design incorporates a structured testability design technique (scan path, signature analysis), are all the design rules satisfied? • Is the number of fan-outs for each internal circuit limited to a predetermined value? • Are all memory elements clocked by a derivative of the master clock? (Avoid elements clocked by data from other elements.) • Does the design include data wrap-around circuitry at major interfaces? • Is a known output defined for every word in a read only memory? • Are sockets provided for microprocessors and other complex components? • Does the design support testing of "bit slices"? • Do all buses have a default value when unselected?
Diagnostic Capability Integration	
<ul style="list-style-type: none"> • Have vertical testability concepts been established, employed, and documented? • Has the diagnostic strategy (dependency charts, logic diagrams) been documented? 	<ul style="list-style-type: none"> • Has a means been established to ensure compatibility of testing resources with other diagnostic resources at each level of maintenance (technical information, personnel, and training)?
Mechanical Systems Condition Monitoring (MSCM) Checklist	
<ul style="list-style-type: none"> • Have MSCM and battle damage monitoring functions been integrated with other performance monitoring functions? 	<ul style="list-style-type: none"> • Are preventive maintenance monitoring functions (oil analysis, gear box cracks) in place? • Have scheduled maintenance procedures been established?
Sensors Checklist	
<ul style="list-style-type: none"> • Are pressure sensors placed very close to pressure sensing points to obtain wideband dynamic data? • Has the selection of sensors taken into account the environmental conditions under which they will operate? 	<ul style="list-style-type: none"> • Have procedures for calibration of sensing devices been established? • Has the thermal lag between the test media and sensing elements been considered?
Test Requirements Checklist	
<ul style="list-style-type: none"> • Has a "level of repair analysis" been accomplished? • For each maintenance level, has a decision been made for each item on how BIT, ATE, and General Purpose Electronic Test Equipment (GPETE), will support fault detection and isolation? 	<ul style="list-style-type: none"> • For each item, does the planned degree of testability design support the level of repair, test mix, and degree of automation decisions? • Is the planned degree of test automation consistent with the capabilities of the maintenance technician?

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.12-3: INHERENT TESTABILITY CHECKLIST (CONT'D)

Built-in-Test (BIT) Checklist	
<ul style="list-style-type: none"> • Can BIT in each item be exercised under control of the test equipment? • Does the BIT use a building-block approach (all inputs to a function are verified before that function is tested)? • Does on-board ROM contain self-test routines? • Does BIT include a method of saving on-line test data for the analysis of intermittent failures and operational failures which are non-repeatable in the maintenance environment? • Is the additional volume due to BIT within stated constraints? • Does the allocation of BIT capability to each item reflect the relative failure rate of the items and the criticality of the items' functions? • Are the data provided by BIT tailored to the differing needs of the system operator and the system maintainer? • Is sufficient memory allocated for confidence tests and diagnostic software? • Are BIT threshold limits for each parameter determined as a result of considering each parameter's distribution statistics, the BIT measurement error and the optimum fault detection/false alarm characteristics? • Is BIT optimally allocated in hardware, software, and firmware? • Have means been established to identify whether hardware or software has caused a failure indication? 	<ul style="list-style-type: none"> • Is the failure latency associated with a particular implementation of BIT consistent with the criticality of the function being monitored? • Is the test program set designed to take advantage of BIT capabilities? • Does building-block BIT make maximum use of mission circuitry? • Is the self-test circuitry designed to be testable? • Is the predicted failure rate contribution of the BIT circuitry within stated constraints? • Is the additional power consumption due to BIT within stated constraints? • Are BIT threshold values, which may require changing as a result of operational experience, incorporated in software or easily-modified firmware? • Are on-board BIT indicators used for important functions? Are BIT indicators designed such that a BIT failure will give a "fail" indication? • Is the additional weight due to BIT within stated constraints? • Is the additional part count due to BIT within stated constraints? • Is processing or filtering of BIT sensor data performed to minimize BIT false alarms? • Does mission software include sufficient hardware error detection capability?
Test Data Checklist	
<ul style="list-style-type: none"> • Do state diagrams for sequential circuits identify invalid sequences and indeterminate outputs? • For computer-assisted test generation, is the available software sufficient in terms of program capacity, fault modeling, component libraries, and post-processing of test response data? • If a computer-aided design system is used for design, does the CAD data base effectively support the test generation process and test evaluation process? • Is the tolerance band known for each signal on the item? 	<ul style="list-style-type: none"> • Are testability features included by the system designer documented in the Test Requirement Document (TRD) in terms of purpose and rationale for the benefit of the test designer? • For large scale ICs used in the design, are data available to accurately model the circuits and generate high-confidence tests? • Are test diagrams included for each major test? Is the diagram limited to a small number of sheets? Are inter-sheet connections clearly marked?

7.13.2 Definition of Safety Terms and Acronyms

The meanings of some terms and acronyms are unique to this section and are therefore included here to aid the reader.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Fail Safe: A design feature that either ensures that the system remains safe, or, in the event of a failure, forces the system to revert to a state which will not cause a mishap.

Hazard: A condition that is prerequisite to a mishap.

Hazard Probability: The aggregate probability of occurrence of the individual events that create a specific hazard.

Hazardous Material: Anything that due to its chemical, physical, or biological nature causes safety, public health, or environmental concerns that result in an elevated level of effort to manage.

Mishap: An unplanned event or series of events that result in death, injury, occupational illness, or damage to or loss of equipment or property or damage to the environment. An accident.

Risk: An expression of the possibility of a mishap in terms of hazard severity and hazard probability.

Risk Assessment: A comprehensive evaluation of the risk and its associated impact.

Safety: Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property or damage to the environment.

Safety Critical: A term applied to a condition, event, operation, process or item of whose proper recognition, control, performance or tolerance is essential to safe operation or use; e.g., safety critical function, safety critical path or safety critical component.

Safety-Critical Computer Software Components: Those computer software components and units whose errors can result in a potential hazard, or loss of predictability or control of a system.

System Safety: The application of engineering and management principles, criteria, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

7.13.3 Program Management and Control Elements

7.13.3.1 System Safety Program

A basic system safety program consists of the following safety-related elements.

7.13.3.2 System Safety Program Plan

This plan describes in detail those elements and activities of safety system management and system safety engineering required to identify, evaluate, and eliminate hazards, or reduce the

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

associated risk to a level acceptable to the managing activity throughout the system life cycle. It normally includes a description of the planned methods to be used to implement a system safety program plan, including organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

7.13.3.3 Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering Firms

This element consists of appropriate management surveillance procedures to ensure uniform system safety requirements are developed.

7.13.3.4 System Safety Program Reviews/Audits

This element is a forum for reviewing the system safety program, to periodically report the status of the system safety program, and, when needed, to support special requirements, such as certifications and first flight readiness reviews.

7.13.3.5 System Safety Group/System Safety Working Group Support

This element is a forum for suppliers and vendors to support system safety groups (SSGs) and system safety working groups (SSWGs) established in accordance with government regulations or as otherwise defined by the integrating supplier.

7.13.3.6 Hazard Tracking and Risk Resolution

This element is a single closed-loop hazard tracking system to document and track hazards from identification until the hazard is eliminated or the associated risk is reduced to an acceptable level.

7.13.3.7 System Safety Progress Summary

This element consists of periodic progress reports summarizing the pertinent system safety management and engineering activity that occurred during the reporting period.

7.13.4 Design and Integration Elements

7.13.4.1 Preliminary Hazard List

This element is a preliminary hazard list (PHL) identifying any especially hazardous areas for added management emphasis. The PHL should be developed very early in the development phase of an item.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.13.4.2 Preliminary Hazard Analysis

The purpose of the Preliminary Hazard Analysis (PHA) is to identify safety critical areas, evaluate hazards, and identify the safety design criteria to be used.

7.13.4.3 Safety Requirements/Criteria Analysis

The Safety Requirements/Criteria Analysis (SRCA) relates the hazards identified to the system design and identifies or develops design requirements to eliminate or reduce the risk of the hazards to an acceptable level. The SRCA is based on the PHL or PHA, if available. The SRCA is also used to incorporate design requirements that are safety related but not tied to a specific hazard.

7.13.4.4 Subsystem Hazard Analysis

The Subsystem Hazard Analysis (SSHA) identifies hazards associated with design of subsystems including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipments comprising each subsystem.

7.13.4.5 System Hazard Analysis

The System Hazard Analysis (SHA) documents the primary safety problem areas of the total system design including potential safety critical human errors.

7.13.4.6 Operating and Support Hazard Analysis

The Operating and Support Hazard Analysis (O&SHA) identifies associated hazards and recommends alternatives that may be used during all phases of intended system use.

7.13.4.7 Occupational Health Hazard Assessment

The Occupational Health Hazard Assessment (OHHA) identifies human health hazards and proposes protective measures to reduce the associated risks to levels acceptable to the managing activity.

7.13.5 Design Evaluation Elements

7.13.5.1 Safety Assessment

This element is a comprehensive evaluation of the mishap risk that is being assumed prior to the test or operation of a system or at the contract completion.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.13.5.2 Test and Evaluation Safety

The purpose of this element is to ensure that safety is considered (and safety responsibility assigned) in test and evaluation, to provide existing analysis reports and other safety data, and to respond to all safety requirements necessary for testing in-house, at other supplier facilities, and at Government ranges, centers, or laboratories.

7.13.5.3 Safety Review of Engineering Change Proposals and Requests for Deviation/Waiver

This element consists of performing and documenting the analyses of engineering change proposals (ECPs) and requests for deviation/waiver to determine the safety impact, if any, upon the system.

7.13.6 Compliance and Verification**7.13.6.1 Safety Verification**

Safety Verification is conducted to verify compliance with safety requirements by defining and performing tests and demonstrations or other verification methods on safety critical hardware, software, and procedures.

7.13.6.2 Safety Compliance Assessment

The element consists of performing and documenting a safety compliance assessment to verify compliance with all military, federal, national, and industry codes imposed contractually or by law. This element is intended to ensure the safe design of a system, and to comprehensively evaluate the safety risk that is being assumed prior to any test or operation of a system or at the completion of the contract.

7.13.6.3 Explosive Hazard Classification and Characteristics Data

The purpose of this element is to ensure the availability of tests and procedures need to assign an Explosive Hazard Classification (EHC) to new or modified ammunition, explosives (including solid propellants), and devices containing explosives, and to develop hazard characteristics data for these items.

7.13.6.4 Explosive Ordnance Disposal Source Data

The purpose of this element is to ensure that the following resources are available as needed: source data, explosive ordnance disposal procedures, recommended “render safe” procedures, and test items for new or modified weapons systems, explosive ordnance items, and aircraft systems.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.13.7 Tailoring Guidelines

A system safety program needs to be matched to the scope and complexity of the development program, i.e., tailored to the program requirements. The requirements of MIL-STD-882 are tailored primarily by the selection of the applicable elements. Tables 7.13-1, and 7.13-2 taken from MIL-STD-882, Appendix A, are element application matrices used to indicate the applicable elements for development programs, and for facilities acquisition programs.

7.14 Finite Element Analysis

7.14.1 Introduction and General Information

Finite element analysis (FEA) is an automated technique for determining the effects of mechanical loads and thermal stress on a structure or device. It is a computer simulation that can predict the material response or behavior of a model of that device or structure represented as a network of simple elements.

FEA is a powerful method for identifying areas of stress concentration that are susceptible to mechanical failure. A device is modeled by decomposing it into a collection of simple shapes, such as plate elements or three dimensional brick elements. The elements are connected together at node points. The analysis can provide material temperatures and stresses at each node point by simulating thermal or dynamic loading situations.

FEA can be used to assess the potential for thermal and mechanical failures before manufacture and testing. It may be used to analyze mechanical systems ranging in size from a portion of a microcircuit chip to a large space antenna. For this reason, FEA is an important numerical analysis technique.

7.14.2 Finite Element Analysis Application

FEA is most appropriately applied to structures too large to test economically, to irregular shaped objects or those composed of many different materials, which do not lend themselves to direct analysis, and to microelectronic devices that may exist only as electronic design representations. In each case, it will reveal areas at risk from mechanical or thermal stress.

A realistic test of a tower, large antenna, etc., cannot be done without going through the expense of constructing the structure. In most cases, this is much too costly, yet it is too risky to commit the design for a large structure to production without assurance of its reliability. FEA can provide the necessary assurance at a relatively insignificant expense. It can also be used when tests are impossible, such as when the structure is intended for use in outer space.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.13-1: APPLICATION MATRIX FOR SYSTEM PROGRAM DEVELOPMENT

TASK	TITLE	TASK TYPE	CONCEPT	PROGRAM PHASE		PROD
				VALID	FSKD	
100	System Safety Program	MGT	G	G	G	G
101	System Safety Program Plan	MGT	G	G	G	G
102	Integration/Management of Associate Contractors	MGT	S	S	S	S
103	Subcontractors and AE Firms	MGT	S	S	S	S
104	System Safety Program Review	MGT	G	G	G	G
105	SSG/SSWG Support	MGT	S	G	G	G
106	Hazard Tracking and Risk Resolution	MGT	G	G	G	G
107	Test and Evaluation Safety	MGT	G	G	G	G
108	System Safety Progress Summary	MGT	S	S	S	S
201	Qualifications of Key System Safety Personnel	MGT	S	S	S	S
201	Preliminary Hazard List	ENG	G	S	S	N/A
202	Preliminary Hazard Analysis	ENG	G	G	G	CC
203	Sub-system Hazard Analysis	ENG	N/A	G	G	CC
204	System Hazard Analysis	ENG	N/A	G	G	CC
205	Operating and Support Hazard Analysis	ENG	S	G	G	CC
206	Occupational Health Hazard Assessment	ENG	G	G	G	CC
207	Safety Verification	ENG	S	G	G	CC
208	Training	MGT	N/A	S	S	S
209	Safety Assessment	MGT	S	S	S	S
210	Safety Compliance Assessment	MGT	S	S	S	S
211	Safety Review of BCPs and Warnings	MGT	N/A	G	G	G
212	- RESERVED -	-	-	-	-	-
213	CPE/CPP System Safety Analysis	ENG	S	G	G	G
301	Software Req. Hazard Analysis	ENG	S	G	G	CC
302	Top-Level Design Hazard Analysis	ENG	S	G	G	CC
303	Detailed Design Hazard Analysis	ENG	S	G	G	CC
304	Code-Level Software Hazard Analysis	ENG	S	G	G	CC
305	Software Safety Testing	ENG	S	G	G	CC
306	Software/User Interface Analysis	ENG	S	G	G	CC
307	Software Change Hazard Analysis	ENG	S	G	G	CC

Notes: TASK TYPE
 ENG - System Safety Engineer
 MGT - Management

APPLICABILITY CODES
 S - Selectively Applicable
 G - Generally Applicable
 N/A - Not Applicable

PROGRAM PHASE
 CONCEPT - Conceptual
 VALID - Validation
 FSKD - Full Scale Engineering Development
 PROD - Production

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

TABLE 7.13-2: APPLICATION MATRIX FOR FACILITIES ACQUISITION

TASK	TITLE	TASK TYPE	CONCEPT	PROGRAM PHASE			PROD
				VALID	PSUED	PSUED	
100	System Safety Program	MGT	G	G	G	G	G
101	System Safety Program Plan	MGT	S	G	G	S	S
102	Integration Management of Associate Contractors, Subcontractors, and AE Firms	MGT	S	S	S	S	S
103	System Safety Program Reviews	MGT	G	G	G	G	G
104	SSG/ISSWG Support	MGT	G	G	G	G	G
105	Hazard Tracking and Risk Resolution	MGT	G	G	G	G	G
106	Test and Evaluation Safety	MGT	G	G	G	G	G
107	System Safety Progress Summary	MGT	S	S	S	S	S
108	Qualifications of Key System Safety Personnel	MGT	S	S	S	S	S
201	Preliminary Hazard List	BNG	G	N/A	N/A	N/A	N/A
202	Preliminary Hazard Analysis	BNG	G	S	N/A	N/A	N/A
203	Subsystem Hazard Analysis	BNG	N/A	S	G	G	G
204	System Hazard Analysis	BNG	N/A	G	G	G	G
205	Operating and Support Hazard Analysis	BNG	S	G	G	G	G
206	Occupational Health Hazard Assessment	BNG	G	S	N/A	N/A	N/A
207	Safety Verification	BNG	N/A	S	S	S	S
208	Training	MGT	S	S	S	S	S
209	Safety Assessment	MGT	N/A	S	G	S	S
210	Safety Compliance Assessment	MGT	N/A	S	S	S	S
211	Safety Review of EOPs and Waivers	MGT	S	S	S	S	S
212	- RESERVED -	-	-	-	-	-	-
213	GFE/IGFP System Safety Analysis	BNG	S	S	S	S	S
301	Software Req. Hazard Analysis	BNG	S	S	S	S	GC
302	Top-Level Design Hazard Analysis	BNG	S	S	S	S	GC
303	Detailed Design Hazard Analysis	BNG	S	S	S	S	GC
304	Code-Level Software Hazard Analysis	BNG	S	S	S	S	GC
305	Software Safety Testing	BNG	S	S	S	S	GC
306	Software/User Interface Analysis	BNG	S	S	S	S	GC
307	Software Change Hazard Analysis	BNG	S	S	S	S	GC

Notes: TASK TYPE
 BNG - System Safety Engineering
 MST - Management

APPLICABILITY CODES
 S - Selectively Applicable
 G - Generally Applicable
 N/A - Not Applicable

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

Conventional mathematical analysis of structures become intractable when they are complex or composed of many different materials. These same factors confound the estimation of temperatures within the structure. Judiciously applied, FEA can reduce the risks of using less conservative structural designs. Even smaller designs can benefit from using FEA simulated structures to reduce the need for prototypes and expensive tests.

Mechanical systems have historically been designed with large safety margins. However, many applications preclude this. Airborne structures, for example, must be lightweight, severely limiting the selection and the amount of material available. To accommodate such constraints without courting disaster requires a comprehensive stress analysis. Even when large safety factors are possible, the knowledge provided by FEA permits sound design to be achieved with the minimum amount of materials, thus generating significant cost savings.

The optimum time to detect a structural design flaw is before any construction begins. Changing a design while it is still only a file in a computer is almost trivial. The cost of fixing design errors after prototypes or production models are produced can be significant. The most costly fixes are those required after the system is operational, and the need for these is often revealed by some disaster. FEA provides the means for the early detection of problems in proposed structures, and hence, economical corrective action.

FEA, however, can be time consuming and analysis candidates must be carefully selected. Candidates for FEA include devices, components, or design concepts that: (a) are unproven and for which little or no prior experience or test information is available; (b) use advanced or unique packaging or design concepts; (c) will encounter severe environmental loads; or (d) have critical thermal or mechanical performance and behavior constraints. The most difficult and time consuming portion of an FEA is creating the model. This aspect of FEA is being addressed by the development of intelligent modeling software and automated mesh generators.

FEA can take many different forms, some specific types of FEA include:

- (1) Linear Static Analysis - Responses of a linear system to statically applied loads
- (2) Linear and Modal Dynamic Analyses - Responses to time-dependent loads
- (3) Heat Transfer Analysis - Analyses the flow or transfer of heat within a system
- (4) FEAP - Analyzes mechanical stress effects on electronic equipment, printed circuit boards (PCB), avionic equipment, etc.

Many commercial general purpose and special purpose software products for FEA are available.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.14.3 Finite Element Analysis Procedure

The following is a brief outline of a typical Finite Element Analysis - that of a hypothetical microcircuit/printed circuit board interface application.

First, the entire device (or a symmetrical part of the entire device) is modeled with a coarse mesh of relatively large sized elements such as 3-dimensional brick elements. The loading, material property, heat sink temperature, and structural support data are entered into the data file in the proper format and sequence as required by the FEA solver. The deflections and material stresses for all node point locations, see Figure 7.14-1, on the model are the desired output from the FEA.

Step 1: Perform FEA

- (1) Establish FEA mesh
- (2) Apply loading and boundary conditions
- (3) Perform simulation

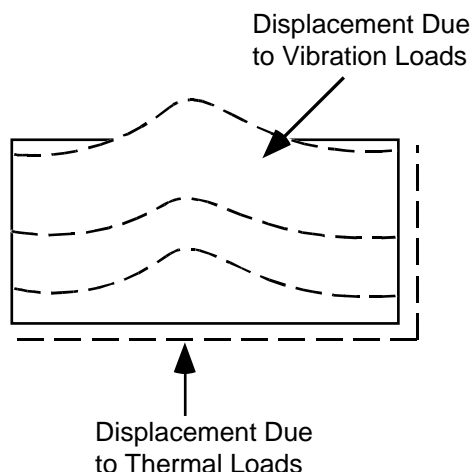


FIGURE 7.14-1: NODAL ANALYSIS

Step 2: Interpretation of Local Displacements/Stresses

For microelectronic devices, second or third follow-on models of refined regions of interest may be required because of the geometrically small feature sizes involved. The boundary nodes for the follow-on model are given initial temperatures and displacements that were acquired from the circuit board model. Figure 7.14-2 shows a refined region containing a single chip carrier and its leads. The more refined models provide accurate temperature, deflection, and stress information

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

for reliability analyses. For example, the results of Step 2 could be a maximum stress value in a corner lead of a chip carrier caused by temperature or vibration cycling.

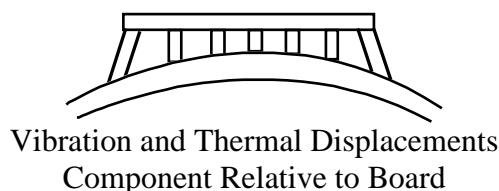


FIGURE 7.14-2: DISPLACEMENT/STRESS INTERPRETATION

Step 3: Perform Life Analysis

A deterministic life analysis is then made by locating the stress value, S_1 , on a graph of stress versus cycles-to-failure for the appropriate material, reading cycles to failures, N_1 , on the abscissa as shown in Figure 7.14-3. Cycles to failure and time to failure are related by the temperature cycling rate or the natural frequency for thermal or dynamic environments, respectively.

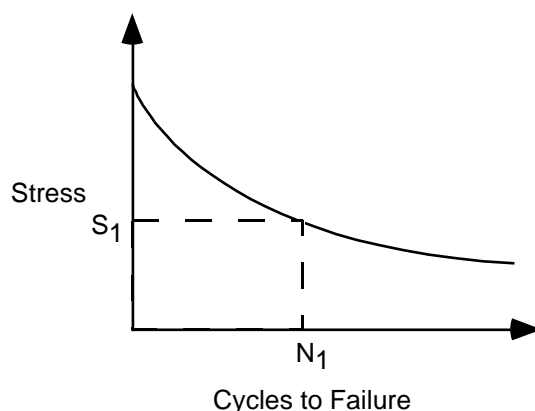


FIGURE 7.14-3: DETERMINISTIC ANALYSIS

Step 4: Estimate Circuit Board Lifetime

A distribution of stress coupled with a distribution of strength (i.e. scatter in fatigue data) will result in a probability distribution function and an estimate of the circuit board lifetime as shown in Figure 7.14-4.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

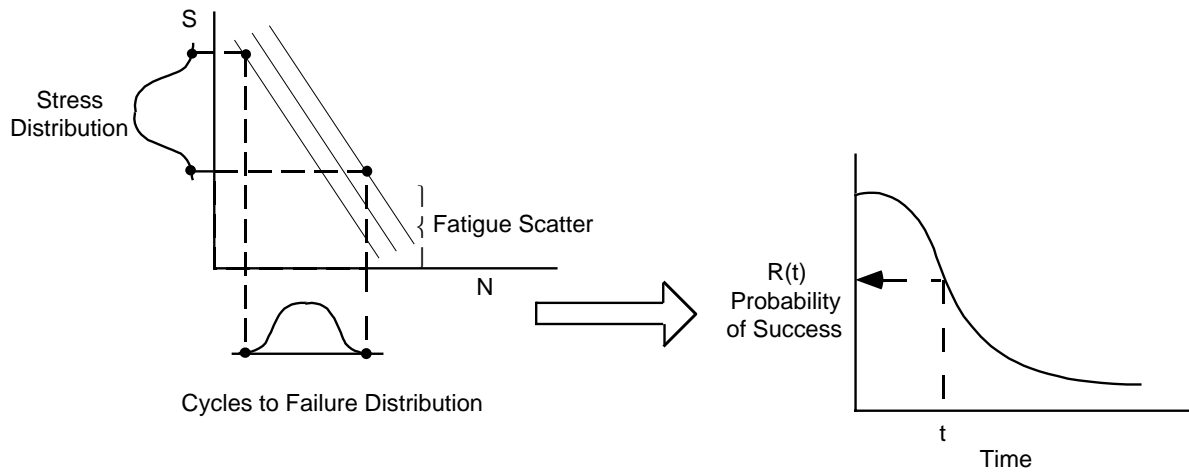


FIGURE 7.14-4: LIFETIME ESTIMATE

7.14.4 Applications

Two examples of how an FEA might be applied are:

- a. assess the number of thermal or vibration cycles to failure of an electronic device
- b. determine the probability of a fatigue failure at a critical region or location within a device after a given number of operating hours

7.14.5 Limitations

The adequacy of FEA is determined, or limited, by the following factors:

- a. Numerical accuracy
- b. Model accuracy
- c. Material properties

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

7.15 References for Section 7

1. Parts Selection, Application, and Control (PASC), Reliability Analysis Center, Rome, NY, 1993.
2. Reliable Application of Plastic Encapsulated Microcircuits, (PEM2), Reliability Analysis Center, Rome, NY, 1995.
3. Analog Testing Handbook, (ATH), Reliability Analysis Center, Rome, NY, 1993.
4. 767 AWACS Strategies for Reducing Diminishing Manufacturing Sources (DMS) Risk, DMSMS (Diminishing Manufacturing Sources and Material Shortages) 96 Conference, Montgomery, Texas, 7-9 May 96.
5. Best Practices - How to Avoid Surprises in the World's Most Complicated Technical Process, NAVSO P6071.
6. Precondition of Plastic Surface Mount Devices Prior to Reliability Testing, JESD 22-A113.
7. General Standard for Statistical Process Control, JEDEC Publication 19.
8. JEDEC Registered and Standard Outlines for Semiconductor Devices, JEDEC Publication 95.
9. Impact of Moisture on Plastic IC Package Cracking IPC-SM-786.
10. Test Method, Surface Mount Component Cracking, IPC-TM-650.
11. Buying Commercial and Nondevelopmental Items: A Handbook, SD-2, Office of the Under Secretary of Defense for Acquisition and Technology, April 1996.
12. Lipson, C., et al., Reliability Prediction -- Mechanical Stress/Strength Interference Models, RADC-TR-68-403, March 1967.
13. Lipson, C., et al., Reliability Prediction--Mechanical Stress/Strength Interference (nonferrous), RADC-TR-68-403, December 1968.
14. Nonelectronic Reliability Notebook, RADC-TR-85-194, October 1985.
15. Electronic Engineers' Handbook. Fink, D.G. and D. Christiansen, ed., New York, NY: McGraw Hill Book Co., 1982.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

16. Engineering Design Handbook: Reliable Military Electronics. AMCP 706-124, Headquarters U.S. Army Materiel Command, 5001 Eisenhower Ave, Alexandria, VA 22333, AD#A025665.
17. IEEE Recommended Practice on Surge Voltages in Low Voltage AC Power Circuits , IEEE Standard C62.41-1991.
18. Engineering Design Handbook: Design for Reliability, AMCP 706-196, AD#A027230, January 1976.
19. Lewis, E.E., Introduction to Reliability Engineering, John Wiley & Sons, Inc., New York, 1996.
20. Practical Reliability, Vol. 1 - Parameter Variations Analysis, NASA CR-1126, Research Triangle Institute, Research Triangle Park, NC, July 1968.
21. Ross, P., Taguchi Techniques for Quality Engineering, McGraw-Hill, New York, 1988.
22. Klion, J., A Redundancy Notebook, RADC-TR-77-287, December 1977, AD#A050837.
23. Shooman, M., Probabilistic Reliability: An Engineering Approach, New York, NY, McGraw-Hill Book Co., 1968.
24. Barrett, L.S., Reliability Design and Application Considerations for Classical and Current Redundancy Schemes, Lockheed Missiles and Space Co., Inc., Sunnyvale, CA, September 30,1973.
25. Application of Markov Techniques, IEC 1165, 1995.
26. Engineering Design Handbook: Environmental Series, Part One: Basic Environmental Concepts, AMCP 706-115, AD#784999.
27. Engineering Design Handbook: Environmental Series, Part Two: natural Environmental Factors, AMCP 706-116, AD#012648.
28. Engineering Design Handbook: Environmental Series, Part Three: Induced Environmental Factors, AMCP 706-117, AD#023512.
29. Engineering Design Handbook: Environmental Series, Part Four: Life Cycle Environments, AMCP 706-118, AD#0151799.
30. Engineering Design Handbook: Environmental Series, Part Five: Glossary of Environmental Terms, AMCP 706-119.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

31. Engineering Design Handbook: Design for Reliability. AMCP 706-196, AD#A027370, January 1976.
32. Arsenault, J.E. and J.A. Roberts, "Reliability and Maintainability of Electronic Systems," Computer Science Press, 9125 Fall River lane, Potomac, MD 20854, 1980.
33. Pavia, R.V., An Investigation into Engine Wear Caused by Dirt, Aeronautical Research Committee Report, ACA-50, July 1950.
34. Engineering Design Handbook: Design Engineer's Nuclear Effects Manual, Vol. I, Munitions and Weapon Systems (U), AMCP 706-335 (SRD).
35. Engineering Design Handbook: Design Engineer's Nuclear Effects Manual, Vol. II, Electronic Systems and Logistical Systems (U), AMCP 706-336 (SRD).
36. Engineering Design Handbook: Design Engineer's Nuclear Effects Manual, Vol. III, Nuclear Environment (U), AMCP 706-337 (SRD).
37. Engineering Design Handbook: Design Engineer's Nuclear Effects Manual, Vol. IV, Nuclear Effects (U), AMCP 706-338 (SRD).
38. Dougherty, E.M. and J.R. Fragola, Human Reliability Analysis, Wiley, 1988.
39. Lee, K.W., F.A. Tillman, and J.J. Higging, "A Literature search of the Human Reliability Component in a Man-Machine System," *IEEE Transactions on Reliability*, Vol. 37, No. 1, 1988 Apr, pp. 24-34.
40. Meister, D., "A Comparative Analysis of Human Reliability Models, Final Report, Contract N00024-71-C-1257," Naval Sea Systems Command, 1971 Nov.
41. Apostolakis, G.E., G. Mancini, R.W. van Otterloo, and F.R. Farmer, eds., "Special Issue on Human Reliability Analysis," *Reliability Engineering & System Safety*, Vol. 29, No. 3, ISBN:0951-8320, 1990.
42. LaSala, K.P., "Survey of Industry Human Performance Reliability Practices," *IEEE Reliability Society Newsletter*, Vol. 36, No. 2, 1990 Apr, pp. 7-8.
43. D.D. Woods, L.J. Johannesen, Richard I Cook, N.B. Sarter, Behind Human Error: Cognitive Systems, Computers, and Hindsight, Crew Systems Ergonomics Information Analysis Center, 1994.
44. Watson, P.A. and W. Hebenstreit, "Manpower, Personnel, and Training Workshop Group Report (IDA Record Document D-35)," Institute of Defense Analysis, 1983.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

45. Reason, J., Human Error, Cambridge University Press, 1992.
46. Siegel, A.I., K.P. LaSala, and C. Sontz, Human Reliability Prediction System User's Manual, Naval Sea Systems Command, 1977 Dec.
47. Blanchard, B.S., System Engineering Management, Wiley, 1991.
48. Advisory Group on Reliability of Electronic Equipment (AGREE), "Reliability of Military Electronic Equipment," Office of the Assistant Secretary of Defense, 1957 4 Jun, pp. 52-57.
49. Blanchard, B.S. and W.J. Fabricky, System Engineering Analysis, Prentice-Hall, 1990.
50. Taha, H., Operations Research: An Introduction, Macmillan, 1971.
51. Bazovski, I., Sr., "Weapon System Operational Readiness," *Proceedings 1975 R&M Symposium*, IEEE, 1975, pp. 174-178.
52. Van Cott, H.P. and R.G. Kinkade, Human Engineering Guide to Equipment Design (2nd Edition), Joint Army-Navy-Air Force Steering Committee, US Government Printing Office, 1972.
53. Boff, K.R., L. Kaufman, and J. Thomas, Handbook of Perception and Human Performance (Vols. 1 and 2), Wiley, 1986.
54. Boff, K. R. and Lincoln, J. E., Engineering Data Compendium: Perception and Performance (Vols. 1-3), Wright-Patterson AFB, OH: Armstrong Aerospace Medical Research Laboratory, 1988.
55. Booher, H. R., Ed, MANPRINT: An Approach to Systems Integration, Van Nostrand Reinhold, 1990.
56. Munger, S.J., R.W. Smith, and D. Paynes, "An Index of Electronic Equipment Operability: Data Store," (Air-C-43-1/62-RP[1]) (DTIC No. AD 607161), Pittsburgh PA, American Institute for Research, 1962 Jan.
57. Topmiller, D.A., J.S. Eckel, and E.J. Kozinsky, "Human Reliability Data Bank for Nuclear Power Plant Operations, Volume 1: A Review of Existing Human Error Reliability Data Banks" (NUREG/CR-2744/1 of 2 and SAND82-70571/1 of 2, AN, RX), Dayton OH, General Physics Corp., 1982 Dec .
58. Haney, L.N., H.S. Blackman, B.J. Bell, S.E. Rose, D.J. Hesse, L.A. Minton, and J.P. Jenkins, "Comparison and Application of Quantitative Human Reliability Analysis

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

-
- Methods for the Risk Methods Integration and Evaluation Program (RMIEP)," NUREG/CR-4835, Idaho National Engineering Laboratory, Idaho Falls, ID, Jan. 1989.
59. Lydell, B.O.Y., "Human Reliability Methodology. A Discussion of the State of the Art," *Reliability Engineering and System Safety*, 36 (1992), pp. 15-21.
 60. Dougherty, E.M., "Human Reliability Analysis; Need, Status, Trends, and Limitations," *Reliability Engineering and System Safety*, 29(1990), pp. 283-289.
 61. Swain, A.D., "Human Reliability Analysis: Need, Status, Trends and Limitations," *Reliability Engineering and Systems Safety*, 29(1990), pp. 301-313.
 62. Swain, A.D., "THERP", SC-R-64-1338, Sandia National Laboratories, Albuquerque, NM, 1964 Aug.
 63. Swain, A. D., and Guttman, H.E., Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (NUREG/CR-1278, SAND800 200, RX, AN), Sandia National Laboratories, Albuquerque, NM, 1983 Aug.
 64. Poucet, A., "The European Benchmark Exercise on Human Reliability Analysis," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, PSA '89, American Nuclear Society, Inc., La Grange, IL, 1989, pp. 103-110.
 65. Guassardo, G., "Comparison of the Results Obtained from the Application of Three Operator Action Models," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, PSA '89, American Nuclear Society, Inc., La Grange , IL, 1989, pp. 111-119.
 66. Krois., P.A., P.M. Haas, J.J. Manning, and R. Bovell, "Human Factors Review for Severe Accident Sequence Analysis" NUREG/CR-3887, Oak Ridge National Laboratory, Oak Ridge TN, 1985 Nov., p. 26.
 67. Hannaman, G.W., A.J. Spurgin, and Y.D. Lukic, "Human Cognitive Reliability for PRA Analysis," NUS-4531, NUS Corp., 1984, Dec.
 68. Joksimovich, V., A.J. Spurgin, D.D. Orvis, and P. Moieni, "EPRI Operator Reliability Experiments Program: Model Development/Testing," *Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment, PSA '89*, American Nuclear Society, Inc., La Grange Park IL, 1989 Apr., pp. 120-127.
 69. Dhillon, B.S., Human Reliability With Human Factors, Pergamon, 1988.
 70. Dhillon, B.S., "Modeling Human Errors in Repairable Systems", Proceedings of the 1989 Reliability and Maintainability Symposium, IEEE, New York, NY, pp. 418-423.
-

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

71. Siegel, A.I., and J.J. Wolf, Man-Machine Simulation Models, Wiley, 1969.
72. Siegel, A.I., W.D. Barter, J.J. Wolf, and H.E. Knee, "Maintenance Personnel Performance Simulation (MAPPS) Model: Description of Model Content, Structure, and Sensitivity Testing," NUREG/CR-3626, Oak Ridge National Laboratory, Oak Ridge, TN, 1984 Dec.
73. Woods, D.D., E.M. Roth, and H. Pople, Jr, "Cognitive Environment Simulation: An Artificial Intelligence System for Human Performance Assessment," NUREG/CR-4862, Westinghouse Research and Development Center, Pittsburgh, PA, 1987 Nov.
74. Embrey, D.E., "The Use of Performance Shaping Factors and Quantified Expert Judgement in the Evaluation of Human Reliability: An Initial Appraisal," NUREG/CR-2986, Brookhaven National Laboratory, 1983.
75. Embrey, D.E., P. Humphreys, E.A.Rosa, B. Kirwan, K. Rea, "SLIM-MAUD, An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement," NUREG/CR-3518, U.S. Nuclear Regulatory Commission, 1984.
76. Rosa, E.A., P.C. Humphreys, C.M. Spettell, and D.E. Embrey, "Application of SLIM-MAUD: A Test of an Interactive Computer-based Method for Organizing Expert Assessment of Human Performance and Reliability," NUREG/CR-4016, Brookhaven National Laboratory, Upton, NY, 1985 Sep.
77. Ireson, W.G., and C.F. Coombs, Handbook of Reliability Engineering and Management, New York, McGraw-Hill, 1988, Ch 12.
78. Procedures for Performing a Failure Mode, Effects, and Criticality Analysis, MIL-STD-1629, 28 Nov 1984.
79. Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA) , IEC 812, 1985.
80. Surface Vehicle Recommended Practice: Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects in Manufacturing (Process FMEA) Reference Manual , SAE J-1739, July 1994.
81. Michels, J.M., "Computer Evaluation of the Safety Fault Tree Model," Proceedings System Safety Symposium, 1965, available from University of Washington Library, Seattle, WA.
82. Henley, E.J., and J.W. Lynn (Eds), Generic Techniques in System Reliability Assessment, Nordhoff, Leyden, Holland, 1976.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

83. Vesely, W.E., "A Time-Dependent Methodology for Fault Tree Evaluation," Nuclear Engineering and Design, 13, 2 August 1970.
84. Fault Tree Handbook. NUREG-0492, available from Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.
85. Fault Tree Analysis, IEC 1025, 1990.
86. Sneak Circuit Analysis for the Common Man, RADC-TR-89-223.
87. Integration of Sneak Circuit Analysis with Design, RADC-TR-90-109.
88. Automated Sneak Circuit Analysis Technique, Rome Air Development Center, Griffiss Air Force Base, N.Y., 13441, 1990.
89. SCAT: Sneak Circuit Analysis Tool, Version 3.0, RL-TR-95-232.
90. Clardy, R.C., "Sneak Circuit Analysis Development and Application," 1976 Region V, IEEE Conference Digest, 1976, pp. 112-116.
91. Hill, E.J., and L.J. Bose, "Sneak Circuit Analysis of Military Systems," Proceedings of the 2nd International System Safety Conference, July 1975, pp. 351-372.
92. Buratti, D.L., and Goday, S.G., Sneak Analysis Application Guidelines. RADC-TR-82-179, Rome Air Development Center, Griffiss Air Force Base, N.Y., 13441, June 1982.
93. Godoy, S.G., and G.J. Engels, "Sneak Circuit and Software Sneak Analysis," Journal of Aircraft, Vol. 15, August 1978, pp. 509-513.
94. Definition of Terms for Testing Measurement and Diagnostics, MIL-STD-1309, February 1992.
95. Testability Program for Electronic Systems and Equipments, MIL-HDBK-2165, July 1995.
96. Skeberdis, P.W., E.G. White, Fault Logging Using a Micro Time Stress Measurement Device, RL-TR-95-289, Westinghouse Electronics Systems, January 1996.
97. Havey, G., S. Louis, S. Buska, Micro-Time Stress Measurement Device Development, RL-TR-94-196, Honeywell, Inc., November 1994.
98. Environmental Characterization Device Sourcebook (ECDS), Reliability Analysis Center, PO Box 4700, Rome, NY 13342-4700, September 1995.

SECTION 7: RELIABILITY ENGINEERING DESIGN GUIDELINES

99. Testability Design Rating System: Testability Handbook and Analytical Procedure, (2 Vols.), RL-TR-92-12.
100. Testability Program for Systems and Equipment, MIL-HDBK-2165, January 1985.
101. Electromagnetic Properties and Effects of Advanced Composite Materials: Measurement and Modeling, RADC-TR-78-156.
102. Electromagnetic Shielding Effectiveness for Isotropic and Anisotropic Materials, RADC-TR-81-162.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

8.0 RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION,
AND GROWTH

8.1 Introduction

Successful or satisfactory operation - the goal of all design efforts - yields little information on which to base improvements. Failures, on the other hand, contribute a wealth of data on “what to improve” or “what to design against” in subsequent efforts. The feedback of information obtained from the analysis of failures is one of the principal stepping stones of progress.

The prediction or assessment of reliability is actually an evaluation of unreliability, the rate at which failures occur. The nature and underlying cause of failures must be identified and corrected to improve reliability. Reliability data consist of reports of failures and reports of duration of successful operation of the monitored equipment/system.

Reliability data is used for three main purposes:

- (1) To verify that the equipment is meeting its reliability requirements
- (2) To discover deficiencies in the equipment to provide the basis for corrective action
- (3) To establish failure histories for comparison and for use in prediction

Reliability data can also be useful in providing information about logistics, maintenance, and operations. The data can provide a good estimate of the degradation and wearout characteristics of parts and components and how spare parts requirements are affected.

From this information, not only can effective preventive maintenance routines to control frequent trouble areas be developed, but also an estimate can be obtained of the number of maintenance manhours required to assure a desired level of reliability.

It is important that the data be factual so that a high degree of credence may be placed in the conclusions derived from it. Incomplete and inaccurate reporting will inevitably lead to either complete loss of confidence in the data or to incorrect conclusions and, hence, incorrect decisions and actions based on the conclusions.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

Reliability/failure data can be obtained from a number of sources.

- (1) An in-house failure analysis and corrective action system (FRACAS)
- (2) Reliability test data
- (3) Subcontractor or vendor data
- (4) Field data
- (5) Reliability data banks

The most useful of the above sources are (1) and (2), and possibly (5). The other sources are not as reliable since they are, in most cases, incomplete. For example, the military maintenance collection systems for collecting field data (e.g., the Army's TAMMS, the Navy's 3M, and the Air Force's REMIS and other maintenance data collection systems) are primarily maintenance oriented (see Section 11). Thus, field reliability cannot be assessed by using data from these systems alone. All of the factors influencing the data need to be clearly understood. These factors include the ground rules for collecting the data, assumptions made during analysis, and so forth. Clearly understanding these factors assures that the data will be properly interpreted and that conclusions will be credible.

The following section provides more details on a FRACAS system. The sections on Reliability Testing and Growth discuss the collection and analysis of reliability test data.

8.2 Failure Reporting, Analysis, and Corrective Action System (FRACAS) and Failure Review Board (FRB)

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

The purpose of FRACAS is to collect failure data, provide procedures to determine failure cause, and document corrective action taken. It requires the contractor to have a system that collects, analyzes and records failures that occur for specified levels of assembly prior to acceptance of the hardware by the procuring activity.

Failure reporting and analysis is necessary to ensure that a product's reliability and maintainability will be achieved and sustained. The FRACAS program is a key element in "failure recurrence" control for newly developed and production equipment. A FRACAS program must include provisions to ensure that failures are accurately reported and thoroughly analyzed and that corrective actions are taken on a timely basis to reduce or prevent recurrence.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

An in-plant FRACAS determines the basic causes of failures associated with design or manufacturing, and provides a closed-loop method of implementing corrective action. The system should emphasize the investigation and analysis of all failures, regardless of their apparent frequency or impact, and classification of failures according to categories of design/part procurement, manufacture, or assembly and inspection. It is well known that the most economical repair of a failure occurs at the component part level. A conventional rule of thumb is that a repair action at the subassembly level costs an order of magnitude more than at the part level, and a repair at the product level costs an order of magnitude more than a repair at the subassembly level.

Data on electronic equipment malfunctions can be obtained from any or all of the following types of data sources:

- (1) Design verification tests
- (2) Pre-production tests
- (3) Production tests
- (4) Subcontractor tests
- (5) Field data

The FRACAS system must provide essential information on:

- (1) What failed
- (2) How it failed
- (3) Why it failed
- (4) How future failures can be eliminated

8.2.1.1 Closed Loop Failure Reporting/Corrective Actions System

Figure 8.2-1 indicates the main steps in a closed-loop FRACAS. As shown in Figure 8.2-1, a typical FRACAS consists of fourteen steps.

