TM 5-698-3

TECHNICAL MANUAL

RELIABILITY PRIMER FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) FACILITIES

HEADQUARTERS, DEPARTMENT OF THE ARMY

10 JULY 2003

REPRODUCTION AUTHORIZATION/RESTRICTIONS

Technical Manual

No. 5-698-3

HEADQUARTERS
DEPARTMENT OF THE ARMY
WASHINGTON, DC, *10 July 2003*

APPROVED FOR PUBLIC RELEASE: DISTRIBUTION IS UNLIMITED

RELIABILITY PRIMER FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) FACILITIES

CONTENTS

Paragraph *Page*

CHAPTER 1. INTRODUCTION TO RELIABILITY

CHAPTER 2. RELIABILITY AND ITS MATHEMATICAL FOUNDATIONS

CHAPTER 3. RELIABILITY PREDICTION

CHAPTER 4. DESIGNING FOR RELIABILITY

CHAPTER 5. PRODUCING RELIABLE SYSTEMS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION TO RELIABILITY

1-1. Purpose

The purpose of this technical manual is to provide a basic introduction to and overview of the subject of reliability. It is particularly written for personnel involved with the acquisition and support of Command, Control, Communication, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) equipment.

1-2. Scope

The information in this manual reflects the theoretical and practical aspects of the reliability discipline. It includes information from commercial practices and lessons learned over many years of developing and implementing reliability programs for a wide variety of systems and equipment. Although some theory is presented, it is purposely limited and kept as simple as possible.

1-3. References

Appendix A contains a complete list of references used in this manual.

1-4. Definitions

The key terms used in this TM are reliability, mission reliability, basic reliability, mission, function, failure, and probability, among others. Definitions are found in the glossary.

1-5. Historical perspective

Reliability is, in one sense, as old as humankind's development of tools, using tools in the broadest sense to include all types of inventions and products. No one has ever set out to make a tool that doesn't work well over time (a very fundamental way of viewing reliability is the ability of an item to perform its function over time). Until the 20th century, however, people did not consciously "design and manufacture for reliability, and reliability was not a known discipline. It was during World War II that reliability as a distinct discipline had its origins. The V-1 missile team, led by Dr. Wernher von Braun, developed what was probably the first reliability model. The model was based on a theory advanced by Eric Pieruschka that if the probability of survival of an element is 1/x, then the probability that a set of n identical elements will survive is $(1/x)^n$. The formula derived from this theory is sometimes called Lusser's law (Robert Lusser is considered a pioneer of reliability) but is more frequently known as the formula for the reliability of a series system: $R_s = R_1 \times R_2 \times \ldots \times R_n$.

1-6. Importance of reliability

Reliability has increased in importance over the past 30 years as systems have become more complex, support costs have increased, and defense budgets have decreased. Reliability is a basic factor affecting availability, readiness, support costs, and mission success. Research into how things fail, the development of probabilistic approaches to design, an understanding of the distributions of times to failure, and other advances have made reliability a science.

a. *Applies to all products.* Although reliability grew out of a military development program, reliability has become an essential design parameter and performance measure for nearly every product and system, commercial and military. Thus, companies developing valves and other components and equipment used to control the flow of petroleum from the sea bottom, machinery used to manufacture products, medical devices, and commercial airliners all have a vested interest in designing and producing for reliability.

b. *A fundamental performance parameter*. Customers may not use the term reliability when specifying requirements or measuring the performance of their products and systems. Instead, they may have goals such as high availability, high readiness, low life cycle costs, long service life, and so forth. As we will see, achieving these goals begins by designing and producing for reliability, a fundamental performance parameter.

(1) Reliability is a basic factor in mission success. Military commanders are concerned with mission success. The reliability characteristics of a system are used in all operational planning. Fleet sizing, manning requirements, operational doctrine, and strategic targeting all rely directly or indirectly on the reliability of the system and hardware involved.

(2) Reliability is a basic factor driving support requirements. The more reliable a system, the less need for support. If reliability could be taken to the extreme, 100% reliability (zero failure rate), a system would never require any maintenance. No spares would need to be bought nor would any test equipment or maintenance facilities be necessary. The only maintenance people who would be needed would be those involved with servicing, cleaning, and other non-failure related tasks. Understanding the reliability characteristics of a system, its subsystems, and components is essential in using a Reliability-Centered Maintenance approach for developing a preventive maintenance program. For information on applying RCM to C4ISR facilities, see TM 5-698-2.

(3) Reliability affects safety. Although safety focuses more on preventing failures from causing serious consequences to human operators, maintainers, and bystanders, and reliability focuses more on preventing the failures themselves, safety and reliability are related. Many of the analyses performed for safety are similar to, can use the inputs from, or provide information for many reliability analyses.

(4) Reliability is one of the three factors determining availability. A perfectly reliable system would always be available for use. The availability would be 100%. Given that perfect reliability is impractical and unachievable, availability will always be less than 100%. However, availability is also affected by two other factors: the speed at which a repair can be made (a function of design referred to as maintainability), and the support system (number of spares, ability to get spares to where they are needed, etc.). If repair could be conducted in 0 time (another impracticality), availability would be 100%. Thus, availability, like reliability is bounded – it cannot be greater than 100% or less than 0. Different combinations of reliability and maintainability can yield the same level of availability. See appendix B.

(5) Reliability significantly affects life cycle costs. As already stated, reliability affects support requirements, and thereby support costs. The higher the reliability, the lower the support costs. However, achieving high levels of reliability requires investment during acquisition. For instance, high reliability can require hi-rel parts, require special production lines, close quality control, screening of all parts, and carefully controlled production environments. Therefore, trades must be made between cost of ownership and cost of acquisition in order to keep total cost, life cycle cost, as low as possible consistent with mission requirements.

CHAPTER 2

RELIABILITY AND ITS MATHEMATICAL FOUNDATIONS

2-1. Reliability as an engineering discipline

Reliability is a measure of a product's performance that affects both mission accomplishment and operating and support (O&S) costs. Too often we think of performance only in terms of speed, capacity, range, and other "normal" measures. However, if a product fails so often (i.e., poor reliability) that it's seldom available, speed, range, and capacity are irrelevant. Reliability is very much like these other performance parameters, however, in a very important way. Reliability results from a conscious effort to design for reliable performance and to ensure that manufacturing processes do not compromise the "designed-in" level of reliability.

a. *Designing for reliability.* Perfect reliability (i.e., no failures, ever, during the life of the product) is difficult if not impossible to achieve. So even when a "good" level of reliability is achieved, some failures are expected. To keep the number of failures, especially those that could result in catastrophic or serious consequences, designers must conduct analyses, use good design practices, and conduct development tests.

(1) The designer has many analytical methods for identifying potential failure modes, determining the probability of a given failure, identifying single-point and multiple failures, identifying weaknesses in the design, and prioritizing redesign efforts to correct weaknesses. More traditional analytical methods are being complemented or, in some cases, replaced by computer simulation methods.

(2) Some designs are more reliable than others. The most reliable designs tend to be simple, be made with parts appropriately applied, be robust (i.e., tolerant to variations in manufacturing process and operating stresses), and be developed for a known operating environment.

(3) Although designers may apply many analytical tools and design techniques to make the product as reliable as necessary, these tools and techniques are not perfect. One way to compensate for the imperfections of analysis and design techniques is to conduct tests. These tests are intended to validate the design, demonstrate functionality, identify weaknesses, and provide information for improving the design. Some tests are conducted specifically for verifying reliability and identifying areas where the reliability can or must be improved. Even tests that are not conducted specifically for reliability purposes can yield information useful in designing for reliability.

b. *Retaining the "designed-in" level of reliability*. Once a design is "fixed," it must be "transformed" to a real product with as much fidelity as possible. The process of transforming a design to a product is manufacturing. Building a product involves processes such as welding and assembly, inspecting materials and parts from suppliers, integrating lower-level assemblies into high-level assemblies, and performing some type of final inspection. Poor workmanship, levels of part quality that are less than specified by the designer, out-of-control processes, and inadequate inspection can degrade the designed-in level of reliability. To ensure that manufacturing can make the product as it was designed, manufacturing/production engineers and managers should be involved during design. In this way, they will know if new equipment or processes are needed, gain insight into the type of training needed for the manufacturing/production personnel, potential problems, and so forth. They can also help the designers by describing current manufacturing/production capabilities and limitations.

2-2. Mathematical foundations: probability and statistics

Reliability engineering is not equivalent to probability and statistics or vice versa. One would never equate mechanical engineering with calculus – mathematics only provides the basis for measurement in engineering. To quote William Thomson, Lord Kelvin, "When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind: it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science." Probability and statistics are the mathematical foundation of reliability.

a. *The mathematics of reliability*. Probability and statistics constitute the mathematics of reliability engineering. They allow us to express our discipline in numbers, thereby making a science of what would otherwise be "opinion." But, they do not constitute the whole of reliability engineering. Far from it. One would not expect a mathematician to design an aircraft. Likewise, one should not expect a statistician to design a reliable product.

b. *Probability*. Probability had its beginnings in gambling. Whether playing cards or throwing dice, a player has always wanted to increase his or her chances of winning. In any game of chance, a certain level of uncertainty exists, often indicated by the odds. The higher the odds, the higher the degree of uncertainty.

(1) The odds that a toss of an honest coin will be heads or tails (ignoring the extremely unlikely event of the coin landing on its edge) are 1 in 2, or 50%. In the language of probability, we can say that the probability of tossing a head is 0.5, as is the probability of tossing a tail. Now it is possible to toss 2, 3, or even more heads in a row with an honest coin. In the long run, however, we would expect to toss 50% heads and 50% tails.

(2) The reason that the probability of tossing a head or a tail is 0.5 is that there is no reason that either outcome should be favored. Thus, we say that the outcome of the coin toss is random, and each possible outcome, in the case of a coin there are two, is equally likely to occur.