- (1) A failure is observed during some operation or test.
- (2) The observed failure is fully documented, including, as a minimum
 - (a) Location of failure
 - (b) Date and time of failure

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

- (c) Part number of the failed system/equipment
- (d) Serial number of the failed system/equipment
- (e) Model number of the failed system/equipment
- (f) Observed failure symptoms
- (g) Name of the individual who observed the failure
- (h) All significant conditions which existed at the time of the observed failure

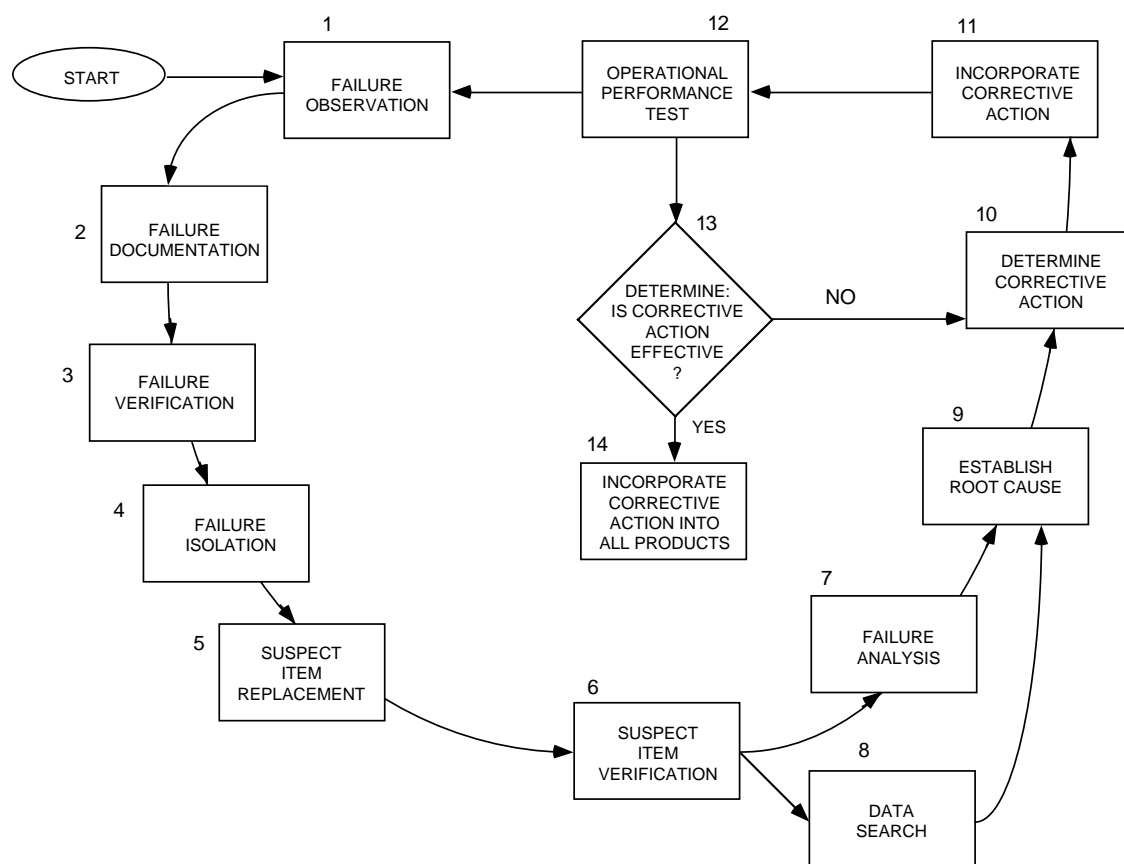


FIGURE 8.2-1: CLOSED LOOP FAILURE REPORTING AND
CORRECTIVE ACTION SYSTEM

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

- (3) Failure verification (i.e., reconfirmation of the validity of the initial failure observation).
- (4) Failure isolation (i.e., localization of the failure to the lowest replaceable defective item within the system/equipment).
- (5) Replacement of the suspected defective item with a known good item and retest of the system/equipment to provide assurance that the replacement item does in fact correct the originally reported failure.
- (6) Retest of the suspect item at the system/equipment level or at a lower level to verify that the suspect item is defective.
- (7) Failure analysis of the defective item to establish the internal failure mechanism responsible for the observed failure or failure mode.
- (8) A search of existing data to uncover similar failure occurrences in this or related items (i.e., establishing the historical perspective of the observed failure mode/failure mechanism).
- (9) Utilizing the data derived from Steps 7 and 8, determine the antecedent or root cause of the observed failure.
- (10) Determine the necessary corrective action, design change, process change, procedure change, etc. to prevent future failure recurrence. The decision regarding the appropriate corrective action should be made by an interdisciplinary design team.
- (11) Incorporation of the recommended corrective action into the original test system/equipment.
- (12) Retest of the system/equipment with the proposed corrective action modification incorporated.
- (13) After suitable retest and review of all applicable data, determine if proposed corrective action is effective.
- (14) After the effectiveness of the proposed corrective action has been proven, the corrective action is then incorporated into the deliverable systems/equipment.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

There are several “keys” that make the failure reporting and corrective action cycle effective. These are:

- (1) The discipline of the report writing itself must be maintained so that an accurate description of failure occurrence and proper identification of the failed items are ensured.
- (2) The proper assignment of priority and the decision for failure analysis must be made with the aid of cognizant design engineers and systems engineers.
- (3) The status of all failure analyses must be known. It is of prime importance that failure analyses be expedited as priority demands and that corrective action be implemented as soon as possible.
- (4) The root cause of every failure must be understood. Without this understanding, no logically derived corrective actions can follow.
- (5) There must be a means of tabulating failure information for determining failure trends and the mean times between failures of system elements. There should also be a means for management visibility into the status of failure report dispositions and corrective actions.
- (6) The system must provide for high level technical management concurrence in the results of failure analysis, the soundness of corrective action, and the completion of formal actions in the correction and recurrence prevention loop.
- (7) An extremely valuable assurance mechanism is to have active Government involvement in surveillance of the adequacy of the failure reporting, analysis, and corrective action effort.

The contractor's program plan should clearly describe his proposed FRACAS. Furthermore it should identify those provisions incorporated therein to ensure that effective corrective actions are taken on a timely basis. The applicable statement of work (SOW) should identify the extent to which the contractor's FRACAS must be compatible with the procuring agency's data system. It should also identify the levels of assembly and test to be addressed by the FRACAS, give definitions for each of the failure cause categories, identify the applicable logistics support requirements and identify the data items required for delivery.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

8.2.1.2 Failure Reporting Systems

Normally a manufacturer's reliability engineering organization is responsible for instituting and managing FRACAS. They establish policy, provide direction, and monitor the status of FRACAS investigations. The cognizant inspection and testing organizations, including reliability and quality engineering, are responsible for initiating failure reports promptly as they are observed. The project management office generally reviews recommendations, coordinates analyses and test activities with the government, authorizes the implementation of acceptable fixes or corrective measures and provides direction relative to continuation of tests. Often, it is the quality assurance organization that transmits reports to the government and coordinates implementation of corrective actions.

8.2.1.3 Failure Reporting Forms

It is imperative that failure reporting and resultant corrective actions be documented. Therefore, failure reporting and corrective actions forms must be designed to meet the needs of the individual system development and production program as well as the organizational responsibilities, requirements, and constraints of the manufacturer. Figure 8.2-2 is an example of a typical failure report form used in a FRACAS system.

8.2.1.4 Data Collection and Retention

Maintaining accurate and up-to-date records through the implementation of the data reporting, analysis and corrective action system described in the preceding subsections provides a dynamic, expanding experience base. This experience base, consisting of test failures and corrective actions, is not only useful in tracking current programs but can also be applied to the development of subsequent hardware development programs. Furthermore, the experience data can be used to:

- (1) Assess and track reliability
- (2) Perform comparative analysis and assessments
- (3) Determine the effectiveness of quality and reliability activities
- (4) Identify critical components and problem areas
- (5) Compute historical part failure rates for new design reliability prediction (in lieu of using generic failure rates found in MIL-HDBK-217, for example)

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

8.2.2 Failure Review Board

For the acquisition of certain critical (extremely expensive and complex) systems and equipments, a separate Failure Review Board (FRB) may sometimes be established specifically to oversee the effective functioning of the FRACAS. The Failure Review Board activity is reliability management. A closed loop FRACAS with an FRB is illustrated in Figure 8.2-3.

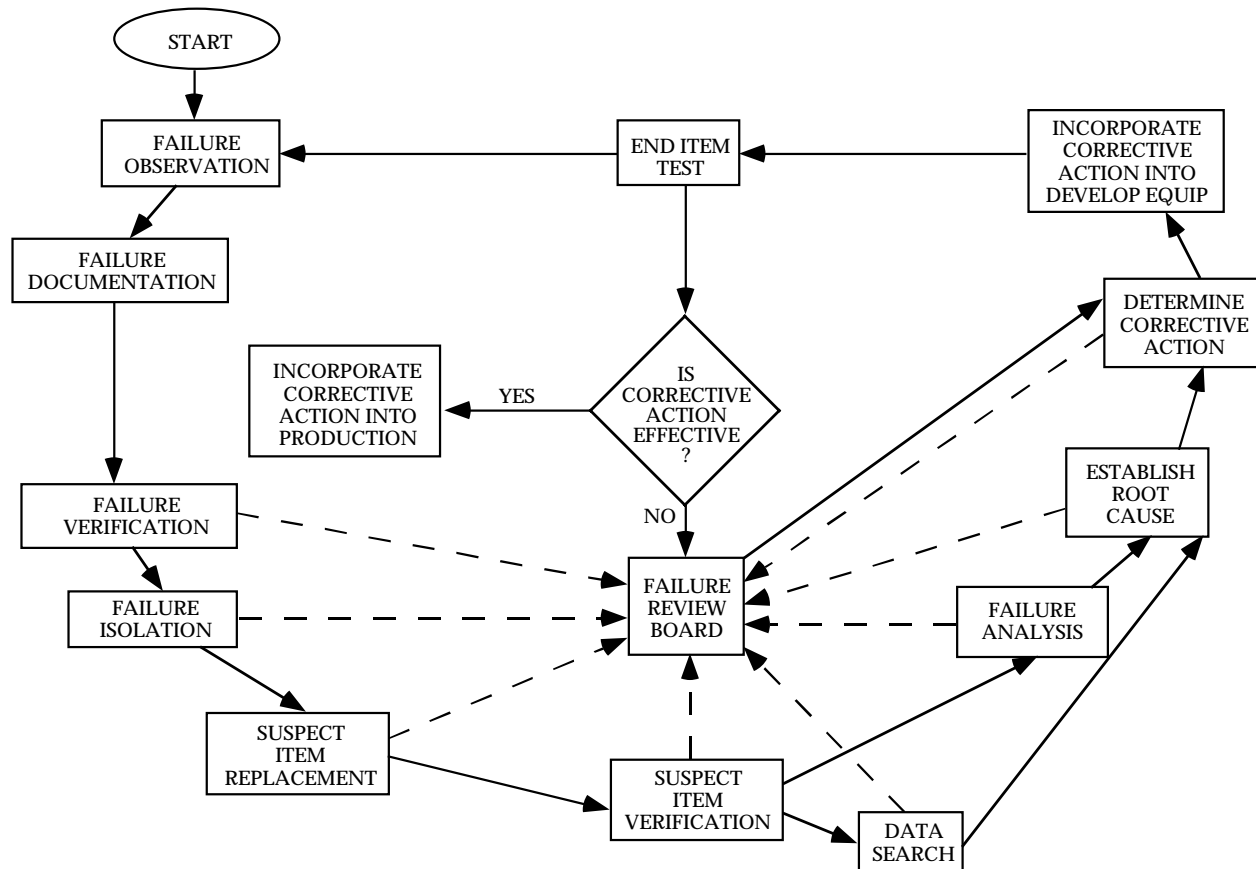


FIGURE 8.2-3: CLOSED LOOP FAILURE REPORTING AND CORRECTIVE ACTION
SYSTEM WITH FAILURE REVIEW BOARD

The purpose of the Failure Review Board is to provide increased management visibility and control of the FRACAS. Its intent is to improve reliability and maintainability of hardware and associated software by the timely and disciplined utilization of failure and maintenance data. The FRB consists of a group of representatives from appropriate organizations with sufficient level of responsibility to ensure that failure causes are identified with enough detail to generate and implement effective corrective actions which are intended to prevent failure recurrence and to simplify or reduce the maintenance tasks.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

The FRB usually consists of higher level management personnel who possess the authority to set priorities, establish schedules, assign specific responsibility and authorize adequate funding to insure the implementation of any necessary changes when dealing with complex and difficult problems. The acquiring activity usually reserves the right to appoint a representative to the FRB as an observer.

8.3 Reliability Data Analysis

From a reliability assessment viewpoint, failure data are used to:

- (1) Determine the underlying probability distribution of time to failure and estimate its parameters (if not already known)
- (2) Determine a point estimate of a specific reliability parameter, e.g., MTBF
- (3) Determine a confidence interval that is believed to contain the true value of the parameter

Two methods are used to analyze failure data:

- (1) Graphical methods
- (2) Statistical analysis

In many practical cases, graphical methods are simple to apply and produce adequate results for estimating the underlying distribution. They are virtually always a useful preliminary to more detailed statistical analysis. The two methods will be discussed in more detail in the following subsections.

8.3.1 Graphical Methods

The basic idea of graphical methods is the use of special probability plotting papers in which the cumulative distribution function (cdf) or the cumulative hazard function can be plotted as a straight line for the particular distribution being studied. Since a straight line has two parameters (slope and intercept), two parameters of the distribution can be determined. Thus, reliability data can be evaluated quickly, without a detailed knowledge of the statistical mathematics being necessary. This facilitates analysis and presentation of data.

Graphical curve-fitting techniques and special probability-plotting papers have been developed for all of the distributions commonly associated with reliability analysis (Refs. [4], [5]).

Ranking of Data

Probability graph papers are based upon plots of the variable of interest against the cumulative

 SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

percentage probability. The data, therefore, need to be ordered, and the cumulative probability calculated. For reliability work, the data are ordered from the smallest to largest; this is referred to as order statistics. For example, consider the data on times-to-failure of 20 items (Table 8.3-1). For the first failure, the cumulative percent failed is 1/20 or 5%. For the second, the cumulative percent failed is 2/20 or 10%, and so on to 20/20 or 100% for the 20th failure. However, for probability plotting, it is better to make an adjustment to allow for the fact that each failure represents a point on a distribution. Thus, considering that the whole population of 20 items represents a sample, the times by which 5, 10, ..., 100% will have failed in several samples of 20 will be randomly distributed. However, the data in Table 8.3.1-1 show a bias, in that the first failure is shown much further from the zero cumulative percentage point than is the last from 100% (in fact, it coincides). To overcome this, and thus to improve the accuracy of the estimation, mean or median ranking of cumulative percentages is used for probability plotting. Mean ranking is used for symmetrical distributions, e.g., normal; median ranking is used for skewed distributions, e.g., Weibull.

The usual method for mean ranking is to use $(n + 1)$ in the denominator, instead of n , when calculating the cumulative percentage position. Thus in Table 8.3-1 the cumulative percentages (mean ranks) would be:

$$\begin{aligned} \frac{1}{20 + 1} &= .048 \cong 5\% \\ \frac{2}{20 + 1} &= .096 \cong 10\% \\ &\cdot \\ &\cdot \\ &\cdot \\ \frac{20}{20 + 1} &= .952 \cong 95\% \end{aligned}$$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

TABLE 8.3-1: DATA ON TIMES TO FAILURE OF 20 ITEMS

Order No.	Time to Failure (hours)	Cumulative % (Cdf)	Mean Rank (%) (Cdf)
1	175	5	5
2	695	10	10
3	872	15	14
4	1250	20	19
5	1291	25	24
6	1402	30	29
7	1404	35	33
8	1713	40	38
9	1741	45	43
10	1893	50	48
11	2025	55	52
12	2115	60	57
13	2172	65	62
14	2418	70	67
15	2583	75	71
16	2725	80	76
17	2844	85	81
18	2980	90	86
19	3268	95	90
20	3538	100	95

These data are shown plotted on normal probability paper in Figure 8.3-1 (circles). The plotted points show a reasonably close fit to the straight line drawn 'by eye.' Therefore, we can say that the data appear to fit the cumulative normal distribution represented by the line.

Median ranking, as was previously stated, is used for skewed distributions such as the Weibull because it provides a better correction. The most common approximation for median ranking (Ref. [4]) is given by:

$$\text{Median rank } (n,i) = r_i = \frac{i - 0.3}{n + 0.4}$$

where r_i is the i^{th} order value and n is the sample size. Median ranking is the method most used in probability plotting, particularly if the data are known not to be normally distributed. Also, to save calculations, tables of median ranks are available for use. These are included in Table 8.3-2 and will be used in the examples to be described later.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

8.3.1.1 Examples of Graphical Methods

Reference [5] provides an excellent discussion of caveats that must be considered in graphical estimation. Now, let us turn to some examples.

Example 1: Normal Distribution1. When to Use

This method estimates μ and σ , the mean and standard deviation when failure times are normally distributed. This method yields a less accurate estimate than statistical analysis but requires very minimal calculations.

2. Conditions for Use

- a. Failure times must be collected, but may be censored; censored data is discussed in the next section.
- b. Normal probability paper is required.

3. Method

- a. On normal probability paper plot the i^{th} failure time in a sample of n ordered failure times on the lower axis vs. $\frac{i}{n+1}$ on the right hand axis.

Example

- a. The sample data used in Table 8.3-1 are repeated here, with the necessary plotting positions (mean ranks).

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

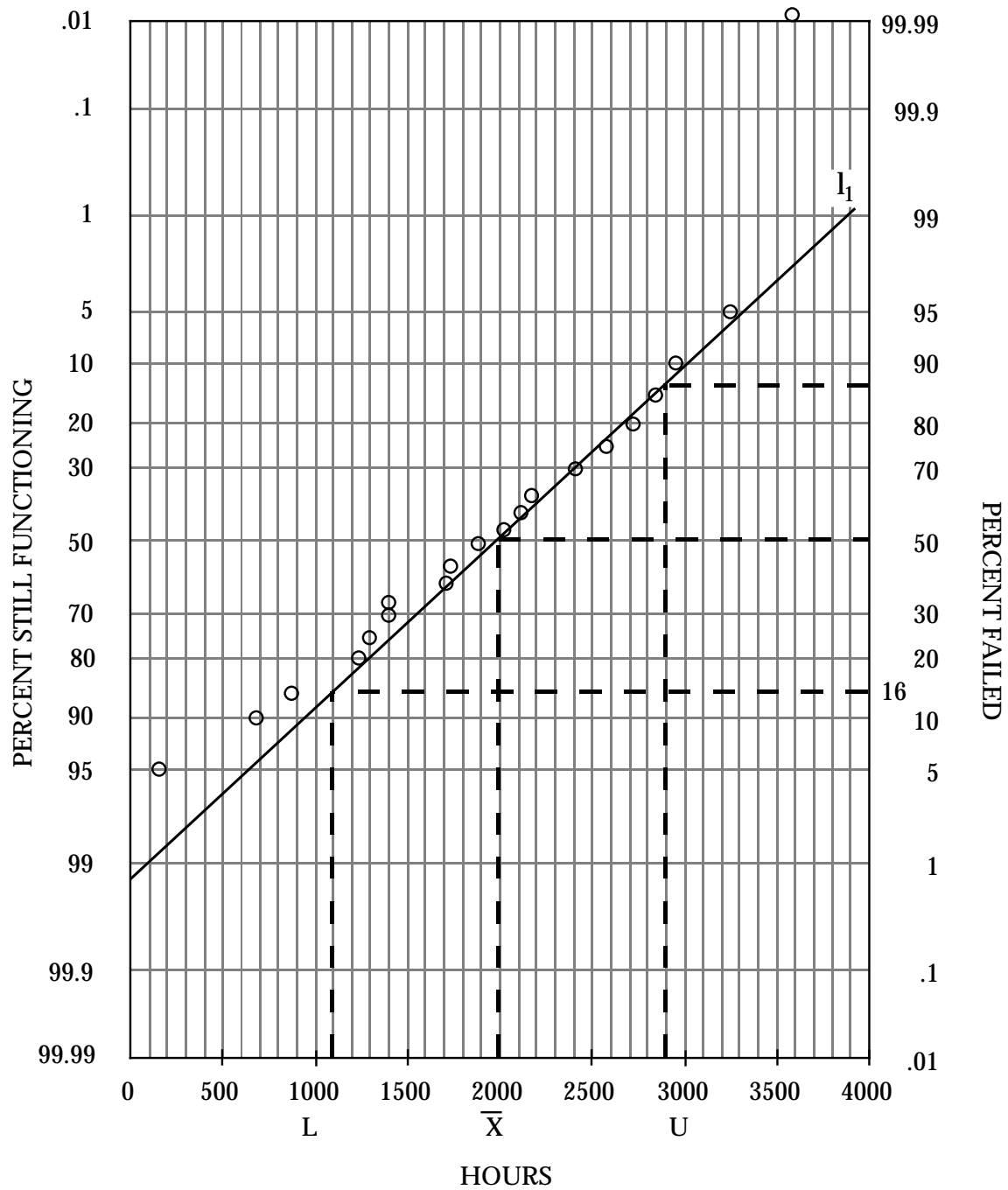


FIGURE 8.3-1: GRAPHICAL POINT ESTIMATION FOR THE NORMAL DISTRIBUTION

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

TABLE 8.3-2: MEDIAN RANKS

sample size = n

failure rank = i

i	n									
	1	2	3	4	5	6	7	8	9	10
1	.5000	.2929	.2063	.1591	.1294	.1091	.0943	.0830	.0741	.0670
2		.7071	.5000	.3864	.3147	.2655	.2295	.2021	.1806	.1632
3			.7937	.6136	.5000	.4218	.3648	.3213	.2871	.2594
4				.8409	.6853	.5782	.5000	.4404	.3935	.3557
5					.8706	.7345	.6352	.5596	.5000	.4519
6						.8906	.7705	.6787	.6065	.5481
7							.9057	.7979	.7129	.6443
8								.9170	.8194	.7406
9									.9259	.8368
10										.9330

i	n									
	11	12	13	14	15	16	17	18	19	20
1	.0611	.0561	.0519	.0483	.0452	.0424	.0400	.0378	.0358	.0341
2	.1489	.1368	.1266	.1188	.1101	.1034	.0975	.0922	.0874	.0831
3	.2366	.2175	.2013	.1873	.1751	.1644	.1550	.1465	.1390	.1322
4	.3244	.2982	.2760	.2568	.2401	.2254	.2125	.20099	.1905	.1812
5	.4122	.3789	.3506	.3263	.3051	.2865	.2700	.2553	.2421	.2302
6	.5000	.4596	.4253	.3958	.3700	.3475	.3275	.3097	.2937	.2793
7	.5878	.5404	.5000	.4653	.4350	.4085	.3850	.3641	.3453	.3283
8	.6756	.6211	.5747	.5347	.5000	.4695	.4425	.4184	.3968	.3774
9	.7634	.7018	.6494	.6042	.5650	.5305	.5000	.4728	.4484	.4264
10	.8511	.7825	.7240	.6737	.6300	.5915	.5575	.5272	.5000	.4755
11	.8389	.8632	.7987	.7432	.6949	.6525	.6150	.5816	.5516	.5245
12		.9439	.8734	.8127	.7599	.7135	.6725	.6359	.6032	.5736
13			.9481	.8822	.8249	.7746	.7300	.6903	.6547	.6226
14				.9517	.8899	.8356	.7875	.7447	.7063	.6717
15					.9548	.8966	.8450	.7991	.7579	.7207
16						.9576	.9025	.8535	.8095	.7698
17							.9600	.9078	.8610	.8188
18								.9622	.9126	.8678
19									.9642	.9169
20										.9659

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. Method (continued)Example

Failure Time (Hours)	Plotting Position $\frac{i}{n+1}$
175	.05
695	.10
872	.14
1250	.19
1291	.24
1402	.29
1404	.33
1713	.38
1741	.43
1893	.48
2025	.52
2115	.57
2172	.62
2418	.67
2583	.71
2725	.76
2844	.81
2980	.86
3268	.90
3538	.95

b. Draw the line of best fit through the plotted points by using the last point plotted as a reference point for a straight edge and dividing the rest of the points into two equal groups above and below the line.

c. The mean, μ , is estimated by projecting the 50% probability of failure point on the right hand axis to the line and then projecting that intersection point down to the lower axis. The estimate of μ , \bar{x} , is read there.

b. Figure 8.3-1 is the plot of this data on normal paper. The normal line has been labeled l_1 .

c. The value of \bar{X} is read as 2000 hours.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

d. The estimate of σ is obtained by first projecting the intersection of the 84% probability of failure point on the right hand axis with the normal line to the lower axis. Call that point on the lower axis U.

d. U = 2900 hours

e. Repeat step d with the 16% point. Call the point L

e. L = 1100 hours

f. The estimate of σ is

$$s = \frac{U - L}{2}$$

f. The sample standard deviation is

$$s = \frac{U - L}{2} = \frac{2900 - 1100}{2} = 900 \text{ hours}$$

g. The 95% confidence limits around the mean are given by $\bar{X} \pm t s/\sqrt{n}$ where t is shown below for various sample sizes, n.

g. $2000 \pm (2.09) (900)/\sqrt{20}$
2000 \pm 420 hours

<u>n</u>	<u>t</u>
5	2.57
10	2.23
20	2.09
30	2.04
50	2.00
∞	1.96

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

Example 2: Weibull Distribution

1. When to Use. The flexibility of the Weibull distribution makes it useful in describing the probability density function for a variety of cases. The Weibull cumulative distribution function is given by:

$$F(t) = 1 - e^{-\left[1(t/\theta)^\beta\right]}, \quad 0 \leq t \leq \infty$$

The Weibull distribution is used to describe the distribution of times to failure and of strengths of brittle materials, and the weakest link phenomena. It is an appropriate failure law model whenever the system consists of a number of components, and failure is essentially due to the “most severe” fault among a large number of faults in the system. By making an appropriate choice of the shape parameter, β , either an increasing or a decreasing failure rate can be obtained. Estimates of the Weibull shape (β) and scale (θ) parameters may be obtained graphically using *ln-ln* (or a special Weibull probability) graph paper. Less accurate than statistical methods, this method can be done quickly and easily.

2. Steps in Using the Graphical Method

- a. Collect failure times for items under test, put in ascending order, and assign an order number to each. The failure times are the values to be plotted on the x-axis. Note that failure time may be in hours, cycles, or whatever measure of life is appropriate for the item in question.
- b. Assign the median rank for each order number. The median ranks are the values to be plotted on the y-axis. The median rank is one model used for the cumulative probability of failures, $F(t)$. It is usable when the number of failures is greater than 20. The formula is:

$$\text{Median Rank (n,i)} = \frac{i - 0.3}{n + 0.4}$$

where: n = number of failures
i = order number

- c. Plot the pairings of median ranks and failure times on Weibull probability graph paper. Draw a straight line that best fits the data (i.e., roughly an equal number of data points will be on either side of the line).

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

- d. The slope of the line is β . The slope is calculated using the following equation:

$$\beta = \frac{\Delta Y}{\Delta X} = \frac{\ln \ln \left(\frac{1}{1-F(t_2)} \right) - \ln \ln \left(\frac{1}{1-F(t_1)} \right)}{\ln t_2 - \ln t_1}$$

Note 1: This equation assumes that *ln-ln* paper is used. Log-log paper can also be used with the following equation:

$$\beta = \frac{\log \ln \left(\frac{-1}{1-F(t_2)} \right) - \log \ln \left(\frac{-1}{1-F(t_1)} \right)}{\log t_2 - \log t_1}$$

Note 2: Some special Weibull graph paper allows β to be read directly.

3. Example

The following failure data are collected from a test in which 20 items were tested to failure.

Order Number	Failure Time (in hours)	Median Rank (%)
1	92	3.41
2	130	8.31
3	233	13.22
4	260	18.12
5	320	23.02
6	325	27.93
7	420	32.83
8	430	37.74
9	465	42.64
10	518	47.55
11	640	52.45
12	700	57.36
13	710	62.26
14	770	67.17
15	830	72.07
16	1010	76.98
17	1020	81.88
18	1280	86.78
19	1330	91.69
20	1690	96.59

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

Figure 8.3-2 shows the data plotted on $\ln-\ln$ graph paper. From the graph, θ is 739.41 hours. β is:

$$\beta = \frac{\Delta Y}{\Delta X} = \frac{\ln \ln \left(\frac{1}{1-.99} \right) - \ln \ln \left(\frac{1}{1-.05} \right)}{\ln 2000 - \ln 105} = 1.53$$

The reliability at $t = 1000$ hours is found by drawing a line up vertically from $t=1000$ on the abscissa to the line. Then, from that point a horizontal line is drawn to the ordinate. It intersects the ordinate at $F(t) = 80\%$. The reliability is $1 - F(t) = 20\%$ (i.e., 20 percent probability of no failure).

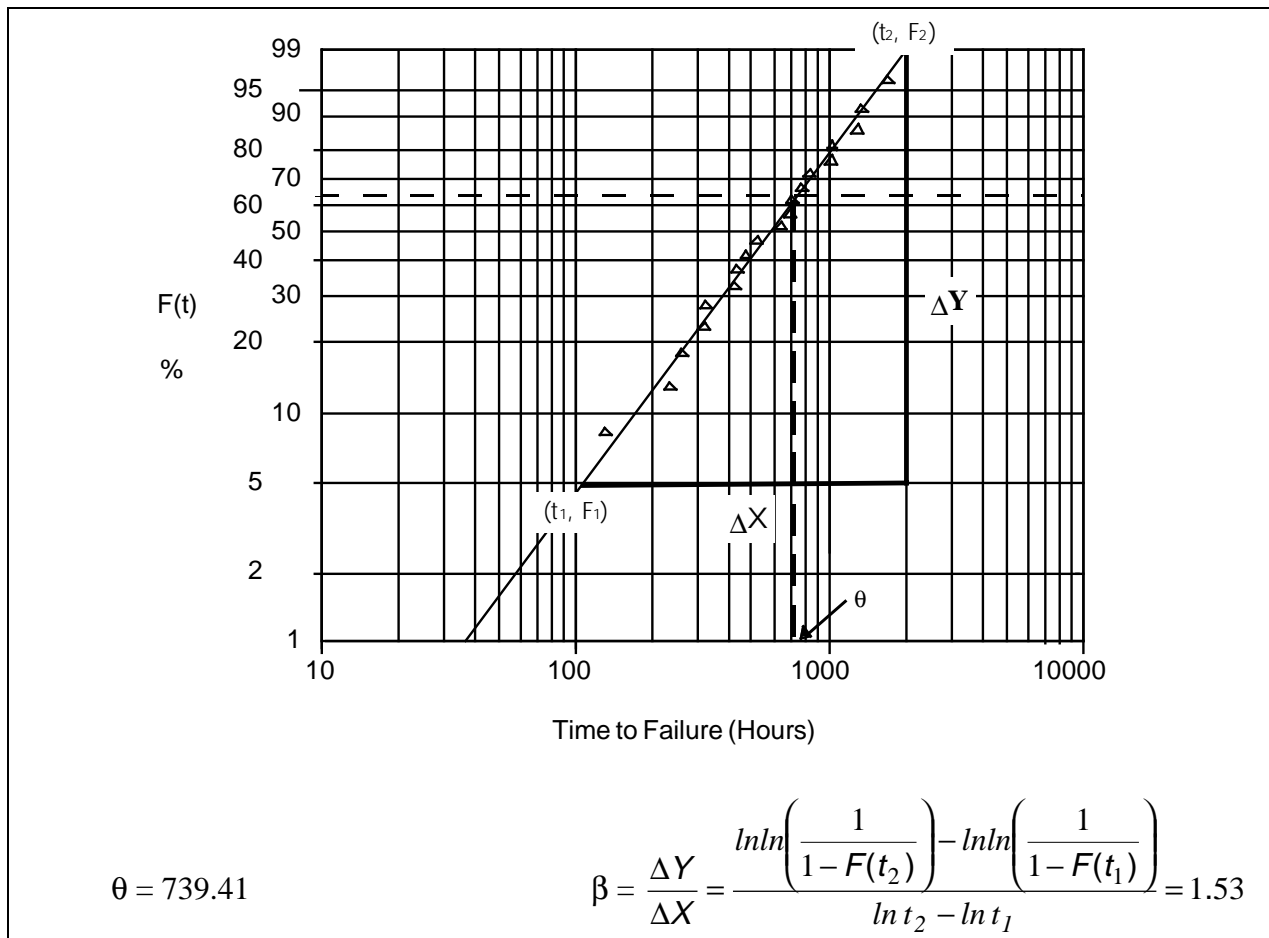


FIGURE 8.3-2: GRAPHICAL POINT ESTIMATION FOR THE WEIBULL DISTRIBUTION

 SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

Example 3: Exponential Distribution

A simple graphical procedure to test the validity of the exponential distribution is to plot the cumulative test or operating time against the cumulative number of failures as shown in Figure 8.3-3. If the plot is reasonably close to a straight line, then a constant failure rate is indicated. An exponential distribution of failures may be assumed.

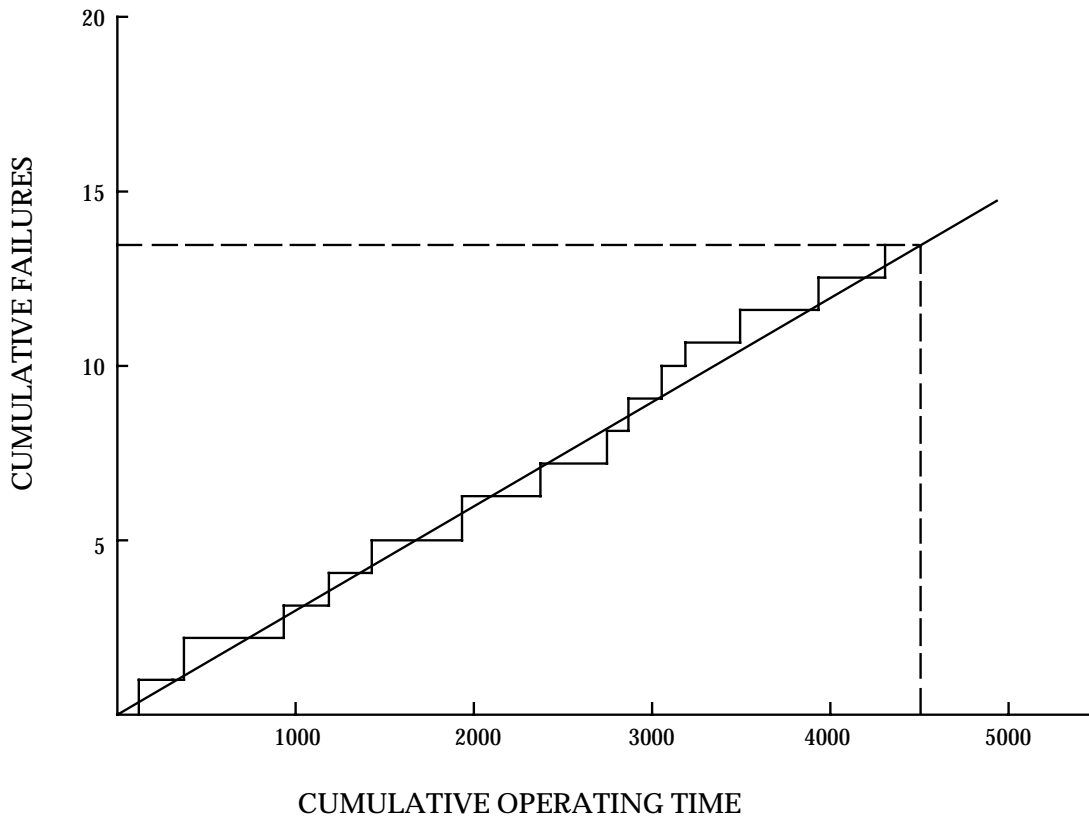


FIGURE 8.3-3: DISTRIBUTION GRAPHICAL EVALUATION

8.3.2 Statistical Analysis

8.3.2.1 Introduction

Since the available data usually only constitute a sample from the total population, statistical methods are used to estimate the reliability parameters of interest, e.g., MTBF, failure rate, probability of survival, etc.

The main advantage of statistics is that it can provide a measure of the uncertainty involved in a numerical analysis. The secondary advantage is that it does provide methods for estimating effects that might otherwise be lost in the random variations in the data.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

It is important to keep in mind the fact that data constitute a sample from the total population, that random sampling peculiarities must be smoothed out, that population density parameters must be estimated, that the estimation errors must themselves be estimated, and - what is even more difficult - that the very nature of the population density must be estimated. To achieve these ends, it is necessary to learn as much as one can about the possible population density functions, and especially what kind of results we can expect when samples are drawn, the data are studied, and we attempt to go from data backward to the population itself. It is also important to know what types of population densities are produced from any given set of engineering conditions. This implies the necessity for developing probability models, or going from a set of assumed engineering characteristics to a population density.

It is customary, even necessary, in statistical analysis to develop, from physical engineering principles, the nature of the underlying distribution. The sample of data is then compared against the assumed distribution.

The usual parameter of interest in reliability is the distribution of times to failure, called the probability density function or failure density function. The failure density function may be discrete, that is, only certain (integer) values may occur, as in tests of an explosive squib. Success or failure will occur on any trial, time not being considered. Or it may be continuous, any value of time to failure being possible.

Typically histograms are plotted (e.g., time-to-failure plots) and statistical techniques used to first test the data to determine the applicable form of the probability distribution, and then identify and evaluate the relationship between the reliability parameter(s), such as failure rate, and the critical hardware characteristics/attributes which affect reliability (such as technology, complexity, application factors, etc.) as defined by the data.

8.3.2.2 Treatment of Failure Data

Failure data are usually obtained from a) test results or b) field failure reports. Experience has shown that a good way to present these data is to compute and plot either the failure density function, $f(t)$, or the hazard rate, $h(t)$, as a function of time.

Remember from Section 5 that $f(t)$ is given by the ratio of the number of failures occurring in the time interval to the size of the original population, divided by the length of the time interval. The hazard rate, $h(t)$, on the other hand, is given by the ratio of the number of failures occurring in the time interval to the number of survivors at the beginning of the time interval, divided by the length of the time interval.

Although $f(t)$ and $h(t)$ are defined as continuous functions, piecewise continuous functions of $f(t)$ and $h(t)$ are computed, graphed results are examined, and a continuous model is chosen which best fits the data.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

Once having found $f(t)$ from the data, $F(t)$ (the cumulative distribution of time to failure) and $R(t) = 1 - F(t)$, the reliability function or survival probability, can be readily determined from the relationships.

$$F(t) = \int_{-\infty}^t f(t) dt \quad (8.1)$$

$$R(t) = 1 - F(t) \quad (8.2)$$

Two examples follow.

Example 4:

TABLE 8.3-3: FAILURE DATA FOR TEN HYPOTHETICAL
ELECTRONIC COMPONENTS

Failure Number	Operating Time, Hr.
1	8
2	20
3	34
4	46
5	63
6	86
7	111
8	141
9	186
10	266

From Table 8.3-4 and Eq. (8.1) and (8.2) one can calculate and plot $F(t)$ and $R(t)$. The data plots for the various function of interest are shown in Figure 8.3-4.

Note, from the dashed lines of Figure 8.3-4 (a) and (b), that the exponential distribution of time to failure represents a good approximation to the data.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

TABLE 8.3-4: COMPUTATION OF DATA FAILURE DENSITY
AND DATA HAZARD RATE

Time Interval, Hour t	Failure Density per Hour $f(t) \times 10^{-2}$	Hazard Rate per Hour $h(t) \times 10^{-2}$
0 - 8	$\frac{1}{10 \times 8} = 1.25$	$\frac{1}{10 \times 8} = 1.25$
8 - 20	$\frac{1}{10 \times 12} = 0.83$	$\frac{1}{9 \times 12} = 0.93$
20 - 34	$\frac{1}{10 \times 14} = 0.71$	$\frac{1}{8 \times 14} = 0.89$
34 - 46	$\frac{1}{10 \times 12} = 0.83$	$\frac{1}{7 \times 12} = 1.19$
46 - 63	$\frac{1}{10 \times 17} = 0.59$	$\frac{1}{6 \times 17} = 0.98$
63 - 86	$\frac{1}{10 \times 23} = 0.43$	$\frac{1}{5 \times 23} = 0.87$
86 - 111	$\frac{1}{10 \times 25} = 0.40$	$\frac{1}{4 \times 25} = 1.00$
111 - 141	$\frac{1}{10 \times 30} = 0.33$	$\frac{1}{3 \times 30} = 1.11$
141 - 186	$\frac{1}{10 \times 45} = 0.22$	$\frac{1}{2 \times 45} = 1.11$
186 - 266	$\frac{1}{10 \times 80} = 0.13$	$\frac{1}{1 \times 80} = 1.25$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

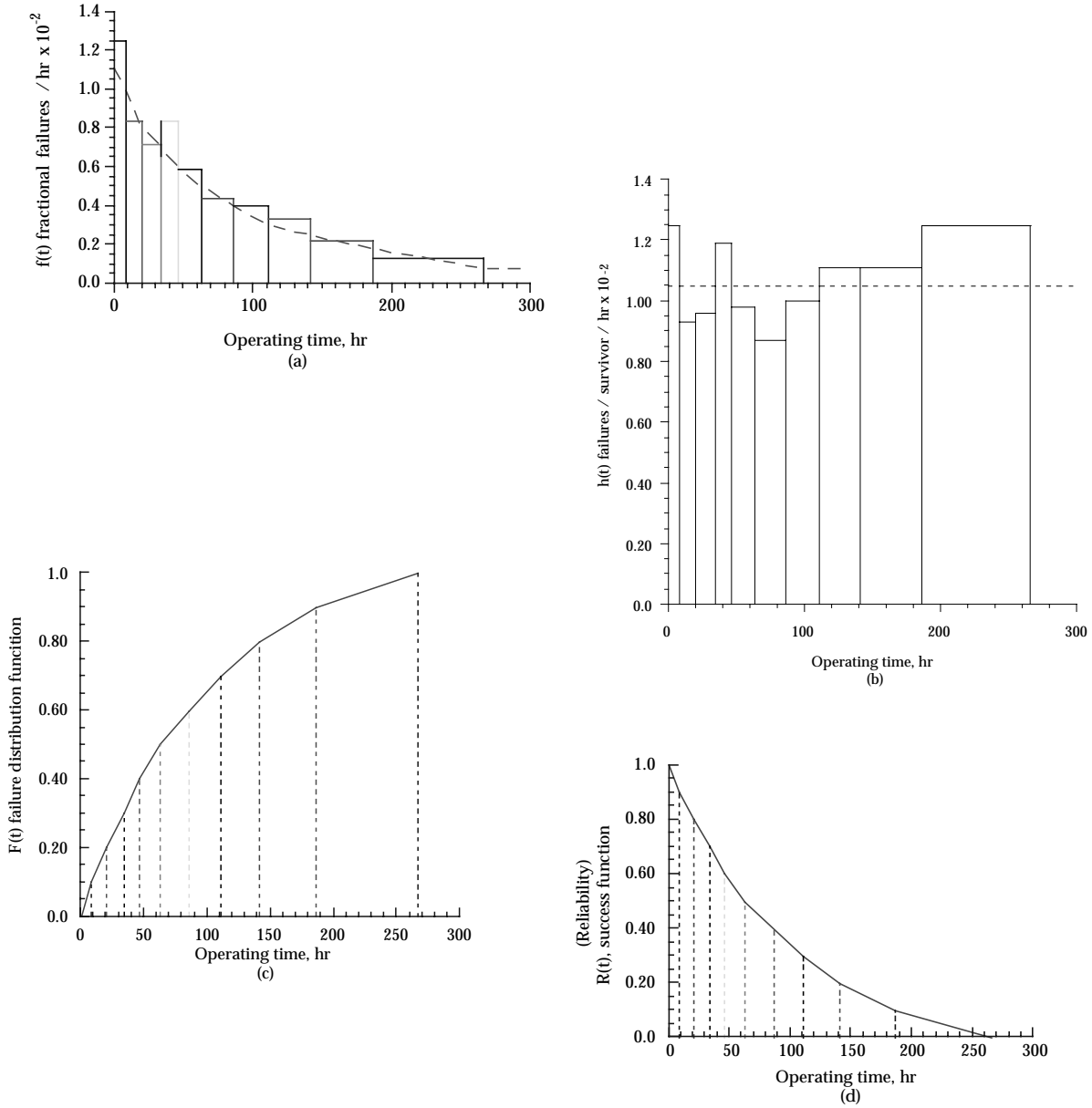


FIGURE 8.3-4: HAZARD AND DENSITY FUNCTIONS FOR TABLE 8.3-3

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTHExample 5:

Data for a single B-52 performing 1000 missions of 2 to 24 hours, or the equivalent of 1000 B-52s performing a single mission of 2 to 24 hours, are shown in Tables 8.3-5 and 8.3-6 and Figure 8.3-5 (Ref. [6]). This data shows that the B-52 is most likely to fail in the first two hours of its mission. The exponential distribution of times to failure does not fit well to the data.