(3) A coin toss is perhaps the simplest example that can be used to describe probability. Consider another gambling object – the die. Rolling an honest die can result in one of six random events: 1, 2, 3, 4, 5, or 6. The result of any single roll of the die or toss of a coin is called a *random variable*. Since both a coin and a die have a limited number of outcomes, we say that the outcome is a *discrete random variable*. If we call x the value of this discrete random variable for a roll of the die or toss of a coin, then the probability, or likelihood, of x is f(x). That is, the probability is a function. For the coin, f(heads) = f(tails) = 0.5. For the die, f(1) = f(2) = f(3) = f(4) = f(5) = f(6) = 1/6 = 0.167, or 16.7%.

(4) More complicated examples can, of course, be given of calculating probability in gambling. Take, for example, an honest deck of 52 cards. The probability of drawing any given card, the ace of spades, for example, is 1 in 52, or 1.92%. To calculate the probability of drawing another ace, given that we drew an ace of spades the first time requires some thought. If we have drawn an ace of spades, only three aces remain and only 51 cards. Therefore, the probability of drawing another ace of any suit (except for spades, of course) is 3 in 51, or 5.88%. The probability of drawing an ace of spades and one other ace is, therefore, 1.92% x 5.88% = 0.11%.

(5) For discrete random variables, such as the outcome of a coin toss or roll of a die, the random events have an underlying probability function. When there are an infinite number of possible outcomes, such as the height of a person, we say that the random variable is continuous. Continuous random variables have an underlying probability density function (pdf). A pdf familiar to many people is the Normal or Gaussian. It has the familiar bell-shaped curve as shown in figure 2-1. This distribution can be applicable even when some of the possible value can be negative as shown in the figure. The Normal distribution is symmetrical, with half of the possible values above the mean value and half below. For example, the average or mean height of an American male, a continuous random variable, tends to be Normally distributed, with half of the men taller than some mean (e.g., 5 feet-9 inches) and half shorter. Appendix A describes some of the pdfs most used in reliability calculations.

(6) The probability of an event is bounded – it can never be greater than 1 (absolute certainty) or less than 0 (absolute uncertainty). As we have seen, if one rolls a die, the probability of any possible outcome is 1/6. The sum of the probabilities of all possible outcomes (1/6 + 1/6 + 1/6 + 1/6 + 1/6 + 1/6) is 1. This is true for discrete and continuous random variables. For this reason, the area under the pdf for a continuous random variable is 1. One way of calculating the area under any curve is take the integral. So the integral of the pdf over the complete range of possible values is 1.

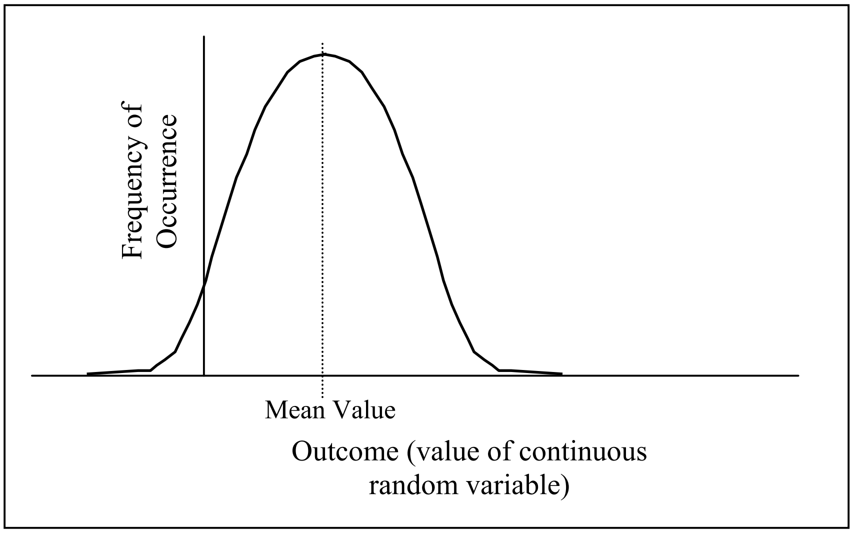


Figure 2-1. Graph of the normal or gaussian probability density function.

c. *Statistics*. One definition of statistics is "a numerical characteristic of a sample population." If the sample population is all males in America, then one statistic, or numerical characteristic of that population, is the average or mean height, assuming that the height is Normally distributed. So the parameters of a population from which we might draw a sample are called statistics. Statistics include means, averages, medians, modes, and standard deviations.

(1) Since we seldom can measure an entire sample population, we can never be absolutely sure of the probability distribution. Hence, we draw a sample from the population. We do this for many purposes, and examples include exit polls during an election and opinion polls. On the basis of the sample, we attempt to determine the most likely probability distribution of the population from which the sample was drawn, and the numerical characteristics of the population. Paragraph 2-4 will discuss sampling in more detail.

(2) Probability and statistics are used to measure reliability. Hence, we can talk about the probability of an item failing over a given time under stated conditions. Or we can talk about mean life or mean time to (or between) failures. Chapter 3 will discuss the various measures of reliability and how they are determined.

2-3. Reliability

Having some background on probability and statistics, we can now discuss reliability in more detail than was given in chapter 1.

a. *Mission success probability.* Reliability is defined as the probability that an item will operate for some period of time within some limits of performance. Reliability is then expressed as a decimal fraction of the number of times that the item will operate for the full mission time. Like the mean for a normally distributed population which states that 0.50 of the population are more than or less than this mean value, this reliability value expresses the decimal fraction of a population of equipment that could be expected to operate for the full mission time. The actual operating time for a single item within a system can be greater or less than the mission time. The reliability value only expresses the probability of completing the mission. To arrive at this figure, however, the basic underlying probability distribution is needed. When the underlying probability distribution is the exponential distribution, reliability is equal to e (the base of natural logarithms) raised to the negative power of the failure rate times the time, or $R(t) = e^{-\lambda t}$, where λ is the failure rate.

b. *MTBF.* Earlier we looked at the probability distribution of the height of a large group of American males. The assumed distribution was the normal distribution and the average height was the mean or expected value. If we had considered the operating times to failure of a population of equipment, instead of the height of men, and if these times were normally distributed, then the expected value of the time to failure of a single equipment would have been the mean of the times to failure, or Mean Time to Failure (MTTF). If the equipment were reparable and we had considered the operating times between failures of a population of equipment, then the expected value of the time between repaired failures would have been this mean, commonly described as Mean Time Between Failure, MTBF. Thus, reliability can be defined in terms of the average or mean time a device or item will operate without failure, or the average time between failures for a reparable item. For the exponential distribution, MTBF or MTTF is equal to the inverse of the failure rate, λ.

(1) Note that, like the average height of males, the MTBF of a particular system is an average and that it is very unlikely that the actual time between any two failures will exactly equal the MTBF. Thus, for example, if a UHF receiver has an MTBF of 100 hours, we can expect that 50% of the time the receiver will fail at or before this time and that 50% of the time it will fail after this time (assuming a Normal distribution).

(2) Over a very long period of time or for a very large number of receivers, the times between failures will average out to the MTBF. It is extremely important to realize that an MTBF is neither a minimum value nor a simple arithmetic average.

2-4. Sampling and estimation

If we could measure the height of every male in America, we would know the exact mean height and the amount of variation in height among males (indicated by the "spread" of the Normal curve). Likewise, if we could observe how long a population of non-repairable valves, for example, operated before failing, we would know the exact mean time to failure, could determine the exact underlying pdf of times to failure, and could calculate the probability of the valves failing before a certain time. We seldom have the luxury of measuring an entire population or waiting until an entire population of parts has failed to make a measurement. Most of the time, we want to estimate a statistic of the population based on a sample.

a. *Unbiased sample.* When taking a sample, it would be possible to skew the results one way or the other, purposely or unintentionally. For example, when taking an opinion poll to determine what percentage of Americans are Republicans, you could take a poll of those leaving the Republican convention. Obviously, such a sample would be biased and not representative of the American population. You must have an unbiased sample. The same principle holds when trying to assess the reliability of a population of valves, for example, based on a sample of the population of valves.

b. *Estimating a statistic*. Once we have an unbiased sample, we can estimate a population statistic based on the sample. For example, we can select a sample of 1,000 valves, test them to failure, determine the underlying distribution of times to failure, and then calculate the reliability as the mean life of the sample. We then use this value of mean life as an estimate of the mean life of the population of valves. Again, we are assuming that the sample is representative of the population. The process of estimating the reliability of an item is usually called prediction and will be addressed in chapter 3.

CHAPTER 3

RELIABILITY PREDICTION

3-1. Introduction to reliability prediction

It is unfortunate that the term "prediction" was ever used in connection with assessing the reliability of a design or product. Prediction has connotations of reading tea leaves or Tarot cards, or gazing into a crystal ball. Even if one compares reliability prediction to weather prediction, those unfamiliar with reliability but all too familiar with weather reports will form an uncomplimentary opinion of reliability prediction. A reliability prediction is nothing more than a quantitative assessment of the level of reliability inherent in a design or achieved in a test model or production product.

3-2. Uses of predictions

Although prediction is the subject of much controversy and debate, few people question the need to quantitatively assess the reliability of an item. Predictions are need for several reasons.

a. *Evaluate alternatives.* In creating a design, the engineer must decide on which parts, what materials, and, in coordination with the manufacturing/production engineers, the types of processes that will be used. Many factors influence these decisions, including costs, established lists of qualified parts and suppliers, existing manufacturing/production capabilities, and so forth. Reliability must also be a factor in selecting parts, materials, and processes. It is not necessary to always select the most reliable alternative. For example, it is not as important to use extremely reliable, and therefore expensive, parts, as it is to properly apply the parts that are selected. By using what is known as robust design techniques, even modestly reliable parts can be used in products where high reliability is required. Predictions assist in the process of evaluating alternatives.

b. *Provide a quantitative basis for design trade-offs.* In designing any product, but especially when designing complex systems such as those used by the military, it is seldom if ever possible to optimize all aspects of the product. It has been said that systems engineering is a process of compromises, in which individual performance parameters or characteristics may be sub-optimized to optimize the overall product performance. For example, a structure may need to be as light as possible but have extremely good fatigue characteristics and carry very high loads. These requirements conflict – maximizing any one may compromise another. Reliability is just one of many product requirements that must be considered in design trades. The most common trade is with the design characteristic of maintainability. That is, it may be possible to relax a reliability requirement if the time to repair can be decreased, thereby yielding the required level of system availability. Predictions help us make such trades on a quantitative basis.

c. *Compare established reliability requirements with state-of-the-art feasibility.* All too often, a requirement is levied on a supplier without determining if the requirement is realistic. Consequently, much time and resources are spent trying to achieve what is inherently unachievable. Although it is natural to want products and systems that are as reliable as possible, we must concentrate on the level of reliability that is needed, to stay within schedule and budget constraints. This level is the one that is dictated by mission and life cycle cost considerations, is achievable given the state of the art of the technology being used, and is consistent with the other system performance requirements. Predictions allow us to assess the feasibility of a requirement.

d. *Provide guidance in budget and schedule decisions.* Assessing the reliability of a design throughout the design process helps to determine if budgets and schedules are sufficient or, on the other hand, determine if we can achieve the required level of reliability within budget and schedule constraints. Early estimates of reliability can be important inputs into determining a program budget and schedule.

e. *Provide a uniform basis for proposal preparation, evaluation, and selection.* When multiple sources are available to bid on a new product or system contract, the customer must be able to select the best supplier. Obviously cost is one way of choosing between suppliers, provided all the suppliers can design and build a system with the required performance with the same level of program risk. By making reliability a requirement and asking suppliers to describe how they plan to achieve the required level of reliability and provide early predictions, suppliers have a basis for preparing their proposals. The customer, in turn, has a basis for evaluating each proposal for the level of risk, and in selecting the "best value" supplier. Of course, reliability is just one consideration in source selection.

f. *Identify and rank potential problem areas and suggest possible solutions.* In the course of design and development test, many problems will emerge. Some of these will be critical and the program cannot proceed until and unless they are solved. Many others, however, will not fall into this "critical" category. With limited time and resources, the issue is to prioritize these problems. Using predictions to determine which problems contribute most to unreliability facilitates the prioritization process.

g. *Provide a basis for selecting economic warranty period.* For many products, warranty is an important subject. Although most commonly associated with commercial products, some military systems and equipment is procured with a warranty. The cost of the warranty is included in the price of the product of system. The question that the supplier must address is how much to charge for the warranty and for how long a period to warrant the product. Predicting the reliability is an important method for projecting the number of returns or claims under the warranty (using past experience is another method). Based on the number of projected claims, and the reliability as a function of time, the optimum warranty period, as well as the price, of the warranty can be determined.

h. *Determine spares requirements.* Whether it is one's personal automobile or the power generation system in a C4ISR facility, failures will occur. The failed items must be repaired or replaced. The latter requires spare parts or assemblies. In addition, some items will be replaced on a regular basis, as part of a preventive maintenance program. Again, spares are needed. Predictions play an important role in determining how many spares of each type are needed.

3-3. The basics

When designing a new product or system, it is difficult, impractical, and sometimes impossible to predict the reliability of the entire product in one step. It is more common to predict the reliability of individual subsystems, assemblies, or even parts and then to "sum" up the individual reliabilities to assess the overall product reliability. It is very much like estimating the weight of a product. One would first estimate (or perhaps know from past experience or from supplier specifications) the weights of all the individual items that make up the product. By summing them up, the weight of the product can be estimated. Of course, as we will see, the process of "summing" individual reliabilities is more complicated than simply adding the reliabilities together.

a. *Hazard function*. The probability that an item will fail in the next instant of time, given that it has not yet failed, is called the hazard function, which is the probability of failure as a function of time. For parts that wear out, gears for example, the hazard function increases with time. That is, the probability of failure is continuously increasing with time. For many items that do not wear out, the hazard function is constant with time. A system under development, for which design improvements are being made as a result of failures found during test or analysis, will have a decreasing hazard function. A system that is used beyond its designed useful life will begin to exhibit an increasing hazard function.

b. *Failure rate.* If the hazard function is constant, the probability of failure is constant over time. In such cases, it is commonly to use the term "failure rate" instead of hazard function. The hazard function is constant when the times to failure follow the exponential probability density function (pdf). It is also true that systems tend to behave as if the times to failure are exponentially distributed even if some parts within the system do not (i.e., they wear out). The reason is that systems are made up of may different types of parts, each type having its own underlying pdf for times to failure. As a result, the system behaves as if it has a failure rate, the inverse of which if the mean time between failure (MTBF). Of course, this is true only if the system is not under development (decreasing hazard function) or being used beyond its useful life (increasing hazard function).

c. *Basic reliability versus mission reliability prediction.* Many parts or assemblies in a system do not affect the system's ability to perform one or more of its functions. For example, the loss of one pump will not affect fluid flow if there is another pump that can take over. Even though the mission can be performed, the failed pump must be repaired (or replaced). Otherwise, another failure (of the other pump) will result in a mission failure. When we are interested in all failures, to determine spares and maintenance labor requirements, for example, we are addressing basic reliability, also called logistics reliability. When we are interested in only those failures that cause the mission to fail, we are addressing mission reliability. This distinction is important for many reasons. One of these, as we will see, is that the methods used for increasing mission reliability can actually cause basic reliability to decrease.

d. *Prediction iteration*. Reliability prediction for an individual component or an entire system is a process. Just as the design of a system evolves, with the designer going from a functional requirement to the physical solution, so the reliability prediction must evolve. Initially, data may not be available and predictions methods are based on similarity or generic part failure rates. As data becomes available, methods that capitalize on the data should be used. During design, this data will be the type, quantity, and quality of parts used, the manner in which the parts interface, the method of assembly and production, and the operational environment. As prototype/test products are available, actual operation/failure information can be gained from testing. Each iteration of the reliability prediction builds on previous work, adding the benefit of current information. The original estimate is very general, based on broad observations and is, therefore, itself very general. Each subsequent prediction, however, is based on more specific information, builds on the previous information, and the amount of uncertainty associated with the prediction decreases. After the demise of a system, the total failures, operating hours, etc., could be actually counted and the final and actual reliability calculated. In a very real sense then, we can visualize the prediction process as progressing from very crude estimates to an exact number. Seldom, however, can we extract every single bit of required data for even a retired system. Even when it is possible, such an exact number only serves as the broad basis to predict the reliability of a new, similar system. During the development and acquisition of a new system, we must recognize the uncertainty associated with any estimate.

3-4. Prediction method

A prediction can be made using a variety of methods, each with its own set of constraints and advantages. No one method is applicable for a product throughout its life cycle. A discussion of some of the most widely used and accepted methods follows. Examples of methods a. through e. are given in appendix C.

a. *Parts count.* This method uses the failure rates of the individual elements in a higher-level assembly to calculate the assembly failure rate. Note that in using failure rates, we are implicitly assuming that the times to failure are exponentially distributed. In using the parts count method, it is important that all portions of the higher-level assembly are used in and exposed to the same environment. The failure rates used can be based on first-hand experience and observation but are often the rates for generic part types. These generic failure rates are available from various sources, such as the Reliability Analysis Center, for a wide range of electronic and mechanical parts. As discussed in Paragraph 3-4e, these rates often are a cumulative average and the actual hazard function is not constant.

b. *Similarity analysis.* If a new product or system is being developed that is similar to a current product or system, the reliability prediction for the new product or system can be based on the current one. Of course, some "adjustments" must be made to account for any differences in the technology being used, the way in which the product will be used, and any differences in the operating environment. Although such adjustments are not exact, similarity analysis is a good way to obtain a very early estimate of the level of reliability that can be expected. Even if the entire product is not similar to an existing one, subsystems or assemblies may be. Often, a specific pump, generator, or other component will be used in different systems. If the operating environment and usage is similar, then the reliability of the component in one system should be similar to the reliability in another system.

c. *Stress-strength interference method.* This method can be used to obtain a point estimate of reliability for an unlimited number of mechanical components. Stress and strength are treated as random variables defined by probability density functions (pdfs). As shown in figure 3-1, the curves for the two pdfs overlap forming an area of interference. (Note that although the curves shown in the figure are of two Normal distributions, the actual pdfs for stress and strength can be any distribution.) The interference is equal to the unreliability (i.e., a weak part meeting a high stress).

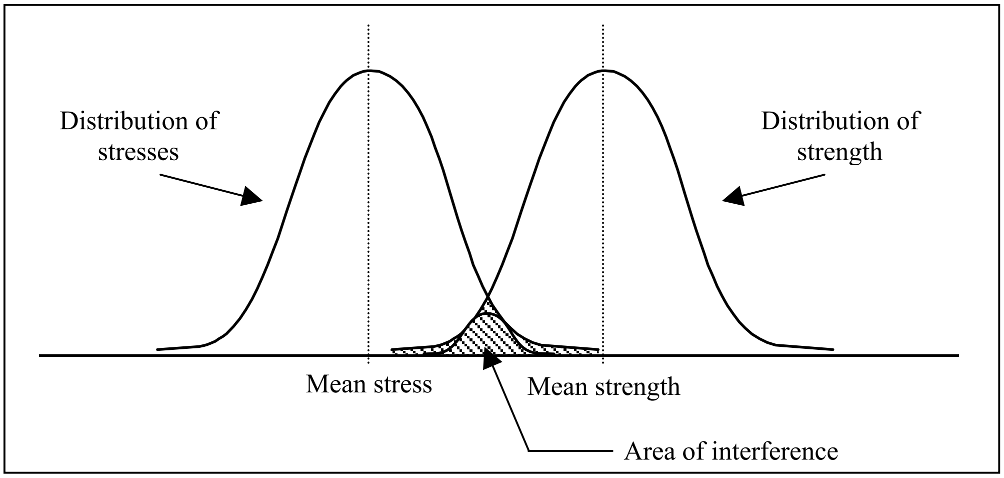


Figure 3-1. The area of interference in the stress-strength interference method is the probability of failure (the unreliability).

d. *Empirical models*. Models and formulas are available for many components that are based on actual data observed over a range of conditions. These models are sensitive to and only valid for the primary variables causing failure. A point estimate of reliability can be obtained at points of interest, allowing design trade-offs to be made early in the design phase. Table 3-1 describes two of the more common empirical models used today.