TABLE 8.3-5: FAILURE DATA FOR 1,000 B-52 AIRCRAFT

Time Until Failure, Hour	Number of Failures in Interval	f(t) Failure Density/Hr.	h(t) Hazard Rate/Hr.
0 - 2	222	$\frac{222}{1,000 \times 2} = 0.1110$	$\frac{222}{1,000 \times 2} = 0.1110$
2 - 4	45	$\frac{45}{1,000 \times 2} = 0.0225$	$\frac{45}{778 \times 2} = 0.0289$
4 - 6	32	$\frac{32}{1,000 \times 2} = 0.0160$	$\frac{32}{733 \times 2} = 0.0218$
6 - 8	27	$\frac{27}{1,000 \times 2} = 0.0135$	$\frac{27}{701 \times 2} = 0.0192$
8 - 10	21	$\frac{21}{1,000 \times 2} = 0.0105$	$\frac{21}{674 \times 2} = 0.0156$
10 - 12	15	$\frac{15}{1,000 \times 2} = 0.0075$	$\frac{15}{653 \times 2} = 0.0113$
12 - 14	17	$\frac{17}{1,000 \times 2} = 0.0085$	$\frac{17}{638 \times 2} = 0.0133$
14 - 16	7	$\frac{7}{1,000 \times 2} = 0.0035$	$\frac{7}{621 \times 2} = 0.0056$
16 - 18	14	$\frac{14}{1,000 \times 2} = 0.0070$	$\frac{14}{614 \times 2} = 0.0114$
18 - 20	9	$\frac{9}{1,000 \times 2} = 0.0045$	$\frac{9}{600 \times 2} = 0.0075$
20 - 22	8	$\frac{8}{1,000 \times 2} = 0.0040$	$\frac{8}{591 \times 2} = 0.0068$
22 - 24	3	$\frac{3}{1,000 \times 2} = 0.0015$	$\frac{3}{583 \times 2} = 0.0026$
TOTAL	420		

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

TABLE 8.3-6: TIME-TO-FAILURE DATA FOR S = 1000 MISSION HOURS

TIME-TO- FAILURE (HOURS)	CUMULATIVE FAILURES = F	$R = \frac{1000 - F}{1000}$
2	222	.778
4	267	.733
6	299	.701
8	326	.674
10	347	.653
12	362	.638
14	379	.621
16	386	.614
18	400	.600
20	409	.591
22	417	.583
24	420	.580

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

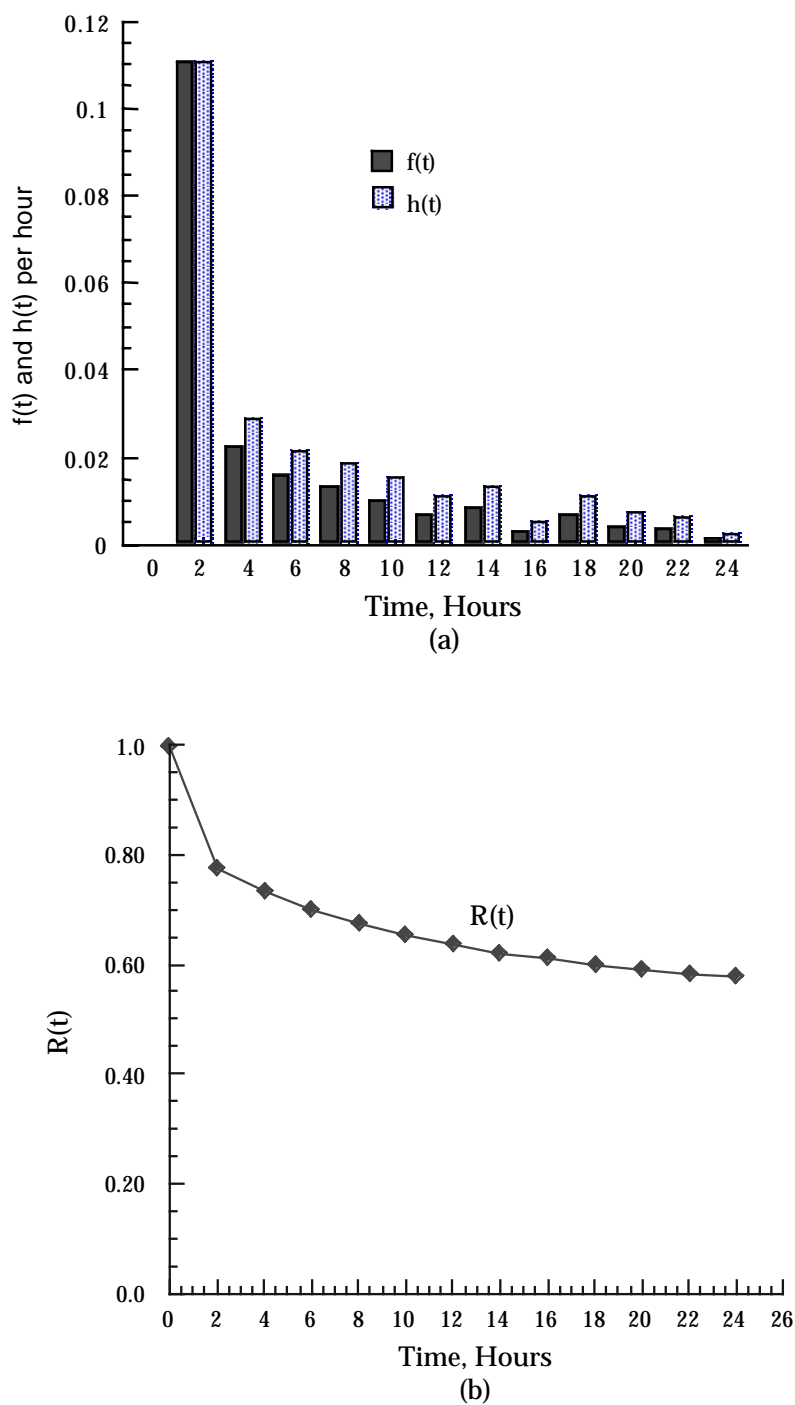


FIGURE 8.3-5: RELIABILITY FUNCTIONS FOR THE EXAMPLE
GIVEN IN TABLE 8.3-4

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

8.3.2.3 Reliability Function (Survival Curves)

A survival curve or reliability function, $R(t)$, is a graphic representation of the relationship between the probability of survival and time. Here, probability of survival is synonymous with probability of nonfailure or probability of satisfactory performance. Three types of survival curves are of primary interest. The first is a discrete or point-type curve derived from observed data by nonparametric or distribution-free methods. The second type is a continuous curve based on an assumption as to the form of the distribution (Gaussian, exponential, etc.) and on values of the distribution parameters estimated from the observed data. The third type of curve is the true reliability function of the population from which the sample observations were drawn. This last function can only be estimated (i.e., not determined precisely), although the limits within which it will fall a given percentage of the time can be defined.

Figure 8.3-6 presents a frequency distribution of failures in a fixed population of 90 items, over a 6-hour period. To obtain a survival curve from these data, the following simplified method is used.

During the first period of observation, from 0 to 1 hour, 4 of the original 90 items failed. The failure rate during this period was $4/90$, or 0.0444, which is equivalent to a survival rate of $1 - 0.0444$, or 0.9556. In the second period of observation, 21 of the 86 remaining items failed. The failure rate was $21/86$, or 0.244, and the survival rate was $1 - 0.244$, or 0.756. The tabulation above Figure 8.3-7 gives the failure rates and survival rates for the remaining periods of observation. It will be noted that the failure rate increases with time.

To obtain a survival curve, which is the cumulative probability of survival with time, the probability of survival in each time period is multiplied by the survival rate in the succeeding time period. Thus, $0.9556 \times 0.756 = 0.723$; $0.723 \times 0.538 = 0.388$, etc. The probability values are plotted versus the centers of the time periods as shown at the bottom of 8.3-7.

Figure 8.3-8 presents a frequency distribution of failures for a population of 90 items in which the removal rate is constant with time. The approach described in connection with the normal curve yields the tabulation and exponential survival curve shown in Figure 8.3-9. (Note in this example, only 83 of 90 items failed in six hours).

Survival curves for most electronic equipment/systems are of the exponential form. Survival curves for mechanical parts, on the other hand, are frequently of the normal or Weibull form. As parts wear out, their failure rate increases and their probability of survival decreases. A large number of such parts, all having normal or Weibull survival curves but each having a different mean life and variance, will produce a system malfunction rate which is essentially constant, since the mean lives of the parts will be randomly distributed.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

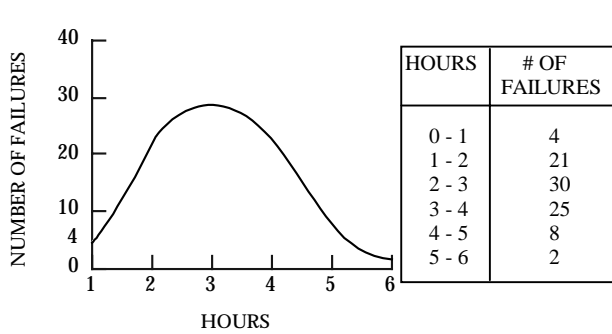


FIGURE 8.3-6: NORMAL DISTRIBUTION OF FAILURE IN TIME

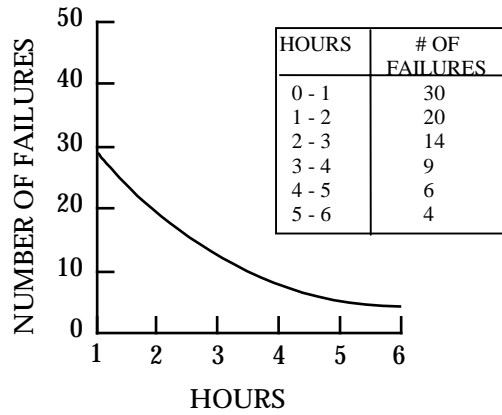


FIGURE 8.3-8: EXPONENTIAL DISTRIBUTION OF FAILURES IN TIME

TIME	FAILURE RATE	SURVIVAL RATE	PROBABILITY OF SURVIVAL
0 - 1	0.444	0.9556	0.9555
1 - 2	0.2442	0.7558	0.7230
2 - 3	0.4615	0.5385	0.3880
3 - 4	0.7143	0.2857	0.1110
4 - 5	0.8000	0.2000	0.0220
5 - 6	1.0000	0.0000	---

TIME	FAILURE RATE	SURVIVAL RATE	PROBABILITY OF SURVIVAL
0 - 1	0.333	0.667	0.667
1 - 2	0.333	0.667	0.444
2 - 3	0.350	0.650	0.289
3 - 4	0.346	0.654	0.189
4 - 5	0.353	0.647	0.122
5 - 6	0.364	0.636	0.078

NOTE: Population is 90 for all figures.

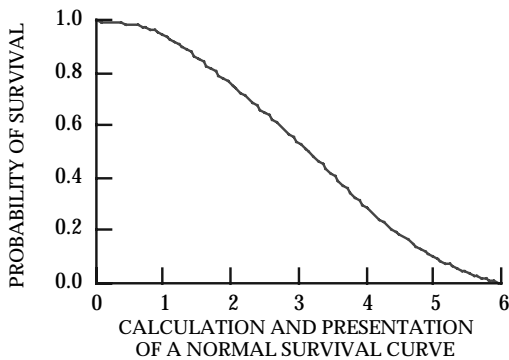


FIGURE 8.3-7: CALCULATION AND PRESENTATION OF A NORMAL SURVIVAL CURVE

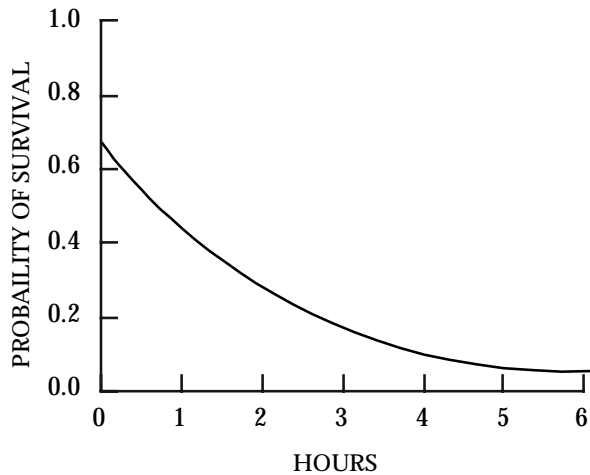


FIGURE 8.3-9: CALCULATION AND PRESENTATION OF AN EXPONENTIAL CURVE

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

To determine what type of population gives rise to a particular survival curve, the theoretical reliability function most closely resembling the curve is computed from sample parameters. The theoretical function is then matched to the observed curve by statistical techniques. If this procedure establishes that there is no significant difference between the observed and theoretical curves, the theoretical curve is usually employed for all additional calculations.

Figures 8.3-10 and 8.3-11 portray observed and theoretical probability of survival curves for the case of exponential and normal distributions of time to failure. Note that the mean life for the exponential case has $R(t) = 0.368$, whereas for the normal case, $R(t) = 0.5$. This is due to the symmetrical characteristic of the normal distribution, versus the skewed characteristic of the exponential.

Thus, if one can develop a mathematical expression for $R(t)$, it can be shown that the mean time to failure is given by:

$$\text{MTTF} = \int_0^{\infty} R(t) dt \quad (8.3)$$

8.3.2.3.1 Computation of Theoretical Exponential Reliability Function

When the form of the distribution is sufficiently well defined, it is possible to estimate the reliability function in terms of the parameters of the distribution. This method has the advantage of permitting utilization of all the accumulated knowledge concerning the items in the population. In addition, the reliability function can be summarized by specifying the values of the parameters, and can be compared with other reliability functions merely by comparing the values of the summarized data.

For the case of an equipment/system which is repaired upon failure, the reliability function is given by:

$$R(t) = e^{-t/\text{MTBF}} \quad (8.4)$$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

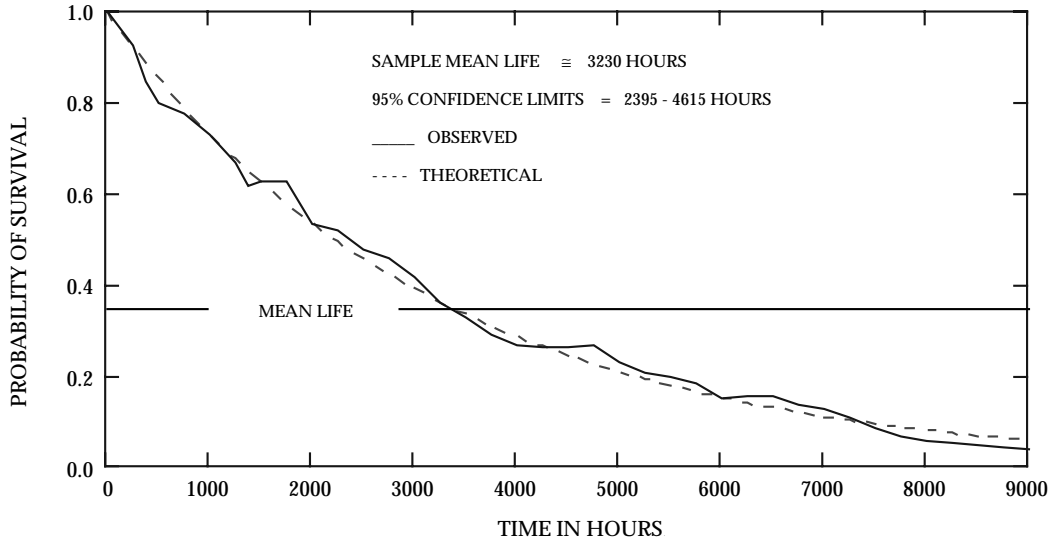


FIGURE 8.3-10: OBSERVED AND THEORETICAL EXPONENTIAL SURVIVAL CURVES

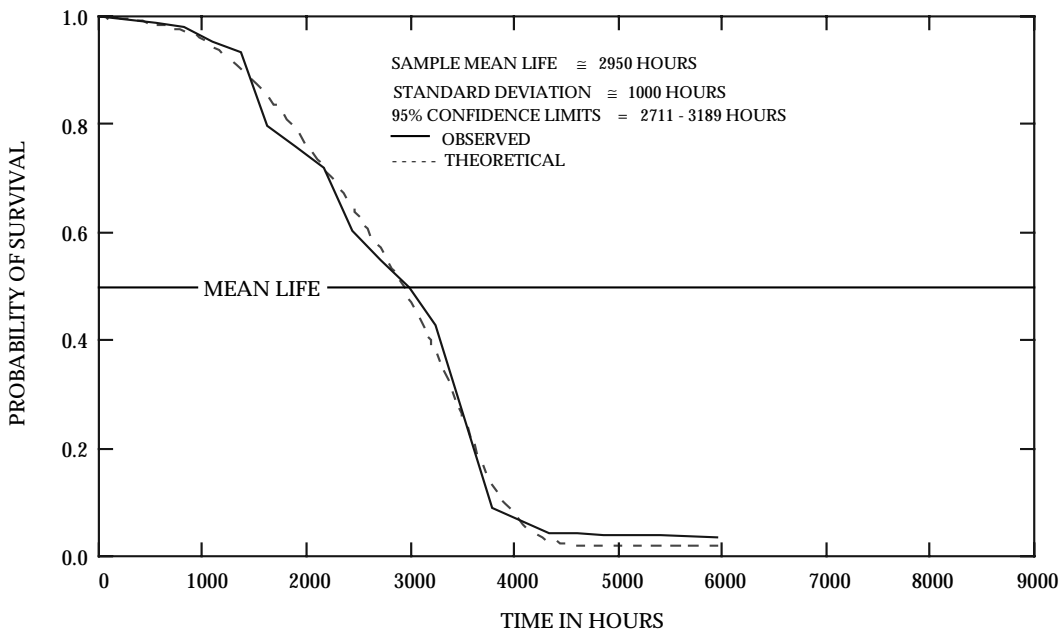


FIGURE 8.3-11: OBSERVED AND THEORETICAL NORMAL SURVIVAL CURVES

 SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

where:

t = time at which R(t) is calculated
 MTBF = mean time between failures, given by

$$MTBF = \frac{nt}{r} \quad (8.5)$$

and

n = the number of equipments operated to time t
 r = the number of failures, with the last failure occurring at time t

For example, assume that in a sample of twenty equipments operated for 773 hours, we observed 10 failures (each of which was repaired), with the last failure occurring at 773 hours.

Then

$$MTBF = \frac{nt}{r} = \frac{(20)(773)}{10} = 1546 \text{ hours}$$

$$R(t) = e^{-t/1546}$$

Table 8.3-7 shows the computations for R(t) for selected values of t. Figure 8.3-12 shows the actual reliability function (solid line) plotted from the data versus the theoretical exponential function from column 3 of Table 8.3-7. Determination of confidence intervals is discussed briefly in the next section.

8.3.2.3.2 Computation For Normal Reliability Function

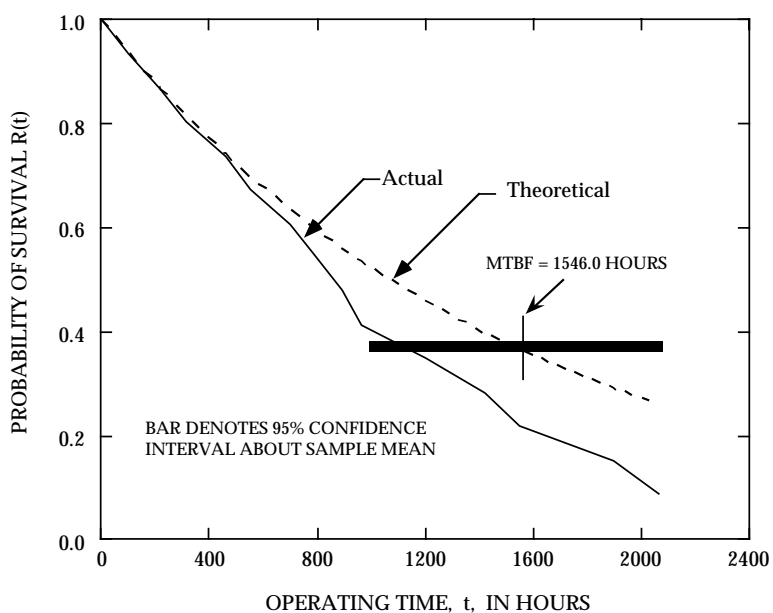
Table 8.3-8 presents some observed failure data for a sample of twenty units tested to failure, and the failure times observed. The units were known to follow a normal distribution of time to failure.

The sample mean, \bar{X} , an estimate of μ , is given by:

$$\bar{X} = \sum_{i=1}^{20} X_i / n = \frac{39104}{20} = 1955.2 \text{ hours}$$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTHTABLE 8.3-7: COMPUTATION OF THEORETICAL EXPONENTIAL
RELIABILITY FUNCTION FOR MTBF = 1546 HOURS

(1) t	(2) t/MTBF	(3) $e^{-t/MTBF}$
0	0	1.000
96	0.0621	0.9389
216	0.1397	0.8696
312	0.2018	0.8173
456	0.2950	0.7445
552	0.3571	0.6997
696	0.4502	0.6375
792	0.5123	0.5991
888	0.5744	0.5630
960	0.6210	0.5374
1200	0.7762	0.4602
1416	0.9159	0.4002
1546	1.0000	0.3679
1896	1.2264	0.2933
2064	1.3351	0.2631

FIGURE 8.3-12: ACTUAL RELIABILITY FUNCTION AND THEORETICAL
EXPONENTIAL RELIABILITY FUNCTION

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

TABLE 8.3-8: OBSERVED FAILURE DATA

Time	Probability of Survival, R	Time	Probability of Survival, R
175	0.95	2025	0.45
695	0.90	2115	0.40
872	0.85	2172	0.35
1250	0.80	2418	0.30
1291	0.75	2583	0.25
1402	0.70	2725	0.20
1404	0.65	2844	0.15
1713	0.60	2980	0.10
1741	0.55	3268	0.05
1893	0.50	3538	0.00

The sample standard deviation, s , an estimate of σ , is given by:

$$s = \left[\frac{\sum_{i=1}^{20} (X_i - \bar{X})^2}{n-1} \right]^{.5} = 886.6 \text{ hours}$$

where:

$$\begin{aligned} X_i &= i^{\text{th}} \text{ failure time} \\ n &= \text{sample size} \\ \bar{X} &= \text{sample mean} \end{aligned}$$

Figure 8.3-13 shows the actual or nonparametric reliability function plotted from the data versus the theoretical function calculated using the estimates of μ and σ . The theoretical values were obtained from the expression

$$R(x) = P \left(z > \frac{X - \mu}{\sigma} \right)$$

where the value of z was obtained from a table of the Standard Normal Distribution (Table 5.3.1 of Section 5).

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

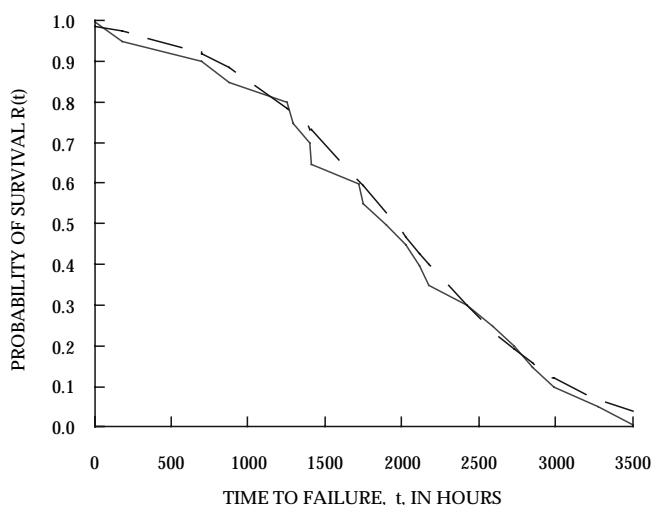


FIGURE 8.3-13: NON-PARAMETRIC AND THEORETICAL
NORMAL RELIABILITY FUNCTIONS

8.3.2.4 Censored Data

If a sample contains both complete and incomplete lifetimes, the incomplete lifetimes are referred to as “censored” observations. These consist primarily of lifetimes which are too long to be observed completely (“terminated” observations) and lifetimes in which the item being observed is lost before completion of observation (“lost” observation). In the case of terminated observations, the length of observation time is controlled; in the case of lost observations, the length of observation time is not controlled. In either case, the investigator knows that the lifetime of the item exceeds the period of time during which the item was being observed. Terminated observations do not present a problem to the investigator other than to increase the complexity of the calculations, but lost observations may constitute a real problem because they maybe associated with only a portion of the population.

For example, for the case of the exponential distribution in which n items are put on test, r of them fail at time t_1, t_2, \dots, t_r , with the test discontinued at t_r when the r^{th} failure occurs, the MTBF is given by

$$\text{MTBF} = \frac{\sum_{i=1}^r t_i + (n - r)t_r}{n} \quad (8.6)$$

 SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

where t_i is the time of each failure and $(n - r)$ represents the number of surviving items at time t_r . In this nonreplacement case, the failed items are not repaired or replaced upon failure.

The mathematics become somewhat more difficult when analyzing censored data where distributions other than the exponential are involved, or when using nonparametric methods. These cases are treated in detail in References [1], [3], [4] and [5].

8.3.2.5 Confidence Limits and Intervals

Previously, we discussed methods of obtaining point estimates of reliability parameters, e.g., $R(t)$, λ , MTBF, etc. For most practical applications, we are interested in the accuracy of the point estimate and the confidence which we can attach to it. We know that statistical estimates are more likely to be closer to the true value as the sample size increases. Only the impossible situation of having an infinitely large number of samples to test could give us 100 percent confidence or certainty that a measured value of a parameter coincides with the true value. For any practical situation, therefore, we must establish confidence intervals or ranges of values between which we know, with a probability determined by the finite sample size, that the true value of the parameter lies.

Confidence intervals around point estimates are defined in terms of a lower confidence limit, L , and an upper confidence limit, U . If, for example, we calculate the confidence limits for a probability of, say, 95 percent, this means that in repeated sampling, 95 percent of the calculated intervals will contain the true value of the reliability parameter. If we want to be 99 percent sure that the true value lies within certain limits for a given sample size, we must widen the interval or test a larger number of samples if we wish to maintain the same interval width. The problem, then, is reduced to one of either determining the interval within which the true parametric value lies with a given probability for a given sample size, or determining the sample size required to assure us with a specified probability that true parametric value lies within a specific interval.

Thus, we would like to be able to make assertions such as

$$P \left[\left(\hat{\theta}_L < \theta < \hat{\theta}_U \right) \right] = \eta \quad (8.8)$$

where θ is some unknown population parameter, θ_L and θ_U are estimators associated with a random sample and η is a probability value such as 0.99, 0.95, 0.90, etc. If, for instance, $\eta = 0.95$ we refer to the interval

$$(\theta_L < \theta < \theta_U) \quad (8.9)$$

for particular values of $\hat{\theta}_L$ and $\hat{\theta}_U$ as a 95% confidence interval. In this case we are willing to accept a 5% probability (risk) that our assertion is not, in fact, true.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

Or, we may also want to make statements such as

$$P [\theta > \hat{\theta}_L] = \eta \quad (8.10)$$

in which case we make statements like, “we are 90% confident that the true MTBF is greater than some lower confidence limit (or measured value).” Eq. (8.10) is the case of the one-sided confidence limit, versus Eq. (8.9) which is a two-sided confidence limit, or confidence interval.

To help clarify the concept of a confidence interval we can look at the situation in a geometrical way. Suppose we draw repeated samples (x_1, x_2) from a population, one of whose parameters we desire to bracket with a confidence interval. We construct a three-dimensional space with the vertical axis corresponding to θ and with the two horizontal axes corresponding to values of X_1 and X_2 (see Figure 8.3-14). The actual value of the population parameter θ is marked on the vertical axis and a horizontal plane is passed through this point. Now we take a random sample (X_1, X_2) from which we calculate the values $\hat{\theta}_U$ and $\hat{\theta}_L$ at, say, the 95% confidence level. The interval defined by $\hat{\theta}_U$ and $\hat{\theta}_L$ is plotted on the figure.

Next, we take a second sample (X'_1, X'_2) from which we calculate the value $\hat{\theta}'_U$ and $\hat{\theta}'_L$ at the 95% level. This interval is plotted on the figure. A third sample (X''_1, X''_2) yields the values $\hat{\theta}''_U$ and $\hat{\theta}''_L$, etc. In this way we can generate a large family of confidence intervals. The confidence intervals depend only on the sample values (X_1, X_2) , (X'_1, X'_2) , etc., and hence we can calculate these intervals without knowledge of the true value of θ . If the confidence intervals are all calculated on the basis of 95% confidence and if we have a very large family of these intervals, then 95% of them will cut the horizontal plane through θ (and thus include θ) and 5% of them will not.

The process of taking a random sample and computing from it a confidence interval is equivalent to the process of reaching into a bag containing thousands of confidence intervals and grabbing one at random. If they are all 95% intervals, our chance of choosing one that does indeed include θ will be 95%. In contrast, 5% of the time we will be unlucky and select one that does not include θ (like the interval $(\hat{\theta}''_U, \hat{\theta}''_L)$ in Figure 8.3-14. If a risk of 5% is judged too high, we can go to 99% intervals, for which the risk is only 1%. As we go to higher confidence levels (and lower risks) the lengths of the intervals increase until for 100% confidence levels (and lower risks) the interval includes every conceivable value of θ (I am 100% confident that the number of defective items in a population of 10,000 is somewhere between 0 and 10,000). For this reason 100% confidence intervals are of little interest.

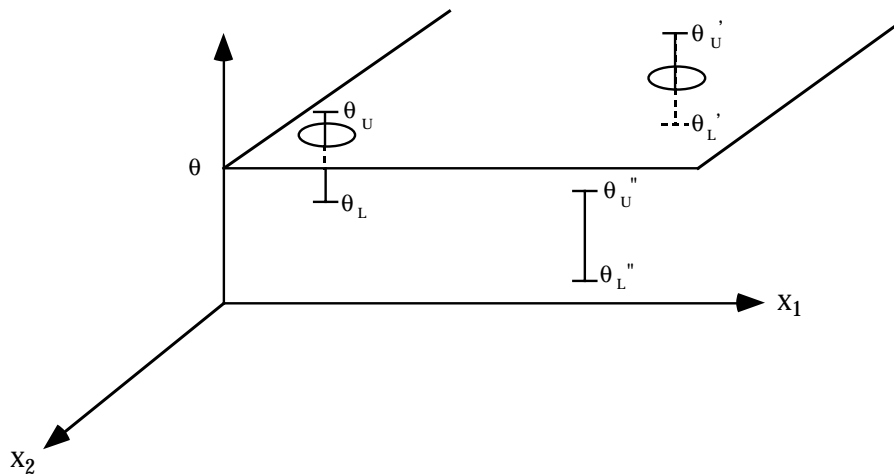
SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

FIGURE 8.3-14: GEOMETRICAL INTERPRETATION OF THE CONCEPT OF A CONFIDENCE INTERVAL

Let us now look at some simple examples of how these concepts are applied to analyze reliability for some of the more commonly-used distributions.

8.3.2.5.1 Confidence Limits - Normal Distribution

When the lives of n components are known from a wearout test and we compute their mean, \hat{M} , and their standard deviation, s , and when n is large so that we can assume that $s \approx \sigma$, the upper and lower confidence limits can be readily evaluated from Table 8.3-9 for the more commonly-used confidence levels.

Strictly speaking, this procedure of assigning confidence intervals to an estimate is correct only when the true standard deviation, σ , of component wearout is known and used instead of s in Table 8.3-9. However, it can be applied in reliability work as an approximation whenever the estimate s , of σ , was obtained from a large sample, i.e., when the number of failures is at least 25, and preferably, more. In fact, it can be shown for samples of 20, $k_{\alpha/2}$ (at the 95% confidence level) is 2.09 vs. a value of 1.96 for an infinite number of samples. α is equal to $100(1 - \text{confidence level})\%$.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

TABLE 8.3-9: CONFIDENCE LIMITS - NORMAL DISTRIBUTION

$k_{\alpha/2}$	Two-sided Confidence intervals $\hat{M} \pm K_{\alpha/2} s/\sqrt{n}$	Confidence levels $100(1 - \alpha)\%$
0.84	$\hat{M} \pm 0.84s/\sqrt{n}$	60.0
1.28	$\hat{M} \pm 1.28s/\sqrt{n}$	80.0
1.64	$\hat{M} \pm 1.64s/\sqrt{n}$	90.0
1.96	$\hat{M} \pm 1.96s/\sqrt{n}$	95.0
2.58	$\hat{M} \pm 2.58s/\sqrt{n}$	99.0

Figure 8.3-15 graphically illustrates what is being done. Since the normal distribution is symmetrical, we are computing the confidence interval as the area $(1 - \alpha)$ under the curve, leaving an area $\alpha/2$ in each of the left and right hand tails which is outside of the confidence interval (CI). For example, using the calculated values of \hat{M} (or \bar{X}) and s obtained from the data in Table 8.3-10, the CI at the 95% level is

$$\begin{aligned} \hat{M} \pm 1.96 s/\sqrt{n} &= 1955.2 \pm 1.96 (886.6)/\sqrt{20} \\ &= 1955.2 \pm 388.6 \\ &= (2343.8, 1566.6) \end{aligned}$$

In other words, we can be 95% confident that the true value of the mean life (M) lies between 1566.6 and 2343.8 hours.

Actually, in reliability work, we are usually more interested in the lower confidence limit L of the mean wearout life than in the upper limit. Given a measured value of \hat{M} , we would like to make some statement about our confidence that the true value of M exceeds some minimum value.

When only the lower confidence limit, L , is of interest, we apply the procedure of so-called “one-sided” confidence limits, as opposed to the two-sided CI of the preceding example. The problem is to assure ourselves (or our customer) that the true mean life, M , is equal to or larger than some specified minimum value with a probability of $(1 - \alpha)$.

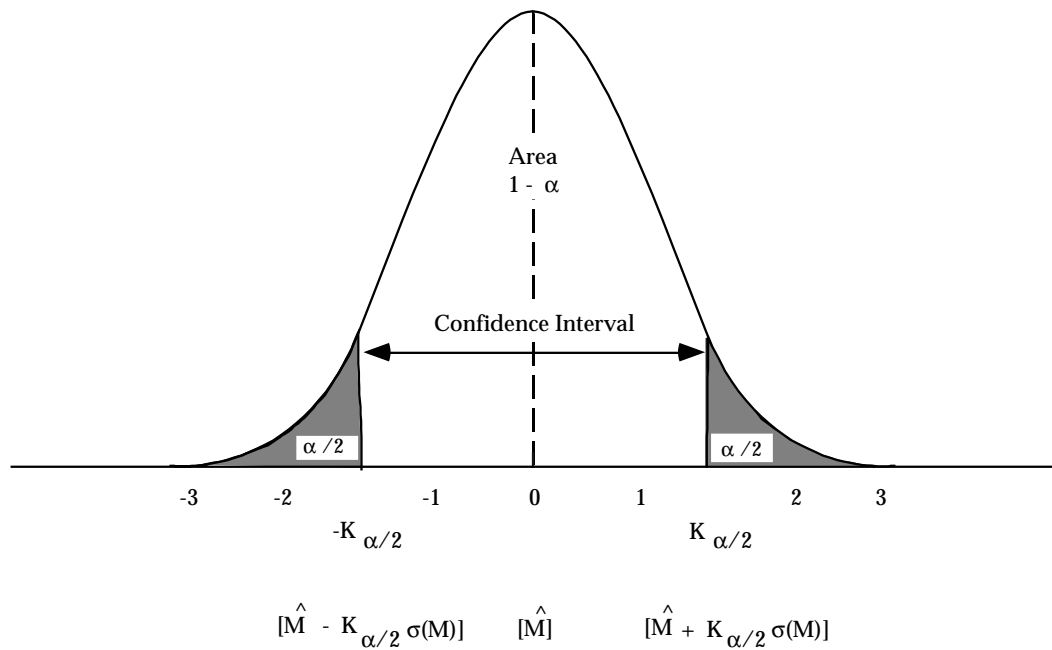
SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

FIGURE 8.3-15: TWO-SIDED CONFIDENCE INTERVAL AND LIMITS

Whereas in the case of the two-sided confidence limits, we had an area of $\alpha/2$ under the left tail of the normal curve (Figure 8.3-15), we now have an area α to the left of L and an area $(1 - \alpha)$ to the right.

Therefore, the estimate of mean life obtained from the data should be:

$$\hat{M} \geq L + K_{\alpha} \sigma/\sqrt{n} \quad (8.11)$$

If this equation is not satisfied, the requirement that the true M must be at least L at the specified 100 $(1 - \alpha)$ percent confidence level has not been fulfilled.

Table 8.3-10, in which the assumption $s \approx \sigma$ is made, allows a quick check as to whether an estimate, \hat{M} , obtained from a sample of size n fulfills the requirement that the true M must not be smaller than the specified minimum L . Only the more commonly-used confidence levels are given.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

TABLE 8.3-10: CONFIDENCE INTERVAL

$K_{\alpha/2}$	The estimate \hat{M} must exceed: $L + K_{\alpha/2} s/\sqrt{n}$	Confidence levels 100 (1 - α)%
0.25	$L + 0.25s/\sqrt{n}$	60
0.52	$L + 0.52s/\sqrt{n}$	70
0.84	$L + 0.84s/\sqrt{n}$	80
1.28	$L + 1.28s/\sqrt{n}$	90
1.64	$L + 1.64s/\sqrt{n}$	95
2.33	$L + 2.33s/\sqrt{n}$	99

Once again, using the data and calculated values of \hat{M} and s from Table 8.3-10, assume that we would like to be 95% confident that the true $M \geq 1500$ hours. The equation from Table 8.3-10 is

$$\hat{M} \geq L + 1.64 s/\sqrt{n}$$

$$1955.2 \geq 1500 + 1.64 (886.6)/\sqrt{20}$$

$$1955.2 \geq 1500 + 325$$

$$1955.2 \geq 1825$$

Since the inequality is satisfied, the requirement has been met.

As previously mentioned, the above procedure can be applied if the sample size n is at least 25. However, similar procedures also apply to smaller sample sizes except that now we cannot assume that $s \approx \sigma$, and we must use another set of equations based on Student's t distribution.

Actually, all we do is replace the normal percentage points $K_{\alpha/2}$ and K_{α} in the previously developed equations by the tabulated percentage points $t_{\alpha/2;n-1}$ and $t_{\alpha;n-1}$ of the t distribution, where $n-1$ is called the degrees of freedom and n is the number of failures. Student's t tables are available in most standard statistical texts.

For example, for the two-sided CI example using the data from Table 8.3-10 and calculated values of \hat{M} and s ,

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

$$\begin{aligned}\hat{M} \pm t_{\alpha/2;n-1} s/\sqrt{n} &= 1955.2 \pm 2.09 (886.6)/\sqrt{20} \\ &= 1955.2 \pm 414.4 \\ &= (2370, 1541.2)\end{aligned}$$

which is a slightly wider CI than the case where it was assumed the $s \approx \sigma$.

8.3.2.5.2 Confidence Limits - Exponential Distribution

Two situations have to be considered for estimating confidence intervals: one in which the test is run until a preassigned number of failures (r^*) occurs, and one in which the test is stopped after a preassigned number of test hours (t^*) is accumulated. The formula for the confidence interval employs the X_2 (chi-square) distribution. A short table of X^2 values is given in Table 8.3-11. The general notation used is

$$\chi^2_{p,d}$$

where p and d are two constants used to choose the correct value from the table.

The quantity p is a function of the confidence coefficient; d , known as the degrees of freedom, is a function of the number of failures. $X^2_{\alpha/2, 2r+2}$ for example, is the $\frac{\alpha}{2}$ percentage point of the chi-square distribution for $(2r+2)$ degrees of freedom.

Equations (8.12) and (8.13) are for one-sided or two-sided $100(1 - \alpha)$ percent confidence intervals. For nonreplacement tests with a fixed truncation time, the limits are only approximate. Also, for non-replacement tests, only one sided intervals are possible for $r = 0$.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTHTABLE 8.3-11: DISTRIBUTION OF χ^2 (CHI-SQUARE)

DF	Probability														
	0.99	0.975	0.95	0.90	0.80	0.75	0.50	0.25	0.20	0.10	0.05	0.025	0.01	0.001	
1	0.00016	0.00098	0.00393	0.0158	0.0642	0.10133	0.455	1.325	1.642	2.706	3.841	5.024	6.635	10.827	
2	0.0201	0.0506	0.103	0.211	0.446	0.5753	1.386	2.772	3.219	4.605	5.991	7.377	9.210	13.815	
3	0.115	0.216	0.352	0.584	1.005	1.2125	2.366	4.108	4.642	6.251	7.815	9.348	11.341	16.268	
4	0.297	0.484	0.711	1.064	1.649	1.9225	3.357	5.385	5.989	7.779	9.488	11.143	13.277	18.465	
5	0.554	0.831	1.145	1.610	2.343	2.674	4.351	6.625	7.289	9.236	11.070	12.832	15.086	20.517	
6	0.872	1.237	1.635	2.204	3.070	3.454	5.348	7.840	8.558	10.645	12.592	14.449	16.812	22.457	
7	1.239	1.689	2.167	2.833	3.822	4.254	6.346	9.037	9.803	12.017	14.067	16.013	18.475	24.322	
8	1.646	2.179	2.733	3.490	4.594	5.070	7.344	10.218	11.030	13.362	15.507	17.534	20.090	26.125	
9	2.088	2.700	3.325	4.168	5.380	5.898	8.343	11.388	12.242	14.684	16.919	19.023	21.666	27.877	
10	2.558	3.247	3.940	4.865	6.179	6.737	9.342	12.548	13.442	15.987	18.307	20.483	23.209	29.588	
11	3.053	3.816	4.575	5.578	6.989	7.584	10.341	13.701	14.631	17.275	19.675	21.920	24.725	31.264	
12	3.571	4.404	5.226	6.304	7.807	8.438	11.340	14.845	15.812	18.549	21.026	23.336	26.217	32.909	
13	4.107	5.008	5.892	7.042	8.634	9.299	12.340	15.984	16.985	19.812	22.362	24.735	27.688	34.528	
14	4.660	5.628	6.571	7.790	9.467	10.165	13.339	17.117	18.151	21.064	23.685	26.119	29.141	36.123	
15	5.229	6.262	7.261	8.547	10.307	11.036	14.339	18.245	19.311	22.307	24.996	27.488	30.578	37.697	
16	5.812	6.907	7.962	9.312	11.152	11.912	15.338	19.368	20.465	23.542	26.296	28.845	32.000	39.252	
17	6.408	7.564	8.672	10.085	12.002	12.791	16.338	20.488	21.615	24.769	27.587	30.191	33.409	40.790	
18	7.015	8.231	9.390	10.865	12.857	13.675	17.338	21.605	22.760	25.989	28.869	31.526	34.805	42.312	
19	7.633	8.906	10.117	11.651	13.716	14.562	18.338	22.717	23.900	27.204	30.144	32.852	36.191	43.820	
20	8.260	9.591	10.851	12.443	14.578	15.452	19.337	23.827	25.038	28.412	31.410	34.169	37.566	45.315	
21	8.897	10.283	11.591	13.240	15.445	16.344	20.337	24.935	26.171	29.615	32.671	35.479	38.932	46.797	
22	9.542	10.982	12.338	14.041	16.314	17.239	21.337	26.039	27.301	30.813	33.924	36.780	40.289	48.268	
23	10.196	11.688	13.091	14.848	17.187	18.137	22.337	27.141	28.429	32.007	35.172	38.075	41.638	49.728	
24	10.856	12.400	13.848	15.659	18.062	19.037	23.337	28.241	29.553	33.196	36.415	39.364	42.980	51.179	
25	11.524	13.119	14.611	16.473	18.940	19.939	24.337	29.339	30.675	34.382	37.652	40.646	44.314	52.620	
26	12.198	13.844	15.379	17.292	19.820	20.843	25.336	30.434	31.795	35.563	38.885	41.923	45.642	54.052	
27	12.879	14.573	16.151	18.114	20.703	21.749	26.336	31.528	32.912	36.741	40.113	43.194	46.963	55.476	
28	13.565	15.308	16.928	18.933	21.588	22.657	27.336	32.620	34.027	37.916	41.337	44.460	48.278	56.893	
29	14.256	16.047	17.708	19.768	22.475	23.566	28.336	33.711	35.139	39.087	42.557	45.722	49.588	58.302	
30	14.953	16.791	18.493	20.599	23.364	24.476	29.336	34.799	36.250	40.256	43.773	46.98	50.892	59.703	

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

Equations for Confidence Limits on Mean Life

Type of Confidence Limits	Fixed Number of Failures, r^*	Fixed Truncation Time t^*	
One Sided (Lower Limit)	$\left(\frac{2T}{\chi^2(\alpha, 2r)}, \infty \right)$	$\left(\frac{2T}{\chi^2(\alpha, 2r + 2)}, \infty \right)$	(8.12)
Two Sided (Upper and Lower Limits)	$\left(\frac{2T}{\chi^2(\frac{\alpha}{2}, 2r)}, \frac{2T}{\chi^2(1-\frac{\alpha}{2}, 2r)} \right)$	$\left(\frac{2T}{\chi^2(\frac{\alpha}{2}, 2r+2)}, \frac{2T}{\chi^2(1-\frac{\alpha}{2}, 2r)} \right)$	(8.13)

The terms used are identified as follows:

n	=	number of items placed on test at time $t = 0$
t^*	=	time at which the life test is terminated
θ	=	mean life (or MTBF for the case of replacement or repair upon failure)
r	=	number of failures accumulated at time t^*
r^*	=	preassigned number of failures
α	=	acceptable risk of error
$1 - \alpha$	=	confidence level
T	=	total test time

Note that T is computed as follows, depending on the type of test procedure.