Table 3-1. Two empirical models for predicting reliability

Model Type	Equation or Model	Notes
Bearing Life Prediction	$B_{10} = \left(\frac{C}{P}\right)^K \text{ x } 10^6$ revolutions	B_{10} is the number of revolutions at which 90% of a population of bearings would survive. C is the load rating and K is a factor that varies depending on the type of bearing. C and K come from the manufacturer's literature.
Fatigue Curves	Curves that indicate fatigue life of a material in number of stress cycles before failure.	Curves are available for many ferrous and non-ferrous alloys, can reflect the effect of surface hardening, crack growth rate, effects of environmental stress variables, stress risers (e.g., holes), etc.

e. *Failure data analysis*. When data are available from test or form field use, the data can be used to assess the reliability of the item. When the data are for part failures, a valve for example, and the times to each failure have been collected, Weibull analysis can be used. The Weibull is a probability density function developed by a Swedish engineer Waloddi Weibull, who was studying fatigue failures. Weibull analysis is a powerful tool that can be used when the underlying distribution of the times to failure are actually Weibull, Normal, or exponential. It can be used when a lot of test or operating time has been accumulated but very few failures have been observed. Often, the times to failure are not known. In this case, we will know only the total time accumulated and the total number of failures. This type of data is called grouped data. Using grouped data, an average failure rate, the total number of failures divided by the total time, can be used. This rate actually represents a cumulative average that is valid for the time period over which the data were collected. If the hazard function for the part is actually increasing, the cumulative average will change depending on the period of interest. Figure 3-2 illustrates how grouped data is used to calculate a cumulative average failure rate.

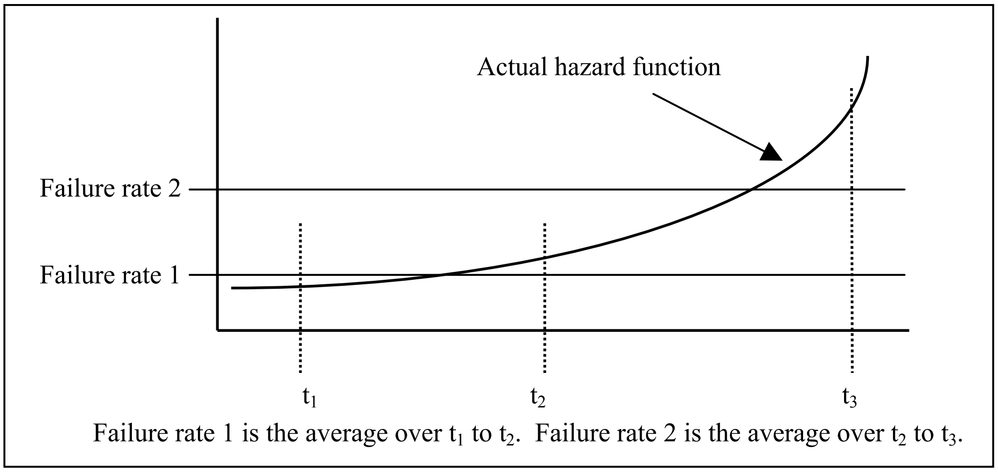


Figure 3-2. The relationship of the average cumulative failure rate and the actual hazard function for a part.

f. *Trending*. When monitoring the reliability of systems under development or in use, it is useful to determine if the system reliability is staying the same, getting worse, or improving. During development, as the design matures, one would expect the reliability be improving. As a system approaches the end of its useful life, one would expect the system reliability to start degrading. Between the end of design and the end of the useful life, one would expect the reliability to stay the same. It will stay constant unless some change is made. The change could be a change in the way the system is used, a change in a manufacturing process or source of a part or assembly, or a change in the competency level of the operators or maintainers. Many techniques exist for performing trending. One of these will be discussed in chapter 6.

3-5. Reliability modeling

Parts and assemblies can be connected in several different configurations. A reliability model is a way of depicting the connections from a reliability perspective. The most common modeling approach used today is the Reliability Block Diagram (RBD). The RBD consists of three basic types of building blocks: series configurations, parallel configurations, and combinations of series and parallel configurations.

a. *Series configuration.* The simplest way to think of a series configuration is as a chain. Just as a chain is only as strong as its weakest link, so the reliability of a series configuration is limited by the least reliable element in the series. For example, if a road crosses three bridges, the loss of any one bridge will prevent traffic from moving. Figure 3-3 shows a simple series configuration and how the system reliability is calculated using the reliability of each element.

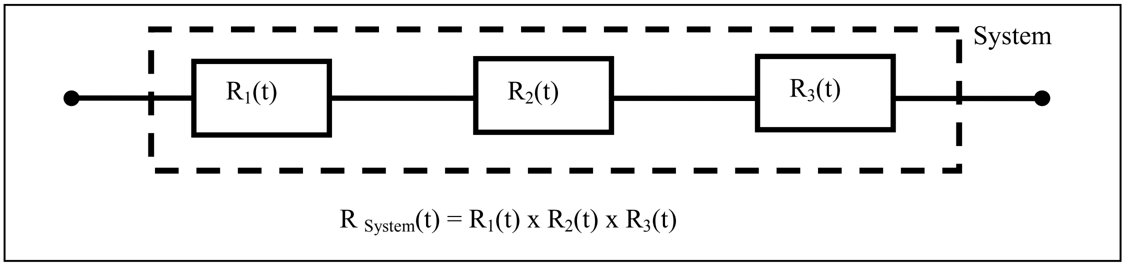
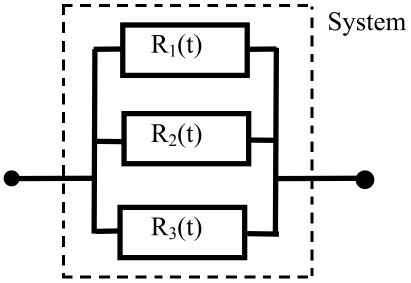


Figure 3-3. The reliability of a system when all the elements in the system are in series is the product of the individual reliabilities.

b. *Parallel (or redundant) configuration.* In a parallel configuration, two or more alternate paths are available for performing a function. Consider the following example. If a road comes to a river that has three bridges over it, traffic can cross over any of the bridges, and any one bridge is sufficient to carry the amount of traffic that crosses each day, then all three bridges would have to fail before traffic would stop. The three bridges are said to be in parallel configuration, and this configuration is obviously more reliable than a series configuration, in which the failure of only one bridge will cause the flow of traffic to stop. Many types of parallel configurations can be used. Brief descriptions of three of these configurations follow.

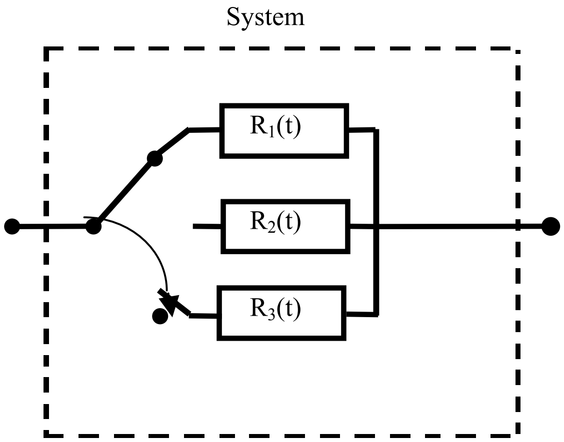
(1) Active parallel configuration (redundancy): all elements are on all of the time that the system is on and are immediately available to take over the function in the event any one element fails. The easiest way to calculate the reliability of the configuration is to determine the probability of all failing, and then to subtract this probability from 1. See figure 3-4.



$$R_{System}(t) = 1- ([1-R_1(t)] \times [1-R_2(t)] \times [1-R_3(t)])$$

Figure 3-4. In an active parallel configuration, the system reliability is calculated by multiplying the unreliability of the elements and subtracting the product from 1.

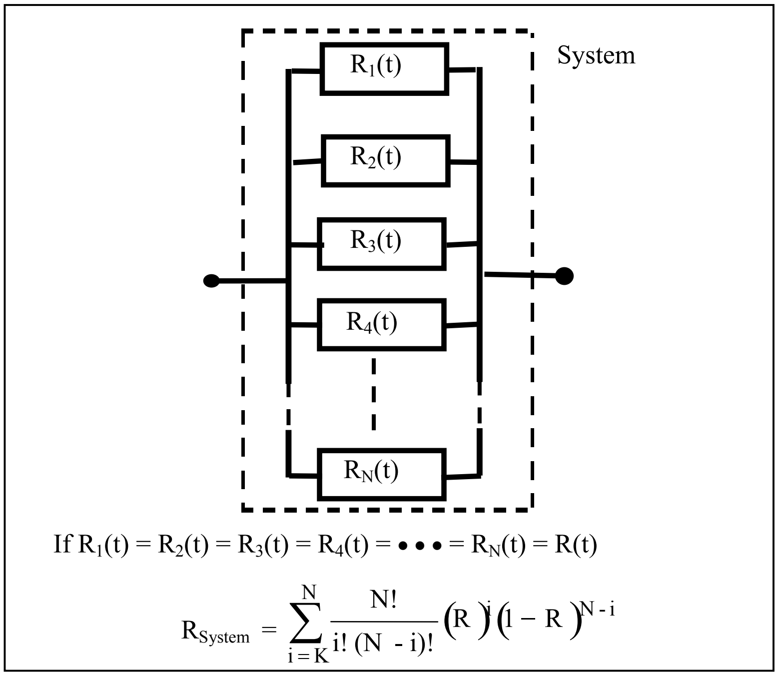
(2) Standby parallel configuration (redundancy): one element is performing the necessary function and another element must be switched on in the event of failure. In this configuration, there must be some method for detecting a failure and switching in the parallel element. Since the switch can fail, this configuration introduces additional opportunities for failure. The other element may be operating or not. If it is not, then the switching capability must also include some way of powering the inactive element on. Figure 3-5 shows this configuration with the reliability calculation when the switching is perfect (i.e., reliability of the switch is 100%), the standby elements are unpowered, and the times to failure for each of the elements are exponentially distributed (i.e., constant hazard function).



$$R_{System}(t) = e^{-\lambda t} + \lambda t e^{-\lambda t} + .5(\lambda t)^2 e^{-\lambda t}$$

Figure 3-5. Calculating the reliability of a parallel configuration with perfect switching, unpowered standby elements, and constant hazard function for each parallel element.