Replacement Tests (failure replaced or repaired) $T = nt^*$ (8.14)

Non-Replacement Tests $T = \sum_{i=1}^r t_i + (n - r)t^*$ (8.15)

where t_i = time of the i^{th} failure

Censored Items (withdrawal or loss of items which have not failed)

(a) If failures are replaced and censored items are not replaced

$$T = \sum_{j=1}^c t_j + (n - c)t^* \quad (8.16)$$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

where:

- t_j = time of censorship
 c = number of censored items

(b) If failures are not replaced

$$T = \sum_{i=1}^r t_i + \sum_{j=1}^c t_j + (n - r - c)t^* \quad (8.17)$$

Example 6:

Twenty items undergo a replacement test. Testing continues until ten failures are observed. The tenth failure occurs at 80 hours. Determine (1) the mean life of the items; and (2) the one-sided and two-sided 95% confidence intervals for the MTBF.

(1) From Equation (8.4)

$$\text{MTBF} = \frac{nt^*}{r} = \frac{(20)(80)}{10} = 160 \text{ hours}$$

(2) $\alpha = 1 - \text{Confidence Level} = 1 - 0.95 = 0.05$

$$2r = 2(\text{number of failures}) = 2(10) = 20$$

$$C \left[\frac{2T}{\chi^2_{(\alpha, 2r)}}, \infty \right] = C \left[\frac{2(1600)}{\chi^2_{(0.05, 20)}}, \infty \right] = C \left[\frac{3200}{31.41}, \infty \right] = C [101.88, \infty] = .95$$

That is, 101.88 hours is the lower (one-sided) 95% confidence limit of θ , the true mean life where $\chi^2_{(0.05, 20)} = 31.41$ is from Table 8.3-11.

In other words, we are 95% confident that the true MTBF exceeds 101.88 hours.

(3) From Equation (8.13)

$$C \left(\frac{2T}{\chi^2_{\left(\frac{\alpha}{2}, 2r\right)}}, \frac{2T}{\chi^2_{\left(1 - \frac{\alpha}{2}, 2r\right)}} \right) = C \left(\frac{3200}{34.17}, \frac{3200}{9.591} \right) = C(93.65, 333.65) = .95$$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

That is, 93.65 hours is the lower (two-sided) 95% confidence limit for the mean life and 333.65 hours is the upper (two-sided) 95% confidence limit for that true mean. We are 95% confident that the interval between 93.65 and 333.65 hours contains the true MTBF.

Example 7:

Twenty items undergo a nonreplacement test, which is terminated at 100 hours. Failure times observed were 10, 16, 17, 25, 31, 46, and 65 hours. Calculate (1) the one-sided approximate 90% confidence interval ($\alpha = 0.10$), and (2) the two-sided approximate 90% confidence limits of θ , the mean life.

- (1) From Equations (8.12) and (8.15)

$$C = C \left(\frac{2 \left[\sum_{i=1}^7 t_i \right] + (20-7)(100)}{\chi^2(.10, 16)}, \infty \right)$$

$$= C \left(\frac{3020}{23.54}, \infty \right) = C(128.3, \infty) = .90$$

128.3 hours is the lower single-sided 90% confidence limit for θ , the true mean life.

- (2) From Equation (8.13)

$$C \left(\frac{2T}{\chi^2 \left(\frac{\alpha}{2}, 2r+2 \right)}, \frac{2T}{\chi^2 \left(1 - \frac{\alpha}{2}, 2r \right)} \right) = C \left(\frac{3020}{26.30}, \frac{3020}{6.57} \right)$$

$$= C(114.83, 459.67) = .90$$

That is, 114.83 hours is the lower (two-sided) 90% confidence limit for θ , the true mean life, and 459.67 hours is the upper (two-sided) 90% confidence limit.

Table 8.3-12 presents the factor $2/\chi^2_{p,d}$ for one-sided and two-sided confidence limits, at six confidence levels for each. Multiplying the appropriate factor by the observed total life T gives a confidence limit on σ . Figure 8.3-16 presents a graphical technique for determining upper and lower confidence limits for tests truncated at a fixed time, when the number of failures is known.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

TABLE 8.3-12: FACTORS FOR CALCULATION OF MEAN LIFE CONFIDENCE INTERVALS FROM TEST DATA (FACTORS = $2/\chi^2_{P,D}$)
(Assumption of Exponential Distribution)

d	99-1/2% One-Sided										Upper Limit	
	99% Two-Sided					99% One-Sided					99-1/2% One-Sided	95% One-Sided
	98% One-Sided		95% Two-Sided			97-1/2% One-Sided			90% One-Sided			
	90% Two-Sided		80% Two-Sided	60% Two-Sided	80% One-Sided	90% Two-Sided		60% Two-Sided	80% One-Sided	Lower Limit		
2	.185	.217	.272	.333	.433	.619	4.47	9.462	19.388	39.58	100.0	200.0
4	.135	.151	.180	.210	.257	.334	1.21	1.882	2.826	4.102	6.667	10.00
6	.108	.119	.139	.159	.188	.234	.652	.909	1.221	1.613	2.3077	3.007
8	.0909	.100	.114	.129	.150	.181	.437	.573	0.733	.921	1.212	1.481
10	.0800	.0857	.0976	.109	.125	.149	.324	.411	.508	.600	.789	.909
12	.0702	.0759	.0856	.0952	.107	.126	.256	.317	.383	.454	.555	.645
14	.0635	.0690	.0765	.0843	.0948	.109	.211	.257	.305	.355	.431	.500
16	.0588	.0625	.0693	.0760	.0848	.0976	.179	.215	.251	.290	.345	.385
18	.0536	.0571	.0633	.0693	.0769	.0878	.156	.184	.213	.243	.286	.322
20	.0500	.0531	.0585	.0635	.0703	.0799	.137	.158	.184	.208	.242	.270
22	.0465	.0495	.0543	.0589	.0648	.0732	.123	.142	.162	.182	.208	.232
24	.0439	.0463	.0507	.0548	.0601	.0676	.111	.128	.144	.161	.185	.200
26	.0417	.0438	.0476	.0513	.0561	.0629	.101	.116	.130	.144	.164	.178
28	.0392	.0413	.0449	.0483	.0527	.0588	.0927	.106	.118	.131	.147	.161
30	.0373	.0393	.0425	.0456	.0496	.0551	.0856	.0971	.108	.119	.133	.145
32	.0355	.0374	.0404	.0433	.0469	.0519	.0795	.0899	.0997	.109	.122	.131
34	.0339	.0357	.0385	.0411	.0445	.0491	.0742	.0834	.0925	.101	.113	.122
36	.0325	.0342	.0367	.0392	.0423	.0466	.0696	.0781	.0899	.0939	.104	.111
38	.0311	.0327	.0351	.0375	.0404	.0443	.0656	.0732	.0804	.0874	.0971	.103
40	.0299	.0314	.0337	.0359	.0386	.0423	.0619	.0689	.0756	.0820	.0901	.0968

To Use: Multiply value shown by total part hours to get MTBF figures in hours
 Note: $d = 2r$, except for the lower limit on tests truncated at a fixed time and where $r < n$. In such cases, use $d = 2(r + 1)$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

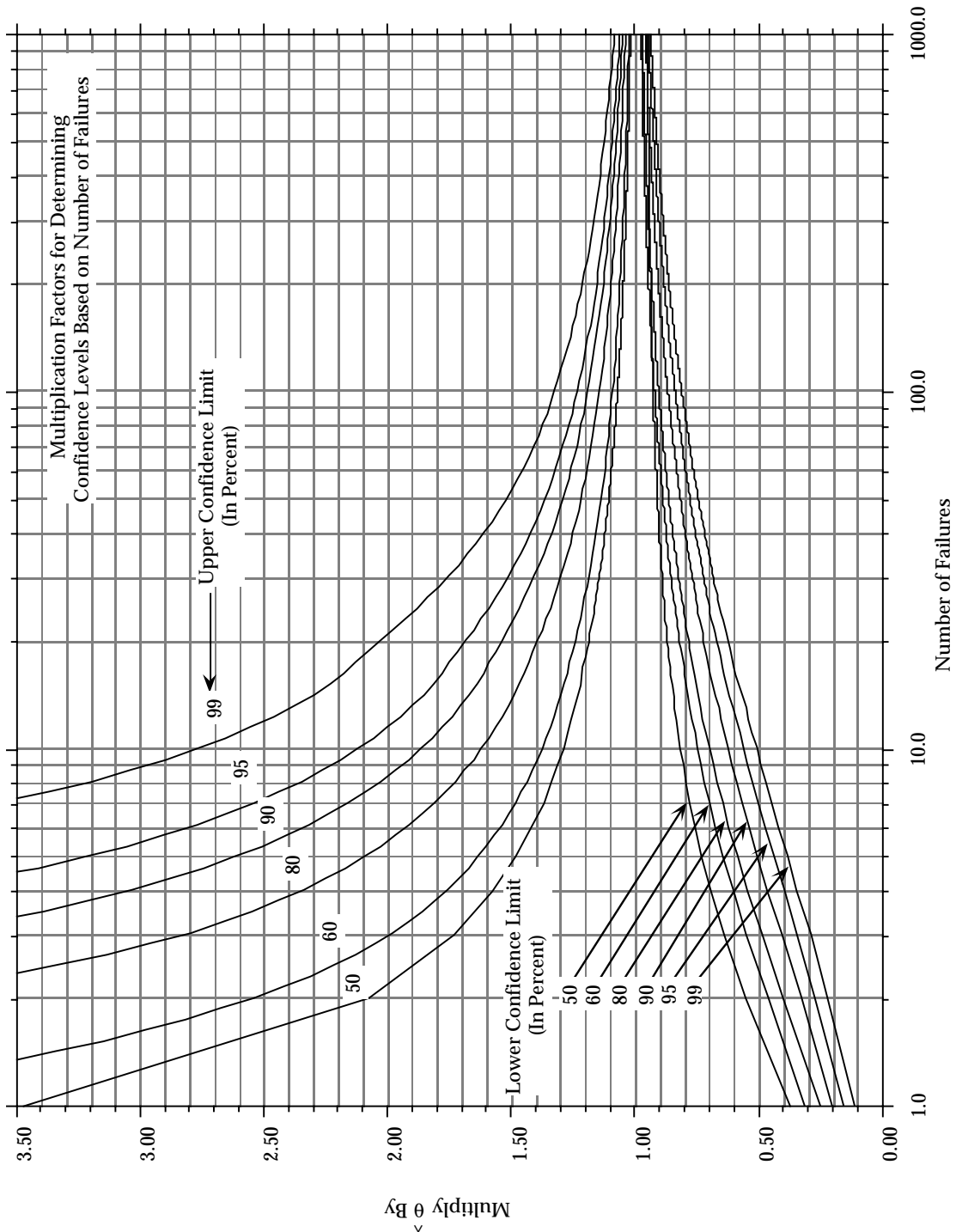


FIGURE 8.3-16: MULTIPLICATION RATIOS FOR DETERMINING UPPER AND LOWER CONFIDENCE LIMITS VS. NUMBER OF FAILURES FOR TEST TRUNCATED AT A FIXED TIME

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

Reliability Estimates (Exponential Distribution)

We know the probability of (or proportion of items) surviving t hours is found by:

$$\hat{R}(t) = e^{-t/\theta} \quad (8.18)$$

The confidence interval on $R(t)$ is

$$C \left(e^{-t/\hat{\theta}_L} < R(t) < e^{-t/\hat{\theta}_U} \right) = 1 - \alpha$$

where:

$\hat{\theta}_L$ and $\hat{\theta}_U$ are the lower and upper confidence limits on θ .

Example 8:

Based on the data of Example 1, (1) what is the probability of an item surviving 100 hours? (2) what are the two-sided 95% confidence limits on this probability?

- (1) From Equation (8.18)

$$\hat{R}(100) = e^{-100/\hat{\theta}} = e^{-100/160} = 0.535$$

- (2) The two-sided confidence limits on the reliability are

$$\left(e^{-100/93.65}, e^{-100/333.65} \right) = (0.344, 0.741) = 95\%$$

8.3.2.5.3 Confidence-Interval Estimates for the Binomial Distribution

For situations where reliability is measured as a ratio of the number of successes to the total number of trials, e.g., one-shot items, missiles, etc., the confidence interval is determined by consideration of the binomial distribution. Table XI of Hald's Statistical Tables and Formulas (John Wiley and Sons, Inc., New York, 1952) and Ref. [10] gives 95% and 99% confidence limits for a wide range of values. Figure 8.3-17 allows a rough estimate to be made when the number of successes (S) and the number of trials (N) are known.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

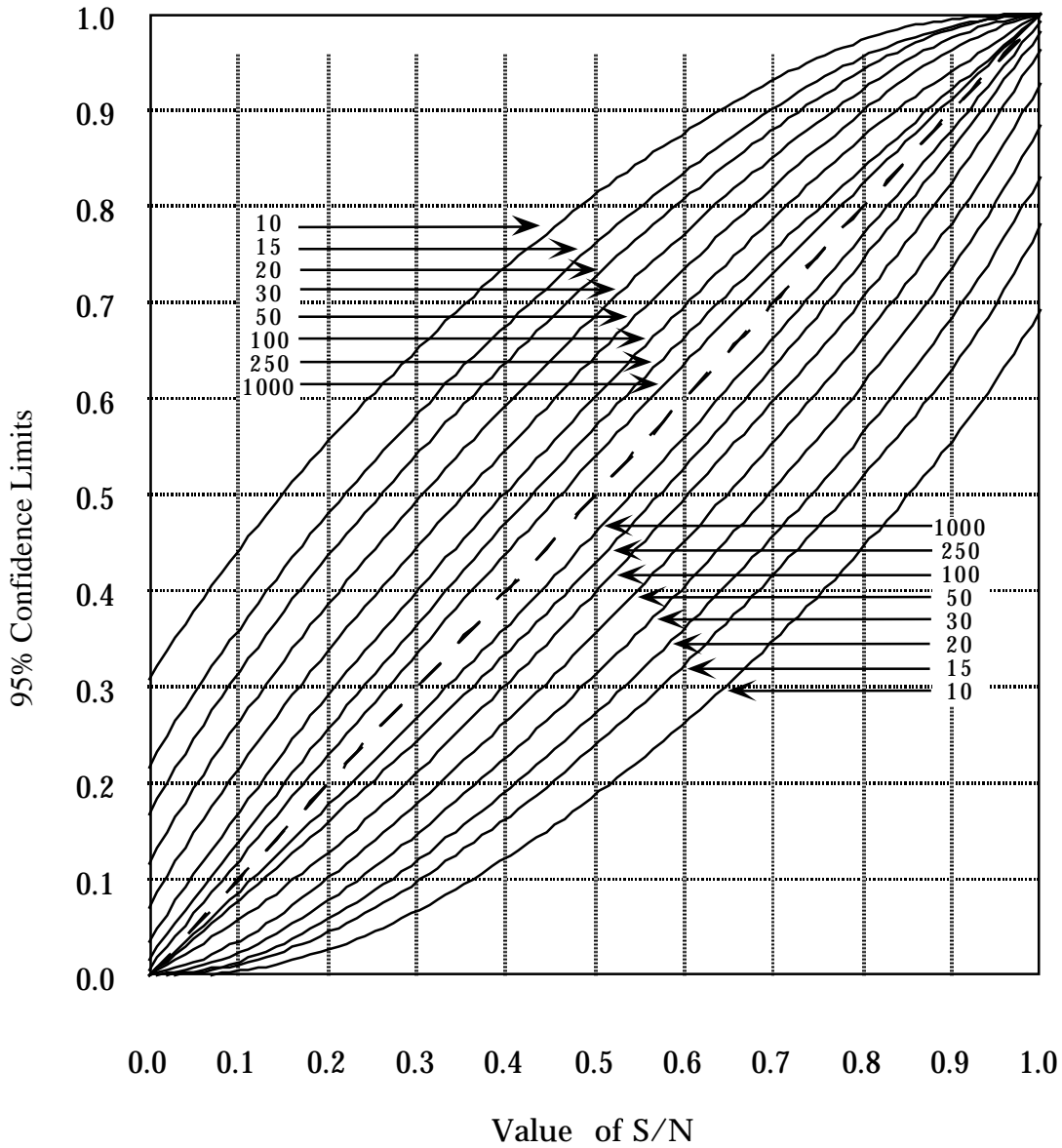


FIGURE 8.3-17: CHART FOR 95% CONFIDENCE LIMITS
ON THE PROBABILITY S/N^1

¹ From Clopper, C.J., and Pearson, E.S., "The Use of Confidence or Fiducial Limits Illustrated in the Case of the Binomial," BIOMETRIKA, Vol. 26 (1934), p. 410. Reprinted with permission.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

Example 9:

$S = 8$; $N = 10$. (a) What is the reliability estimate? (b) What are the two-sided upper and lower 95% confidence limits? Answers: (a) 0.80; (b) 0.98 and 0.43.

More detailed analyses of confidence limits and intervals, with many more examples under a variety of circumstances, and for a variety of distributions, e.g., binomial, gamma, Weibull, etc., are given in Refs. [5], [8], [9] and [10].

8.3.2.6 Tests for Validity of the Assumption Of A Theoretical Reliability Parameter Distribution

The validity of many statistical techniques used in the calculation, analysis, or prediction of reliability parameters depends on the distribution of the failure times. Many techniques are based on specific assumptions about the probability distribution and are often sensitive to departures from the assumed distributions. That is, if the actual distribution differs from that assumed, these methods sometimes yield seriously wrong results. Therefore, in order to determine whether or not certain techniques are applicable to a particular situation, some judgment must be made as to the underlying probability distribution of the failure times.

As was discussed in Section 8.3.1, some theoretical reliability functions, such as those based on the exponential, normal, lognormal, and Weibull distributions will plot as straight lines on special types of graph paper. This is the simplest procedure and should be used as a "first cut" in determining the underlying distribution. Plot the failure data on the appropriate graph paper for the assumed underlying distribution; "eyeball" it, and if it quite closely approximates a straight line, you are home free.

If it cannot be determined visually that the reliability function follows a straight line when plotted on special graph paper, then one must resort to the application of analytical "goodness-of-fit" tests.

The two goodness-of-fit tests described in this section assume a null hypothesis, i.e., the sample is from the assumed distribution. Then a statistic, evaluated from the sample data, is calculated and looked-up in a table that shows how "lucky" or "unlucky" the sample. The luck is determined by the size of the two-sided tail area. If that tail is very small (you were very unlucky if the null hypothesis is true), the null hypothesis (there is no difference between the actual and the assumed distributions) is rejected. Otherwise, the null hypothesis is accepted, i.e., the actual distribution could easily have generated that set of data (within the range of the data); the test says nothing about the behavior of the distribution outside the range of the data.

Goodness-of-fit tests are statistical tests, not engineering tests. No matter what the distribution or what the test, it is possible to take a sample small enough so that virtually no distribution will be rejected, or large enough so that virtually every distribution will be rejected.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

Thus, while a method for small sample sizes is presented as well as one for large sample sizes, it is a fact of life that must be accepted that tests based on small samples are simply not very powerful (power is the probability of rejecting the null hypothesis where it, indeed, is incorrect). Therefore, the methodology is presented here for completeness, but very likely a more logical approach is to first make an assumption regarding the failure distribution based on engineering judgment or on historical data or on knowledge of the failure characteristics of similar parts. Once the failure distribution has been assumed the test can be performed for goodness-of-fit for that particular distribution. If the hypothesized distribution is shown not to fit, it is quite certain that the assumed distribution was not the one from which the samples were selected. If, however, the goodness-of-fit test shows that the data could have come from the hypothesized distribution, then it is virtually certain that tests for fit to other distributions would yield like results.

In summary then, it must be realized that the tests presented in the next two sections have limitations. The only cure for these limitations is a larger number of observations. If this proves uneconomical or not feasible from the standpoint of the test time required to generate the desired number of failures or the cost of testing, or some other practical constraint, then the only alternative is to use the results of small sample size analyses with proper discretion.

8.3.2.6.1 Kolmogorov-Smirnov (K-S) Goodness-of-Fit Test (also called “d” test)

This test is based upon the fact that the observed cumulative distribution of a sample is expected to be fairly close to the true cumulative distribution. The goodness-of-fit is measured by finding the point at which the sample and the population are farthest apart and comparing this distance with the entry in a table of critical values, Table 8.3-13, which will then indicate whether such a large distance is likely to occur. If the distance is too large, the chance that the observations actually come from a population with the specified distribution is very small. This is evidence that the specified distribution is not the correct one.

1. When to Use

When failure times from a sample have been observed and it is desired to determine the underlying distribution of failure times.

2. Conditions for Use

- (a) Usually historical data or engineering judgment suggest that item failure times of interest are from a given statistical failure distribution. This test then follows the step of assuming a given failure distribution and is useful to determine if empirical data disprove this hypothesis.

**SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH**

- (b) The Kolmogorov-Smirnov test for goodness-of-fit is distribution free and can therefore be used regardless of the failure distribution that the data are assumed to follow.
- (c) The discriminating ability of the statistical test is dependent on sample size; the larger the sample size, the more reliable the results. When large sample sizes are available, the χ^2 Test for Goodness-of-Fit is more powerful but requires additional manipulation of the data. Where sample sizes are small, the Kolmogorov-Smirnov test provides limited information but is a better choice than the χ^2 alternative.
- (d) Strictly speaking, this test method requires prior knowledge of the parameters. If the parameters are estimated from the sample the exact error risks are unknown.
- (e) A Kolmogorov-Smirnov table is required (see Table 8.3-13).

TABLE 8.3-13: CRITICAL VALUES $d_{\alpha;n}$ OF THE MAXIMUM ABSOLUTE DIFFERENCE BETWEEN SAMPLE AND POPULATION RELIABILITY FUNCTIONS

Sample Size, N	Level of Significance, α				
	0.20	0.15	0.10	0.05	0.01
3	0.565	0.597	0.642	0.708	0.828
4	0.494	0.525	0.564	0.624	0.733
5	0.446	0.474	0.474	0.565	0.669
10	0.322	0.342	0.368	0.410	0.490
15	0.266	0.283	0.304	0.338	0.404
20	0.231	0.246	0.264	0.294	0.356
25	0.21	0.22	0.24	0.27	0.32
30	0.19	0.20	0.22	0.24	0.29
35	0.18	0.19	0.21	0.23	0.27
40	0.17	0.18	0.19	0.21	0.25
45	0.16	0.17	0.18	0.20	0.24
50	0.15	0.16	0.17	0.19	0.23
over } 50 }	$\frac{1.07}{\sqrt{N}}$	$\frac{1.14}{\sqrt{N}}$	$\frac{1.22}{\sqrt{N}}$	$\frac{1.36}{\sqrt{N}}$	$\frac{1.63}{\sqrt{N}}$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. Graphic Method (Example Using Exponential Distribution)

Forty-eight samples of an equipment's time-to-failure are acquired. Based upon the assumption of an exponential distribution of time-to-failure, the point estimate of MTBF is calculated to be 1546 hours.

We would like to test the hypothesis that the sample came from a population where time-to-failure followed an exponential distribution with an MTBF of 1546 hours (see Figure 8.3-18).

- (a) Draw the curve (dashed line) for the theoretical distribution of $R(t)$ which is assumed to be an exponential with an $MTBF = 1546$ hours.
- (b) Find the value, d , using Table 8.3-13 which corresponds to sample size, $n = 48$, and level of significance, $\alpha = 0.05$: $d = (1.36/\sqrt{48} = 0.196)$.
- (c) Draw curves at a distance $d = 0.196$ above and below the theoretical curve drawn in step (a), providing upper and lower boundaries as shown in Figure 8.3-18.
- (d) On the same graph draw the observed cumulative function (solid line).
- (e) If the observed function falls outside the confidence band drawn in step (c), there would be a five percent chance that the sample came from an exponential population with a mean life of 1546 hours.
- (f) If the observed function remains inside the band, as it does in the example, this does not prove that the assumed distribution is exactly right, but only that it might be correct and that it is not unreasonable to assume that it is.

This example could have also been solved analytically by calculating the difference between the theoretical cumulative distribution function (CDF) and the actual CDF at each data point, finding the maximum deviation and comparing it with the value derived from Table 8.3-13 ($d = 0.196$). If the maximum deviation is less than 0.196, we accept the hypothesis (at the .05 significance level) that the time to failure is exponentially distributed with an MTBF of 1546 hours.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

4. Analytical Method

Example (Weibull Distribution)

a. Observe and record part failure times

a. Given the following 20 failure times in hours

92	640
130	700
233	710
260	770
320	830
325	1010
420	1020
430	1280
465	1330
518	1690

b. Assume a distribution of failure times based on historical information or on engineering judgment

b. Assume failure times are distributed according to the two-parameter Weibull distribution.

c. Estimate the parameters of the assumed distribution from the observed data.

c. By the graphic method or the method of least squares, find the Weibull parameters. The Weibull shape parameter β equals 1.50 and the Weibull scale parameter α equals 28400.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

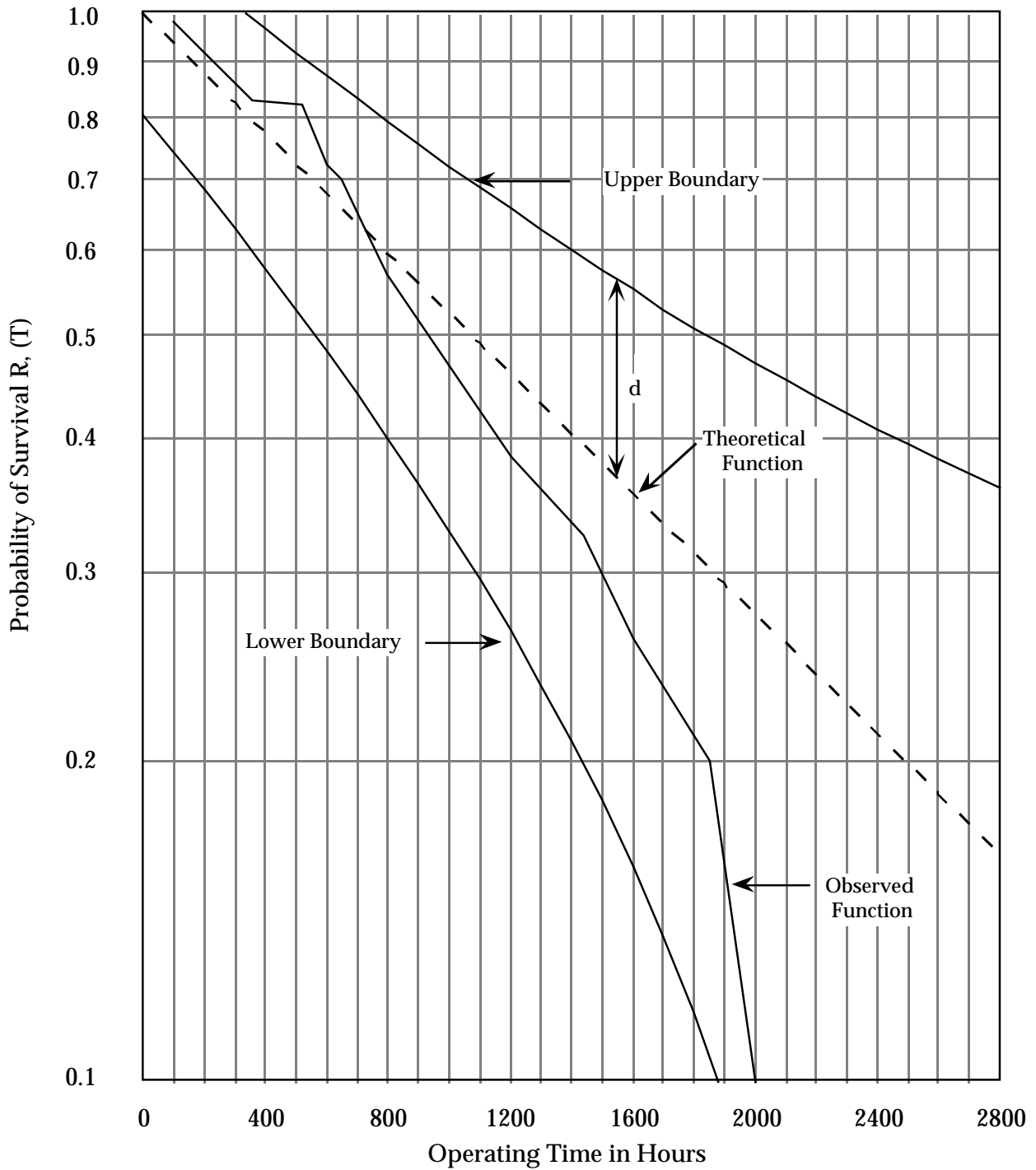


FIGURE 8.3-18: EXAMPLE OF THE APPLICATION OF THE "d" TEST

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

- d. Calculate the probability of failure for each observation from the cumulative failure function for the assumed distribution.

- d. For the Weibull distribution the cumulative failure function is

$$\hat{F}(X) = 1 - \exp\left(-\frac{X^\beta}{\alpha}\right)$$

where X = observed failure time,
 $\beta = 1.5$ = Weibull shape parameter,
 $\alpha = 28400$ = Weibull scale

parameter, $\hat{F}(X)$ = probability of failure at or before time X .

For the 20 observations of this example, the probability of failure at the respective times is:

X	$\hat{F}(X)$
92	.03
130	.05
233	.12
260	.14
320	.18
325	.19
420	.26
430	.27
465	.30
518	.34
640	.43
700	.48
710	.49
770	.53
830	.57
1010	.68
1020	.68
1280	.80
1330	.82
1690	.91

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

- e. Calculate the percentile for each of (i) failure times by the relationship

$$F(i) = \frac{i}{n+1} \cdot \text{Subtract those of}$$

Step d. above. Record the absolute value of the difference.

- e. For $n = 20$, $\frac{i}{n+1}$ gives the following results:

$\hat{F}(x)$	$F(i)$	$ \hat{F}(x) - F(i) $
.03	.05	.02
.05	.10	.05
.12	.14	.02
.14	.19	.05
.18	.24	.06
.19	.29	.10
.26	.33	.07
.27	.38	.11
.30	.43	.13
.34	.48	.14
.43	.52	.09
.48	.57	.09
.49	.62	.13
.53	.67	.14
.57	.71	.14
.68	.76	.08
.68	.81	.13
.80	.86	.06
.82	.90	.08
.91	.95	.04

- f. Compare the largest difference from step e with a value at the desired significance level in the Kolmogorov-Smirnov tables to test for goodness-of-fit. If the tabled value is not exceeded then it is not possible to reject the hypothesis that the failure times are from the assumed distribution.

- f. The largest difference in Step e. was .14. From the Kolmogorov-Smirnov table for a significance of .05 and for a sample of size 20 a difference of greater than .294 must be observed before it can be said that the data could not have come from a Weibull distribution with $\beta = 1.5$, $\alpha = 28400$.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

8.3.2.6.2 Chi-Square Goodness-of-Fit Test

The chi-square goodness-of-fit test may be used to test the validity of any assumed distribution, discrete or continuous. The test may be summarized as follows for a continuous distribution.

- (a) Determine the underlying distribution to be tested.
- (b) Determine a level of significance, α , which is defined as the risk of rejecting the underlying distribution if it is, in fact, the real distribution.
- (c) Divide the continuous scale into k intervals. For reliability analysis, this scale is usually time.
- (d) Determine the number of sample observations falling within each interval.
- (e) Using the assumed underlying distribution, determine the expected number of observations in each interval. Combining of intervals may be required because the expected number of observations in an interval must be at least 5.0. This determination may require an estimation of the distribution parameters from the sample data (w is the number of estimated parameters).
- (f) Compute

$$\chi^2 = \sum_{i=1}^k \frac{(O_i - E_i)^2}{E_i} \quad (8.19)$$

where:

O_i = number of sample observations in the i^{th} interval

E_i = expected number of observations in the i^{th} interval

k = number of intervals

- (g) Let w be the number of parameters estimated from the data and let $\chi^2_{\alpha, k-w-1}$ be the value found in Table 8.3-11.
- (h) Compare the calculated χ^2 statistic with the tabled χ^2 value for the discrete level of the signature

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

$$\text{If } \chi^2 = \sum_{i=1}^k \frac{(O_i - E_i)^2}{E_i} > \chi^2_{\alpha, k-w-1} \quad (8.20)$$

reject the distribution under test. Otherwise, we do not have sufficient evidence to reject the assumed underlying distribution.

1. When to Use

When failure times are available from a relatively large sample and it is desired to determine the underlying distribution of failure times.

2. Conditions for Use

- (a) In the statistical analysis of failure data it is common practice to assume that failure times follow a given failure distribution family. This assumption can be based on historical data or on engineering judgment. This test for goodness-of-fit is used to determine if the empirical data disproves the hypothesis of fit to the assumed distribution.
- (b) The χ^2 test for goodness-of-fit is “distribution-free” and can therefore be used regardless of the failure distribution that the data are assumed to follow.
- (c) This test is not directly dependent on sample size but on the number of intervals into which the scale of failure times is divided with the restriction that no interval should be so narrow that there are not at least 5 theoretical failures within the interval. Therefore, the test is only useful if a relatively large number of failures has been observed.
- (d) A table of χ^2 percentage points is required (see Table 8.3-12).

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. Method (Example Using Exponential Distribution)

Consider the data in Figure 8.3-19 indicating the failure times obtained from testing a sample of 100 fuel systems. Using a significance level of $\alpha = 0.05$, test whether the assumption of an exponential distribution is reasonable. The sample mean was found to be 8.9 hours.

(a) Figure 8.3-20 is used as a means of computing

$$\sum_{i=1}^k \frac{(O_i - E_i)^2}{E_i}$$

(b) The expected frequency, E_i , is found by multiplying the sample size by the probability of falling within the i^{th} interval if the assumed (exponential) distribution is true.

$$\begin{aligned} E_i &= n \left[\exp\left(\frac{-L_i}{\hat{\theta}}\right) - \exp\left(\frac{-U_i}{\hat{\theta}}\right) \right] \\ &= 100 \left[\exp\left(\frac{-L_i}{8.9}\right) - \exp\left(\frac{-U_i}{8.9}\right) \right] \end{aligned}$$

Interval (Hours)	Frequency
0 - 5.05	48
5.05 - 10.05	22
10.05 - 15.05	11
15.05 - 20.05	7
20.05 - 25.05	3
25.05 - 30.05	5
30.05 - 35.05	2
35.05 - 40.05	0
40.05 - 45.05	1
45.05 - 50.05	0
50.05 - 55.05	1
	100

FIGURE 8.3-19: FUEL SYSTEM FAILURE TIMES

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

Interval (hours) ($L_i - U_i$)	Observed Frequency (O_i)	Expected Frequency (E_i)	$O_i - E_i$	$(O_i - E_i)^2$	$\frac{(O_i - E_i)^2}{E_i}$
0 - 5.05	48	43	5	25	.58
5.05 - 10.05	22	24	-2	4	.17
10.05 - 15.05	11	14	-3	9	.64
15.05 - 20.05	7	8	-1	1	.13
20.05 - 25.05	3	5	-2	4	.80
25.05 - 30.05	5	3	2	4	1.33
30.05 - 35.05	2	3	1	1	.33
35.05 - 40.05	0				
40.05 - 45.05	1				
45.05 - 50.05	0				
50.05 - 55.05	1				3.98

FIGURE 8.3-20: COMPUTATION

where U_i and L_i are the upper and lower limits of the i^{th} interval, $U_i = L_i + 5$, and $\theta = 8.9$ hours.

- (c) Some of the original intervals were combined to satisfy the requirement that no E_i value be less than 2.5.

$$\chi^2 = \sum_{i=1}^7 \frac{(O_i - E_i)^2}{E_i} = 3.98$$

$$\chi^2_{\alpha, k-w-1} = \chi^2_{.05, 7-1-1} = \chi^2_{0.5, 5} = 11.070$$

(See Table 8.3-11)

$$\text{Since } \chi^2 = \sum_{i=1}^7 \frac{(O_i - E_i)^2}{E_i} = 3.97 < \chi^2_{0.5, 5} = 11.070,$$

we do not have sufficient evidence to reject the exponential distribution as a model for these failure times.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

4. MethodExample (Weibull Distribution)

- a. Observe and record part failure times.

- a. The following is the number of cycles to failure for a group of 50 relays on a life test:

1283	6820	16306
1887	7733	17621
1888	8025	17807
2357	8185	20747
3137	8559	21990
3606	8843	23449
3752	9305	28946
3914	9460	29254
4394	9595	30822
4398	10247	38319
4865	11492	41554
5147	12913	42870
5350	12937	62690
5353	13210	63910
5410	14833	68888
5536	14840	73473
6499	14988	

- b. Assume a distribution of failure times based on historical information or on engineering judgment.

- b. Assume failure times are distributed according to the two-parameter Weibull distribution.

- c. Estimate the parameters of the assumed distribution from the observed data.

- c. By the graphical method or method of least squares find the Weibull parameters. The Weibull shape parameter $\beta=1.21$ and the Weibull scale parameter $\alpha =127978$.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

- | | |
|--|--|
| <p>d. Divide the spectrum of failure times into intervals of such a width that the theoretical number of failures in each interval will be at least five. The width of intervals need not be equal but extra care must be used in determining the expected frequencies in this case.</p> | <p>d. Divide the relay cycles-to-failure into the following intervals:</p> |
|--|--|
- | | | |
|-------|---|-------|
| 0 | - | 4000 |
| 4001 | - | 7200 |
| 7201 | - | 13000 |
| 13001 | - | 18000 |
| 18001 | - | 25000 |
| 25001 | - | above |
- | | |
|---|--|
| <p>e. Calculate the theoretical number of failures for each interval.</p> | <p>e. The expected number of failures in each interval is obtained as follows:</p> |
|---|--|

For the Weibull distribution the cumulative failure function is

$$F(X) = 1 - \exp \left(-\frac{X^\beta}{\alpha} \right)$$

where: X = observed failure times
 β = Weibull shape parameter
 α = Weibull scale parameter

Then $F(X_n) - F(X_{n-1})$ = probability that a failure time falls within the interval. Then for each interval the probability of failure in that interval, multiplied by the sample size, equals the theoretical number of failures for each interval.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

(1) Upper Boundary of Interval	(2) F(X)	(3) F(X _n) - F(X _(n-1))	(4) Theoretical Failure Frequency (Col. 3x50) E _i
4000	.16	.16	8
7200	.30	.14	7
13000	.52	.22	11
18000	.66	.14	7
25000	.80	.14	7
∞	1.00	.20	10

NOTE: The theoretical frequency must not be less than 5 for any interval.

- f. Calculate the χ^2 statistic by the formula

$$\chi^2 = \sum_{i=1}^k \frac{(O_i - E_i)^2}{E_i}$$

where: k = number of intervals
 O_i = observed frequency
 interval
 E_i = theoretical
 frequency per
 interval

Upper Boundary of Interval	E _i	O _i	$\frac{(O_i - E_i)^2}{E_i}$
4000	8	8	0
7200	7	10	1.29
13000	11	12	.09
18000	7	7	0
25000	7	3	2.29
∞	<u>10</u>	<u>10</u>	<u>0</u>
	50	50	$\chi^2 = 3.67$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

g. Determine if the χ^2 statistic indicates that the data could have come from the hypothesized distributions using χ^2 tables (Table 8.3-11) and $(k-1) - p$ degrees of freedom.

where: k = number of intervals
 p = number of parameters estimated

g. The degrees of freedom for this example are calculated as:

$$\begin{aligned} \text{d.f.} &= (k-1) - p \\ \text{d.f.} &= (6-1) - 2 = 3 \end{aligned}$$

The value from the χ^2 table for 3 degrees of freedom at the 0.05 level of significance is 7.815. Since 3.69 does not exceed the tabled value, then the hypothesis that this data came from a Weibull distribution cannot be rejected.

8.3.2.6.3 Comparison of K-S and Chi-Square Goodness-of-Fit Tests

The K-S test is superior to χ^2 in the following ways:

- (1) The K-S Test can be used to test for deviations in a given direction, while Chi-Square Test can be used only for a two-sided test.
- (2) The K-S Test uses ungrouped data so that every observation represents a point of comparison, while the Chi-Square Test requires the data to be grouped into cells with arbitrary choice of interval, size, and selection in starting point. Minimum expected frequency values are required.
- (3) The K-S Test can be used in a sequential test where data become available from smallest to largest, computations being continued only up to the point at which rejection occurs.

The Chi-Square Test is superior to the K-S Test in the following ways:

- (1) Chi-square can be partitioned and added
- (2) Chi-square can be applied to discrete populations

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

8.4 Reliability Demonstration

8.4.1 Introduction

The single purpose of a reliability demonstration test is to determine conformance to specified, quantitative reliability requirements as a basis for qualification or acceptance; this is to answer the question, “Does the item meet or exceed (not by how much) the specified minimum reliability requirement?”

Reliability testing involves an empirical measurement of time-to-failure during equipment operation for the purpose of determining whether an equipment meets the established reliability requirements. A reliability test is effectively a “sampling” test in the sense that it is a test involving a sample of objects selected from a population. In reliability testing, the population being measured encompasses all failures that will occur during the life span of the equipment. A test sample is drawn from this population by observing those failures occurring during a small portion of the equipment's life. In reliability testing, as in any sampling test, the sample is assumed to be representative of the population, and the mean value of the various elements of the sample (e.g., times-to-failure) is assumed to be a measure of the true mean (MTBF, etc.) of the population.

A sample in a reliability test consists of a number of times-to-failure, and the population is all the times-to-failure that could occur either from the one equipment or the more than one equipment on test. The “test” equipments (assuming more than one equipment) are considered identical and, thus, their populations are also identical. Under the assumption of an exponential failure model (*constant* λ), a test of 10 devices for 100 hours each is mathematically equivalent to a test of 1 device for 1000 hours. If all possible samples of the same number of times-to-failure were drawn from the same or identical equipment, the resulting set of sample means would be distributed about the true MTBF (θ) of the equipment, following a normal distribution as is shown in Figure 8.4-1.

Since it is not economically feasible to test the complete population, we have to be satisfied with a sample of the population. From the data in the sample we then make some statement about the population parameter.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

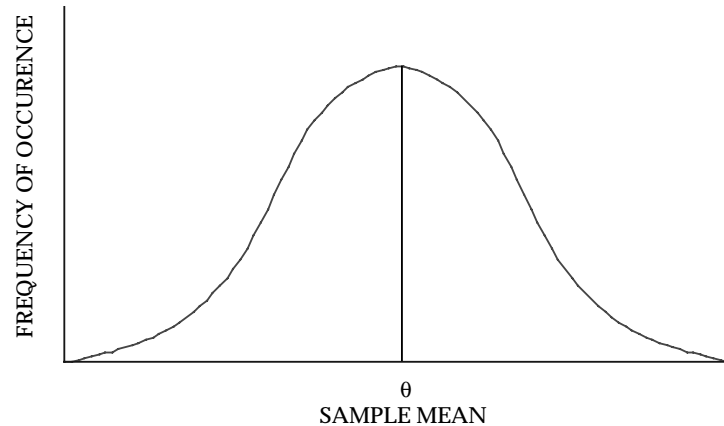


FIGURE 8.4-1: NORMAL DISTRIBUTION

What we are doing is testing a statistical hypothesis: For example, we might test

H_0 : (null hypothesis) $\theta_0 \geq 200$ hours

H_1 : (alternate hypothesis) $\theta_1 \leq 100$ hours www.kekaoxing.com

Based upon the test results, we either accept H_0 or reject it. In making our decision we have to keep several risks in mind.