(3) k of N parallel configuration (redundancy): several elements are in parallel and two or more (but less than all) of the elements are needed to perform the function. See figure 3-6.

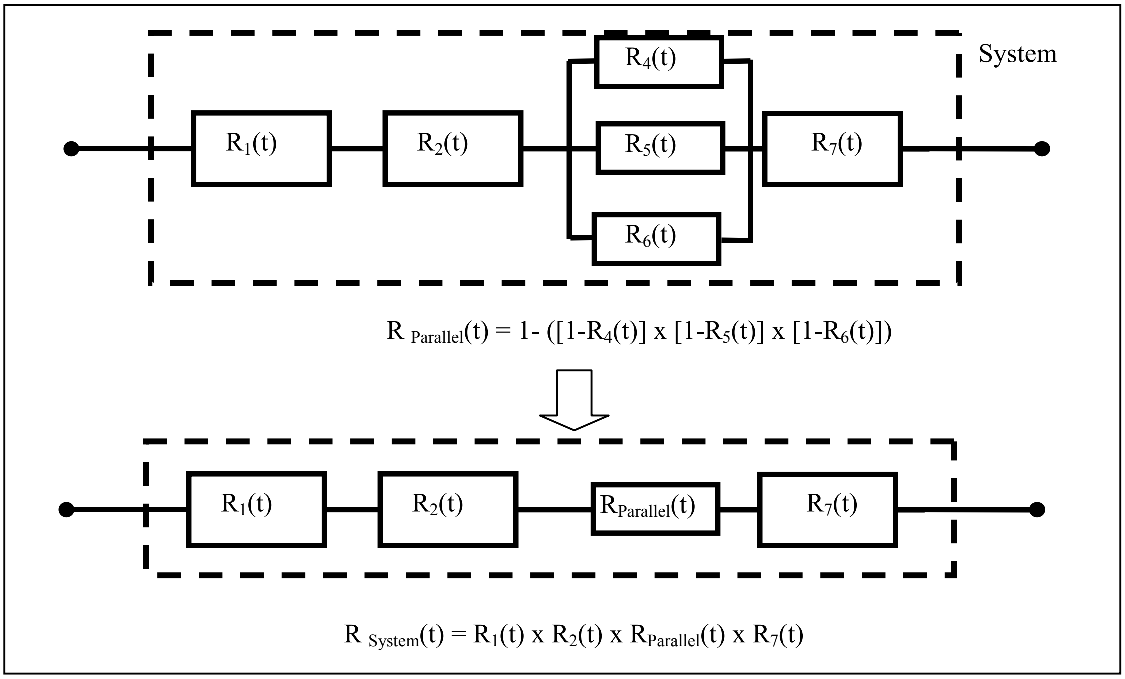


If $R_1(t) = R_2(t) = R_3(t) = R_4(t) = \bullet\bullet\bullet = R_N(t) = R(t)$

$$R_{System} = \sum_{i=K}^{N} \frac{N!}{i!\,(N-i)!} (R)^{i} (1-R)^{N-i}$$

Figure 3-6. Calculating the reliability of k of N parallel elements of equal reliability.

c. *Combined configuration*. Any combination of series and the various parallel configurations is possible. To calculate the system reliability, first calculate the reliability of each individual configuration. The result is a series configuration for which the reliabilities can be multiplied to find the system reliability. See figure 3-7 for a simple example of a combined configuration.



$R_{Parallel}(t) = 1- ([1-R_4(t)] \times [1-R_5(t)] \times [1-R_6(t)])$

$R_{System}(t) = R_1(t) \times R_2(t) \times R_{Parallel}(t) \times R_7(t)$

Figure 3-7. Calculating the reliability of a combined configuration.

CHAPTER 4

DESIGNING FOR RELIABILITY

4-1. Establish and allocate requirements

For a new product or system, developing requirements is the first step, whether the requirement is reliability or any other performance characteristic. Requirements must be realistic. They should be derived from the customer's or user's needs (the mission), economic considerations (life cycle cost), and other factors. For guidance in addressing the reliability and availability of C4ISR facilities during design and in operation, see TM 5-698-1.

a. *Deriving requirements.* Many ways of deriving reliability requirements are used. Some are based on achieving incremental improvements in each successive model of a product. Others are derived from sophisticated simulations that model the way in which the system will be used. Still others, benchmarking for example, are based on staying competitive with other suppliers. It is important to note that customers often state reliability requirements in a way that is not directly usable by designers. Also, designers do not always have direct control over all of the factors that influence the reliability that will be achieved in use.

(1) Customers and system users often think not of reliability, but of availability – how often the system will be available for use – or a maximum number of warranty returns. It is difficult for designers to work directly with these types of requirements. Consequently, a "translation" must be made to convert these higher-level requirements to design measures, such as probability of failure or MTBF. For example, if availability is the customer's requirement, many combinations of reliabilities and repair times will result in the required availability.

(2) The reliability achieved for a system in use is affected not only by the design and manufacturing processes, but also by the skill and experience of the operators and maintainers, and by changes in the way the system is operated. Designers may not be able to control all of these factors. For example, designers can consciously attempt to minimize the possibility of failures being induced during maintenance but cannot prevent all such failures from occurring. However, the design requirement can be "adjusted" so that even with some reasonable number of maintenance-induced failures, the reliability in actual use will meet the customer's needs. This adjustment means that the design requirement must be higher than one would first imagine.

b. *Allocating requirements.* Customers and users usually state the reliability requirement (or a high-level requirement having reliability as a key element) at the product or system level. For example, the reliability for an electrical power generation system might be 99.9% for a given power level into a given load for a stated period of time. But what should be the reliability requirement for a transformer used in the system?

(1) To better understand the reliability allocation process, consider how weight is treated. If a maximum weight is specified for a system, each element of the system must be assigned a weight "budget" that the designers must meet. If, for example, a system consists of 5 elements A through E and the system weight must be no more than 2,000 lbs., we might assign budget as follows: A - 200 lbs., B - 500 lbs., C - 350 lbs., D - 400 lbs., and E - 550 lbs. The sum of the element weights must, of course, add up to no more than the maximum system weight. The assignment of the budgets would be made on past experience or some other logical basis.

(2) The allocation of a system reliability requirement is similar to the assignment of weight budgets. The idea is to assign reliability requirements to lower levels of indenture within the system such that if the lower-level requirements are met, the system requirement will be met. For example, if the system reliability for a 10-hour mission is specified as 95%, and the system is made up of three major subsystems A, B, and C, then $R_A \times R_B \times R_C$ must be equal to 0.95.

(3) Several methods are used to make reliability allocations. These include the Equal Allocation Method, the ARINC Method, and the Feasibility of Objectives Method. These and other methods are described in several of the references listed in appendix A.

4-2. Develop system reliability model

Early in the development of a new system, a reliability model must be developed. The most commonly used model is the reliability block diagram (RBD) discussed in chapter 3. The process for modeling a system for reliability purposes consists of three steps.

a. *Select system.* Define the specific system to be modeled. This definition includes the exact configuration and, if appropriate, the block or version.

b. *Construct functional block diagram*. The functional relationships among the parts, assemblies, and subsystems must be understood because reliability deals with functional failures. In fact, failure is usually defined as the loss of a function. The functional block diagram shows inputs and outputs but does not necessarily depict how the system elements are physically connected or positioned. Figure 4-1 shows an example of a functional block diagram.

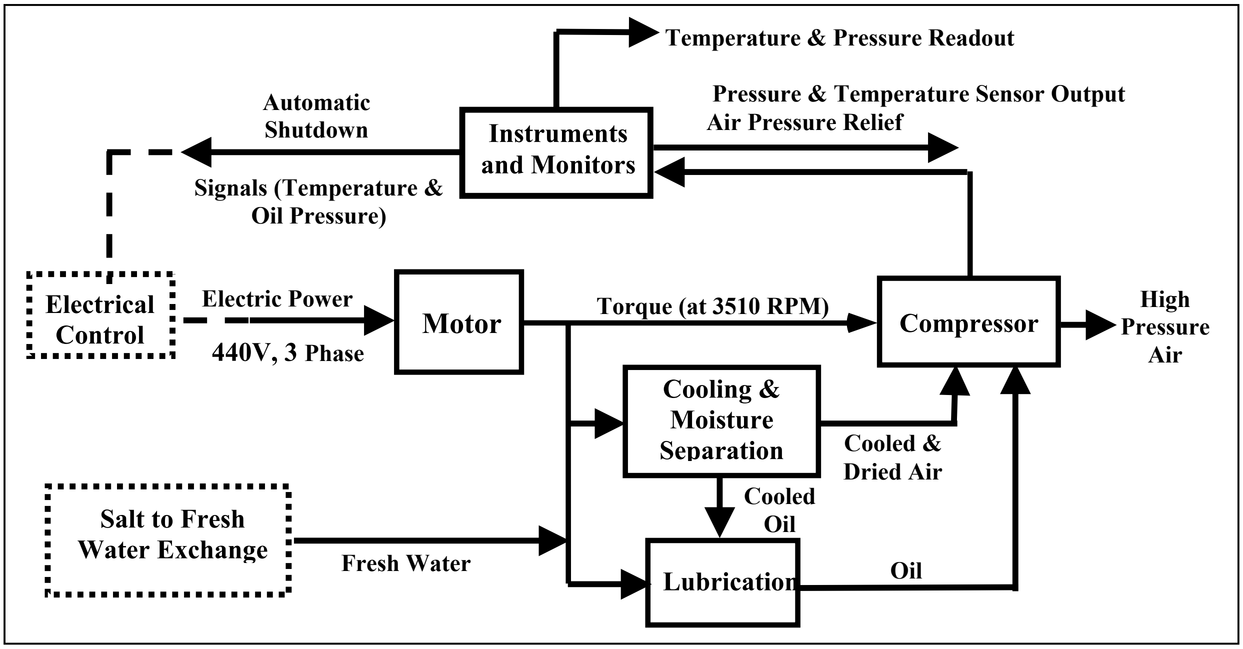


Figure 4-1. Example of a functional block diagram.

c. *Construct reliability block diagrams as necessary.* It is often impractical to develop one RBD for the entire system that has all subsystems, assemblies, and parts. A single RBD for an entire C4ISR facility would be huge and unmanageable. More commonly, RBDs are developed for lower-level portions of the system, such as the subsystem, assembly, and even part level. The reliability of each of these portions can then be assessed and used in a system assessment. Figure 4-2 illustrates this process.

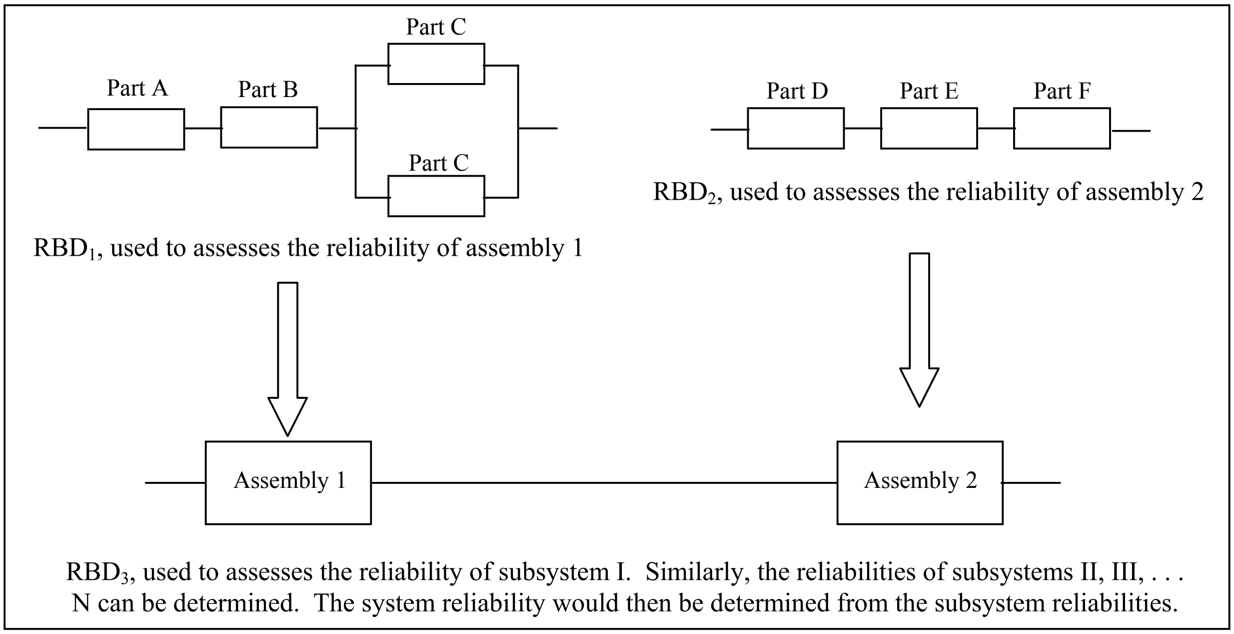


Figure 4-2. An example of how lower-level RBDs are used to assesses the reliabilities of assemblies. The resulting assembly reliabilities are used in an RBD of a subsystem made up of the assemblies. This process can be repeated until the system reliability can be assessed.

4-3. Conduct analyses

A variety of analyses can be used in designing for reliability. Table 4-1 lists the titles and purposes of some of these analyses.

a. *Related analyses*. Many analyses are conducted for reasons not specifically stated as reliability, such as safety and structural integrity. However, many of these analyses directly or indirectly support the effort of designing for reliability. Designers should always have the objective of using the results of analyses for as many purposes as practical. An integrated systems approach facilitates extracting as much benefit from all analyses (as well as tests).

Table 4-1. Typical reliability-related analyses and their purposes

Analysis	Purpose
Dormancy Analysis	Used to calculate failure rates of devices while dormant (e.g., storage).
Durability Assessment	Used to confirm a design life for a product. It is more effectively applied earlier in development to ensure that design life is adequate.
Failure Modes, Effects, and Criticality Analysis	Used ideally as a design and assessment tool to understand and alleviate failure consequences, it can also be an independently applied tool to check that certain failure consequences are avoided. A qualitative measurement.
Fault Tree Analysis (FTA)	Used ideally as a design and assessment tool to understand and alleviate failure consequences, it can also be an independently applied tool to check that certain failure consequences are avoided. A qualitative measurement.
Finite Element Analysis (FEA)	FEA is a computer simulation technique used for predicting material response or behavior of modeled device, determining material stresses and temperature, and determining thermal and dynamic loading.
Sneak Circuit Analysis (SCA)	Used ideally as a design and assessment tool to discover unintended paths and functions, it can also be an independently applied tool to check that certain failure consequences are avoided. A qualitative measurement.
Thermal Analysis (TA)	Used to calculate junction temperatures, thermal gradients, and operating temperatures.
Worst Case Circuit Analysis (WCCA)	A tool used to effectively assess design tolerance to parameter variation, it can also be used as an independent check of the susceptibility to variation.

b. *The Role of the designer.* In some cases, designers will and should be directly involved in performing a given analysis. Other individuals may perform specific and highly specialized analyses. In any case, it is important that the designers understand the purpose and benefit of each analysis, and "buy in" to the need for conducting the analysis.

4-4. Design for reliability

Achieving the required level of reliability begins with design. Some key issues that must be addressed during design are control of parts and materials, use of redundancy, robust design, design from the environment, designing for simplicity, and configuration control.

a. *Control selection of parts and materials.* Part of the design for reliability process is the selection of parts and materials. In selecting parts and materials, the designers must consider functionality, performance, reliability, quality, cost, producibility, long-term availability, and other factors.

(1) When possible, standard parts and materials having well-established characteristics should be preferred to non-standard or newly developed parts and materials. For some products or use environments, the anticipated stresses are so low that any commercially available part may be acceptable. In such cases, parts control may consist entirely of configuration management (knowing what parts are used) and ensuring that they are obtained from a reputable source. In other cases, the stresses that will be encountered by the product may eliminate many types of parts or mandate certain application criteria (e.g., derating). In addition, some types of parts may be obsolete before the product is delivered. In these cases, parts control should be more extensive and rigorous.

(2) After selecting the appropriate part it should be applied in a conservative manner (a process called derating). Using a part at its maximum capability increases the failure rate and does not allow for transients or overloads. Just how conservatively a part may be used depends on factors such as cost, mission criticality, and environment, which cannot be generalized.

b. *Use redundancy appropriately.* You will recall that components or subsystems connected in parallel must all fail in order to have system failure. This addition of components or subsystems in parallel is termed redundant configurations. Simply stated, redundancy provides alternate paths or modes of operation that allow for proper system operation. Redundancy has some drawbacks, however, and cannot be blindly used. Adding parallel items increases weight and cost. It increases complexity. Finally, redundancy does nothing to increase the reliability of individual items, only the system-level mission reliability. It actually decreases basic reliability. Thus, more failures (albeit not mission failures) will occur requiring repair or replacement, driving up support costs.

c. *Use robust design.* A robust system design is one that is tolerant of failures and occasional spikes in stresses. One way to achieve a robust design is to use Design of Experiments to determine which parameters are critical and then to optimize those parameters. Another method involves the use of Highly Accelerated Life Testing (HALT). HALT requires successively higher stresses to be applied during test and making design changes to eliminate the failures observed at each level of stress. The magnitude of the stresses is not intended to represent actual use but to force failures. Using HALT results in "over-designed" systems and products, but over-design may be warranted in critical applications.

d. *Design for the environment.* Without an understanding of the environment to which a system will be exposed during its useful life, designers cannot adequately design for or predict reliability. The process of understanding a system's environment is referred to as environmental characterization. The environment includes not only the operating environment but also all other environments applicable to the system. Often, the operating environment does not impose the greatest stresses. Table 4-2 lists some of the environments that must be considered in designing for reliability.

Table 4-2. Environments to consider in designing for reliability

Environment	Comments	Environmental Stresses and Factors*
Operating	Includes all potential ways and climates in which the system will be used.	Temperature Humidity Mechanical/acoustical vibration Mechanical/acoustical shock Moisture Sand Dirt Electromagnetic interference Radiation Mechanical loads Corrosion Chemical reaction
Support	The environment in which a system is repaired and serviced must be considered.	
Installation	For some systems, the process of installation imposes stresses that are higher than those of operation.	
Storage	For systems and products stored for long periods of time, the storage environment can be the dominant cause of failure.	
Transportation	The shipping and handling of systems and products can impose stresses, such as shock and vibration, that are different from or higher than those of operation.	

*Typical environmental stresses and factors that can occur in any of the listed environments.

e. *Design for simplicity*. The basic tenet of reliable design is to keep it simple. The more complicated a design, the more opportunity for failure. This principle is sometimes derided as elementary and intuitive; nevertheless, it is often needlessly violated and is included here as a reminder of its importance.

f. *Institute configuration control.* As changes are made to improve reliability, or for any other reason, and the design matures, it should be complemented by a progressively mature control of hardware design. It is important to know which current configuration served as the basis for a given reliability prediction or analysis.