Producer's risk (α) is the probability of rejecting H_0 when it is true (probability of rejecting good equipment)

Consumer's risk (β) is the probability of accepting H_0 when it is false (probability of accepting bad equipment)

Looking at it another way, if θ_0 and θ_1 represent the hypotheses, then the α and β errors are the hatched areas shown in Figure 8.4-2A. Of course, if we could take enough samples, then the standard deviation about each of the means would be reduced and the α and β errors would also be reduced.

However, this is usually impractical so the sample size is set as low as possible to reduce costs by specifying the maximum acceptable α and β risks that can be associated with θ_0 and the smallest acceptable θ_1 . Why two values? Let's look at our decision rule, or accept/reject criteria. We would like it to look like Figure 8.4-3A.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

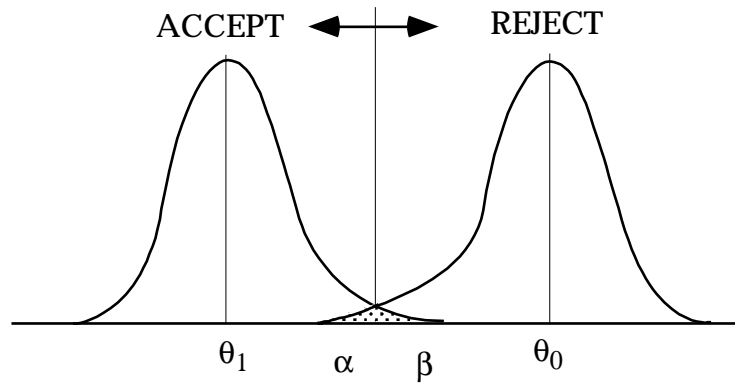


FIGURE 8.4-2A: HYPOTHESIS TEST A

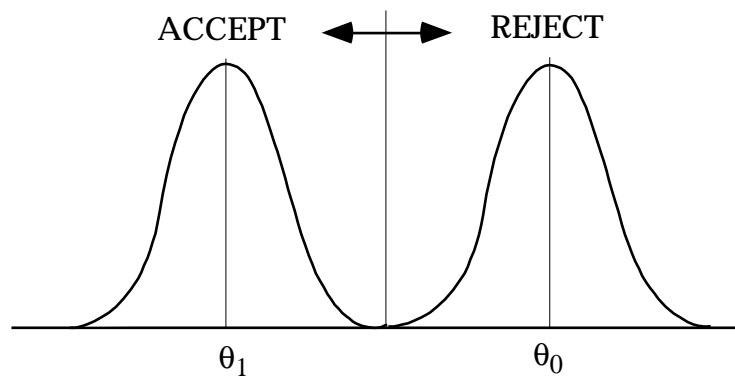


FIGURE 8.4-2B: HYPOTHESIS TEST B

This relationship between the probability of acceptance and the requirement (e.g. MTBF) is called the *operating characteristic curve*. The ideal curve shown in Figure 8.4-2B would require an infinite number of samples. In real life we settle for something that gives a small probability of acceptance (P_A) for MTBF's below the requirement and high P_A for MTBF's above the requirement, M_0 .

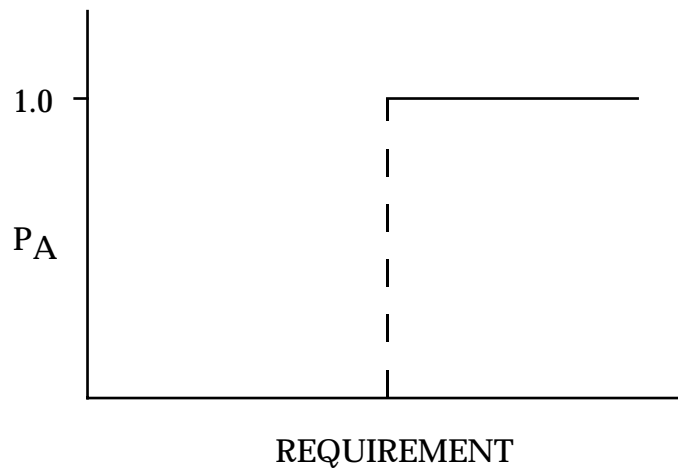
SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

FIGURE 8.4-3A: IDEAL OPERATING CHARACTERISTIC (OC) CURVE

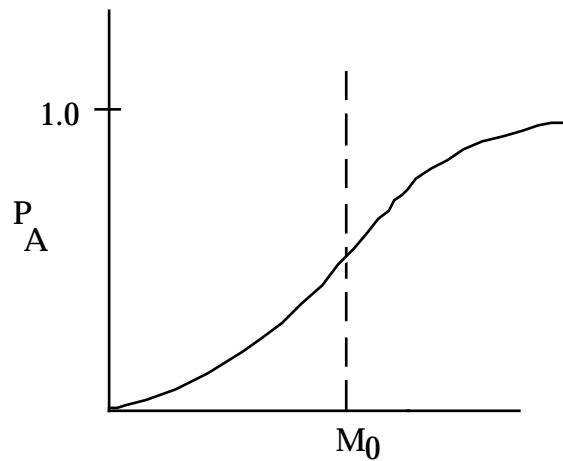


FIGURE 8.4-3B: TYPICAL OPERATING CHARACTERISTIC CURVE

For example, suppose we had an MTBF requirement of 200 hours, a demonstration test of 1000 hours, and the decision rule,

Accept H_0 if $r \leq 5$

Reject H_0 if $r > 5$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

where r is the number of failures which is Poisson distributed (fixed time test) as

$$P(r) = P_R = \frac{(t/m)^r e^{-t/m}}{r!} \quad (8.21)$$

where m is the MTBF.

We plot $P_A (r \leq 5)$ for various values of m based upon the expected number of failures, as shown in Figure 8.4-4.

MTBF	t/m	$P_A(r \leq 5)$
100	10	0.067
125	8	0.191
167	6	0.446
200	5	0.616
333	3	0.916
500	2	0.983

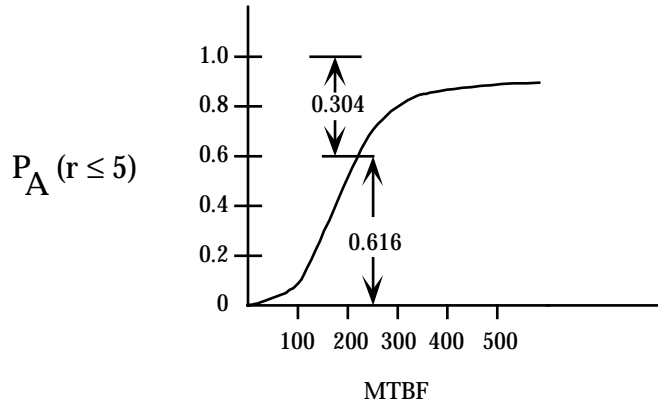


FIGURE 8.4-4: ACTUAL OPERATING CHARACTERISTIC CURVE

The decision rule “tends” to give the right decision, but won't always result in an accept decision for $m > 200$ or a reject decision for $m < 200$. Remember $P_A + P_R = 1$. Thus, we can see that we have almost a fifty-fifty chance of accepting an m of 167 hours (0.446) and a greater than 20% chance of rejecting an $m = 250$ hours. Neither the producer or consumer would be happy with this. Each would like a lower risk probability. But since $P_A = 1 - P_R$, if we lower P_A for $m \leq 200$ to 0.1, we raise P_R for $m > 200$ to $1 - 0.1 = 0.9$. What do we do now?

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

In order to overcome this difficulty it is necessary to specify the reliability requirements, either explicitly or implicitly, in terms of two MTBF values rather than a single MTBF value. The lower value is defined as the lower test MTBF (M_m or θ_1) and the higher value is defined as the upper test MTBF (M_R or θ_0). The test plan can then be designed to give a low probability of an **accept decision** for equipment with an MTBF of $m < M_m$ (or θ_1) and a low probability of **reject decision** when $m > M_R$. P_A at $m = M_m$ (or θ_1) is the **consumers risk** (β); P_R at $m = M_R$ (or θ_0) is the **producer's risk** (α). Thus, specifying the two MTBF values $M_m(\theta_1)$ and $M_R(\theta_0)$ and the two risks (α and β) defines two points on the OC curve as shown in Figure 8.4-5.

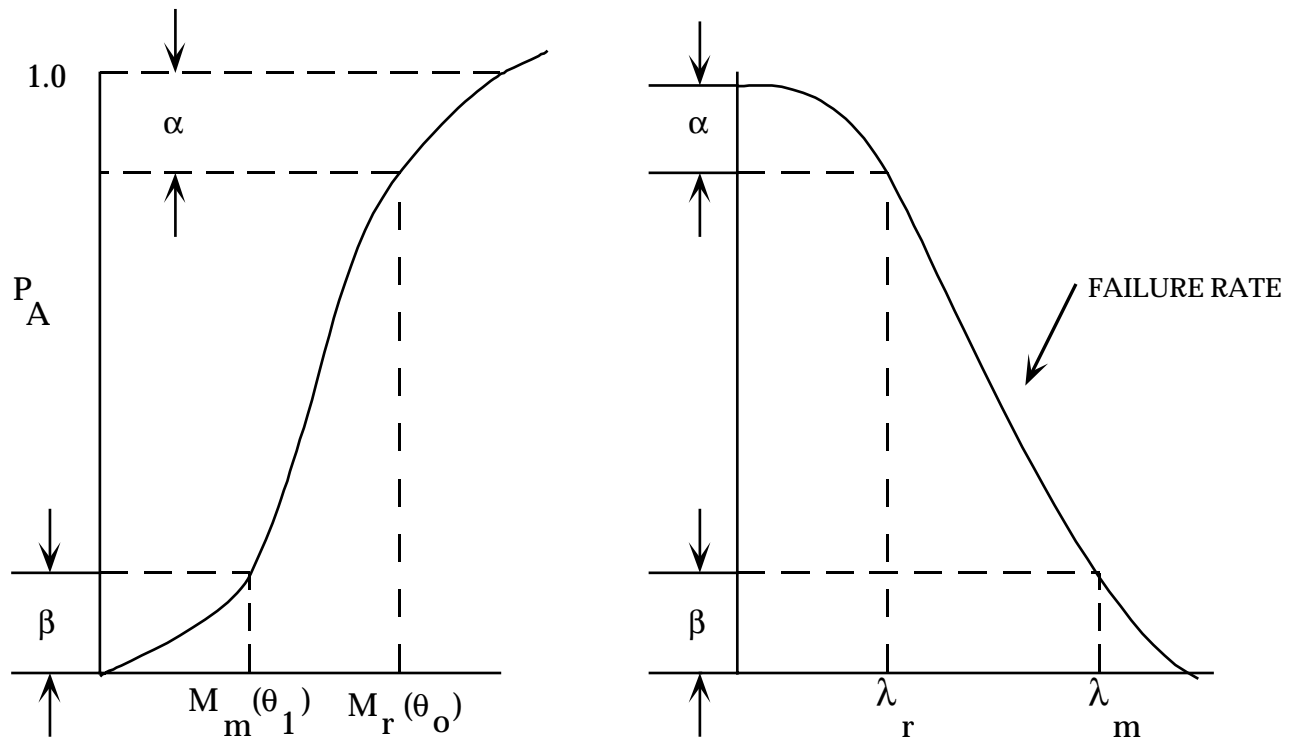


FIGURE 8.4-5: OC CURVE CHARACTERISTICS

The curve on the right is the OC curve for failure rate (α) rather than for MTBF. $\lambda_m = 1/M_m$ is the **maximum acceptable** failure rate. $\lambda_R = 1/M_R$ is the **design-required** (specified) failure rate with $\lambda_R < \lambda_m$.

The method used to design a **fixed time** reliability (R) demonstration test is mathematically equivalent to the method used to construct confidence limits for MTBF. Therefore, if a fixed time R demonstration involving a test time T and an accept number r_0 provides a consumer risk

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

of β with respect to a minimum acceptable MTBF (M_m or θ_1), it will be found that if the maximum allowable number of failures, r_0 , actually occurs, the lower $100(1 - \beta)\%$ confidence limit for MTBF as calculated from the test data is exactly M_m . For this reason, the value $(1 - \beta)$, or $100(1 - \beta)\%$ is often called the *confidence level* of the demonstration test. Thus, a fixed time R demonstration test providing a 10% consumer risk is called “a demonstration test at a 90% confidence level,” or is said to “demonstrate with 90% confidence that the lower test MTBF is achieved.” This is not really correct since, technically, confidence level is used in the estimation of a parameter while an R demonstration test is testing a hypothesis about the parameter, m , rather than constructing an interval estimate for m .

There are six characteristics of any reliability demonstration test that must be specified:

- (1) The reliability deemed to be acceptable, R_0 , “upper test MTBF”
- (2) A value of reliability deemed to be unacceptable, R_1 , “lower test MTBF”
- (3) Producer's risk, or α
- (4) Consumer's risk, or β
- (5) The probability distribution to be used for number of failures or for time-to-failure
- (6) The sampling scheme

Another term frequently used in connection with reliability demonstration tests should be defined here although it is derived from two of the six characteristics. The discrimination ratio is the ratio of upper test reliability to the lower test reliability. R_0/R_1 is an additional method of specifying certain test plans.

There are, of course, an infinite number of possible values for the actual reliability. In the specification of two numerical values, R_0 and R_1 , the experimenter achieves the producer's risk, α , and consumer's risk, β , only for those specific reliabilities.

For other values, the relationship is:

- | | | | | | |
|-------------------------------|--------|--------------|-----------|--------|--------------|
| (a) Probability of Acceptance | \geq | $1 - \alpha$ | for R | \geq | R_0 |
| (b) Probability of Acceptance | \leq | β | for R | \leq | R_1 |
| (c) Probability of Acceptance | $>$ | β | for R_1 | \leq | $R \leq R_0$ |

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

8.4.2 Attributes and Variables

Demonstration tests are classified according to the method of assessing reliability. If each component tested is merely classified as acceptable or unacceptable, then the demonstration test is an **attributes** test. If the service life of the items under test is recorded in time units, and service life is assumed to have a specific probability distribution such as the normal or Weibull, then the test is a **variables** test. Attributes tests may be performed even if a probability distribution such as the normal or Weibull is assumed by dichotomizing the life distribution into acceptable and unacceptable time-to-failure. Attributes tests are usually simpler and cheaper to perform, but require larger sample sizes to achieve the same α and β as variables tests.

8.4.3 Fixed Sample and Sequential Tests

When R_0 , R_1 , α , and β have been specified, along with the probability distribution for time to failure, the test designer often has a choice of sampling schemes. To achieve the desired α and β , statistical theory will dictate the precise number of items which must be tested if a fixed sample size is desired. Alternatively, a sequential test may be selected, where the conclusion to accept or reject will be reached after an indeterminate number of observations. For reliability at R_0 or R_1 , the average sample size in a sequential test will invariably be lower than in a fixed sample test, but the sample size will be unknown, and could be substantially larger in a specific case. Usually, an upper bound for sample size is known in sequential tests.

8.4.4 Determinants of Sample Size

Whether a fixed sample or sequential test is selected, the number of observations required will be related to the degree of discrimination asked for. In general,

- (a) The closer R_1 is to R_0 , the larger the sample size required
- (b) The smaller the α specified, the larger the sample size required
- (c) The smaller the β specified, the larger the sample size required

If the test is sequential, substitute “average sample size” for sample size in the above remarks.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

8.4.5 Tests Designed Around Sample Size

It is possible to set the sample size (or average sample size in sequential tests) independently. For example, the sample size, N , may be limited by test facilities, cost, or time. If this is done, then one cannot specify all of the values R_0 , R_1 , α , and β . One of the four will be fixed when the remaining three and N are specified. The usual practice where N must be fixed is to specify R_0 and β and then to include a plot of $1 - \beta$ as a function of R_1 , the corresponding probability of rejection, $1 - \beta$. If the discriminating power is unacceptable, then R_1 , α , β , or N must be altered in the direction noted in Section 8.4.4.

8.4.6 Parameterization of Reliability

In the case of variables tests, the desired reliability will be a function of the parameters of whatever probability distribution is selected. For example, if equipment mean life is normally distributed, then

$$R = \int_{\tau}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} \exp \left[-\frac{1}{2} \left(\frac{x - \mu}{\sigma} \right)^2 \right] dx \quad (8.22)$$

where:

- T = desired life
- μ = population mean
- σ = population standard deviation

Suppose that R_0 is specified at 0.995 for a service life, T , of 10,000 hours. Clearly, these specifications place numerical requirements on μ and σ to make the equation true. Therefore, the demonstration test may be performed on (μ_0, σ_0) , rather than on R_0 . Demonstration tests are often specified in terms of the probability distribution parameters, rather than reliabilities.

8.4.7 Instructions on the Use of Reliability Demonstration Test Plans

Instructions and examples are given for the following test plans:

- (1) Attributes Demonstration Tests
 - (a) Plans for Small Lots
 - (b) Plans for Large Lots
 - (c) Plans for Large Lots (Poisson Approximation Method)
 - (d) Attributes Sampling Using ANSI/ASQC Z1.4-1993
 - (e) Sequential Binomial Test Plans

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

- (2) Variables Demonstration Tests
 - (a) Time Truncated Test Plans
 - (1) Exponential Distribution
 - (2) Normal Distribution
 - (3) Weibull Distribution
 - (b) Failure Truncated Tests
 - (1) Exponential Distribution
 - (2) Normal Distribution (Known)
 - (3) Normal Distribution (Unknown)
 - (4) Weibull Distribution
 - (c) Sequential Tests
 - (1) Exponential Distribution
 - (2) Normal Distribution
 - (d) Interference Demonstration Tests
 - (e) Bayes Sequential Tests

8.4.7.1 Attributes Demonstration Tests8.4.7.1.1 Attributes Plans for Small Lots1. When to Use

When testing items from a small lot where the accept/reject decision is based on attributes, the hypergeometric distribution is applicable. Attributes tests should be used when the accept/reject criterion is a go-no-go situation, when the probability distribution of times to failure is unknown, or when variables tests are found to be too expensive. The example demonstrating the method is based on a small lot and small sample size. This situation frequently characterizes the demonstration test problem associated with large systems. The sample size limits the discriminatory power of the demonstration test plan but frequently cost and time constraints force us into-larger-than desired risks.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

2. Conditions for Use

The definition of successfully passing the test may be that an item survives the test. The parameter to be evaluated then is the fraction of the items in the lot that survive. The estimation of the parameter would be based on a fixed sample size and testing without repair. The selection of the criteria for success (survive, detonate on impact, time) can be derived from a requirement or, if the items being tested are known to follow a particular probability distribution, the specification of the criteria for success can be based on defining acceptable and unacceptable portions of the range of failures. If the lot size is large, say 30 or more, then the Poisson approximation may be used to make the calculation simpler.

3. Method

Example

- | | |
|---|--|
| a. Define criterion for success/failure. | a. A missile that seeks and destroys the target. Missiles that fail to destroy the target are considered failures. |
| b. Define acceptable lot quality level
(1 - p ₀). | b. Lots in which (1 - p ₀) = 90% of the missiles will destroy the target are to be accepted by this demonstration test plan with high probability. |
| c. Specify producer's risk (α), i.e., the probability that acceptable lots will be rejected. | c. Let $\alpha = .2$. This decision is an engineering one based on the consequences of allowing good lots to be rejected and based on the time and dollar constraints associated with inspecting the lot. |

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
<p>d. Define unacceptable quality level $(1 - p_1)$.</p>	<p>d. Lots in which only $(1 - p_1) = 20\%$ of the missiles destroy the target will be accepted by the demonstrations test plan with low probability.</p>
<p>e. Specify the consumer's risk (β), i.e., the probability that unacceptable quality lots will pass the demonstration test).</p>	<p>e. Let $\beta = .022$ (taken for convenience in calculations).</p>
<p>f. Now that α, β, $1 - p_0$, and $1 - p_1$ have been specified the following steps describe the calculations required to determine the sample size and accept/reject criteria which will satisfy the stated risks.</p>	<p>f. Given: lot size $N = 10$</p> $1 - p_0 = .9$ $1 - p_1 = .2$ $\alpha = .2$ $\beta = .022$
<p>g. The process consists of a trial and error solution of the hyper-geometric equation using N, $1 - p_0$, $1 - p_1$ and various sample sizes until the conditions of α and β are met. The equation used is</p> $\Pr(x) = \frac{\binom{r}{x} \binom{N-r}{n-x}}{\binom{N}{n}}$ <p style="text-align: center;">$x = 0, 1, 2 \dots \min(n,r)$</p> <p>where: x = number of successes in sample</p>	<p>g. The calculations are as follows: If $N = 10$ and it is assumed that the samples are taken from a lot with $1 - p_0 = .9$ then that lot contains 9 good items and 1 defective item. As the first step in the trial and error procedure assume a sample size of two. The possible outcomes are either 0, 1 or 2 good items.</p> <p>The probability of each outcome using the hypergeometric formula is</p> $\Pr(2) = \frac{\binom{9}{2} \binom{1}{0}}{\binom{10}{2}} = .8$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
<p>g. r = number of successes in lot N = lot size n = sample size</p> $\binom{r}{x} = \frac{r!}{x!(r-x)!}$	<p>g. $\Pr(1) = .2$ $\Pr(0) = 0$</p> <p>The same calculations for $1 - p_1 = .2$ result in</p> <p>$\Pr(2) = .022$ $\Pr(1) = .356$ $\Pr(0) = .622$</p>
<p>h. Find the number of successes which satisfies α and β in the calculations involving $1 - p_0$ and $1 - p_1$.</p>	<p>h. From these 2 sets of results it can be seen that if a sample size of 2 is specified, then α and β will be satisfied if the decision rule is made that if 2 successes are observed in the sample the lot is accepted and for all other outcomes the lot is rejected.</p> <p>If $1 - p_0 = .9$, then $\Pr(2) = .8$, therefore $1 - .8 = .2 = \alpha$.</p> <p>If $1 - p_1 = .2$, then $\Pr(2) = .022$ $= \beta$;</p> <p>NOTE: A different sample size can be traded off against different α, β, $1 - p_0$ and $1 - p_1$.</p>
<p>i. The demonstration test is then specified.</p>	<p>i. The test procedure is as follows:</p> <ol style="list-style-type: none"> 1. Test a random sample of 2 missiles from a lot of 10 missiles. 2. If both missiles destroy the target, accept the lot. 3. If 0 or 1 successes are observed reject the lot.

 SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

4. For Further Information

There are "*Tables of the Hypergeometric Distribution*" by G.J. Lieberman and D.B. Owen, Stanford University Press, Stanford, California, 1961 to perform the mathematical calculations of Step g. Also if N becomes large (say 30) then the binomial or the Poisson distribution can be used as an approximation for the hypergeometric distribution.

8.4.7.1.2 Attributes Plans for Large Lots1. When to Use

When testing parts from a large lot where the accept/reject decision is based on attributes, the binomial distribution is applicable. Strictly speaking, all reliability testing should follow the hypergeometric distribution as long as individual items are placed on test and tested to failure without repair. However, when the lot size is large, the binomial distribution is a good approximation for the hypergeometric and, therefore, the example presented in this section covers the use of the binomial. Attributes tests should be used when the accept/reject criterion is go/no-go, when the distribution of failure times is unknown, or when variables tests are found to be too expensive.

2. Conditions for Use

The definition of successfully passing the test may be that an item performs as specified. The parameter to be evaluated then is the fraction of the items in the lot that perform as specified. The estimation of the parameter would be based on a fixed sample size and testing without repair. The selection of the criteria for success can be derived from a requirement, or if the items being tested are known to follow a particular probability distribution, the specification of the criteria for success can be based on defining acceptable and unacceptable portions of the range of failure times. If the lot size is large, say 30 or more, then the Poisson approximation may be used to make the calculation simpler.

3. MethodExample

- | | |
|--|---|
| a. Define criterion for success/ failure | a. An artillery fuze that detonates on impact is considered a success. Fuzes that fail to detonate on impact are considered failures. |
|--|---|

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
b. Define acceptable lot quality level ($1 - p_0$).	b. Lots in which $1 - p_0 = .9$ (i.e., 90% of the fuzes in the lot will detonate on impact) are to be accepted by this demonstration test plan with high probability.
c. Specify producer's risk (α), (i.e., the probability that acceptable lots will be rejected).	c. Let $\alpha = .01$.
d. Define unacceptable lot quality level ($1 - p_1$).	d. Lots with only a true fraction of acceptable parts $1 - p_1 = .5$ are to be accepted by this demonstration test plan with low probability.
e. Specify consumer's risk (β), (i.e., the probability that lots of unacceptable quality level will be accepted.)	e. Let $\beta = .12$ (selected for ease of calculation).
f. Now that α , β , $1 - p_0$, and $1 - p_1$ have been specified, the following steps describe the calculations required to determine the sample size and accept/reject criteria which will satisfy the stated risks.	f. Given: lot size $N =$ large, say, 30 $1 - p = .9$ $1 - p_1 = .5$ $\alpha = .01$ $\beta = .12$
g. The process now consists of a trial and error solution of the binomial equation using $1 - p_0$, $1 - p_1$ and various sample sizes until at a given decision point, the conditions of α and β are satisfied. The binomial equation is:	g. Assume a random sample of size $n = 10$ is taken from a lot whose true fraction of good parts is $.9$. Solve the binomial equation for the total number of consecutive outcomes whose summed probabilities equal a starting at 0 successes. The calculations for this decision point are:

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

- | <u>Method</u> | <u>Example</u> |
|--|--|
| <p>$\Pr(x) = \binom{n}{x}(1 - p)^x(p)^{n-x}$</p> <p>where:</p> <ul style="list-style-type: none"> n = sample x = observed successes in sample p = lot fraction defective | <p>$\Pr(10) = \binom{10}{10} (.9)^{10} (.1)^0 = .3486$</p> <p>$\Pr(9) = .387$</p> <p>$\Pr(8) = .1935$</p> <p>$\Pr(7) = .0574$</p> <p>$\Pr(7 \text{ or more}) = .9865$</p> <p>Then</p> <p>$\Pr(6 \text{ or less}) = 1 - \Pr(7 \text{ or more})$ $= 1.0 - .9865 = .0135$ $\approx .01 \text{ (which satisfies the risk.)}$</p> <p>Perform the same type of calculations assuming the true fraction defective is .5. In this instance, sum the probabilities starting at 10 successes until succeeding consecutive probabilities sum to the value of β. This yields the following results:</p> <p>$\Pr(10) = \binom{10}{10} (.5)^{10} (.5)^0 = .001$</p> <p>$\Pr(9) = .01$</p> <p>$\Pr(8) = .045$</p> <p>$\Pr(7) = .117$</p> <p>$\Pr(7 \text{ or more}) \approx .12 \text{ (which satisfies the } \beta \text{ risk).}$</p> |
| <p>h. The demonstration test is then specified.</p> | <p>h. The test procedure is as follows:</p> <ol style="list-style-type: none"> 1. Test a random sample of 10 fuzes. 2. If 7 or more fuzes detonate on impact accept the lot. 3. If 6 or less successes are observed, reject the lot. |

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

4. For Further Information

There are several published tables for use in determining binomial probabilities in the event that the sample size makes calculations too lengthy. One of these is "*Tables of the Binomial Probability Distribution*," National Institute of Standards and Technology, US Department of Commerce. It gives individual terms and the distribution function for $p = .01$ to $p = .50$ in graduations of .01 and $n = 2$ to $n = 49$ in graduations of 1. If n is large say ≥ 30 , the Poisson distribution can be used as an approximation for the binomial distribution.

8.4.7.2 Attributes Demonstration Test Plans for Large Lots, Using the Poisson Approximation Method

1. When to Use

In attributes demonstration test plans, if the lot size gets much above 20, the calculations required to generate a demonstration test plan become very time consuming. The Poisson distribution can be used as an approximation of both the hypergeometric and the binomial distributions if the lot size is large and if the fraction defective in the lot is small. This method can therefore be used in lieu of the previous two methods in many cases.

2. Conditions for Use

If the lot size is large and the fraction defective is small, this method is applicable. Its use is initiated by specifying a desired producer's risk, consumer's risk, acceptable lot fraction defective and unacceptable lot fraction defective. As before, it is also necessary to specify the characteristics that constitute a defective part since this is an attributes type test.

3. Method

Example

- | | |
|---|--|
| a. Define criterion for success/failure. | a. An artillery fuze that detonates on impact is considered a success. Fuzes that fail to detonate on impact are considered failures. |
| b. Define acceptable lot quality level ($1 - p_0$). | b. Lots in which $1 - p_0 = .9$ (90% of the fuzes in the lot detonate on impact) are to be accepted by this demonstration test plan with high-probability. |

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
c. Specify the producer's risk (α), (i.e., the probability that acceptable lots will be rejected).	c. Select $\alpha = .05$.
d. Define unacceptable lot quality level ($1 - p_1$).	d. Lots with only a true fraction of acceptable parts $1 - p_1 = .75$ are to be accepted by this demonstration test plan with low probability.
e. Specify the consumer's risk (β), (i.e., the probability that lots of unacceptable quality level will be accepted by this plan).	e. Select $\beta = .02$.
f. Now that α , β , $1 - p_0$, $1 - p_1$ have been specified, the Table of the Summation of Terms of Poisson's Exponential Binomial Limit* is used to determine the accept/reject criteria.	f. Given: lot size $N = 1000$ $1 - p_0 = .9$ $1 - p_1 = .75$ $\alpha = .05$ $\beta = .02$
g. The process now consists of a trial and error solution using Poisson Tables*, $1 - p_0$, $1 - p_1$ and various assumed sample sizes until the conditions of α and β are satisfied.	g. Assume sample size of 100. Now, calculate the expected number of failures for $1 - p_0$ and $1 - p_1$ as follows: $n(1 - p_0) = 100(.9) = 90$ $n(1 - p_1) = 100(.75) = 75$

*See any good statistical text

The Poisson Tables are constructed for small values of p , so, in this case, to make calculations easier, it is necessary to work with the opposite tail of the distribution. Therefore the numbers to enter the table with are:

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

$$np_0 = 100(.1) = 10$$

$$np_1 = 100(.25) = 25$$

The procedure now is to enter the column labeled c' or np' with the above numbers. Beginning with $1 - p_0 = .9$ and $np_0 = 10$, search across the $np' = 10$ row beginning at c or less = 1.0.

Continue to smaller values of c until the probability of c or less = $1 - \alpha$.

In this example at $c = 15$ or less, the probability of 15 or less is .951 which is approximately $1 - \alpha$.

The same procedure is followed in the table at $1 - p_1 = .75$ and $np_1 = 25$.

In the $np' = 25$ row at $c = 15$, the cumulative probability is .022 which is approximately equal to β .

The decision criteria is now specified as $c = 15$ or less failures.

h. The demonstration is then fully specified.

h. The demonstration test procedure is as follows:

1. Take a random sample of 100 fuzes from each lot of size $N = 1000$ and test each part.
2. If 85 or more fuzes (i.e., 15 or less defectives) detonate on impact, accept the lot.
3. If less than 85 successes are observed, reject the lot.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

4. For Further Information

For additional examples using this method, refer to E. B. Grant "*Statistical Quality Control*," McGraw Hill, 1964.

8.4.7.3 Attributes Sampling Using ANSI/ASQC Z1.4-1993

ANSI/ASQC Z1.4-1993 replaced MIL-STD-105, but all applicable tables, table numbers and procedures used in MIL-STD-105 were retained.

1. When to Use

When the accept/reject criteria for a part is based on attributes decisions ANSI/ASQC Z1.4-1993 is a useful tool. These sampling plans are keyed to fixed AQL's and are expressed in lot size, sample size, AQL and acceptance number. Plans are available for single sampling, double sampling and multiple sampling. The decision as to which type to use is based on a trade-off between the average amount of inspection, the administration cost and the information yielded regarding lot quality. For example, single sampling usually results in the greatest amount of inspection, but this can be offset by the fact that it requires less training of personnel, and record keeping is simpler, and it gives a greater amount of information regarding the lot being sampled.

2. Conditions for Use

The user of a ANSI/ASQC Z1.4-1993 sampling plan must have the following information:

- a. Lot Size
- b. Acceptable Quality Level (AQL)
- c. Sample Size
- d. Acceptance Number
- e. Criteria for Acceptance or Rejection

The specification of the AQL is an engineering decision based on the fraction defective that a user of parts considers acceptable. Lots with this percent defective will be accepted a high fraction of the time. Operating characteristic curves are supplied with each sampling plan and these can be used to evaluate the protection afforded by the plan for various quality levels.

ANSI/ASQC Z1.4-1993 also contains plans for normal, tightened and reduced inspection plans which can be invoked if the fraction defective of lots seems to be varying or trending.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
a. Determine lot size and specify AQL and type of sampling.	a. Given a lot containing 100 parts, with an AQL of 6.5% and single sampling specified.
b. Enter the table with lot size and select the sample size code letter.	b. From Table I Sample Size Code Letters in ANSI/ASQC Z1.4-1993, find the sample size code letter for a lot of size 100. For this example and for normal sampling, the specified code number is F.
c. Enter the single sampling plan table for normal inspection with the code number from Step b.	c. Enter Table II-A Single Sampling Plans for Normal Inspection page 10 with code letter F. Under the column titled Sample Size, find the number 20 in the same row as the letter F. This is the number of parts to be randomly selected and inspected.
d. Enter the same table in the proper column for the specified AQL.	d. Find the column in Table II-A page 10 corresponding to an AQL of 6.5%.
e. Proceed horizontally along the Sample Size Code Number row until it intersects with the AQL column to obtain the acceptance number.	e. At the intersection of row R and column 6.5%, the acceptance number is 3 and the rejection number is 4.
f. The Single Sampling Plan from ANSI/ASQC Z1.4-1993 is to select a random sample of size n from a lot of size N, inspect it and accept the lot if the number of defectives in the lot is equal to or less than the Acceptance Number. If the observed number of defects is equal to or greater than the rejection number, the lot is rejected.	f. For the single sampling plan $N = 100$, $AQL = 6.5\%$, select a random sample of size $n = 20$ and inspect it for attributes criteria. If 3 or less defectives are found in the sample accept the lot. If 4 or more defectives are found in the sample reject the lot.

 SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

4. For Further Information

In addition to the example discussed above, ANSI/ASQC Z1.4-1993 contains other plans for any lot size and for selected AQL's from .01 to 1000. Operating characteristic curves are also included.

8.4.7.4 Sequential Binomial Test Plans1. When to Use

When the accept/reject criterion for the parts on test is based on attributes, and when the exact test time available and sample size to be used are not known or specified then this type of test plan is useful. The test procedure consists of testing parts one at a time and classifying the tested parts as good or defective. After each part is tested, calculations are made based on the test data generated to that point and the decision is made either that the test has been passed, failed, or that another observation should be made. A sequential test will result in a shorter average number of parts tested than either failure-truncated or time-truncated tests when the lot tested has a fraction defective at or close to p_0 or p_1 .

2. Conditions for Use

- a. The parts subjected to test will be classified as either good or defective. In other words, testing will be by attributes.
- b. The acceptable fraction defective in the lot p_0 , the unacceptable fraction defective p_1 , the producer's risk α , and consumer's risk β must be specified.
- c. The test procedure will be to test one part at a time. After the part fails or its test time is sufficient to classify it as a success, the decision to accept, reject or continue testing the lot will be made.

3. MethodExample

- | | |
|---|--|
| <ol style="list-style-type: none"> a. Specify p_0, p_1, α, β. | <ol style="list-style-type: none"> a. Given a lot of parts to be tested by attributes. Lots having only $p_0 = .04$ fraction defective parts are to be accepted by the demonstration test plan 95% of the time (i.e., $\alpha = .05$). Lots having $p_1 = .10$ fraction defective are to be accepted 10% of the time (i.e., $\beta = .10$). |
|---|--|

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

- b. Calculate decision points from the following formula

$$\frac{1 - \beta}{\alpha} \quad \text{and} \quad \frac{\beta}{1 - \alpha}$$

- c. As each part is tested classify it as a part failure or a success and evaluate the following expression:

$$\left(\frac{p_1}{p_0}\right)^f \left(\frac{1 - p_1}{1 - p_0}\right)^s$$

where:

f = total number of failures

s = total number of successes

- d. A graphical solution for critical values of f and s is possible by solving the following equations.

$$1) \ln \left(\frac{1 - \beta}{\alpha}\right) = (f) \ln \left(\frac{p_1}{p_0}\right) +$$

$$(s) \ln \left(\frac{1 - p_1}{1 - p_0}\right)$$

- b. The decision points are:

$$\frac{1 - \beta}{\alpha} = \frac{1 - .10}{.05} = 18$$

$$\frac{\beta}{1 - \alpha} = \frac{.10}{1 - .05} = .105$$

- c. In this example, if the value of the formula

$$\left(\frac{.10}{.04}\right)^f \left(\frac{.90}{.96}\right)^s$$

- 1) exceeds 18, reject the lot.
- 2) < .105 accept the lot.
- 3) is between .105 and 18, the test should be continued.

- d. The equations for the graphical solution in this example are:

$$1) \ln 18 = f \ln 2.5 + s \ln .94$$

$$2) \ln .105 = f \ln 2.5 + s \ln .94$$

Substituting value of f and s in the equations yields the following points.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. Method

$$2) \ln \frac{\beta}{1 - \alpha} = (f) \ln \frac{p_1}{p_0} + (g) \ln$$

$$\frac{\beta}{1 - \alpha} = (f) \ln \frac{p_1}{p_0} +$$

$$(s) \ln \left(\frac{1 - p_1}{1 - p_0} \right)$$

Example

1)		2)	
f	s	f	s
0	-46.6	-2.44	0
3.16	0	-1.78	10
3.84	10	0	36.4
10	101	10	184

Figure 8.4-6 shows the graphical solution for this test plan. As each good part is observed a horizontal line is drawn, and each defective part is recorded by a vertical line. When the line crosses either of the decision lines, the appropriate action is taken.

- e. The Operating Characteristic Curve calculation is as follows:
Four points can be generated by observation.

p	Probability of Acceptance
p_0	$1 - \alpha$
p_1	β
1	0
0	1

One additional point can be calculated with the following formula

$$p = \frac{\ln \left(\frac{1 - p_1}{1 - p_0} \right)}{\ln \left(\frac{1 - p_1}{1 - p_0} \right) - \ln \left(\frac{p_1}{p_0} \right)}$$

$$P_r(\text{Acc}) = \frac{\ln \frac{1 - \beta}{\alpha}}{\ln \frac{1 - \beta}{\alpha} - \ln \frac{\beta}{1 - \alpha}}$$

- e. The OC curve for this test plan yields the following points:

p	Probability of Acceptance
.04	.95
.10	.10
1.00	0.00
0.00	1.00

The 5th point of the OC curve in the example

$$p = \frac{\ln 0.94}{\ln 0.94 - \ln 2.5} = .063$$

$$P_r(\text{Acc}) = \frac{\ln 18}{\ln 18 - \ln 0.105} = .562$$

where $P_r(\text{Acc})$ = probability of acceptance

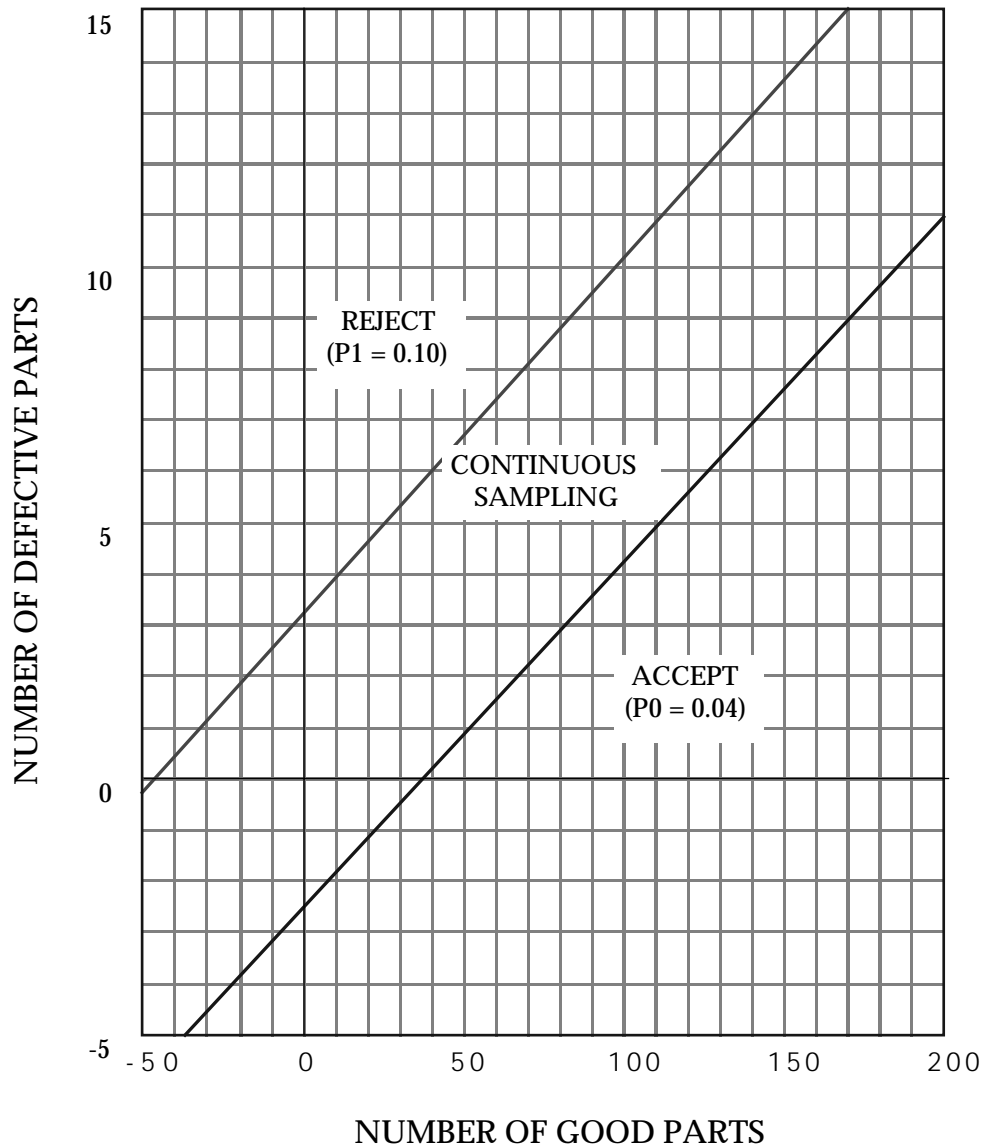
SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

FIGURE 8.4-6: GRAPHICAL SOLUTION OF SEQUENTIAL BINOMIAL TEST

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

4. For Further Information

A more complete discussion of this demonstration test method is presented in "*Introduction to Statistical Analysis*" by W.J. Dixon and F.J. Massey, McGraw Hill, New York, 1951. The theory of sequential testing is presented in "*Sequential Analysis*" by A. Wald, John Wiley & Sons, 1947.

8.4.7.5 Variables Demonstration Tests

8.4.7.5.1 Time Truncated Demonstration Test Plans

8.4.7.5.1.1 Exponential Distribution (H-108)

1. When to Use

When a demonstration test program is constrained by time or schedule and testing is by variables (in this case the variable is mean life) and the distribution of failure times is known, a test plan of this type can be specified.

2. Conditions for Use

- a. The failure times of the items under test must be exponentially distributed.
- b. The acceptable mean life θ_0 , unacceptable mean life θ_1 , producer's risk, (α), and consumer's risk, (β), and test time (T) must be specified.
- c. The decision of testing with or without replacement must be made.

3. Method

Example

- a. Specify θ_0 , θ_1 , α , β .

- a. Given an item type whose failure times are distributed exponentially.

Specify θ_0 = 1000 hours

θ_1 = 500 hours

α = .10

β = .10

- b. Specify a fixed test time.

- b. The program plan allows time for a 200 hour test.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

4. For Further Information

The demonstration test method and example discussed in this section are from "*Quality Control and Reliability Handbook*," MIL-HDBK-H108. In addition to the example presented here, the handbook has tabled sample sizes and reject numbers for testing without replacement with $\alpha = .01, .05, .10$ and $.25$, and $\beta = .01, .05, .10$ and $.25$ and for all combinations thereof. The tables are also constructed for θ_1 / θ_0 values of $2/3, 1/2, 1/3, 1/5$ and $1/10$ and T/θ_0 values of $1/3, 1/5, 1/10$ and $1/20$. A like set of tables is presented also for demonstration test plans for the same values of $\alpha, \beta, \theta_1 / \theta_0$ and T/θ_0 for testing with replacement. Tables are also provided for time truncated tests in which only α, θ_0 and T (test time) are specified ($\alpha = .01, .05, .10, .25$ and $.50$) for plans involving testing with and without replacement. Fixed time test plans are also presented in MIL-HDBK-781.