(1) Initially, the hardware design is conceptual in nature and may be described by equations or design parameters, for example. At this stage, subsystem designers should have little controls placed upon the details. They should be engaged in trade studies, sensitivity analyses, and design variations leading to the next phase of hardware control.

(2) The next level of configuration control is "baselining the system." The baseline permits concentration on a specific design and allows detail design to begin. After a system is baselined, the designer can only change the concept when there is due cause and only after notifying other program elements to assure that each subsystem designer is aware of the design of interfacing subsystems.

(3) At critical design review (drawing release), the detail design is (ideally) complete and formal configuration control process should be instituted. The process should be rigid and designed to ensure that design modifications are undertaken only for understood cause and the full cost and impact is analyzed prior to initiating the change.

4-5. Conduct development testing

Reliability prediction and design requires some knowledge of the failure rates of parts, and how the parts are used. Additionally, the reliability engineer will need to use analytical tools such as FMEAs and stress analysis. In performing analyses and making predictions, the engineer tries to account for all factors affecting reliability. However, as is true of all analysis, the reliability analysis is far from perfect, particularly early in the development of a new product. For instance, initial tests of the product (the product may be a prototype, development model, or production article) may reveal unforeseen failure modes. Then again, it might be determined that initial failure rates and application factors did not sufficiently account for interaction of parts and subsystems (the fact that the whole is not always the simple sum of its parts is attributed to a phenomenon called synergism). Consequently, the MTBF (hardware reliability) or mission reliability may be lower than originally estimated. Since the original design was intended to satisfy a requirement, some action is needed to bring the reliability of the product "up to spec." The process by which the reliability of a product is increased to meet the design level is reliability growth.

a. *Duane's model.* Duane developed learning curves based on cumulative failures and cumulative operating hours for five different products: two hydromechanical devices, two aircraft electrical generators, and a turbojet engine. The products represented a broad range of aircraft type equipment and were identified only by general description. After plotting the data on log-log paper, Duane found that the curves were very nearly linear and that failure rates at any point in time for these relatively complex aircraft accessories were approximately inversely proportional to the square root of the cumulative operating time. Independent and related efforts such as the Godovin Report, work by J.D. Selley, S.G. Miller, and E.O. Codier of General Electric, and others have confirmed the soundness of Duane's hypothesis. In total, this work has given the engineer and the manager an aid in planning, monitoring, and controlling the growth of reliability early in an acquisition program.

b. *Other Models for Growth.* Duane's work has been expanded and extended by engineers and statisticians and a variety of reliability growth models are now available. One, the AMSAA-Crow model is a statistical model based on the Non-Homogeneous Poisson Process (NHPP). The NHPP applies when a trend exists (e.g., reliability is improving or degrading). Since the AMSAA-Crow is a statistical model, it is somewhat more complicated to use than the Duane model.

(1) First, you must determine if a trend exists in the data using a statistic called the Laplace statistic (this statistic will be addressed in more detail in chapter 6). If a trend does not exist at some level of confidence, determined by the user, the model cannot be used.

(2) If the model applies, then you calculate parameters based on sample size and type of test (test ended after a given number of failures or after a given length of time.

(3) You can now determine system failure rate at time of interest

(4) An advantage of the AMSAA-Crow model is that, since it is a statistical model, you can calculate upper and lower bounds on calculated failure rate (or the MTBF).

c. *Achieving reliability growth*. Corrective measures taken to ensure that the equipment reliability "grows" properly include redesign, change in materials or processes, or increased tolerances on critical parameters. All of these efforts represent the expenditure of money.

d. *The nature of growth.* Reliability growth is the decrease in the hazard function during the early portion of development and production. It is the result of design changes and improvements that correct deficiencies of the original design. Its goal is to attain a design which, when in full operational use, has the minimum required level of reliability. When reliability growth is completed, the hazard function (failure rate if the exponential distribution applies) stabilizes at a relatively fixed value. The key attributes of reliability growth follow.

(1) Reliability growth occurs early in the life cycle of a product.

(2) Reliability growth is the result of corrective action. Reliability growth is intended to achieve the required reliability level. Testing provides verification of the predictions made as a result of analytical methods and of the design approach used. When testing reveals that the analyses or design approaches were inadequate or deficient, corrective actions must be taken to the extent necessary to meet the reliability requirements. Assuming the corrective actions are effective, growth occurs.

(3) The hazard function stabilizes when growth ceases. For systems, which tend to exhibit times between failure that are exponentially distributed, this behavior means that once growth ceases, we will observe a constant failure rate (or a constant mean time between failure). The value will, of course, actually fluctuate due to variances in operations and other factors but will be relatively stable. When the system starts to near the end of its useful life, the failure rate will start to increase. Trending is intended to provide an early indication when system reliability is degrading (due to age or for other reasons).

e. *Accelerated testing.* Earlier, HALT was introduced as a technique for achieving a robust design. HALT is one form of accelerated testing. Another, Accelerated Life Testing (ALT), is a technique for achieving reliability growth by accelerating the rate at which failures occur and are addressed by design improvements. The primary difference between HALT and ALT is that the accelerated stresses used in the latter are chosen such that failures not expected in actual use (storage, installation, etc.) are hopefully not introduced during the ALT. This constraint allows the results of ALT to be used to assess the reliability of the item being tested. HALT does not provide an estimate of the true reliability, only some assurance that the reliability is higher than some minimum.

4-6. Iterate the design

As discussed briefly in paragraph 4-5, as changes are made to improve reliability, or for any other reason, the design is changed and gradually matures. This iteration process is an inherent part of design and development, especially when the system is new or significantly different from predecessors. Changes to the design are made on the basis of continuing analyses. These analyses are initially performed on conceptual designs and eventually on test results. When these changes are made to reduce the relative frequency with which a failure occurs, or to reduce or minimize the effects of a failure, the change is related to reliability growth.

4-7. Conduct demonstration tests

At or near the end of development, a key question that must be answered is "Has the reliability requirement been met?" Either the customer will require that some type of test be made to measure the level of reliability achieved or the company itself may require such testing as a matter of policy. Such tests are called demonstration tests because they are intended to demonstrate the level of reliability that has actually been achieved. Ideally, such testing would be conducted on products right off the production line. Practical considerations make this nearly impossible. Indeed, the decision whether or not to proceed with full-scale production often requires the testing to have been completed. Consequently, testing is done using early production models or prototypes that are as close as practical to the full-rate production model.

a. *Standard statistical tests.* For many years, the statistical tests described in MIL-HDBK-781 were used to demonstrate the achieved level of reliability. MIL-HDBK-781 provides for two types of tests: sequential tests (called probability ratio sequential tests) and fixed-length tests. Both types are based on the premise that a product (system) exhibits a constant failure rate (i.e., the underlying pdf is the exponential) and is neither getting more reliability or less reliable. The problem with such tests is that for products having high MTBFs, the test time can be very long. For example, a fixed-length test to verify that a product has an MTBF of 1,000 hours can take as many as 45,000 hours of cumulative test hours. If a sample of only 3 is available, that means the test will take 15,000 calendar hours. Such testing is obviously expensive.

b. *Accelerated life testing.* Accelerated life testing was introduced in Paragraph 4-5e as a technique for accelerating reliability growth. It can also be used to avoid the problem of demonstrating very high reliabilities with MIL-HDBK-781 tests and is finding an increasingly larger following for this purpose. Accelerated testing is intended to accelerate the occurrence of failures that would eventually occur under normal conditions, measure the reliability at these conditions, and then correlate the results back to normal operating stresses. In accelerating the stresses, it is important not to induce failures that would not otherwise occur. Otherwise, correlation is lost. Accelerated testing of complex systems has many uncertainties and not all failure modes can be accelerated.

4-8. Design using a team approach

The engineer and manager are both continually making trade-offs between complexity and flexibility, design costs and logistics support costs, redundancy and simplicity, etc. The ultimate goal of each member of the management and design team should be to obtain the <u>essential</u> operational performance characteristics at the lowest life cycle cost. To this end, the manager, engineer, logistic planner, and entire program team must maintain a daily dialogue, each contributing his talents to the benefit of all.

a. *Production and logistics affect reliability*. The designer works with ideas. Once these ideas were captured in hard-copy drawings and specifications; today they are captured in digital format. These ideas must be converted from the abstract to the concrete; i.e., from drawings and specifications to hardware. The process by which this conversion takes place is production. The manufacturing processes and the control of those processes affect the reliability of the finished system. Logistics also affects reliability.

(1) The manufacturing people can determine if the necessary processes, machines, skills, and skill levels are already in being. If not, they will have time to plan for these items (e.g., procure or develop new machines and

processes, hire new people, develop training, and so forth). The manufacturing people can help the designers by pointing out design approaches that are too complicated or impractical for manufacture. They can describe current capabilities to help designers select appropriate design approaches.

(2) The reliability observed by the customer is also affected by how well maintenance is performed and by the number of induced failures caused by inexperienced, careless, or inadequately trained personnel. The availability, even if the reliability being achieved in use is adequate, will be less than desired if the necessary trained people, spares, test equipment, or other logistics resources are unavailable when needed. Although availability will suffer, reliability is often incorrectly singled out as the problem.

b. *Everyone can benefit from the team approach.* Other people and organization who can contribute to the design for reliability and who can benefit from reliability analyses include the safety engineers, logistics planners, mission planners, packaging and handling specialists, after-sale service organizations, and so forth.

c. *Integrated Product and Process Development.* Within the Department of Defense, the Integrated Product and Process Development (IPPD) approach has been mandated for all DoD acquisition programs. IPPD is described in "DoD Guide to Integrated Product and Process Development" (version 1.0 was released February 5, 1996). Integrated Product Teams (IPTs) that organize for and accomplish the tasks required in acquiring goods and services are the foundation of the IPPD process. IPTs are made up of everyone having a stake in the outcome or product of the team, including the customer and suppliers. Collectively, team members should represent the needed know-how and be given the authority to control the resources necessary for getting the job done.

d. *The systems engineering approach*. Systems engineering is an interdisciplinary approach that focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, then proceeding with design synthesis and system validation while considering the complete problem. The complete problem involves operations, performance, test, manufacturing, cost and schedule, training and support, and disposal. Systems engineering integrates all the disciplines and specialty groups into a team effort and promotes a structured development process that proceeds from concept to production to operation. Systems engineering is focused on the goal of providing a quality product that meets the user needs.