8.4.7.5.1.2 Normal Distribution1. When to Use

When the underlying distribution of failure times is normal and when a fixed calendar time is available for a test, this type of test plan can be specified. This test plan essentially becomes a binomial type problem since the survivors at the end of the time truncation are treated as successes. The failures regardless of their time of occurrence are utilized in specifying the accept/reject criteria.

2. Conditions for Use

- a) The distribution of failure times must be normal.
- b) The acceptable mean life (θ_0), unacceptable mean life (θ_1), the known or desired standard deviation of the distribution of acceptable mean lives (σ_0), the known or desired standard deviation of the distribution of unacceptable mean life (σ_1), the sample size (n), the test truncation time (T), the producer's risk (α), and the consumer's risk (β), must be specified.
- c) The test should be run without replacement of failed parts.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. Method

- a. Specify θ_0 , θ_1 , α , β , σ_0 , σ_1 , n , T . If the requirements are stated in terms of reliability at some time t , it is necessary to solve the following equation.

$$z_0 = \frac{t - \theta_0}{\sigma_0}$$

where z_0 is the standard normal deviate for the desired probability of R_0 , t is the desired mission time, σ_0 is the known standard deviation, and θ_0 is the acceptable mean life. The same procedure is followed to solve for θ_1 and R_1 is specified.

$$z_1 = \frac{t - \theta_1}{\sigma_1}$$

Example

- a. Given an item type whose failure times are normally distributed with a known standard deviation = 50. A reliability of .95 is desired that the equipment will last 100 hours. A product with a reliability of .85 is unacceptable.

The standard normal deviate for $R_0 = .95$ is $z_0 = -1.645$ and for $R_1 = .85$ is $z_1 = -1.04$ from a table of areas under the normal curve (Table 5.3.1-1).

$$z_0 = \frac{t - \theta_0}{\sigma}$$

$$-1.645 = \frac{100 - \theta_0}{50}$$

$$\theta_0 = 182 \text{ hours}$$

$$z_1 = \frac{t - \theta_1}{\sigma}$$

$$-1.04 = \frac{100 - \theta_1}{50}$$

$$\theta_1 = 152 \text{ hours}$$

Therefore, it is possible to specify R_0 and R_1 in terms of θ_0 and θ_1 .

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

$$\theta_0 = 182 \text{ hours}$$

$$\sigma_0 = 50 \text{ hours}$$

$$\theta_1 = 152 \text{ hours}$$

$$\sigma_1 = 50 \text{ hours}$$

The schedule and cost of testing allows 182 hours of test time with 30 samples to be placed on test. α is specified as .10 and $\beta = .05$.

- | | |
|--|---|
| <p>b. Calculate the expected number of failures during the fixed time test if n samples are tested T hours, for samples from lots with mean lives of θ_0, σ_0 and θ_1, σ_1.</p> | <p>b. The $\theta_0 = 182$, $\sigma_0 = 50$, $n = 30$ then the expected number of failures in a test of 182 hours is 15. If $\theta_1 = 152$, $\sigma_1 = 50$, $n = 30$, the expected number failures in a test of 182 hours is 21.6 using a table of areas under the normal curve.</p> |
| <p>c. The problem of specifying accept/reject criterion at the end of a fixed test time, T, is now similar to the example in <u>Attributes Plans For Large Lots</u>. In other words, it is a binomial distribution problem since items that last T hours are listed as having successfully passed the test, while items that do not last T hours are classed as failures regardless of their exact failure times.</p> | <p>c. Items that exceed the fixed test time $T = 182$ hours are counted as successes. The remaining problem to be solved is specifying the accept/reject criterion (i.e., r or more failures out of a sample of 30 items on test for 182 hours results in failure of the demonstration test - regardless of the individual part failure times). Additionally, the test may be terminated at less than $T = 182$ hours if r failures are observed, in which case the demonstration test is failed.</p> |

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

- d. The accept/reject criteria can be calculated using the binomial distribution or, if the expected number of failures ≥ 5 the normal distribution can be used as an approximation to the binomial.
- e. Calculate the decision point based on θ_0 and α using the normal distribution.

- d. From Step b the expected number of failures of $\theta_0 = 182$ is 15 and the expected number of failures when $\theta_1 = 152$ is 21.6. Therefore the normal distribution as an approximation of the binomial is used.
- e. The decision point for $\theta_0 = 182$, $\alpha_0 = 50$, $\alpha = .10$ is calculated as follows:

$$z = 1.28 \text{ for } \alpha = .10$$

$$z = \frac{x - np}{\sqrt{np(1-p)}}$$

$$1.28 = \frac{x - 15}{\sqrt{15(.5)}}$$

$$x = 18.5 \text{ failures}$$

The demonstration test plan procedure is now stated as follows:

Take a random sample of 30 items, test them for 182 hours. If, 18.5 or less failures are observed the test is passed.

- f. Adjust the decision point to a whole number, thus adjusting α slightly.

- f. Either 18 or 19 failures can be set as the rejection number without affecting α too severely. For this example, assume that 19 failures will be allowed and still accepted. α now becomes

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH3. MethodExample

$$z = \frac{19 - 15}{\sqrt{15(.5)}} = 1.46$$

From a Table of Areas under the Normal Curve the probability of exceeding $z = 1.46$ is .09. Therefore, $\alpha = .09$.

- g. Calculate β based on the accept/reject criteria established in Step f.

NOTE: The OC curve for this demonstration test plan can be constructed by assuming different values of θ and performing similar calculations to those of this step. Note that np and $1 - p$ will change for each new value of θ .

- g. If $\theta_1 = 152$ hours, $\sigma_1 = 50$, $T = 182$ hours, $n = 30$, and the decision rule for passing the test is 19 or less failures, then β is calculated as:

$$z = \frac{x - np}{\sqrt{np(1-p)}} = \frac{18 - 21.6}{\sqrt{21.6(.28)}}$$

$$z = -1.46$$

The area under the normal curve not exceeding a z value of -1.46 is .07. Therefore, $\beta = .07$.

- h. Summarize the characteristics of the demonstration test plan.

- h. Test a random sample of 30 items for 182 hours. If 19 or less failures are observed, the test has been passed. If 19 or more failures are observed the test is failed. If the 19th failure occurs before 182 hours, stop testing when it occurs, as the test is failed.

This test plan will reject lots with an average mean life of 182 hours and standard deviation of 50 hours approximately 9% of the time. It will accept lots with an average mean life of 152 hours and a standard deviation of 50 hours approximately 7% of the time.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

4. For Further Information

Additional examples describing this method are presented in most books on elementary statistics.

8.4.7.5.1.3 Weibull Distribution (TR-3, TR-4, TR-6)

1. When to Use

When the distribution of failure times is Weibull and when only a given calendar time is available for a demonstration test, then this type of test plan is useful. Test plans covering this situation have been generated by Kao and Goode and published as a series of Quality Control and Reliability Technical Reports (TR-3, TR-4, TR-6) titled "*Sampling Procedures and Tables for Life and Reliability Testing Based on the Weibull Distribution*" by the Office of the Assistant Secretary of Defense (Installations and Logistics), September 1961, February 1962 and February 1963. (Refs. [13], [14], [15]). The plans are based on the user of the test plans specifying his reliability parameter of interest in terms of mean life, hazard rate, or reliable life (life at given failure %). The plans were generated based on the assumption of a known shape parameter and give protection against a certain fraction of items in a lot not meeting the acceptance criterion. The test procedure essentially states that a sample of n items should be tested t hours. Those surviving the fixed time are classed as successes, while those not surviving are considered failures regardless of the exact time of failure. From this definition of failure it can be seen that these plans are based on the binomial distribution. Tables of the cumulative binomial distribution can be used to generate the OC curves for specific test plans. Each set of test plans features a set of conversion factors relating to ANSI/ASQC Z1.4-1993 Sampling Plans. Tabled test plans are presented for values of the Weibull shape parameter of .33, .5, 1, 1.67, 2.5, 3.33, 4 and 5.

2. Conditions for Use

- a. The failure times of the items being evaluated follow the Weibull distribution with known or assumed shape parameter β .
- b. The acceptable mean life μ_0 , unacceptable mean life μ_1 , producer's risk α , consumer's risk β (care must be taken to differentiate this quantity from the Weibull shape parameter which is also symbolized by β) and the test time t , must be specified.
- c. Testing is without replacement.
- d. It is also possible to select test plans by specifying the fraction defective allowable in a lot having an acceptable quality level.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
<p>a. Specify μ_0, μ_1, α, β (consumer's risk), β (Weibull shape parameter) and test time t.</p> <p>b. Determine the sample size and acceptance number for a plan that will give the protection specified in Step a.</p>	<p>a. Given a lot of items whose failure times follow the Weibull distribution. Historical failure data on the item indicates the Weibull shape parameter β is approximately 2.0. The program schedule allows 2500 hours of reliability demonstration testing. Lots having a mean life μ_0 of 10,000 hours are to pass the demonstration test 95% of the time (i.e., $\alpha = .05$). Lots having a mean life μ_1 of 5,000 hours are to be accepted by this test plan only 10% of the time (i.e., consumer's risk $\beta = .10$).</p> <p>b. Enter Table 3e on page 32 on TR-3 "<i>Sampling Procedures and Tables for Life and Reliability Testing Based on the Weibull Distribution</i>" which is for sampling plans for the case of the Weibull shape parameter $\beta = 2.0$. The quantity that is used to enter the table is</p>

$$t/\mu_1 \times 100 = \frac{2500}{5000} \times 100 = 50$$

Search the column headed by 50 for the parenthesized value in the body of the table corresponding to

$$t/\mu_0 \times 100 = \frac{2500}{10000} \times 100 = 25$$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

<u>3. Method</u>	<u>Example</u>
	<p>b. The table contains values for $t/\mu_0 \times 100$ of 24 and 26. To assure greater protection (i.e., a smaller α) the larger value should be used.</p> <p>The $t/\mu_0 \times 100 = 26$ row specifies a sample size of 50 with an acceptance number of 5.</p>
<p>c. Summarize the test procedure.</p>	<p>c. The test procedure is as follows:</p> <ol style="list-style-type: none"> 1) Select a random sample of 50 items (from a large lot). 2) Test the items for 2500 hours. 3) If the number of failures observed during the test is 5 or less accept the lot. 4) If there are 6 or more failures is reject the lot. 5) If the 6th failure occurs before 2500 hours, the test may be discontinued at that point and the lot rejected.
<u>4. For Further Information</u>	

Frequently, the exact test desired is not covered in the tabled values in which case it is possible to interpolate to some degree at the expense of changing the risks slightly. Operating characteristic curves can be generated using a table of binomial probabilities.

Each of the Technical Reports contains an extensive bibliography describing other publications in which the details leading to these sampling plans were presented by Professors Goode and Kao.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

8.4.7.5.2 Failure Truncated Tests8.4.7.5.2.1 Exponential Distribution (MIL-HDBK-H108)1. When to Use

When tests designed to demonstrate life characteristics of items whose failure times are exponentially distributed are to be performed wherein the test will be terminated after a preassigned number of failures then a test plan of this type can be specified. Plans of this type are available in MIL-HDBK-H108, "*Sampling Procedure and Tables for Life and Reliability Testing (Based on Exponential Distribution)*," also known as "*Quality Control and Reliability Handbook*." Plans are presented for testing with and without replacement. Test criteria are tabled for specified values of α and β equal to .01, .05, .1, and .25 and for all combinations thereof, and for values of θ_1/θ_0 of 2/3, 1/2, 1/3, 1/5 and 1/10. A set of tables is also presented for cases in which α and θ_0 only are specified for various values of termination number r . Since a major factor in specifying a demonstration test plan of this type is the expected waiting time before a decision is made (i.e., a given number of failures occur) there is also included a set of tables for calculating this statistic for various sample sizes and termination numbers. Operating characteristic curves are presented for many of the demonstration test plans to enable the assessment of risk for values of mean life other than θ_0 and θ_1 .

2. Conditions for Use

- a. The failure times of the items placed on test must be exponentially distributed.
- b. The acceptable mean life θ_0 , unacceptable mean life θ_1 , producer's risk α , and consumer's risk β should be specified.
- c. The decision of whether testing will be with or without replacement must be made.
- d. An estimate may be made regarding the time available for the test as this will affect the number of items placed on test.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
<p>a. Specify θ_0, θ_1, α, β.</p>	<p>a. Given an item type whose failure times are distributed exponentially.</p> <p style="margin-left: 40px;">Specify $\theta_0 = 1000$ hours $\theta_1 = 500$ hours $\alpha = .10$ $\beta = .10$</p>
<p>b. Specify whether testing will be with or without replacement.</p>	<p>b. Testing will be without replacement.</p>
<p>c. Calculate θ_1/θ_0.</p>	<p>c. $\theta_1/\theta_0 = \frac{500}{1000} = \frac{1}{2}$</p>
<p>d. Enter the appropriate table in MIL-HDBK-H108 and select a termination number and acceptability constant.</p>	<p>d. Enter Table 2B-5 on page 2.41 of MIL-HDBK-H108 with $\alpha = .10$, $\beta = .10$, and $\theta_1/\theta_0 = \frac{1}{2}$. The termination number is 15 and the acceptability constant is .687.</p>
<p>e. Establish test procedure.</p>	<p>e. The specified demonstration test has the following characteristics:</p> <ol style="list-style-type: none"> 1) Items with a mean life of 1000 hours will be accepted by this test plan 90% of the time. 2) Items with a mean life of only 500 hours will be accepted by this test plan only 10% of the time. 3) Select a random sample of 15 or more items and test until 15 failures are observed. 4) Multiply the acceptability constant by θ_0 (in this example 1000) = .687.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

- | <u>3. Method</u> | <u>Example</u> |
|---|--|
| <p>f. Estimate the expected waiting for an accept/reject decision by entering the appropriate table in MIL-HDBK-H108.</p> | <p>e.</p> <p>5) After 15 failures have been observed stop the test and sum the hours of operating time accumulated on all items that have been on test (both failed and unfailed). Divide the total item operating time by the number of failures (15).</p> <p>6) If this θ is less than 687 hours reject the item.</p> <p>7) If $\theta \geq 687$ the demonstration test has been passed.</p> <p>f. Assume that 20 items had been placed on test in this example and the termination number is 15. From Table 2B-2(a) on page 2.34 of MIL-HDBK-H108, enter the table at $n = 20$ and $r = 15$. This yields an expected waiting time factor of 1.3144. If this is multiplied by θ_0 (1000 hours in the example) the expected time for a decision, if the true mean life of the items on test is 1000 hours, will be 1314 hours.</p> |

4. For Further Information

The statistical theory on which the H-108 sampling plans are based is presented in "*Statistical Techniques in Life Testing*," Technical Report No. 2, Testing of Hypotheses, by Benjamin Epstein, October 1958, and was prepared under Contract No. 2163(00) (NR-042-18) for the Office of Naval Research.

8.4.7.5.2.2 Normal Distribution, σ Known

1. When to Use

When the distribution of failure times is normal and when a given number of items are to be tested to failure, this type of test plan can be specified. Testing is without replacement.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

2. Conditions for Use

- a. The distribution of failure times must be normal.
- b. The standard deviation of failure times must be assumed known.
- c. The acceptable mean life θ_0 , the standard deviation σ_0 of the distribution of acceptable mean life, the standard deviation σ_1 of unacceptable mean life, the sample size n to be tested to failure, the producer's risk α must be specified.
- d. Note that unacceptable mean life θ_1 is not specified in this example. If it were desirable to specify a θ_1 , it could be done but one of the other four test plan parameters θ_1 , α , β , or sample size n would change. In other words, any four of these quantities can be specified but then the fifth is automatically constrained by the selection of the 4.
- e. There is also a tradeoff between the sample size and the accept/reject decision point. In the following example, the sample size to be tested has been specified, but it would be possible to specify a mean life which, if the observed average failure time did not exceed, would result in failure of the lot to pass the demonstration test. With this critical mean life specified, it would be necessary to solve for the sample size to be tested.
- f. Testing should be without replacement.

3. Method

Example

- | | |
|---|--|
| a. Specify θ_0 , σ_0 , σ_1 , β and n . | a. Given a lot whose item failure times are normally distributed as follows: |
|---|--|

$$\theta_0 = 200 \text{ hours}$$

$$\sigma_0 = 50 \text{ hours}$$

$$\alpha = .01$$

$$\sigma_1 = 50 \text{ hours}$$

$$\beta = .05$$

$$n = 25$$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
b. Solve for the accept/reject decision point.	b. The accept/reject point is calculated as follows: $z_0 = \frac{\bar{x} - \theta_0}{\sigma_0/\sqrt{n}}$ $-2.33 = \frac{\bar{x} - 200}{50/\sqrt{25}}$ $\bar{x} = 176.7$
c. Solve for θ_1 .	c. Using the result from Step (b) and the specified $\beta = .05$ $z_1 = \frac{\bar{x} - \theta_1}{\sigma_1/\sqrt{n}} +$ $1.645 = \frac{176.7 - \theta_1}{50/\sqrt{25}}$ $\theta_1 = 160.25$ <p>NOTE: The z values are from a table of "Areas Under the Normal Curve."</p>
d. Summarize the characteristics of the demonstration test plan.	d. The demonstration test procedure is as follows: <ol style="list-style-type: none"> 1) Take a random sample of 25 items from a population whose distribution of failure times is normal.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

- 2) Test until all items have failed, recording the exact failure time of each.
- 3) Take the arithmetic mean of the 25 failures and compare it with the decision point 176.7 hours. If the observed mean equals or exceeds 176.7 hours the demonstration test is passed. If it is less than 176.7 the demonstration test is failed.
- 4) The demonstration test shown in this example will:
- accept lots with a mean life of 200 hours and a standard deviation of 50 hours 99% of the time.
 - accept lots with a mean life of 160.25 hours and standard deviation of 50 hours 5% of the time.
- e. Construct the operating characteristic curve.

- e. This is done by assuming values of θ other than θ_0 and θ_1 and solving for the probability of acceptance of a lot with that θ . Assume

$$\theta = 175, \sigma = 50$$

$$z = \frac{176.7 - 175}{50/\sqrt{25}} = \frac{1.7}{10} = .17$$

From a table of Areas Under the Normal Curve the probability of acceptance of a lot with a mean life of 175 hours, $\sigma = 50$ is approximately .43.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

f. Calculate the expected waiting time for a decision.

f. The expected waiting time for a decision is the expected failure time of the last order statistic. In this ex-ample and sample size $n = 25$, $\alpha = 50$ and $\mu = 200$. These values are used with Table 10A.1, page 186 of the book "*Contributions to Order Statistics*" edited by A.E. Sarhan and B.G. Greenberg, published by John Wiley & Sons, New York, 1962.

Table 10A.1 give a $z = 1.965$ for the last order statistic in a sample of $n = 25$. Applying the formula

$$z = \frac{x - \mu}{\sigma}$$

$$1.965 = \frac{x - 200}{50}$$

$$x = 298 \text{ hours}$$

Therefore the expected waiting time for a decision of $\theta_0 = 200$, and 25 items are tested to failure, is 298 hours.

4. For Further Information

MIL-STD-414 Section D yields a series of variables demonstration test plans for the normal distribution with σ known. The tests are constructed to assure protection in the form of percent defective of the lot from which the sample was drawn, whereas, the example presented here is based on mean life.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

8.4.7.5.2.3 Normal Distribution, σ Unknown (MIL-STD-414)

1. When to Use

When the distribution of failure times is normal, with unknown standard deviation and the criterion for acceptance is a variable (in the case, hours of life expectancy) with the protection desired stated in terms of percent defective in the lot from which the sample was drawn, then this type of demonstration test is useful. This procedure basically is an application of MIL-STD-414, "*Sampling Procedures and Tables for Inspection by Variables for Percent Defective.*" It contains plans for both single and double specification limits. The criteria for acceptance can either be stated in terms of an acceptability constant, k , stated in standard normal deviates or as a maximum allowable percent defective, M . MIL-STD-414 also presents plans based on the calculation of an estimate of the standard deviation from sample data and also presents the range method. In the range method, the sample is segmented and the range of each sub-sample is used to estimate variability. It also contains test plans for the case when the standard deviation is known.

2. Conditions for Use

- a. The distribution of failure times must be normal.
- b. The standard deviation is unknown and must be assumed equal for both acceptable and unacceptable lots (when it is known, see previous example).
- c. Failure is measured in hours or cycles of operation.
- d. All items in the sample will be tested to failure.
- e. The lot size, acceptable quality level AQL, specification limit or limits, and inspection level must be stated.
- f. Testing is performed without replacement of failed items.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
<p>a. Specify the lot size from which the sample is to be randomly drawn, AQL (the percent defective of accept-able lots), the specification limit, and the method to be used (standard deviation or range method) to measure variability.</p>	<p>a. Given an item type whose failure times are normally distributed. The lot to be evaluated contains 100 items with an unknown standard deviation. An AQL of 4% represents an acceptable level of defectives in a lot. The normal inspection level in MIL-STD-414 is IV. The standard deviation method is to be used for determining compliance with the acceptability criterion. The minimum life (L) for items of this type is 300 hours.</p>
<p>b. Determine the sample size to be tested.</p>	<p>b. Enter Table A-2 on page 4 of MIL-STD-414 with the lot size = 100. It is found that for Inspection Level IV, sample size code letter F applies. On page 39 in Table B-1 sample size code letter F calls for a sample size of 10.</p>
<p>c. Determine the acceptability constant k.</p>	<p>c. From Table B-1 enter Row F and the column headed by AQL = 4.00. This yields an acceptability constant $k = 1.23$.</p>

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

- | 3. <u>Method</u> | <u>Example</u> |
|---|--|
| d. Draw a random sample from the lot and test until all items fail recording exact failure times. | d. Ten failure times are re-corded as follows:

Failure Time (Hours)

275
310
315
370
400
425
450
515
625
630 |
| e. Calculate the sample mean and standard deviation from the observed test data. | e. Using standard statistical calculations

$\bar{x} = 432$ hours
$s = 119$ hours |
| f. Calculate the quantity

$\frac{\bar{x} - L}{s}$ | f. $\frac{\bar{x} - L}{s} = \frac{432 - 300}{119} = 1.10$ |
| where L = the specified minimum life. | |
| g. Compare $\frac{\bar{x} - L}{s}$ with k. | g. From Step c, the acceptability constant is k = 1.23. From Step f, $\frac{\bar{x} - L}{s} = 1.10$ Since $1.10 < 1.23$, reject the lot. |

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

4. For Further Information

MIL-STD-414 also presents test plans for cases where the standard deviation is known. Operating characteristic curves are presented in Section A of MIL-STD-414 to enable assessment of the risk at all quality levels. All lot sizes can be accommodated, but only certain values of AQL are covered by test plans. MIL-STD-414 also covers tightened and reduced sampling. A discussion of the methodology of the development of this type of sampling plan is presented in "*Quality Control and Statistics*" by A. J. Duncan, published by Richard D. Irwin, Homewood, Illinois, 1959.

8.4.7.5.2.4 Weibull Distribution1. When to Use

When the underlying distribution of failure time is Weibull, with the shape parameter, β , known or assumed, and the test must be truncated after a specified number of failures has occurred. The ordered failure times are required, along with the number of items on test.

2. Conditions for Use

- a. The two-parameter Weibull distribution must be assumed for failure times.
- b. The parameter, β , must be known and be the same under the null and alternative hypothesis concerning the population mean.
- c. The acceptable mean life, μ_0 , the unacceptable mean life, μ_1 , and the producer's risk must be specified. If the number of failures at which the test is truncated is specified, then the consumer's risk will be determined, and cannot be set arbitrarily.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
<p>a. The method involves replacement of the original failure times x_1, \dots, x_r by a new variable defined as $y_i = x_i \beta$</p> <p>This variable has an exponential distribution with mean α. Hence, the previous method developed for failure-truncated exponential life-distributions may be used (See Section <u>Exponential Distribution (MIL-HDBK-H108)</u>).</p> <p>b. To perform a Weibull demonstration test with parameters μ_0, μ_1, β. Solve the following equations:</p> $\mu_0 = \alpha_0^{1/\beta} \Gamma\left(\frac{1}{\beta} + 1\right)$ $\mu_1 = \alpha_1^{1/\beta} \Gamma\left(\frac{1}{\beta} + 1\right)$ <p>for α_0 and α_1.</p>	<p>a. With producer's risk .05 and consumer's risk .10, test the hypothesis that $\mu_0 = 800$ hours against $\mu_1 = 400$ hours. Assume a Weibull distribution with parameter $\beta = 1.5$. Twenty specimens were placed on test, and the test was concluded after the fourth failure, the observed failure times being 600, 750, 1000, and 1220 hours.</p> <p>b. $\alpha_0 = \left[\frac{\mu_0}{\Gamma\left(\frac{1}{\beta} + 1\right)} \right]^\beta$</p> $= \left(\frac{800}{\Gamma(1.67)} \right)^{1.5}$ $= \left(\frac{800}{.903} \right)^{1.5}$ $= 24600$ $\alpha_1 = \left(\frac{400}{.903} \right)^{1.5}$ $= 9400$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
<p>c. Perform the demonstration test in Section <u>Exponential Distribution (MIL-HDBK-H108)</u> on the observations y_1, y_2, \dots, y_K from the exponential distribution with</p> $\theta_0 = \alpha_0$ $\theta_1 = \alpha_1$ <p>The test is described in MIL-HDBK-H108.</p> <p>On page 2.26 of MIL-HDBK-H108, the formula for $\hat{\theta}$ is</p> $\hat{\theta} = \left[\frac{1}{r} \sum_{i=1}^r y_i + (n-r)y_r \right]$ <p>This is compared with acceptability constant, C, given on page 2.28 of MIL-HDBK-H108. The acceptance region is</p> $\hat{\theta} \geq \theta_0 / (C/\theta_0)$ <p>d. The consumer's risk may be estimated from OC curves provided in the referenced document. Compute θ_1/θ_0 and read the value of the β error from Table 2A-2.</p>	<p>c. $y_1 = 600^{1.5} = 14,700$</p> $y_2 = 750^{1.5} = 20,500$ $y_3 = 1000^{1.5} = 31620$ $y_4 = 1220^{1.5} = 42,600$ $\hat{\theta} = \frac{1}{4} [14,700 + 20500 + 31620 + 42600 + 16(42600)]$ $\hat{\theta} = 197755$ $\theta_0 = 26400$ <p>$C/\theta_0 = .342$ for producer's risk .05 and 4 failures (Table 2B-1) (MIL-HDBK-H108)</p> $\text{Critical Value} = \frac{26400}{.342}$ $= 77200$ <p>Since $197755 > 77200$, accept the value, μ_0, for the Weibull population mean</p> <p>d. $\frac{\theta_1}{\theta_0} = \frac{9400}{26400} = 0.36$</p> <p>$\beta = 0.38$ from Table 2A-2 (MIL-HDBK-H108)</p>

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

3. Method

The larger the value of θ , the smaller the value of β error. To achieve a β error of 0.1, for example, it would be necessary (Table 2-A-2) to continue testing until 9 failures had occurred.

4. For Further Information

Tables of the Gamma Function are presented on page 497 of the *"Handbook of Tables for Probability and Statistics"* edited by W. H. Beyer, Chemical Rubber Company, 1966.

8.4.7.5.3 Sequential Tests

8.4.7.5.3.1 Exponential Distribution (MIL-HDBK-781)

1. When to Use

When the demonstration test is to be based upon time-to-failure data and the underlying probability distribution is exponential, the sequential test is an alternate for the fixed sample size or fixed time tests discussed in Sections Time Truncated Demonstration Test Plans and Failure Truncated Tests. The sequential test leads to a shorter average number of part hours of exposure than either fixed sample or fixed time tests if the lot tested is near θ_0 or θ_1 . Sequential tests should not be used where the exact length, or cost, of the test must be known before-hand, or is specified.

2. Conditions for Use

- a. The failure distribution must be exponential.
- b. The upper test MTBF, θ_0 , lower test MTBF, θ_1 , producer's risk, α , and consumer's risk, β , must be specified.
- c. The test may be run either with or without replacement of failed items, since the pertinent statistic is "total item-hours" of test time.
- d. The producer's risk, α , and consumer's risk, β , are always equal in these test plans.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

- | <u>3. Method</u> | <u>Example</u> |
|--|---|
| <p>a. Specify θ_0, θ_1, α, β. If the requirements are stated in terms of reliability at a time T_0, this will involve solution of the equation.</p> $\exp\left[-(T_0/\theta)\right] = R$ <p>for θ. The solution is</p> $\theta = -\frac{T_0}{\ln R}$ | <p>a. Given equipment type whose failure times are distributed exponentially. A reliability of 0.95 is desired for 150 hours of operation. A product with a reliability of 0.9 or lower is unacceptable. We specify that $\alpha = 0.10$ for 0.95 reliability and $\beta = 0.10$ for 0.90 reliability.</p> <p>We have</p> $\theta_0 = -\frac{150}{\ln 0.95}$ $\theta_0 = 2924 \text{ hours}$ $\theta_1 = -\frac{150}{\ln 0.90}$ $\theta_1 = 1424 \text{ hours}$ |
| <p>b. Compute θ_0/θ_1</p> | <p>b. $\theta_0/\theta_1 = \frac{2924}{1424} = 2.05$</p> |

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. Method Example

- c. Tests in MIL-HDBK-781 are classified by θ_0/θ_1 , α and β . Find the Test Plan which most nearly fits the three values, and record the acceptance and rejection criteria. These are given in terms of θ_1 , and must be multiplied by θ_1 to convert to "equipment hours" criteria.

- c. For $\alpha = \beta = .10$ the nearest test in MIL-HDBK-781 is Test Plan IIID. The criteria given for acceptance and rejection are:

No. of Failures	Equipment Reject	Hours Accept
0	N/A	4.4
1	N/A	5.79
2	N/A	7.18
3	0.7	8.56
4	2.08	9.94

After multiplying by θ_1 , or 1424 hours, we obtain

No. of Failures	Equipment Reject	Hours Accept
0	-	6266
1	-	8245
2	-	10224
3	997	12189
4	2962	14155

For example, if 3 failures are encountered prior to 997 equipment hours, reject the equipment as unsatisfactory.

- d. The OC curve of each sequential test is given as multiples of θ_0 and θ_1 . The document supplies for each Test Plan the expected length and the OC curve.
- d. The expected number of equipment hours to reach a decision, when θ_0 is the population parameter, and the OC curve are given in MIL-HDBK-781A (Ref. [18]).

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

4. For Further Information

The material presented herein is from MIL-HDBK-781, “*Reliability Test Methods, Plans and Environments for Engineering Development, Qualification and Production.*” The theory of sequential testing is developed in “*Sequential Analysis*” by A. Wald, John Wiley and Sons, Inc., 1947. Examples of sequential exponential demonstration tests are given in an article by Benjamin Epstein and Milton Sobel, “*Sequential Life Tests in the Exponential Case,*” *Annals of Mathematical Statistics*, Vol. 25, 1955, pp. 82-93.

8.4.7.5.3.2 Normal Distribution1. When to Use

When the underlying failure distribution is assumed to be normal, and random sample observations are gathered sequentially. This method does not apply to ordered sample observations such as are usually obtained in life testing. It is useful where the cost of a single test is high, testing is done one unit at a time, and it is desired to minimize expected sample size.

As an example, consider the destructive testing of an aluminum alloy exhaust fan, where the component is rotated in a “whirl pit” at increasing velocity until a tensile failure occurs. In service, the component will rotate at a maximum velocity v_0 , and the purpose of the demonstration test is to assure that the population mean velocity at failure is sufficiently high to provide satisfactory reliability at v_0 .

2. Conditions for Use

- a. The distribution of failures must be normal.
- b. The acceptable population mean, μ_0 , unacceptable mean, μ_1 , must be specified, along with the known or assumed population standard deviations, σ_0 and σ_1 , the producer's risk, α , and consumer's risk, β . If α is unknown, and the test involves a strength distribution, α is often assumed to be 5% of the mean, in accordance with the discussion of normal distribution estimation in Section 5 of this handbook.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

- a. Specify μ_0 , μ_1 , σ_0 , σ_1 , α , and β .
 Compute

$$A = \frac{1 - \beta}{\alpha}$$

$$B = \frac{\beta}{1 - \alpha}$$

- b. Compute, as each new observation is obtained, the corresponding unit normal deviates

$$z_{0i} = \frac{x_i - \mu_0}{\sigma_0}$$

$$z_{1i} = \frac{x_i - \mu_1}{\sigma_1}$$

and the corresponding probability density from a table of the normal distribution ordinates (Table 5.3.1-2).

Note that it is not the usual areas under the normal curve but the ordinates that are required.

a. $\mu_0 = 1000$

$$\mu_1 = 800$$

$$\sigma_0 = \sigma_1 = 100$$

$$\alpha = \beta = .05$$

$$A = \frac{.95}{.05} = 19.0$$

$$B = \frac{.05}{.95} = .053$$

- b. The first sample observation was found to be

$$x_1 = 1020, \text{ hence}$$

$$z_{01} = \frac{1020 - 1000}{100} = 0.2$$

$$z_{11} = \frac{1020 - 800}{100} = 2.2$$

The ordinate in the normal table corresponding to 0.2 is 0.3900 while the ordinate corresponding to 2.2 is 0.0355.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

c. Form the product of ordinates

$$L_0 = \sum_{i=1}^k f(z_{0i})$$

and

$$L_1 = \sum_{i=1}^k f(z_{1i})$$

Determine, as each new sample is received, the ratio,

$$\frac{L_1}{L_0}$$

If

$$B < \frac{L_1}{L_0} < A$$

continue testing. If

$$\frac{L_1}{L_0} < B, \text{ accept } \mu_0$$

$$\frac{L_1}{L_0} > A, \text{ accept } \mu_1$$

c. $L_0 = .3900$

$$L_1 = .0355$$

$$\frac{L_1}{L_0} = \frac{.0355}{.3900} = .091$$

Since this is between B and A, continue testing. The second observation was

$$x_2 = 904.$$

Calculating as before,

$$z_{02} = .96$$

$$\text{Ordinate} = .2516$$

$$z_{12} = 1.04$$

$$\text{Ordinate} = .2323$$

$$\frac{L_1}{L_0} = .091 \left(\frac{.2323}{.2516} \right) = .084$$

Therefore, continue testing.

We observe

$$x_3 = 1050$$

$$z_{03} = 0.5$$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

$$\text{Ordinate} = .3521$$

$$z_{13} = 2.5$$

$$\text{Ordinate} = .0175$$

$$\frac{L_1}{L_0} = .084 \left(\frac{.0175}{.3521} \right) = .004$$

Since this is less than B, accept μ_0
as population mean.

- d. The expected sample size
(assuming that the true parameter
is μ_0) may be obtained from the
formula

$$E(N) =$$

$$\frac{(1 - \alpha) \ln B + \alpha \ln A}{\frac{1}{2\sigma^2} [2(\mu_1 - \mu_0)\mu_0 + \mu_0^2 - \mu_1^2]}$$

- d. For this test, the expected number
of observations was

$$E(N) =$$

$$\frac{.95 \ln .053 - .05 \ln 19.0}{\frac{1}{20000} [2 - (200)(1000) + 1 \times 10^6 - 6.4 \times 10^5]}$$

$$\approx 2$$

(Note: sample size must be an
integer)

4. For Further Information

See "*Sequential Analysis*" by Abraham Wald, John Wiley and Sons, N.Y., 1947, p. 77 and p. 53.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

8.4.7.6 Interference Demonstration Tests1. When to Use

Interference demonstration testing is applicable to mechanical systems where a strength distribution and a stress distribution overlap, or interfere. See Section 7 for several detailed examples. In the case of demonstration testing, both the strength and stress distribution must be assumed to be normal. We distinguish four cases:

Case 1: The mean of the stress distribution is assumed to be known, and the standard deviation of the stress distribution is assumed to be zero. See the discussion in Section 7 for conditions where these assumptions are valid. In this case, the interference problem becomes identical to life testing of the normal distribution described in Section 8.4.7.5.2.2, Normal Distribution σ Known. The specified stress level plays the role of the specified life. The strength distribution plays the role of the life distribution, and the demonstration procedure follows the example in Section 8.4.7.5.2.2.

Case 2: The mean of the stress distribution is assumed to be known, along with its standard deviation (often assumed to be 5% of the mean). The standard deviation of the strength distribution is assumed to be known, and its mean unknown. This may be translated to a demonstration test on strength and solved by the methods of Section 8.4.7.5.2.2. An example will be given.

Case 3: The mean of the stress distribution and the mean of the strength distribution are unknown, but their standard deviations are assumed known. In this instance, sampling data will be required from both stress and strength. It is rare that a sample size for each may be specified ahead of testing. Therefore, it is unlikely that the consumer's risk may be set for this test. β will be a function of N and α . An example will be given.

Case 4: The means and standard deviations of the strength and stress distributions are unknown. This case cannot be subjected to a demonstration test using standard statistical methods.

2. Conditions for Use

- a. The strength distribution and stress distribution must be stochastically independent.
- b. The strength distribution and stress distribution must be normal.
- c. A random sample of strength and stress observations must be obtained.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
<p>a. If the strength distribution has normal parameters μ_x, σ_x and the stress distribution has normal parameters μ_y, σ_y, then the statistic</p> $w = x - y$ <p>is normally distributed with parameters</p> $w = \mu_x - \mu_y$ $\sigma_w = \sqrt{\sigma_x^2 + \sigma_y^2}$ <p>and the reliability is defined as the probability that w exceeds zero. Clearly, specifying a particular reliability is the equivalent of requiring the unit normal deviate</p> $z = \frac{(\mu_x - \mu_y) - 0}{\sqrt{\sigma_x^2 + \sigma_y^2}}$ <p>to correspond to this reliability in the right tail of the unit normal.</p>	<p>1. Stress has a specified value of 30 KSI* with standard deviation 1.5 KSI. Strength is expected to be in the vicinity of 40 KSI but the mean is unknown. The standard deviation is assumed to be 2.0 KSI. A reliability of 0.99 is acceptable while a reliability of 0.90 is unacceptable. The producer's risk is .05 and the consumer's risk .10.</p> <p><u>Solution:</u></p> $\sigma_w = \sqrt{2^2 + (1.5)^2}$ $= 2.5 \text{ KSI}$ <p>The unit normal deviates corresponding to 0.99 and 0.90 reliability are 2.33 and 1.28 respectively.</p> <p>Therefore,</p> $2.33 = \frac{(\mu_0 - 30) - 0}{2.5}$ $1.28 = \frac{(\mu_1 - 30) - 0}{2.5}$

* KSI = 1000 lbs/sq. in

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

and the requirements on the strength distribution are

$$\mu_0 = 35.9$$

$$\mu_1 = 33.2$$

with a known $\sigma = 2.0$,
 $\alpha = .05$, $\beta = .10$. The methods of
Section 8.4.7.5.2.2, may now be
used.

2. If we retain the data of example 1,
and delete the information
concerning the mean of the stress
distribution, then,

$$\begin{aligned}\sigma_x &= 2.0 \mu_0 - \mu_X \\ &= 35.9 - 30 = 5.9\end{aligned}$$

$$\begin{aligned}\sigma_y &= 1.5 \mu_1 - \mu_X \\ &= 33.2 - 30 = 3.2\end{aligned}$$

$$\alpha = .05$$

$$\beta = .10$$

If N_x observations of strength and N_y
observations of stress are obtained, the
appropriate statistic is

$$z = \frac{(\bar{x} - \bar{y}) - 5.9}{\sqrt{\frac{\sigma_x^2}{N_x} + \frac{\sigma_x^2}{N_y}}}$$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

Hence, the critical value of
($\bar{x} - \bar{y}$) is

$$z_{\alpha} \sqrt{\frac{\sigma_x^2}{N_x} + \frac{\sigma_y^2}{N_y}} + 5.9$$

For example, ten observations of strength and four observations of stress are available.

For 0.99 reliability, we have from the previous example, $\mu_x - \mu_y = 5.9$, and $z_{\alpha} = z_{.95} = -1.65$

$$\begin{aligned} -1.65 \sqrt{\frac{4.0}{10} + \frac{2.25}{4}} + 5.9 \\ = +4.21 \end{aligned}$$

as the critical value of the statistic
($\bar{x} - \bar{y}$). Accept if

$$\bar{x} - \bar{y} \geq 4.21$$

Otherwise, reject. The β risk for this example would be

$$z = \frac{4.21 - 3.2}{\sqrt{\frac{4.0}{10} + \frac{2.25}{4}}} = +1.03$$

$$\beta = 0.15$$

A larger sample size for either stress or strength will reduce β .

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

8.4.7.7 Bayes Sequential Tests1. When to Use

A test plan of this type can be specified if mean life θ is the parameter of interest and if a prior distribution on θ is known. The use of a test plan of this type results in a smaller sample size than most other test plans described in this section.

2. Conditions of Use

- a. The lot of items being evaluated must have a known prior distribution on the mean life.
- b. The parameters of the prior distribution must be specified as well as θ_1 , the minimum acceptable mean life. It is necessary to specify two other terms K_2 and K_1 as criteria for terminating the test. K_2 is a probability such that if $\Pr(\theta \geq \theta_1/\theta_n) \geq K_2$ the test is deemed passed. It is usually specified at .90, .95 or .99 and is the probability associated with a lower bound at θ_1 . K_1 is usually specified as .01, .05, or .10 and $1 - K_1$ is the probability associated with an upper bound at θ_1 . $K_2 + K_1$ need not equal 1.
- c. In this demonstration test procedure it is possible to pass or fail without testing. If testing is called for, one item is tested at a time and a decision is made after each failure to either accept, reject, or continue testing.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. <u>Method</u>	<u>Example</u>
<p>a. Specify the prior distribution form, its parameters, and the quantities θ_1, K_1 and K_2</p>	<p>a. It has been found that a given item type has a prior distribution on its mean life θ that is inverted gamma with a shape parameter $\lambda = 3$, a scale parameter $\alpha = 100$, a minimum acceptable mean life $\theta_1 = 60$, $K_1 = .10$ and $K_2 = .90$.</p>
<p>b. Compute P_0 to determine if testing should be performed:</p> <p>if $P_0 \geq K_2$, accept and do not test</p> <p>if $P_0 \leq K_1$, reject and do not test</p> <p>if $K_1 < P_0 < K_2$, place an item on test</p>	<p>b. To solve for P_0 use the Tables of Percentage Points of the X^2 distribution for 2λ degrees of freedom (d.f.). In this case use 6 d.f.</p> <p>Next solve the equation</p> $X^2 = \frac{2\alpha}{\theta_1} = \frac{2(100)}{60} = 3.33$ <p>In the X^2 Table for 6 d.f. $X^2 = 3.33$ corresponds to a percentage point (P_0 in this problem) of approximately .23.</p> <p>Therefore, $K_1 < P_0 < K_2 = .10 < .23 < .90$ resulting in the instruction to begin testing.</p>

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. Method Example

c. Construct a table of decision points for each failure time. This is done by solving for

$$\hat{\theta}_n^* = \frac{\theta_1 X_{K2, 2(n+\lambda)}^2 - 2\alpha}{2n}$$

where n = # of failures

and

$$\hat{\theta}_n^* = \frac{\theta_1 X_{K1, 2(n+\lambda)}^2 - 2\alpha}{2n}$$

c. For 1 failure the following decision points are calculated

$$\hat{\theta}_1^* = \frac{60X_{(.90, 8)}^2 - 2(100)}{2(1)}$$

$$\hat{\theta}_1^* = \frac{60(13.36) - 200}{2} = 301$$

$$\hat{\theta}_1^* = \frac{60X_{(.10, 8)}^2 - 2(100)}{2(1)}$$

$$\hat{\theta}_1^* = \frac{60(3.49) - 200}{2} = 4.7$$

The following table gives the accept/reject mean lives for additional failures.

n	Accept if $\hat{\theta}_n^*$	Reject if $\hat{\theta}_n^*$
1	301	4.7
2	190	23.5
3	152	29.7
4	133	33.4
5	-	-

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

3. MethodExample

$\hat{\theta}_{n^*}$ and $\hat{\theta}_{n^*}$ eventually terminate at some n . Therefore, the test could not continue indefinitely.

$$\text{The } \theta_n = \frac{\sum_{i=1}^n t_i}{n}$$

where:

t = failure time

n = number of failures

d. Test the first part and make the decision to accept, reject or continue testing.

d. Test the first item. If its failure time is:

- 1) 4.7 hours or less, reject the product.
- 2) 301 hours or more, accept the product.
- 3) greater than 4.7 and less than 301, test another sample to failure compare again to the accept/reject criteria of Step c.

4. For Further Information

The theoretical development of this method is presented in "A Sequential Bayes Procedure for Reliability Demonstration," by R.E. Schafer and N.D. Singpurwalla, Naval Research Logistics Quarterly, March 1970.

The methodology of fitting prior distributions is developed in RADC-TR-69-389 "Bayesian Reliability Demonstration - Phase I - Data for A Prior Distribution." Further details are provided in RADC-TR-76-296, Vols. I through V, "Reliability Acceptance Sampling Plans Based Upon Prior Distribution," and in RADC-TR-81-106, "Bayesian Reliability Tests Made Practical."

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

8.4.8 Reliability Demonstration Summary

MIL-HDBK-781 covers the detailed requirements for development and production reliability tests for equipment that experiences a distribution of time-to-failure that is exponential. MIL-HDBK-781 contain: test conditions, procedures, and various fixed length and sequential test plans with respective accept/reject criteria. Refs. [5] and [12] provide additional guidance and details on reliability measurement. The reliability test plan should contain, as a minimum, the following information:

- (1) How the equipment/system will be tested
 - The specified test conditions, e.g., environmental conditions, test measures, length of test, equipment operating conditions, accept/reject criteria, test reporting requirements, etc.
- (2) Who will perform the tests
 - Contractor, Government, independent organization
- (3) When the tests will be performed
 - Development, production, field operation
- (4) Where the tests will be performed
 - Contractor's plant, Government organization

Section 8.4.7 presented step-by-step instructions on the use of various types of reliability demonstration test plans. Instructions and examples are given for the following test plans:

- (1) Attributes Demonstration Tests
 - (a) Plans for Small Lots
 - (b) Plans for Large Lots
 - (c) Plans for Large Lots (Poisson Approximation Method)
 - (d) Attributes Sampling Using ANSI/ASQC Z1.4-1993
 - (e) Sequential Binomial Test Plans
- (2) Variables Demonstration Tests
 - (a) Time Truncated Test Plans
 - (1) Exponential Distribution
 - (2) Normal Distribution
 - (3) Weibull Distribution

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

- (b) Failure Truncated Tests
 - (1) Exponential Distribution
 - (2) Normal Distribution (Known)
 - (3) Normal Distribution (Unknown)
 - (4) Weibull Distribution

- (c) Sequential Tests
 - (1) Exponential Distribution
 - (2) Normal Distribution

- (d) Interference Demonstration Tests

- (e) Bayes Sequential Tests

8.5 Reliability Growth

Experience has shown that programs which rely simply on a demonstration test by itself to determine compliance with the specified reliability requirements generally do not achieve the reliability objectives with the allocated resources. This is particularly true of complex systems. Generally, these systems require new technologies and represent a challenge to the state of the art. Moreover, the requirements for reliability, maintainability and other performance parameters are usually highly demanding. Consequently, striving to meet these requirements represents a significant portion of the entire acquisition process and, as a result, the setting of priorities and the allocation and reallocation of resources such as funds, manpower and time are often formidable management tasks.

In order to help ensure that the equipment/system will meet the required operational reliability requirement, the concept of reliability growth testing and management has been developed for equipment/system development programs.

8.5.1 Reliability Growth Concept

Reliability growth is defined as the positive improvement of the reliability of an equipment through the systematic and permanent removal of failure mechanisms. Achievement of reliability growth is dependent upon the extent to which testing and other improvement techniques have been used during development and production to “force out” design and fabrication flaws, and on the rigor with which these flaws are analyzed and corrected.

**SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH**

Figure 8.5-1 suggests an ideal growth process. The initial reliability of the prototype starts at some level that might be considered the state-of-the-art at the beginning of development. Through the development effort, reliability grows up to the pilot production stage. At that time, some loss of growth occurs due to the introduction of manufacturing problems. During the pilot production, corrective actions are continuing that cause resumption of growth. At the beginning of full scale production, some loss in the achieved level of reliability occurs because of the effects of mass production. However, growth will resume as these problems are eliminated. And, at a time when the equipment is released to the field it should have achieved the specified level or, under ideal conditions, the inherent or predicted level. The slope of this curve is affected by many variables and these will be discussed later. Thus, reliability growth is the result of an iterative design process. As the design matures, it is investigated to identify actual (via testing) or potential (via analysis) sources of failures. Further design effort is then spent on correcting these problem areas. The design effort can be applied to either product design or manufacturing process design. There are three essential elements involved in achieving reliability growth:

- (1) Detection of failure sources (by analysis and test)
- (2) Feedback of problems identified
- (3) Effective redesign effort based on problems identified

The rate at which reliability grows is therefore dependent on how rapidly activities in this iterative loop can be accomplished, how real the identified problems are, and how well the redesign effort solves the identified problems. It is important to realize that some activities may act as a bottleneck. The bottleneck activities may vary from one development program to the next. Even within a single program they may vary from one stage of development to the next. In most cases, however, failure sources are detected through testing, and the testing process effectively controls the rate of growth. As a consequence, the reliability growth process becomes familiarly known as one of test, analyze, and fix (TAAF). However, the reliability achieved as a result of the growth process only becomes meaningful when the necessary changes developed and proven during TAAF to achieve that reliability are properly and fully incorporated in configuration-control documentation for production hardware.

Reliability growth testing (RGT) is only one aspect of a total reliability growth program. It must be accompanied by a reliability growth management program. This involves setting interim reliability goals to be met during the development testing program and the necessary allocation and reallocation of resources to attain these goals. A comprehensive approach to reliability growth management throughout the development program consists of planning, evaluating and controlling the growth process.

Note that RGT or TAAF, is intended neither to replace a sound design approach and thorough analytical effort nor compensate for a poor design. RGT should never be used or viewed as a “trial and error” approach to designing a reliable product.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

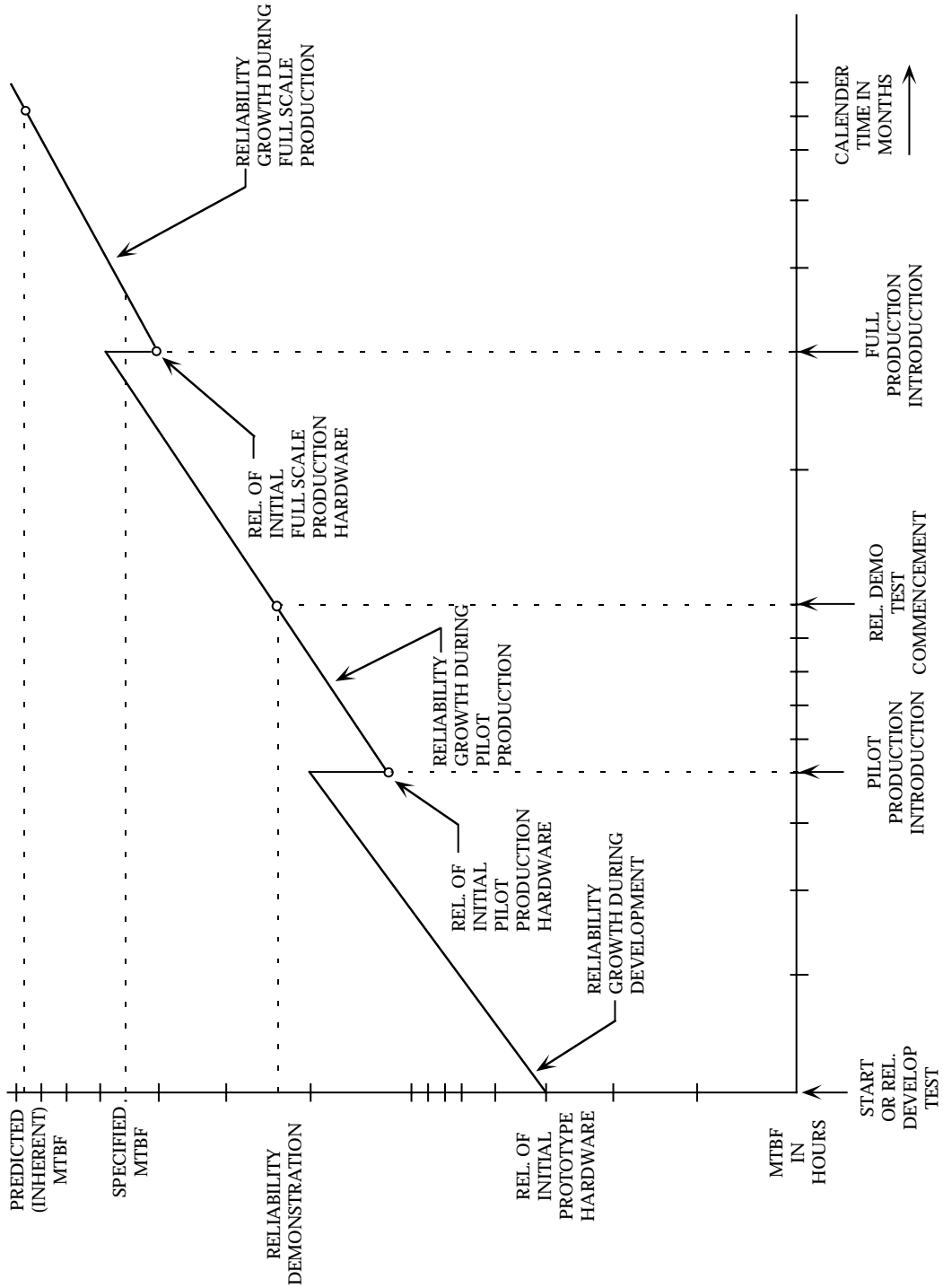


FIGURE 8.5-1: RELIABILITY GROWTH PROCESS

 SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

Reliability growth planning addresses program schedules, amount of testing, resources available and the realism of the test program in achieving the requirements. The planning is qualified and reflected in the construction of a reliability growth program plan curve. This curve establishes interim reliability goals throughout the program. To achieve these goals it is important that the program manager be aware of reliability problems during the conduct of the program so that he can effect whatever changes are necessary, e.g., increased reliability emphasis. It is, therefore, essential that periodic assessments of reliability be made during the test program (e.g., at the end of a test phase) and compared to the planned reliability growth values. These assessments provide visibility of achievements and focus on deficiencies in time to affect the system design. By making appropriate decisions in regard to the timely incorporation of effective fixes into the system commensurately with attaining the milestones and requirements, management can control the growth process.

8.5.2 Reliability Growth Modeling

For complex electronic/electro-mechanical avionic systems, the model used most often for reliability growth processes, and in particular reliability growth testing, is one originally published by J. T. Duane. (Ref. [16]). Essentially, this model 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 where T is the cumulative operating time and α is the rate of growth corresponding to the rapidity with which faults are found and changes made to permanently eliminate the basic causes of the faults observed.

The model is shown graphically in Figure 8.5-2, with each of the growth lines having different slopes, depending upon the emphasis given to the reliability growth program.

Duane's postulate was that as long as reliability improvement efforts continue, the following mathematical expression would hold:

$$\lambda_{\Sigma} = \frac{F}{H} = K H^{-\alpha} \quad (8.23)$$

where:

- λ_{Σ} = cumulative failure rate
- H = total test hours
- F = number of failures, during time H
- K = constant determined by circumstances
- α = growth rate

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

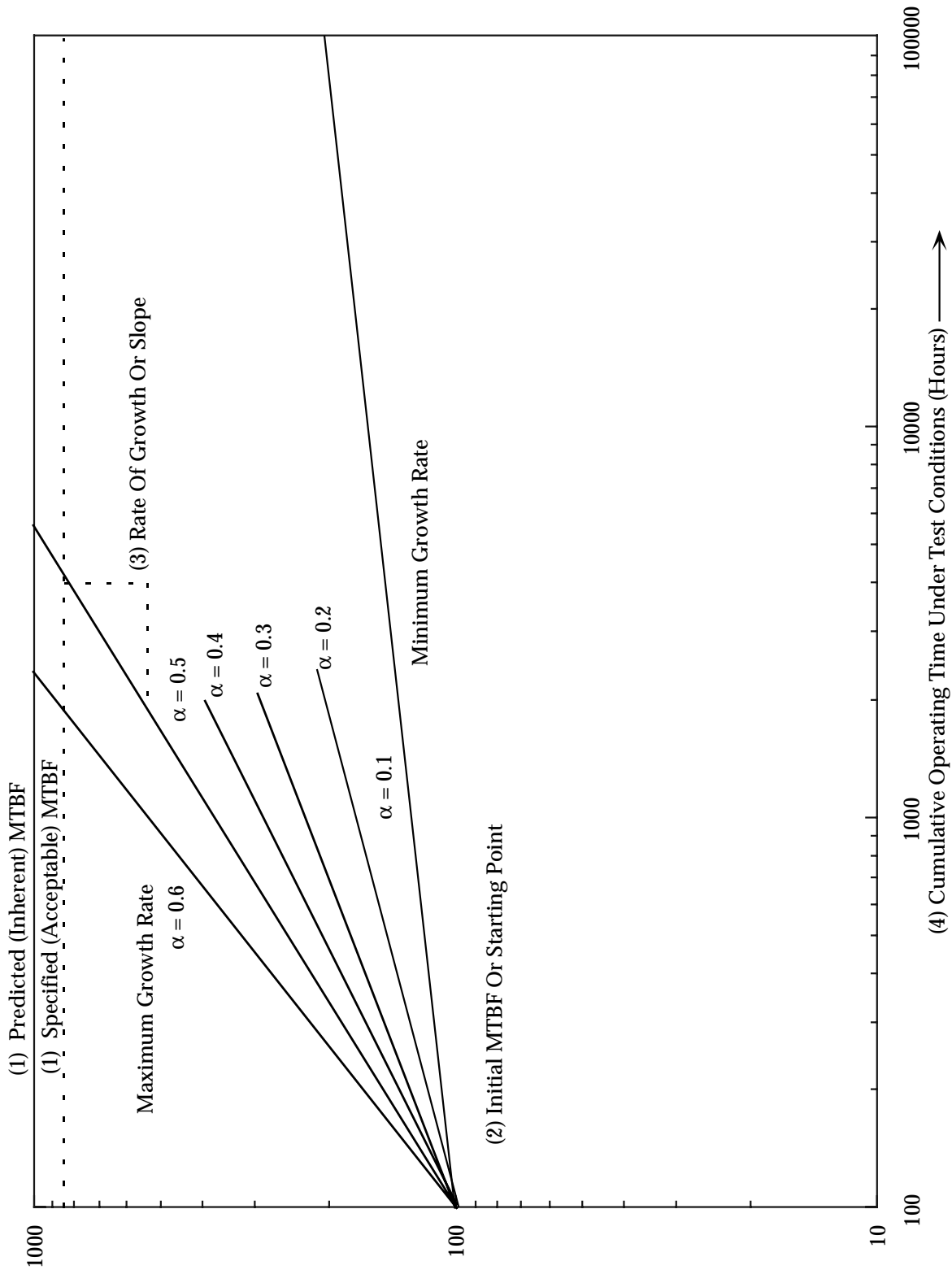


FIGURE 8.5-2: RELIABILITY GROWTH PLOTS

 SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

The original mathematical model was expressed in terms of cumulative failure rate; but currently, since equipment reliability is generally expressed in terms of MTBF, the following expression is used,

$$M_R = M_I \left(\frac{T_t}{t_i} \right)^\alpha \quad (8.24)$$

where:

M_R = required MTBF

M_I = initial MTBF

t_i = time at which initial data point is plotted (preconditioning time)

T_t = time at which the instantaneous MTBF of the equipment under test
will reach the MTBF requirement

α = growth rate

Differentiating Eq. (8.23) with respect to time

Since $\frac{F}{H} = KH^{-\alpha}$

then $F = KH^{(1-\alpha)}$

The instantaneous failure rate is found by differentiating with respect to H (i.e., time).

$$\begin{aligned} \lambda_{\text{instantaneous}} &= \frac{dF}{dH} = \frac{d(KH^{(1-\alpha)})}{dH} \\ &= \frac{Kd(H^{(1-\alpha)})}{dH} = (1-\alpha)KH^{-\alpha} \end{aligned} \quad (8.25)$$

so that the "instantaneous" or current failure rate is $(1 - \alpha)$ times the cumulative failure rate, or the "instantaneous MTBF" is $\frac{1}{1 - \alpha}$ times the cumulative MTBF. An adequate interpretation of "instantaneous MTBF" is: ***The MTBF that the equipment currently on test would exhibit if we stopped the reliability growth and continued testing.***

Thus the "instantaneous" or current MTBF curves are straight lines displaced from the cumulative plot by a factor $\frac{1}{1 - \alpha}$, which shows up as a fixed distance on a logarithmic plot, as

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

shown in Figure 8.5-3.

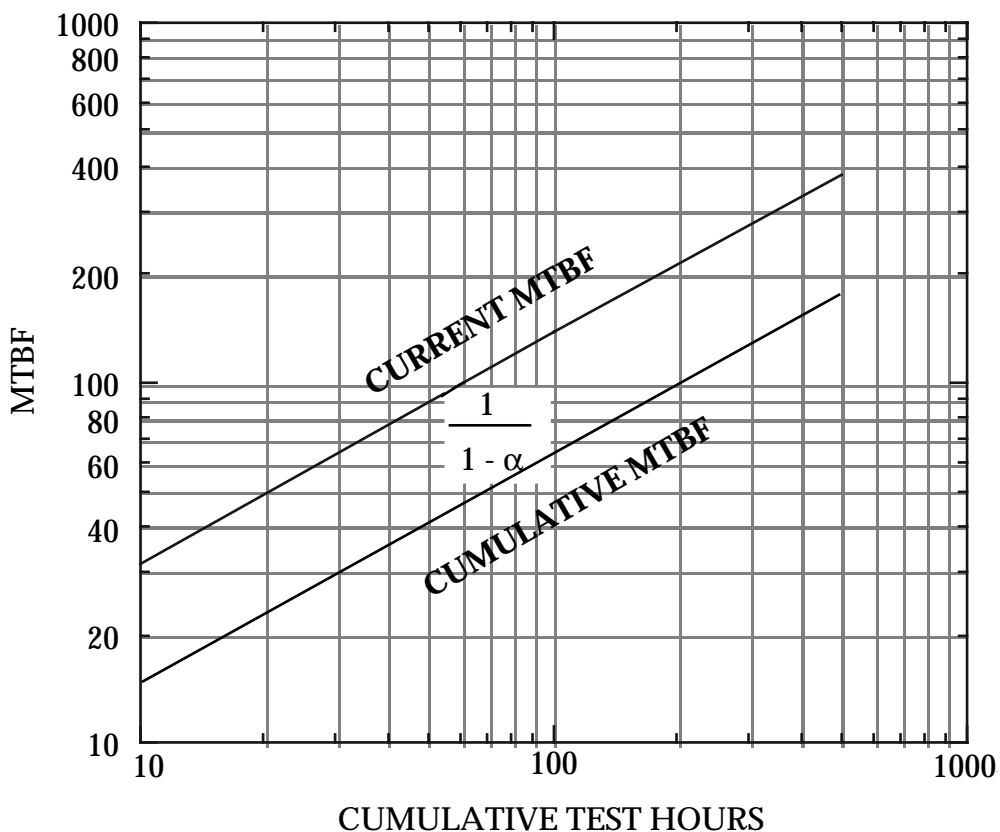


FIGURE 8.5-3: UP-IS-GOOD DUANE CHART WITH PLOT OF CURRENT MTBF

Normally, the cumulative MTBF (M_c) is measured in test and converted to instantaneous (or current) MTBF (M_I) by dividing by $1 - \alpha$, that is,

$$M_I = \frac{M_c}{1 - \alpha} \quad (8.26)$$

The cumulative MTBF is plotted versus cumulative test time, a straight line is fitted to the data and its slope, α , is measured. The current MTBF line is then drawn parallel to the cumulative line but displaced upward by an offset equal to $\frac{1}{1 - \alpha}$. The corresponding test time at which this line reaches the required MTBF is the expected duration of the growth test. Much evidence has been accumulated since Duane's original report that verifies the adequacy of the Duane Model in representing the real world of reliability growth testing.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

In fact, recently the Duane Model has been successfully applied to software growth modeling (Ref. [18]).

Crow presents a formal mathematical development of the growth model. He showed that the failure rate during development follows the Weibull failure rate curve. The development which follows is similar to that given by Crow (Ref. [17]).

Mathematically, this model may be expressed by the equation

$$F(t) = \lambda t^{-\alpha} \quad \lambda^* > 0; \quad 0 < \alpha < 1 \quad (8.27)$$

* λ is used here as a parameter of the Weibull distribution - it is not a failure rate.

where $F(t)$ is the cumulative failure rate of the system at time t and λ and α are parameters. By definition, therefore, it follows that the cumulative failure rate is

$$F(t) = \frac{E(t)}{t} \quad (8.28)$$

where $E(t)$ is the expected number of failures experienced by the system during t time units of development testing. Thus, from the above two equations

$$E(t) = \lambda t^{1-\alpha} \quad (8.29)$$

The instantaneous failure rate, $r(t)$, is of the most interest for applications. It is defined as the change in the expected number of failures per unit time. For a nonexponential system, it varies with time while for an exponential system the failure rate is constant.

Differentiating $E(t)$ with respect to time gives the instantaneous failure rate $r(t)$ as follows:

$$r(t) = \frac{dE(t)}{dt} = (1 - \alpha) \lambda t^{-\alpha} \quad (8.30)$$

By substituting in the previous equations

$$\beta = 1 - \alpha$$

one gets

$$r(t) = \lambda \beta t^{\beta - 1} \quad (8.31)$$

which is the Weibull failure rate function for a repairable system, i.e., for a non-homogeneous

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

Poisson process with a Weibull intensity function.

Thus, if one plans to use the Crow's Model, called the AMSAA Growth Model, during a development program, the Weibull failure rate function can be used to determine the failure rate at a particular development time t . The values of λ and β are estimated from test data. Since λ is only a multiplier and β determines how much the failure rate changes with the development time, β is referred to as the growth parameter. For the systems studied by Duane, a β of approximately 0.5 was estimated.

To gain further insight into the AMSAA Growth Model, consider Figure 8.5-4 which is a plot of the Weibull failure rate versus development time for $\beta = 0.5$ and $\lambda = 0.4$. In the early stages of development the failure rate decreases rather rapidly due to more failures and more rework going on during this time. As the development progresses, the rate of decrease of the failure rate drops off considerably. The AMSAA Model assumes that at some time t_0 which corresponds to about the time that development ends and production starts, the failure rate levels off to a fairly constant value. When the failure rate becomes constant, the time between failures can be described by the exponential distribution with a mean time between failure of

$$MTBF(t_0) = \left[\lambda \beta t_0^{\beta-1} \right]^{-1} \quad (8.32)$$

Crow (Ref. [22]) has developed the maximum likelihood estimates (MLE) of β and λ and also a goodness-of-fit test to determine if the AMSAA Model fits a particular set of data. The MLE estimate for β is

$$\hat{\beta} = \frac{N}{\sum_{r=1}^k \sum_{i=1}^{n_r} N_r(t) \ln \frac{T}{X_{ir}}} \quad (8.33)$$

where:

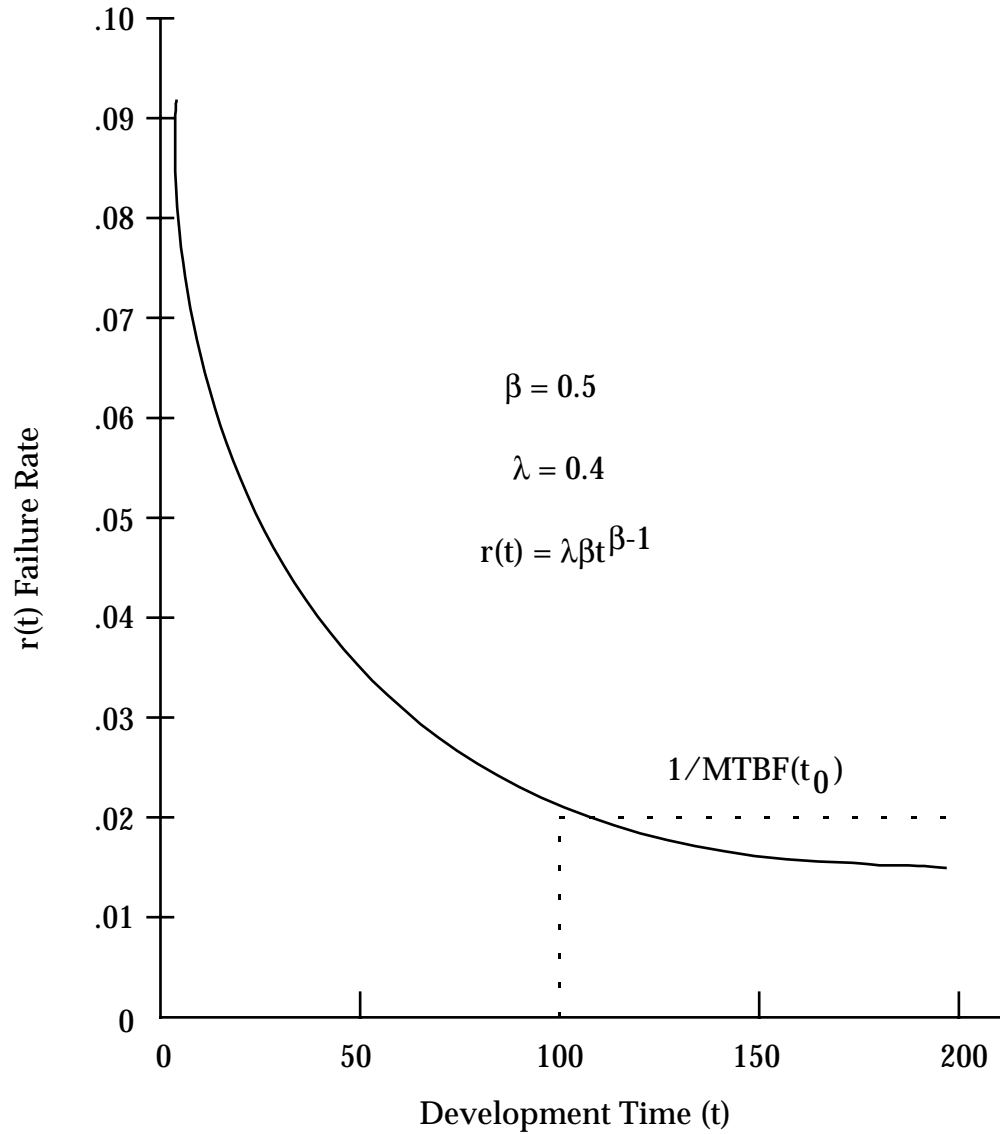
k = number of different subsystems,

T = the operating time for each of the k subsystems,

$N_r(T)$ = number of failures observed for the r^{th} subsystem during T time,

X_{ir} = the age of the r^{th} subsystem at the i^{th} failure (initially at the beginning of development)

$$N = \sum_{i=1}^k N_r(t) \quad (\text{Number of failures})$$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTHFIGURE 8.5-4: FAILURE RATE VS. DEVELOPMENT TIME
FOR WEIBULL FAILURE RATE

**SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH**

The previous MLE estimate of β is biased. The unbiased estimate is obtained by using

$$\bar{\beta} = \frac{N-1}{N} \hat{\beta} \quad (8.34)$$

The MLE of λ is

$$\hat{\lambda} = \frac{N}{kT^{\hat{\beta}}} \quad (8.35)$$

The chi-square goodness-of-fit test can be used to determine if the observed data fits the AMSAA Model. The chi-square statistic is calculated using

$$\chi_c^2 = \sum_{i=1}^c \frac{(O_i - E_i)^2}{E_i} \quad (8.36)$$

To compute the statistic the development time is divided into c intervals. The observed number of failures in the i -th interval, O_i , is obtained from the observed data. The expected number of failures in the i -th interval, E_i , is obtained using

$$E_i = \frac{N \left(\frac{t_i^{\bar{\beta}}}{i} - \frac{t_{i-1}^{\bar{\beta}}}{i-1} \right)}{T^{\bar{\beta}}} \quad (8.37)$$

where t_{i-1} and T_i are the beginning and ending times for the i^{th} interval. The χ_c^2 is compared with the tabled value of chi-square, χ_T^2 with degrees of freedom equal to $c - 1$ and the specified level of significance. If $\chi_c^2 < \chi_T^2$ then it can be concluded that the data fits the AMSAA Model.

8.5.2.1 Application Example

An engine system was analyzed for reliability growth using the AMSAA Model. The data available for analysis were based on 8063 hours of development testing. During this time there were 40 failures and the time of each failure was recorded. The average rates for this system during each interval of 1000 hours are shown in Figure 8.5-5.

Using this data the MLE's of λ and β , using equations 8.34 and 8.35, respectively, were

 SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

computed to be

$$\hat{\lambda} = 0.1279$$

$$\hat{\beta} = 0.6387$$

The unbiased estimate of β , using equation 8.35, is

$$\bar{\beta} = 0.6227$$

The chi-square goodness-of-fit statistic was calculated next using equation 8.36 and six intervals. The result was

$$\chi_c^2 = 10.09$$

Using a 1% level of significance and degrees of freedom of $6 - 1 = 5$, the tabled value of chi-square is

$$\chi_T^2 = 15.086$$

Thus it can be concluded that the AMSAA Model fits the data.

Using the Eq. (8.31), the estimated failure rate for the engine becomes

$$\begin{aligned} r(t) &= .128(.623) t^{.623-1} \\ &= .08 t^{-.377} \end{aligned}$$

A plot of this failure rate curve is given in Figure 8.5-5. Notice the curve is beginning to flatten out. In fact it would take 100,000 hours of development time to get the failure rate down to .001 failures/hour.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

Failure Times:

Interval 1 (0 to 1344 hours)	1, 43, 43, 171, 234, 274, 377, 530, 533, 941, 1074, 1188, 1248
Interval 2 (1345 to 2688 hours)	2298, 2347, 2347, 2381, 2456, 2456, 2500
Interval 3 (2689 to 4032 hours)	2913, 3022, 3038, 3728, 3873
Interval 4 (4033 to 5376 hours)	4724, 5147, 5179
Interval 5 (5377 to 6720 hours)	5587, 5626
Interval 6 (6721 to 8064 hours)	6824, 6983, 7106, 7106, 7568, 7568, 7593, 7642, 7928, 8063

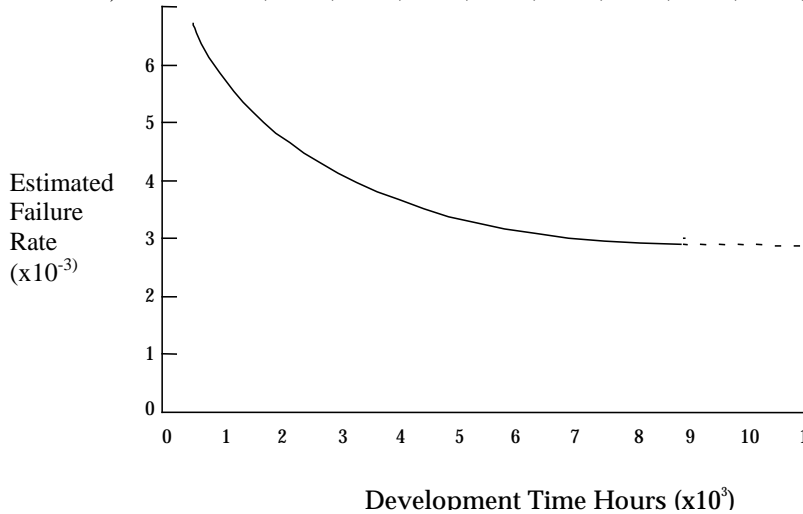


FIGURE 8.5-5: FAILURE RATE VS. DEVELOPMENT TEST TIME FOR WEIBULL FAILURE RATE

8.5.3 Comparison of the Duane and AMSAA Growth Models

The Duane Model and the Army Material Systems Analysis Activity (AMSAA) Model, developed by Dr. L. H. Crow in 1972 are the two most widely-used growth models. The Duane Model is based on an empirical relationship that holds as long as the MTBF is growing:

$$MTBF_{cum} = \frac{1}{K} T^{\alpha}$$

where:

$MTBF_{cum}$ = Cumulative MTBF

K = Constant determined by the initial MTBF

α = Growth rate (the slope of the log-log plot of $MTBF_{cum}$ vs Test Time)

T = Cumulative test time

Typically the log-log plot of cumulative failures vs. test time will result in a linear relationship if the system reliability is improving. The test-analyze-and-fix (TAAF) procedure improves system reliability by the incorporation of design changes. If the slope of the best fit line of such a plot is

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

positive, the system is said to be growing in reliability as time progresses.

The Duane Model assumes that the design fixes are 100% effective and that they are implemented immediately.

The instantaneous MTBF essentially estimates the projected field failure rate by accounting for fixes without purging the failure data.

The Duane Model assumes that growth is a deterministic process, while the AMSAA Model views the process of reliability growth as a probabilistic process. The AMSAA Model is based on the empirical relationship developed by Duane and is equivalent to a non-homogeneous Poisson process model with a Weibull intensity function. A typical AMSAA Model plot is shown in Figure 8.5-6. The AMSAA Model is

$$r_c(t) = \lambda t^{\beta-1}$$

where:

- $r_c(t)$ = The cumulative failure rate at time t
- t = Total test time
- β = Estimate of the time value of the growth parameter
- λ = Scale parameter

The instantaneous failure rate, $r_i(t)$, at time t is the incremental change in number of failures (F) with respect to the change in time.

$$\frac{F}{t} = r_c(t) = \lambda t^{\beta-1} \quad (8.38)$$

$$F = \lambda t^{\beta} \quad (8.39)$$

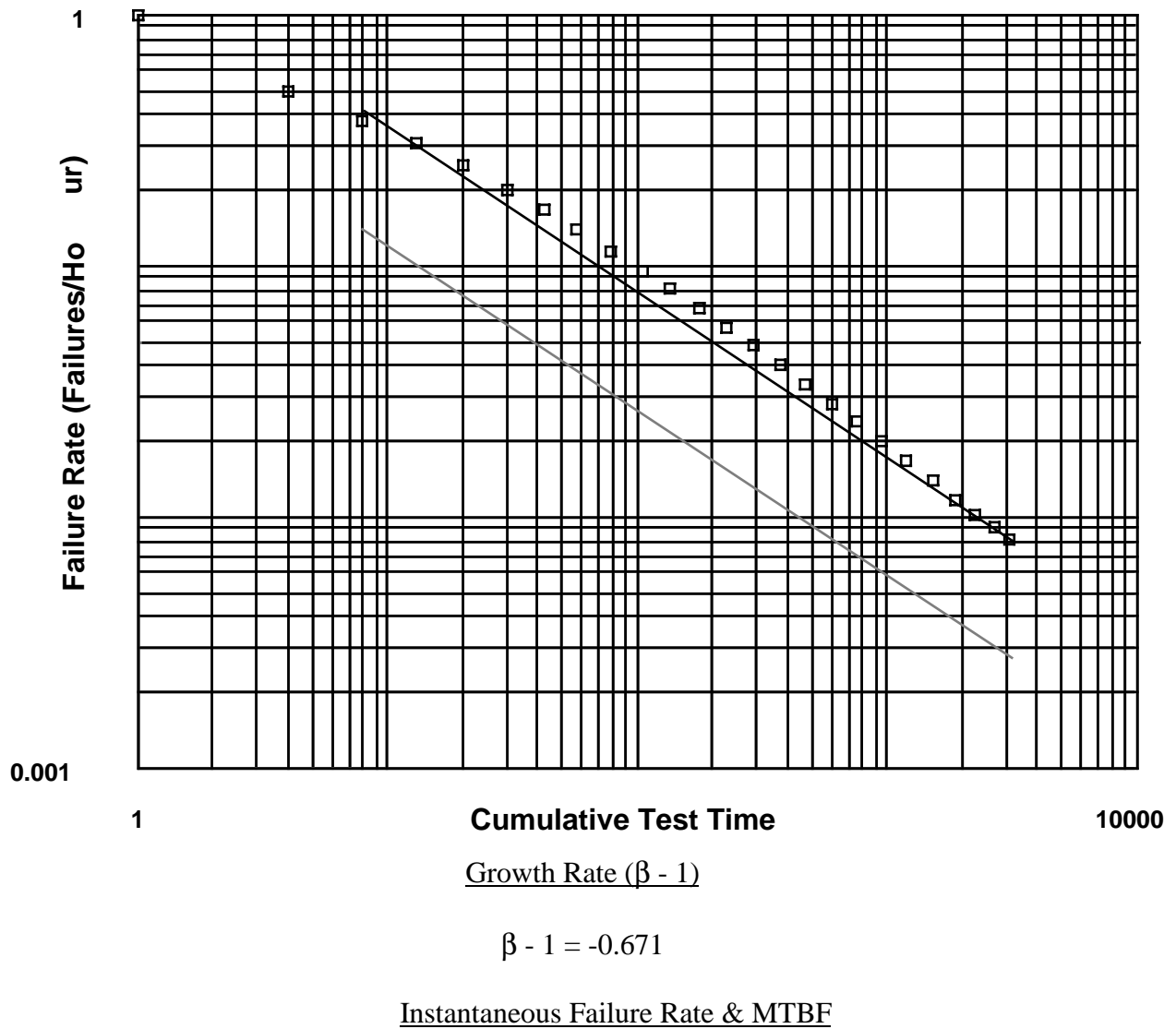
$$\frac{dF}{dt} = \lambda \beta t^{\beta-1} = r_i(t) \quad (8.40)$$

Therefore

$$\beta r_c(t) = r_i(t) \quad (8.41)$$

It can be seen that the parameter α used in the Duane Model is equivalent to $(1 - \beta)$ of the AMSAA Model.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH



$\lambda_{inst} = 0.003$ (F/Hr.)
 MTBF inst = 3,777.164 (Hrs.)

FIGURE 8.5-6: RELIABILITY GROWTH ANALYSIS (AMSAA MODEL)

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

The Duane plot uses a least squares estimate of where the plot would fall while the AMSAA Model takes into account the exponential relationship between each data plot. Therefore in reliability growth plotting, the AMSAA Model tends to give a more accurate representation of the reduction in failure rate with respect to time. However, the Duane Model is typically used for program planning purposes even by proponents of the AMSAA Model because of its inherent simplicity.

8.5.3.1 Other Growth Models

Parametric models imply that there is a pattern to the growth, while nonparametric models allow the growth curve to “fall where it will.” Because of this, only the parametric models are useful for mathematical descriptions of the generic or budgeted growth. Also, the nonparametric models generally do not allow growth projections to be made. However, either parametric or nonparametric models can be effectively used for controlling reliability growth.

Another consideration is the type of failure distribution that the growth model assumes. Many of the models treat the failure distribution in a nonparametric fashion. However, some models are based specifically on the assumption that the failure distribution is exponential.

Finally, although some of the models utilize a continuous time scale, others utilize a discrete scale, implying that the testing is performed in stages.

Although the Duane and the AMSAA reliability growth models have been the most widely used, a number of other models, both discrete and continuous, have been proposed in the literature.

8.5.4 Reliability Growth Testing

Reliability growth testing is the formal process of testing an equipment under natural and induced environmental conditions to discover and identify latent failure modes and mechanisms whose recurrence can be prevented through implementation of corrective action, thus causing the growth of equipment reliability.

These tests are conducted during the development phase on samples which have completed environmental tests prior to production commitment and do not replace other tests described in the contract or equipment specification. MIL-HDBK-781 contains the details on reliability growth test requirements, methods and procedures for application to electronic equipment.

8.5.4.1 When Reliability Growth Testing is Performed

The formal reliability growth test is usually performed near the conclusion of full scale development, concurrent with or after successful completion of environmental qualification testing and prior to reliability qualification (demonstration) testing. Although all testing should be viewed and planned as contributing to reliability growth, the formal test program dedicated to

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

reliability growth is normally deferred until after environmental qualification, when the design of the equipment reflects the anticipated configuration and manufacturing processes to be used in production, but prior to commitment to production. The hardware to be tested should have all significant fixes required as a result of environmental qualification testing incorporated before initiating the reliability growth test. The reliability growth test must be successfully concluded, and all significant fixes incorporated in the test hardware prior to initiating the reliability qualification (demonstration) test. The reliability growth test is for the purpose of detecting reliability problems after all performance design and environmental problems have been resolved. The reliability qualification (demonstration) test discussed in Section 8 is for the purpose of proving reliability.

8.5.4.2 Reliability Growth Approach

The MIL-HDBK-781A (Ref. [18]) approach to reliability growth is patterned after the Duane and the AMSAA Models. With the Duane Model the change in MTBF during development is proportional to T^α where T is the cumulative operating time and " α " is the rate of growth corresponding to the rapidity with which faults are found, and changes are made to permanently eliminate the basic causes of the faults observed.

In order to structure a growth test program (based on the Duane Model) for a newly designed system, a detailed test plan is necessary. This plan should describe the test-analyze-fix concept, and show how it will be applied to the system under development. The plan should incorporate the following:

- (a) Values for specified and predicted (inherent) reliabilities. Methods for predicting reliability (model, data base, etc.) should also be described.
- (b) Criteria for reliability starting points, i.e., criteria for estimating the reliability of initially fabricated hardware, should be determined. For avionics systems, the initial reliability for newly fabricated systems has been found to vary between 10% and 30% of their predicted (inherent) values.
- (c) The reliability growth rate (or rates) should be defined. To support the selected growth rate, the rigor with which the test-analyze-fix conditions are structured should be completely defined.
- (d) Calendar time efficiency factors, which define the relationship of test time, corrective action time and repair time to calendar time, should be determined.

Note that each of the factors listed above impacts the total time (or resources) which should be scheduled to grow reliability to the specified value. Figure 8.5-2 (repeated here as Figure 8.5-7) illustrates the concepts described above.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

In addition, Figure 8.5-7 graphically depicts the four elements needed to structure and plan a growth test program such as is described above. These four elements are further described as follows:

- (a) Inherent Reliability: Represents the value of design reliability estimated during prediction studies, which may correspond to the value above that specified in procurement documents. Ordinarily, the contract specified value of reliability 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.
- (b) Starting Point: Represents an initial value of reliability for the newly manufactured hardware. This usually falls within the range of 10% to 30% of the inherent or predicted reliability. Estimates of the starting point can be derived from prior experience or are based on percentages of the estimated inherent reliability. Starting points should 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, when justified, minimize test time.

Determination of the starting point is often difficult, with little documented guidance available. The following prioritized list provides the recommended procedures for establishing the starting point.

- (1) Use actual data on early design
- (2) Use the results of past reliability growth test and reliability prediction results
- (3) Compute the default ratio (i.e., 10%) of the initial MTBF divided by the MTBF prediction

The first option is to use actual reliability data (i.e., failures, test time) recorded on the system during its early life. The design team necessarily tests the early design as a natural part of the design/development process. This testing is often informal with little standardized or documented reliability reports/data. Nevertheless, this type of data typically exists and it is most indicative of the actual MTBF of the system prior to reliability growth testing. The initial MTBF is computed as the cumulative amount of test time divided by the cumulative number of failures. To obtain this type of data and apply it to develop a planned reliability growth curve, requires a high degree of cooperation and sharing of information between the various engineering disciplines at an organization.

In many instances, this first option is not viable because the requisite data simply cannot be retrieved or the planned growth curve is needed as part of a proposal or early design document before any design activities take place.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

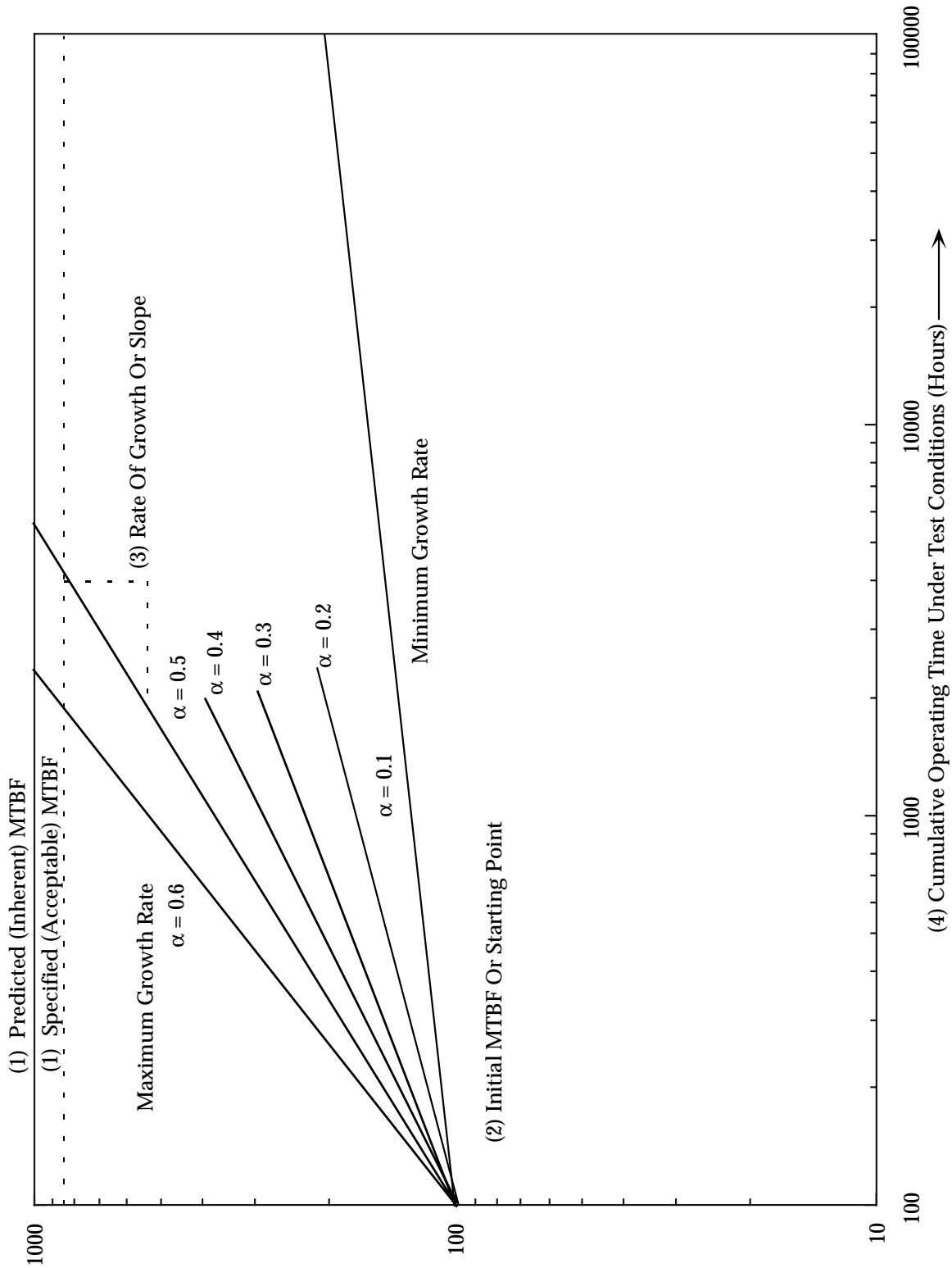


FIGURE 8.5-7: RELIABILITY GROWTH PLOTS

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

The second recommended option involves the use of results of prior reliability growth tests. These results must be from the same organization and indicative of the TAAF philosophy to be enacted. The degree of reliability growth or growth potential is not an inherent design parameter but is dependent on the management philosophy adopted for reliability growth testing. An aggressive management philosophy which is dedicated to seeking out the root-cause of failure and determining effective design fixes will be much more successful than testing programs with a less aggressive approach.

The following example indicates how to use this past data on reliability testing. A 250 hour pre-conditioning period was assumed to determine the actual starting point. It is important to distinguish between the planned and the actual MTBF starting point. Once the test has been conducted and the actual data are available, an actual starting point can be computed, which may differ from what was planned.

MTBF Prediction (MIL-HDBK-217)	Final Test MTBF (MTBF _{inst} at Test Conclusion)	Initial MTBF (at 250 hours)	Initial MTBF/ MTBF Prediction
2,200	2,000	410	.19
800	610	84	.11
1,000	1,100	90	.09
920	830	220	.24
1,550	1,400	310	.20

It is necessary to compute the ratio of the initial MTBF (at the assumed 250 hour pre-conditioning period) divided by the MTBF prediction per MIL-HDBK-217. In the example, the ratio ranges from .09 to .24. In practice, it has been found that these ratios typically range from .10 to .30. In the example, the average ratio is .17.

The next step is to multiply the computed ratio by the MTBF prediction. If the equipment to undergo the reliability growth test has an MTBF prediction of 5,000 hours, then the estimated starting point would be,

$$\text{MTBF}_{\text{starting point}} = (.17)(5,000) = 850 \text{ hours}$$

The final and least preferred option is to apply a default ratio of .10. It has been found that use of this ratio yields a conservative estimate of the starting point. It needs to be recognized that this estimate is not precise; however, it provides a starting point if no other approach is viable. Again, using the 5,000 hour MTBF estimate, the starting point would be,

$$\text{MTBF}_{\text{starting point}} = (.10)(5,000) = 500 \text{ hours}$$

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

- (c) Rate of Growth: Is depicted by the slope of the growth curve. This, in turn, is governed by the amount of control, rigor, and efficiency by which failures are discovered, analyzed, and corrected through design and quality action. Test programs which 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.
- (d) Calendar Time/Test Time: Represents the efficiency factors associated with the growth test program. Efficiency factors include repair time, and operating/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 8.5-7 shows that the value of the parameter “ α ” can vary between 0.1 and 0.6. A growth rate of 0.1 can be expected in those programs where no specific consideration is given to reliability. In those cases, growth is largely due to solution of problems impacting production, and from corrective action taken as a result of user experience. A growth rate of 0.6 can be realized if an aggressive, hard-hitting reliability program with management support is implemented. This type of program must include a formal stress-oriented test program designed to aggravate and force defects and vigorous corrective action.

Figure 8.5-7 also shows the requisite hours of operating and/or test time and the continuous effort required for reliability growth. It shows the dramatic effect that the rate of growth has on the cumulative operating time required to achieve a predetermined reliability level. For example, Figure 8.5-7 shows, for an item product whose MTBF potential is 100 hours, that 100,000 hours of cumulative operating time is required to achieve an MTBF of 200 hours when the growth rate is 0.1. And, as previously stated, a 0.1 rate is expected when no specific attention is given to reliability growth. However, if the growth rate can be accelerated to 0.6 (by growth testing and formal failure analysis activities) then only 300 hours of cumulative operating time is required to achieve an MTBF of 200 hours.

Some general guidance on reliability growth test time is as follows:

Fixed-length test times of 10 to 25 multiples of the specified MTBF will generally provide a test length sufficient to achieve the desired reliability growth for equipment in the 50 to 2000 hour MTBF range. For equipments with specified MTBFs over 2000 hours, test lengths should be based on equipment complexity and the needs of the program, but as a minimum, should be one multiple of the specified MTBF. In any event, the test length should not be less than 2000 hours or more than 10,000 hours.

Where time is not an appropriate measurement parameter for the particular hardware, the Duane Model is adaptable to other measurement parameters such as cycles, events, rounds, etc.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH8.5.4.3 Economics of Reliability Growth Testing

The purpose of reliability growth testing is simple: to save money during the planned service life of the equipment. Experience has shown that an investment in assuring that specified reliability is, in fact, achieved prior to production will result in significantly-reduced life-cycle costs over the planned service life of the equipment due to savings realized by fewer maintenance actions, fewer required spares, and less handling damage, among others. This relationship is illustrated in Figure 8.5-8.

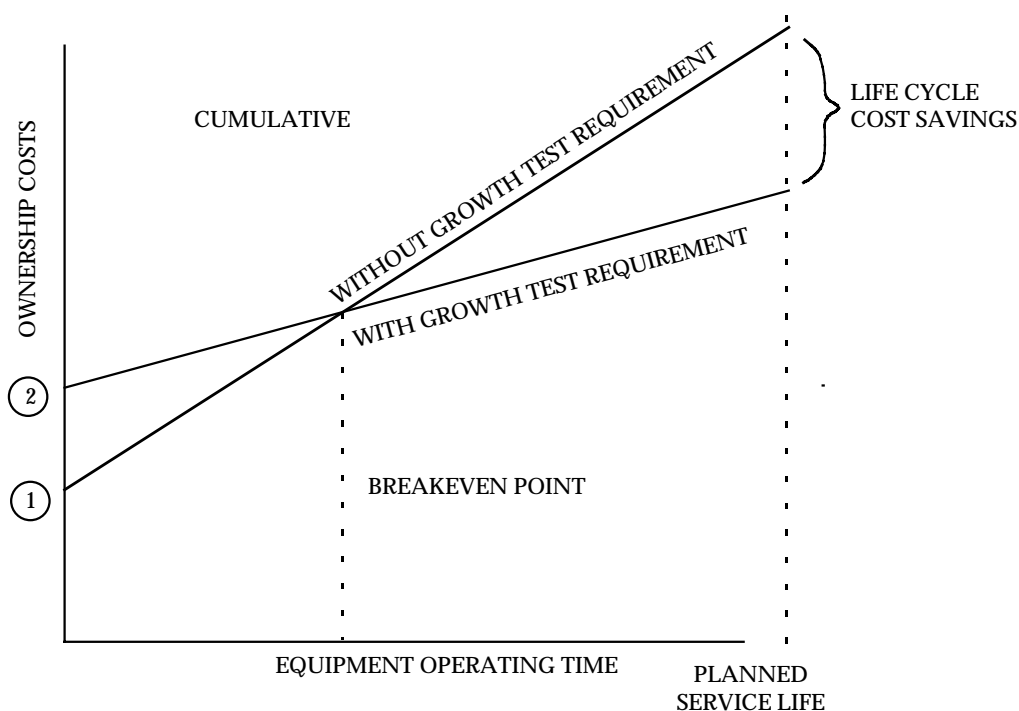


FIGURE 8.5-8: COMPARISON OF CUMULATIVE LIFE CYCLE COSTS WITH AND WITHOUT SPECIFIED RELIABILITY GROWTH TEST REQUIREMENTS

Point (1) represents the acquisition cost of an equipment without a reliability growth test requirement and a delivered MTBF (based on post-production experience) considerably less than the specified MTBF for that equipment. The cumulative cost of ownership rises with equipment operating time to account for equipment repairs and spares support over the life of the equipment.

Point (2) represents the acquisition cost of the same equipment, with the added cost of the reliability growth test program to achieve specified MTBF as a delivered MTBF. The cumulative cost of ownership with equipment operating time increases at a slower rate than the previous case due to less frequent repairs and reduced spares support requirements until a breakeven point is reached. At this point the growth test program has paid for itself and the difference in costs due

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

to the reliability growth program represents a life-cycle cost savings.

8.5.5 Reliability Growth Management

Reliability growth management is the systematic planning for reliability achievement as a function of time and other resources and is used for controlling the ongoing rate of achievement by reallocation of resources based on comparisons between planned and assessed reliability values.

Reliability growth management is part of the system engineering process. It does not take the place of the other basic reliability program activities such as predictions, apportionment, failure mode and effect analysis, and stress analysis. Instead, reliability growth management provides a means of viewing all the reliability program activities in an integrated manner.

It is imperative to recognize that a total reliability program is needed for effective reliability growth management. While it is generally recognized that reliability will grow in the presence of a reliability program, reliability growth planning provides an objective yardstick and an orderly means of measuring progress and directing resources so that reliability requirements may be achieved in a timely and cost effective manner. A good reliability growth plan can greatly improve the chances of achieving total reliability program objectives. However, it is not intended to be the total reliability program.

MIL-HDBK-189 provides procuring activities and development contractors with an understanding of the concepts and principles of reliability growth, advantages of managing reliability growth, and guidelines and procedures to be used in managing reliability growth. It should be noted that this Handbook is not intended to serve as a reliability growth plan to be applied to a program without any tailoring. The Handbook, when used with knowledge of the system and its development program, will allow the development of a reliability growth management plan that will aid in developing a final system that meets its requirements and lowers the life cycle cost of the fielded systems.

8.5.5.1 Management of the Reliability Growth Process

There are innumerable ways in which reliability can grow during development. There are, of course, only a finite number of reliability growth models available. Consequently, acquisition managers cannot conduct their development programs in just any fashion, and have an existing reliability growth model available for estimation and prediction purposes. The manner in which the development program is managed and the choice of the reliability growth model are, therefore, dependent. Essentially, there are two ways by which acquisition managers can evaluate the reliability growth process.

- (a) They may monitor the various reliability oriented activities (FMEA's, stress analysis, etc.) in the growth process to assure themselves that the activities are being

 SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

accomplished in a timely manner and that the level of effort and quality of work is appropriate. This is a qualitative approach.

- (b) They may utilize assessments (quantitative evaluations of the current reliability status) that are based on information from the detection of failure sources.

The assessment approach is, preferable in that it is results-oriented, in the form of quantitative estimates of planned and achieved reliability as the program progresses.

Figure 8.5-9 illustrates how assessments may be used in controlling the growth process. One of the more important points to emphasize is that assessments have been a way of life in reliability work for many years, as have the resultant decisions.

What, then, is new about reliability growth management? What is new is a formal standard against which the assessment may be compared. The fact that managers in the past have made decisions based on assessments implies that they had at least a subjective standard of acceptable reliability growth against which to make comparison. A formal, objective standard has the advantage of remaining constant, unless formally changed, rather than bending in the hope that “tomorrow will be better.”

Figure 8.5-10 illustrates an example of a reliability growth curve, showing both the budgeted (planned) reliability growth and assessments. A comparison between the assessment and the budgeted value will suggest whether the program is progressing as planned, better than planned, or not as well as planned. Based upon the first two data points of assessed growth, the decision would probably be made to continue development with no changes. If reliability progress is falling short, as the two subsequent assessed data points indicate, new strategies should be developed. These strategies will probably involve the reassignment of resources to work on identified problem areas. They may, as a last resort, result in adjustment of the time frame, or relaxation of the original requirement.

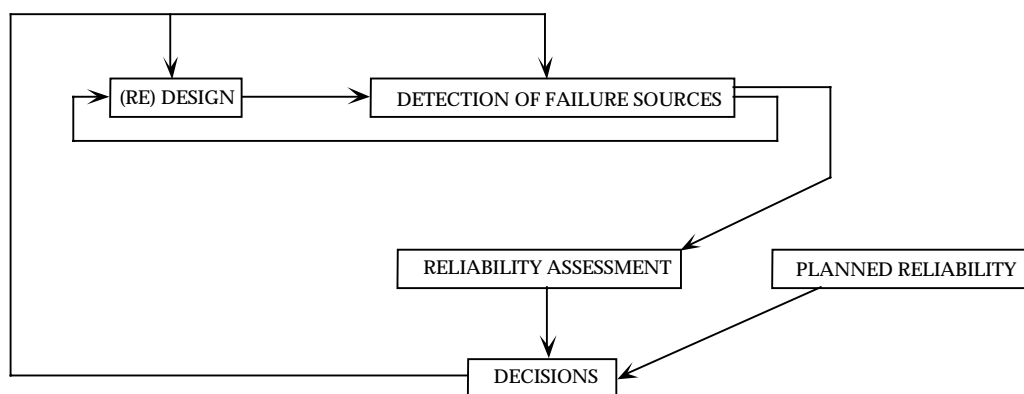


FIGURE 8.5-9: RELIABILITY GROWTH MANAGEMENT MODEL (ASSESSMENT)

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

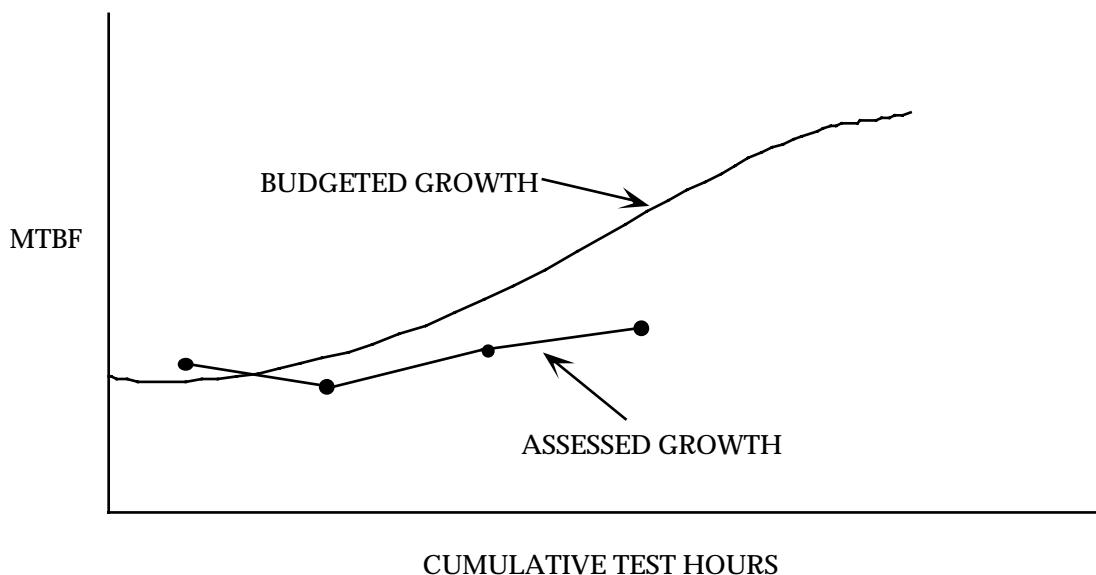


FIGURE 8.5-10: EXAMPLE OF A RELIABILITY GROWTH CURVE

 8.5.5.2 Information Sources That Initiate Reliability Growth

The detection of failure sources is the activity that effectively initiates the growth process by pointing the way for redesign. Because the information sources that are used for detecting failure sources are so varied and because they can be relied on at different times during the life cycle, great program flexibility is possible. Although the total number of information sources that can be used to initiate reliability growth is rather large, they can be grouped into five categories: external experience, analysis, tests, production experience, and operational experience.

- (a) External Experience. This is information generated outside the specific development program which has applicability within the program. Examples of this type of information are historical data, publications, technical experience of personnel, and information from currently operating systems.
- (b) Analysis. This is information generated within the specific development program, excluding the test of hardware. Examples are feasibility studies, probabilistic reliability design, failure mode and effect analysis, and design reviews.
- (c) Tests. Although this source of information is self-explanatory, the various ways in which testing is performed are important considerations. The hardware may be in any level of maturity, ranging from breadboard to final production configurations. Various levels of assembly may be tested, ranging from components to system level. Finally, the environmental conditions can vary all the way from testing under ambient conditions to overstress or accelerated testing. Testing is the most common source of information for initiating growth; it is the source usually modeled because it yields

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

objective measurements.

- (d) Production Experience. The production process itself may identify weak areas in the design.
- (e) Operational Experience. The use of fielded systems will identify design deficiencies which point the way toward reliability growth.

8.5.5.3 Relationships Among Growth Information Sources

The chronological relationship of these information sources is illustrated in Figure 8.5-11. This figure illustrates that growth is at least possible at any point in the life cycle. However, what are the relative merits of growing reliability at these various points? To a large extent, this question can only be answered with respect to a specific development program. But there are two fundamental considerations that must be made. First, changes can be accomplished very economically early in the life cycle. The example usually given is that a change which would cost \$1 on the drawing board will end up costing about \$100 if it is made after the equipment is fielded. Therefore, it is desirable to grow reliability as early as possible. However, the information upon which early changes are based tends to contain many unknown factors, such as operational conditions and component interactions. Second, changes which are made later in the life cycle tend to be better directed, as there are fewer unknowns in the information as hardware maturity nears. The two desired characteristics will be referred to as “timeliness” and “credibility.”

EXTERNAL EXPERIENCE

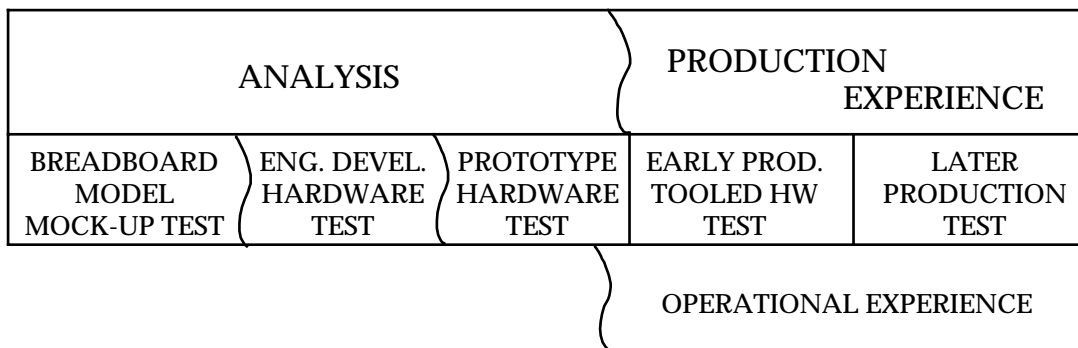


FIGURE 8.5-11: INFORMATION SOURCES THAT INITIATE RELIABILITY GROWTH

Depending on the characteristics of the specific program and system, it may be desirable to place particular emphasis on certain combinations of these information sources. In effect, we would like to achieve a reasonable combination of timeliness, credibility, and economy. The following

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

paragraphs give some suggestions about when it may be desirable to place emphasis on various types of information sources. The rationale that is given here could serve as a basis for a more formal economic model for specific applications. The suggestions that are given here are intended to point out those information sources which have the strongest potential under varying situations. A good program would probably utilize all of the information sources to some degree, but the mix and emphasis will vary from one program to the next.

- (a) Reliability Growth Through External Experience. The strongest feature of external experience is that it may be available at the very beginning of the life cycle, thus emphasizing timeliness. This, of course, assumes that appropriate external experience is available.
- (b) Reliability Growth Through Analysis. Analysis becomes particularly valuable when the system reliability is high, mainly because the next best alternative, testing, will tend to be time-consuming and, therefore, expensive. However, in order to be able to rely heavily on analysis, much detailed knowledge is necessary. The operation of the system must be well understood. This implies that the development must be reasonably within the state-of-the-art. There must be good, detailed knowledge of the environment and use conditions. Finally, appropriate design analysis techniques must either be available or specially developed and there must be a good information base to support these techniques. Many reliability programs put too little emphasis on analysis and the associated information base. One problem with a reliance on analysis is that the effects cannot be measured objectively.
- (c) Reliability Growth Through Testing. Reliability growth models are generally based on test results. Therefore, testing is a very important information source for initiating reliability growth. Testing will have the greatest payoff if many failures are encountered which can be thoroughly analyzed. Therefore, a low system reliability and an inability to perform failed part analysis suggest strong emphasis be placed on testing. One other factor which must be considered is the cost of testing itself. High test costs may discourage strong reliance on testing to achieve growth. However, generally there is no valid substitute for a good test program in the reliability growth process.
- (d) Reliability Growth Through Production Experience. The production process and its quality controls are major contributors to reliability. In fact, a drop in reliability during the transition from development to production is a common phenomenon. It then becomes necessary to grow reliability based on manufacturing process redesign and/or better quality controls. Many process and control problems can be eliminated during the production phase through the use of process capability studies, worst-case analyses, and similar producibility-related techniques. Moreover, it is unlikely that all process and control problems could be eliminated during pre-production; and almost certainly, the payoff from these techniques, expressed as a function of effort, would show a diminishing-returns pattern. It is almost inevitable that some problems can be more

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

cost-effectively eliminated after production starts, particularly when the production run is relatively long and the tooling is relatively inexpensive.

- (e) Reliability Growth Through Operational Experience. Although some reliability growth through operational experience is inevitable, this method is the least desirable of the five sources listed. Improving reliability through retrofitting of fielded systems often costs up to a hundred times as much as the same change made on the drawing board.

8.6 Summary of the Differences Between Reliability Growth Testing and Reliability Demonstration Testing

Reliability growth is the result of an iterative design process. As the design matures, it is investigated to identify actual (via testing) or potential (via analysis) sources of failures. Further design effort is then spent on correcting these problem areas. The design effort can be applied to either product design or manufacturing process design. There are three essential elements involved in achieving reliability growth:

- (1) Detection of failure sources (by analysis and test)
- (2) Feedback of problems identified
- (3) Effective redesign effort based on problems identified

Reliability demonstration tests, on the other hand, are designed for the purpose of proving, with statistical confidence, a specific reliability requirement; not specifically to detect problems, or to grow reliability. The test takes place after the design is frozen and its configuration is not allowed to change. However, in practice, some reliability growth may occur because of the deferred correction of failures observed during the test.

Reliability demonstration is specified in most military system procurement contracts and involves, in many instances, formal testing. Demonstration tests are normally conducted after development has been completed but before high rate production has been initiated. Demonstration tests are normally conducted after growth tests in the development cycle using initial production hardware.

As previously indicated, reliability demonstration testing, carries with it certain statistical confidence levels, and the more demonstration testing, the more confidence. The more reliability growth testing that is performed, the higher the actual reliability. Depending on 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. Option two minimizes reliability growth testing with a resultant lower MTBF at higher confidence. These concepts are shown graphically in Figure 8.6-1.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

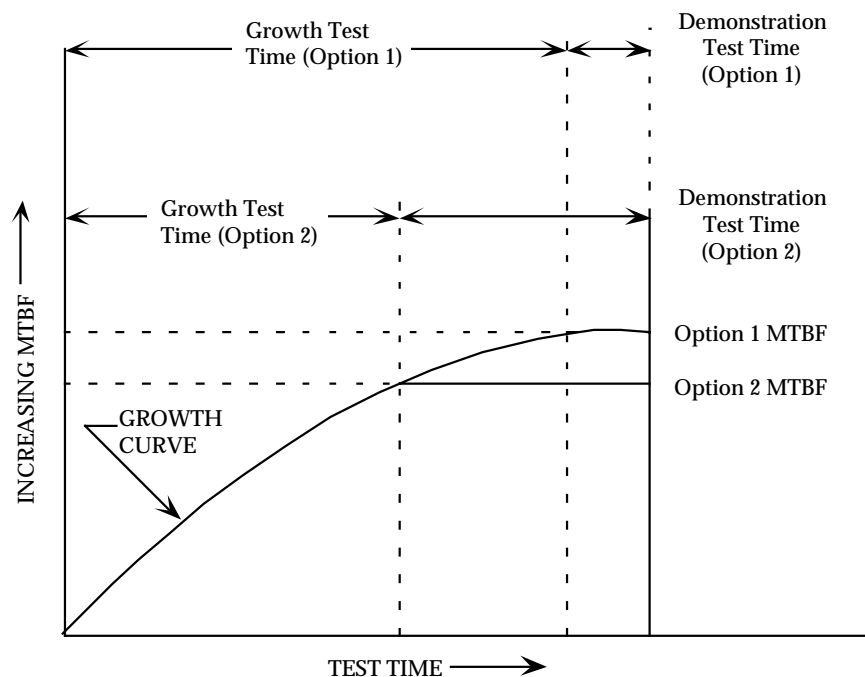


FIGURE 8.6-1: RELIABILITY TESTING OPTIONS

8.7 Accelerated Testing

Although accelerated testing is commonly used today, it frequently means different things to different people. There are potentially two main reasons for performing an accelerated test. These are: a) life estimation or b) problem/weakness identification (or confirmation) and correction. The difference between these reasons, although subtle, can have a very significant impact upon the underlying assumptions upon which the test is based, the models utilized in constructing the test, the test equipment and chambers used, the way in which the test itself is conducted, and the manner in which the resulting data is analyzed and interpreted.

Accelerated Life Testing is the means by which length of life can be determined. Here the primary focus is on estimating the life of an item under “normal” operating conditions, based upon data obtained under much more severe conditions. In this case, the failure mechanism is usually well documented and understood; thus, problem identification and correction is of secondary importance.

Accelerated Stress Testing is used to identify problems and weaknesses inherent in the design, the parts used, or the manufacturing process so that they can be subsequently fixed. This is done by changes in: the design itself, the parts used, or the manufacturing processes employed. A thorough understanding, or at least a workable knowledge, of the basic failure mechanisms is the focus of attention here, estimation of item life may, or may not, be a concern.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

Accelerated testing attempts to get more reliability information from a given test time using a test environment that is more severe than that experienced during normal equipment use, however:

Accelerated testing must always be approached with due caution. There are basic limitations to the technique. Every accelerated test application is unique. Subtle differences in the application can totally invalidate the data recorded during the test or the conclusions reached by the test.

This unfortunate outcome can occur, for example, if the operating range of validity for a given model is exceeded; or if the underlying test/modeling assumptions, while true for most applications, are not valid for a given specific application. Therefore, it is frequently necessary to first perform a preliminary accelerated test to validate the theory for a given application and then determine the applicable relationship (if not already available in the literature) between the applied stress and the resulting acceleration of the associated degradation. This preliminary accelerated test could also be viewed as a “sanity check.”

Given these caveats, accelerating factors which may be used, either singly or in combination, include:

- More frequent power cycling
- Higher temperatures
- More severe temperature cycling
- Higher vibration levels
- Higher humidity

A second very important confounding factor in accelerated testing is the equipment level at which the test is performed. Some accelerating techniques are appropriate only for part level testing, while others can be used only for higher levels of assembly, and a very few techniques may be applicable for both part level and assembly level. The underlying assumptions and modeling approaches which may be perfectly legitimate at the part level may be totally invalid for tests performed on higher level equipment and vice-versa.

In addition to the primary purposes of accelerated testing, it also may be useful for:

- Identifying reliability problems in a chosen design
- Comparing the reliability of competing designs
- Acceptance testing
- Environmental Stress Screening
- Verifying the elimination of a given problem, etc.

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

8.7.1 Accelerated Life Testing

Accelerated life testing requires the use of a model relating the reliability (or life) measured under high stress conditions to that which is expected under normal operation. These tests require: (a) an understanding of the anticipated failure mechanism(s) and (b) a knowledge of the magnitude of the acceleration of this failure mechanism, as a function of the accelerating stress. In most cases appropriate acceleration factors can be obtained from a study of the literature, but in some cases new models may have to be developed. This will probably involve a significant investment of time and money.

It is very important, however, that the range of validity of a given acceleration model not be exceeded and that the accelerating stress change only the rate of failure and not the type of failure experienced. If an accelerated test introduces a new failure mechanism that will never be experienced in normal use, it may lead to false conclusions and possibly to unnecessary design changes. For this reason it is very beneficial to continue the accelerated life test until at least a minimum number of failures have occurred. Post mortem analysis will verify that the anticipated failure mechanism is indeed occurring, and that no new, different failure mechanisms have been introduced.

8.7.2 Accelerated Stress Testing

The main objective of a stress test is to convert latent defects or design weaknesses into actual failures, that is, to identify design, part and manufacturing process problems which could cause subsequent failures in the field. Time compression can frequently be realized by accelerating the environmental stress applied during the test, just as time compression is obtained during accelerated life testing. This same approach may be used both during development tests and during Environmental Stress Screening (ESS).

8.7.3 Equipment Level Accelerated Tests

Accelerated testing of equipment is usually quite limited. Creating a valid model relating the rate of equipment failures at a high stress - to that at normal operating conditions - is extremely difficult. Likewise it is very difficult to formulate stress conditions that do not change the failure mechanisms occurring within the equipment.

One example of an accelerated test that can be used effectively on equipment is that of increasing the duty cycle. Take for example an equipment normally operated at some given duty cycle, e.g., running only during one shift, or avionics equipment operating only a few hours before and during a flight. In such cases a higher duty cycle could easily be used during the test. The system undergoing test could be operated continuously for three shifts a day or the avionics equipment might be cycled continuously, with only enough time between simulated flights to permit the temperature within the equipment to stabilize during non-operating conditions. Although the failure rate per operating hour does not change, the number of failures accrued per day is

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

increased.

This type of accelerated testing is commonly done in reliability qualification test, and although it is not usually recognized as such, this is actually a form of accelerated testing.

Another example of equipment level accelerated testing is ESS. In this case equipment is often subjected to higher stresses, particularly thermal cycling and vibration, as part of the ESS program. Here the purpose of the stresses are to detect defects induced into the equipment during the manufacturing process, e.g., weak solder joints, etc. Assuming that each defect is removed when it is discovered, with ESS there is no need of a model to correlate the rate of failure under stress to the rate of failure under normal operation.

Given these specific exceptions, accelerated testing is seldom applied at the equipment level. However, accelerated testing is an extremely important concept for component testing.

8.7.4 Component Level Accelerated Test

Components (parts) tend to have many fewer failure modes than equipment. Thus it is far easier to identify a stress which can be effectively accelerate the rate of failure without seriously changing the failure mechanism.

There is usually one or more dominant failure mechanisms accelerated by a given stress, e.g., dielectric breakdown of capacitors as a function of voltage, or corrosion as a function of humidity. In this case it is usually relatively easy to find an acceleration model relating failure rate as a function of operating stress. For this reason accelerated life testing is used extensively for components and the technique is highly recommended for most types of parts and for most part applications.

8.7.5 Accelerated Test Models

Accelerated test models relate the failure rate or the life of a component to a given stress such that measurements taken during accelerated testing can then be related back to the expected performance under normal operating conditions. The implicit working assumption here is that the stress will not change the shape of the failure distribution.

Three of the most commonly used acceleration models are:

1. Inverse Power Law
2. Arrhenius Acceleration Model
3. Miner's Rule

These are not the only models that exist, there are other models as well. The most important factor of concern is the correct choice of the model. The model chosen must be one that

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

accurately models the reliability or life under the accelerated conditions to reliability or life under normal operating conditions. Great care is essential in choosing the most appropriate model and in selecting the appropriate range of validity for the chosen model in a specific application. Documenting the rationale for these choices is important.

8.7.5.1 The Inverse Power Law Acceleration Model

The inverse power law states that component life is inversely related to a power of the dominant stress.

$$\frac{\text{Life at normal stress}}{\text{Life at accelerated stress}} = \left(\frac{\text{Accelerated stress}}{\text{Normal stress}} \right)^N \quad (8.42)$$

where N is the acceleration factor.

Assuming that an application is within the valid operating range of the model and that the shape of the failure distribution does not change under accelerated conditions, the inverse power law model can be used to solve such problems as the following.

Example: Suppose the mean life of a population of automobile tires was 20,000 miles when driven at 50 miles per hour. Through testing it has been determined that the mean life of these tires is 10,000 miles at 70 miles per hour. Thus:

$$\frac{20,000}{10,000} = \left(\frac{70}{50} \right)^N \quad \text{Hence: } N = 2.06$$

From this knowledge, we want to use life data collected at 70 mph to show that there is a 90% probability that a tire will last 10,000 miles at 50 mph.

To solve this problem, use the life test data at 70 mph to demonstrate, with a 90% probability, that a tire will last 10,000 miles at 50 mph.

$$\text{Given: } \frac{\text{Life at 50 mph}}{\text{Life at 70 mph}} = \left(\frac{70}{50} \right)^{2.06}$$

Desired result: 90% probability of no failure before 10,000 miles, i.e., no more than 10% of a population fails before 10,000 miles.

The shape of the failure distribution is assumed to be identical at 50 and 70 mph, thus the left side of the inverse power law equation shown above can be used to represent life at 10% failures, or:

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

$$\frac{\text{Life at 10\%, failures at 50 mph (10,000 miles desired)}}{\text{Life at 10\% failures at 70 mph}} = \left(\frac{70}{50}\right)^{2.06}$$

Thus: Life at 70 mph = 10,000/2 = 5,000

Therefore, if 10% or less of the tires tested at 70 mph fail by 5,000 test miles, we can conclude that 10% or less of tires driven at 50 mph will fail in 10,000 miles. Thus we have a 90% probability that a tire will last 10,000 miles at 50 mph.

8.7.5.2 The Arrhenius Acceleration Model

The Arrhenius acceleration model is widely used to predict life as a function of temperature. It applies specifically to those failure mechanisms that are temperature related and which are within the range of validity for the model.

It states that : $\text{Life} = A(e)^{\frac{E}{T}}$ (8.43)

where:

- Life = a measure of life e.g., median life of a population of parts
- A = a constant determined by experiment for the parts involved
- e = the base of the natural logarithms
- E = activation energy (electron volts - a measure of energy) this is a unique value for each failure mechanism (Examples of the activation energies for some silicon semiconductor failure mechanisms are shown in Table 8.7-1.)
- k = Boltzman's constant = 8.62×10^{-5} eV/K
- T = Temperature (Degrees Kelvin)

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTHTABLE 8.7-1: ACTIVATION ENERGIES ASSOCIATED
WITH VARIOUS SILICON SEMICONDUCTOR FAILURE MECHANISMS

DEVICE ASSOCIATION	FAILURE MECHANISM	RELEVANT FACTORS*	ACCELERATING FACTORS*	ACCELERATION (E_A APPARENT ACTIVATION ENERGY)
Silicon Oxide And Silicon-Silicon Oxide Interface	Surface Charge Accumulation Dielectric Breakdown Charge Injection	Mobile Ions V, T E, T E, T	T E E, T	Bipolar: $E_A = 1.0-1.05eV$ MOS: $E_A = 1.2-1.35eV$ $E_A = 0.3-2.0 eV$ $E_A = 1.3eV$ (Slow Trapping) $E_A = 1.2eV$ "P" Channel $E_A = 1.05eV$ "N" Channel
Metallization	Electromigration Corrosion Chemical Galvanic Electrolytic Contact Degradation	T, J, A Gradients of T and J Grain Size Contamination Humidity (H) V, T T, Metals Impurities	T, J H, V, T Varied	$E_A = 0.5-1.2eV$ J to J^4 $E_A = 0.3eV$ Small Grain Size 0.5eV Typical Al 0.9eV Contact Windows Strong H Effect $E_A = 0.3-0.6eV$ (for V may have thresholds $E_A = 0.9eV$
Bonds and Other Mechanical Interfaces	Intermetallic Growth Fatigue	T, Impurities Bond Strength Temperature Cycling, Bond Strength	T T Extremes in Cycling	Al • Au: $E_A = 1.0-1.05eV$ $E_A = 0.3-1.0eV$
Hermeticity	Seal Leaks	Pressure Differential Atmosphere	Pressure Temperature Cycling	

* V - Voltage
T - Temperature

E - Electric Field
J - Current Density

A - Area
H - Humidity

“A” and “E” are typically calculated from test data using graphical methods. Special Arrhenius graph paper with a logarithmic life vertical scale and an inverse absolute temperature horizontal scale (in degrees Centigrade) is used. A straight line plot on this paper supports the assumption that an Arrhenius relationship holds (see Figure 8.7-1).

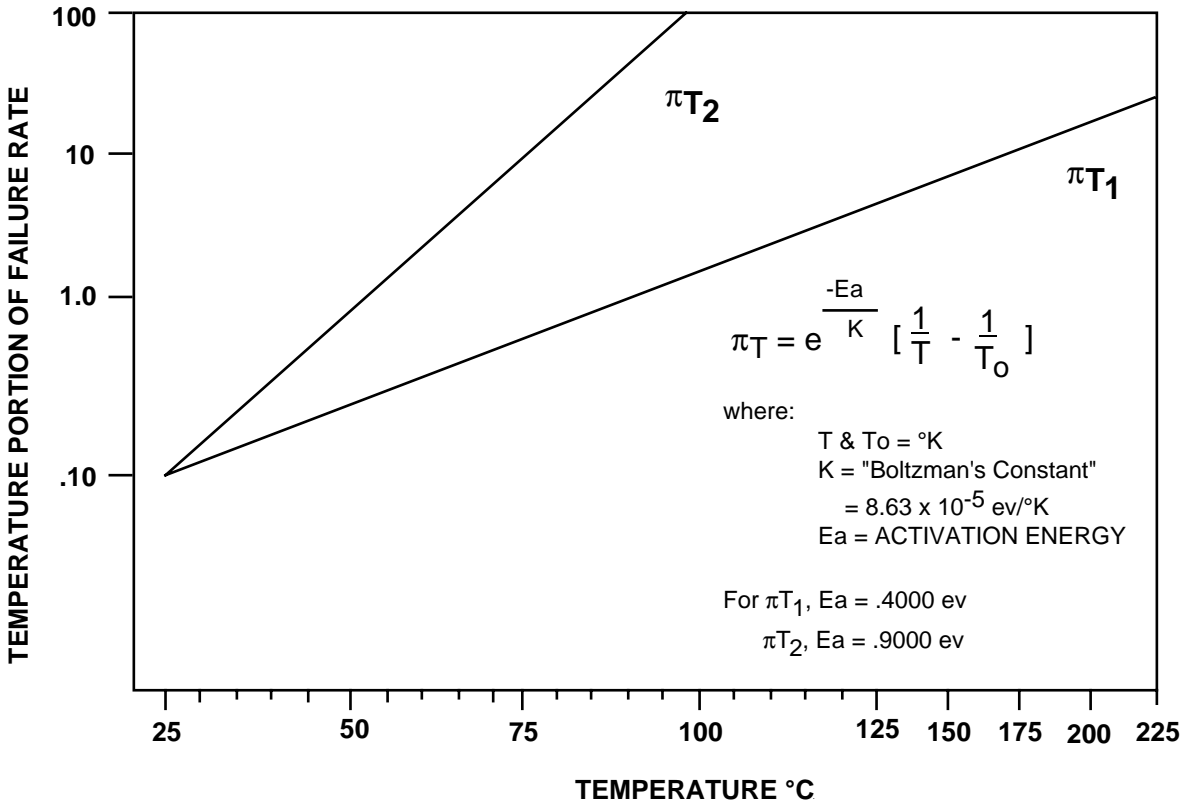
SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

FIGURE 8.7-1: ARRHENIUS ACCELERATION MODEL

8.7.5.3 Miner's Rule - Fatigue Damage

Quantification of metal fatigue under the varying load conditions which an item sees in service is frequently a major design concern. Fatigue researchers have proposed various cumulative damage models. The simplest of these models is Miner's rule. Miner's rule states that cumulative damage (CD) is:

$$CD = \sum_{i=1}^k \frac{C_{S_i}}{N_i} \leq 1 \quad (8.44)$$

where:

- C_{S_i} = number of cycles applied at a given mean stress S_i
- N_i = the number of cycles to failure under stress S_i, (as determined from an S-N diagram for that specific material)
- k = the number of loads applied

SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
DEMONSTRATION, AND GROWTH

Thus it is assumed that at the end of life (point of failure) $CD = 1$.

Miner assumes that every part has a finite useful fatigue life and every cycle uses up a small portion of that life. Failure is likely to occur when the summation of incremental damage from each load equals unity. (Miner's rule does not extend to infinity, however. It is valid only up to the yield strength of the material, beyond that point it is no longer valid.)

We can then construct an accelerated fatigue test by combine Miner's Rule with the previously discussed inverse power law. The inverse power law (equation 8.42) stated that the damage-accumulation rate is proportional to a power of the current stress. Thus:

$$\left[\frac{\text{Life at normal stress}}{\text{Life at accelerated stress}} \right] = \left[\frac{\text{accelerated stress}}{\text{normal stress}} \right]^N$$

where:

N = the acceleration factor derived from the slope of the S-N curve

Accelerated cumulative fatigue damage could therefore be calculated by combining Miner's rule (equation 8.44) and the power law (equation 8.42). Thus from equation 8.45:

$$CD = \sum \frac{C_{s_i}}{N_i}$$

and from equation 8.42, for accelerated stress causing failure in one cycle:

$$\frac{N_i}{1} = \left(\frac{S_1}{S_i} \right)^\alpha$$

where:

- α = N from the inverse power law = material dependent parameter (slope of the S-N curve)
- N_i = the number of cycles to failure under stress S_i
- S_i = stress level associated with N_i cycles
- S_1 = stress level required for failure in 1 stress reversal

Thus:

$$CD = \sum_{i=1}^k \frac{C_{S_i}}{\left(\frac{S_1}{S_i} \right)^\alpha} = \sum_{i=1}^k C_{S_i} \left(\frac{S_i}{S_1} \right)^\alpha = n_i \left(\frac{S_i}{S_1} \right)^\alpha \quad (8.45)$$

 SECTION 8: RELIABILITY DATA COLLECTION AND ANALYSIS,
 DEMONSTRATION, AND GROWTH

where:

- n_i = the number of applied stress reversals at a single stress level i
- s_i = stress level associated with n_i

An S-N diagram is commonly used to present the data from equation 8.45. The S-N diagram plots the number of stress cycles required to break an item at a given stress level. The power of accelerated fatigue testing can then be demonstrated by simplifying equation 8.45 and assuming a material parameter. Since S_1 is a constant:

$$CD \propto n_i (s_i)^\alpha \quad (8.46)$$

The cumulative fatigue damage then becomes proportional to the number of stress cycles and their associated stress level. To illustrate, calculate the increase in cumulative fatigue damage during accelerated testing when the stress level (s_i) is doubled, assuming (for the sake of illustration only that) the material parameter $\alpha = 10$, then:

$$\Delta CD \propto n_i (2)^\alpha = n_i (1024)$$

Thus the fatigue damage accumulates 1024 times (2^{10}) faster than what it would at the baseline stress. Hence, a 20-second test with the applied stress doubled becomes the equivalent of a 300-minute vibration test at normal stress level! Properly applied, this technique can be a powerful tool. In this example (*assuming that the yield strength of the material was not exceeded during the test*), identifying design problems quickly could be readily achieved using an accelerated stress test.

8.7.6 Advanced Concepts In Accelerated Testing

The intent here is not to get deeply involved in the mechanics of accelerated testing, especially not the advanced concepts, but rather to make the user aware of some of the more common practices in the discipline, such as non-constant stress profiles, combined stress profiles and more recent developments in the field.

Historically, most accelerated testing is done using a single stress and a constant stress profile. This includes cycled stress (e.g. temperature cycling between specified limits) where the cycle (upper and lower temperature limits and rate of change of temperature), rather than the temperature is fixed. In accelerated testing, however, the stress profile need not be constant and a combination of stresses may also be used. Some common non-constant stress profiles and combined stress profiles variations include:

- Step Stress Profile Test
- Progressive Stress Profile Test
- Highly Accelerated Life Test (HALT) (Equipment-level)