CHAPTER 5

PRODUCING RELIABLE SYSTEMS

5-1. Control configuration

The concept of Configuration Control was introduced in chapter 4. The process of managing the configuration must continue throughout the manufacturing and production process. Manufacturing and production includes not only the process, machines, and people organic to the developer but also those of suppliers. Preferred parts and supplier lists not only assist designers in selecting parts and materials, but they can help in controlling configuration.

a. *Control of processes, tools, and procedures*. Just as the configuration of the design must be controlled, so too must the configuration of the processes, tools, and procedures used to manufacture the system. Even changes that at first appear to be minor and inconsequential can serious degrade the system reliability. Changes to processes, tools, and procedures must be made with the same level of discipline used for design changes.

b. *Configuration of purchased items*. A variety of criteria can be used in selecting suppliers, including on-time delivery, price, and reliability and quality. Good selection criteria and supplier relationships, especially for critical parts, materials, and assemblies, can help maintain configuration control in several ways.

(1) The supplier is more likely to notify the buyer of unexpected failures, changes in processes or technology, and other changes that could affect the performance of the system.

(2) The supplier is more likely to implement design practices consistent with those being used for the system.

(3) Without insight into or control of the configuration of purchased items, the configuration of the system cannot be determined.

5-2. Design processes

Industrial engineers and manufacturing specialists are responsible for designing the processes, tools, and procedures that will be used to transform the design into a system. In chapter 4, the idea of including the manufacturing staff in the system design process was introduced. Including them has several benefits.

a. *Allows for lead time.* Many parts, some materials, manufacturing machines, and new processes require time to acquire or develop; in other words, they are not readily available "off-the-shelf." This time is referred to as lead time. Without sufficient and timely information as to what manufacturing equipment or processes will be needed, advance planning cannot be done and schedules will not include sufficient lead times. By including manufacturing early in the design process, the manufacturing people will have the information they need to plan for new manufacturing equipment and processes.

b. *Enhances manufacturability.* Some designs are inherently easier to manufacture than others. Certainly, the ease of manufacture is related to the nature of the system: it is easier to make a lamp than a radar. However, the degree of manufacturability is first and foremost a function of conscious efforts to design for manufacture. Including industrial engineers and manufacturing specialists in the design process affords them the opportunity to influence the design to enhance manufacturability. Although ease of manufacture cannot always take precedence over other requirements, it should always be considered in trade-offs. The objective of ease of manufacture can be achieved only if it receives conscious and continual attention during design.

5-3. Train personnel

Table 5-1 includes training in the list of factors affecting production readiness. Training can be required for a variety of reasons and may include certification or similar requirements.

a. *Training for new processes and equipment*. When it is necessary to acquire new production equipment or to acquire or develop new processes to manufacture a product, the operators of the new equipment or processes must be adequately trained. As a matter of practicality, such training should be conducted early enough to allow some level of verification of the effectiveness of both the training and the operation of the equipment and processes. Ideally, operators, equipment, and processes will be "mature" before production begins. In reality, some amount of "learning" will be experienced during the early stages of production. This learning will evidence itself in manufacturing defects, analysis of those defects, development of improvements to eliminate (or reduce to an acceptable level) those defects, and implementation and verification of the improvements.

Table 5-1. Examples of parameters measured for process control

Category	Examples
Physical	Size (length, width, height), weight, strength, etc.
Performance	Gain, frequency, power output, etc.
Failure-related	Service life, failure rate, defect rate, reject rate, etc.
Cycle time	Time to produce, time from order to delivery, design cycle, etc.
Cost	Cost to produce, warranty costs, scrap produced, rework costs, overhead rate, etc.

b. *Retaining current certifications*. Even when no new equipment of processes are needed, it is important that the machine and process operators are fully qualified. For some machines and processes, certifications (required by a government agency, the customer, or the company) are required. Such certifications usually expire unless recertification is earned. It is important that all such certifications be kept up to date.

5-4. Institute quality control

Assuring that the materials and parts, processes, and personnel needed to manufacture a system is the responsibility of quality. A comprehensive quality plan will include many activities. Key among these activities will be incoming inspection, process control, and acceptance testing.

a. *Incoming inspection.* Ensuring that the materials, parts, assemblies, and other items purchased from outside sources meet all design requirements is an important part of quality control. Often, as part of source selection, suppliers will be authorized and required to conduct the acceptance testing. Otherwise, such testing is done at the point of receipt. In any case, the types of tests, test procedures, sample size or 100% inspection, pass/fail criteria, and so forth must be established well in advance of production.

b. *Process control.* Every process has some variation in its output. Supposedly identical manufactured products will vary in size, strength, defect content, etc. The greater the variation, the less often the customer will be satisfied. Keeping a process in control is key to manufacturing products that meet requirements and faithfully reflect the designer's ideas. Statistical process control (SPC) is the default standard in nearly every company and industry. Implementing statistical process control basically involves the use of statistical tools to measure and analyze variability in work processes. The objective is to monitor process output and maintain the process to a fixed level of variation. Usually SPC is considered a part of statistical quality control, which refers to using statistical techniques for measuring and improving the *quality* of processes. These include sampling plans, experimental design, variation reduction, process capability analysis, and process improvement plans.

(1) The first task in measuring variation is to determine the parameters that most impact the customer's satisfaction. These will be measures of quality. Some possibilities are shown in table 5-1.

(2) Control charts. A key SPC tool is the control chart. A control chart is a graphical representation of certain descriptive statistics for specific quantitative measurements of a process. These descriptive statistics are displayed in the control chart and compared with their "in-control" sampling distributions. The comparison will reveal any unusual variation in the process, which could indicate a problem. Several different descriptive statistics can be used in control charts and there are several different types of control charts that can test for different causes. Control charts are also used with product measurements to analyze process capability and for continuous process improvement efforts. Table 5-2 shows some typical control charts.

Table 5-2. Typical control charts

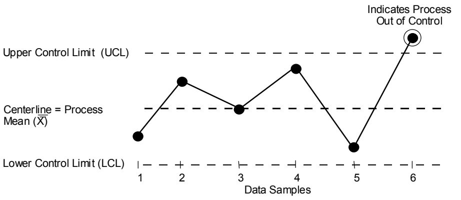
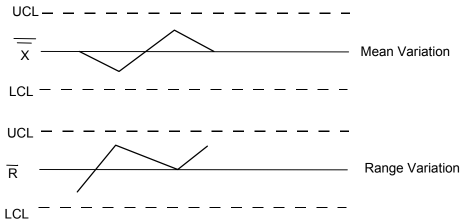
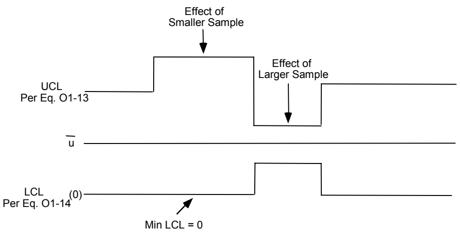
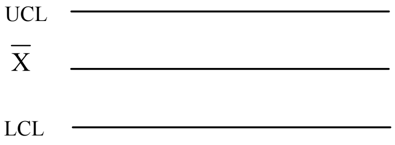
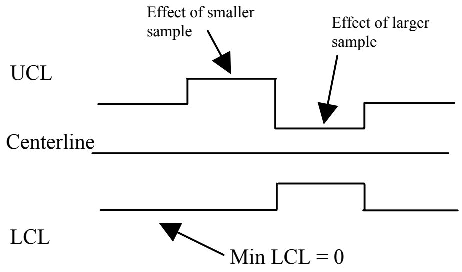
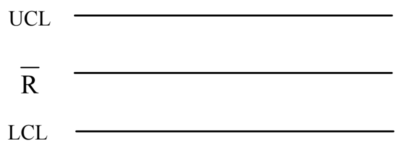
Chart	Equation	Notes
Variable 	$UCL = \overline{\overline{X}} + \frac{3\sigma}{\sqrt{n}}$ $LCL = \overline{\overline{X}} - \frac{3\sigma}{\sqrt{n}}$ $\overline{\overline{X}}$ = Process mean σ = Process standard deviation n = sample size	Chart shown assumes constant sample size
Variable and Range 	UCL $\overline{\overline{X}} = \overline{\overline{X}} + A_2\overline{R}$ LCL $\overline{\overline{X}} = \overline{\overline{X}} - A_2\overline{R}$ UCL ($\overline{R}$) = $D_4\overline{R}$ LCL ($\overline{R}$) = $D_3\overline{R}$ $\overline{\overline{X}}$ = Process Mean $\overline{R}$ = Mean Range	Range = Highest value measured in sample minus lowest value $\overline{R}$ = Mean range of many samples A_2, D_3, D_4 are constants based on sample size (available in statistics texts).
Proportions 	$UCL = \overline{P} + 3\sqrt{\frac{\overline{P}\left(1-\overline{P}\right)}{n}}$ $LCL = \overline{P} - 3\sqrt{\frac{\overline{P}\left(1-\overline{P}\right)}{n}}$ Centerline = $\overline{P}$ $\overline{P}$ = Proportion of product with attribute of interest n = Sample size	$\overline{P}$ could be the proportion of product which is defective, determined from experience, or it may be the specified allowable proportion defective
Proportions – Constant sample size 	$\overline{X} = n\overline{P}$ $UCL = \overline{X} + 3\sqrt{X\left(1-\overline{P}\right)}$ $LCL = \overline{X} - 3\sqrt{X\left(1-\overline{P}\right)}$ n, P as for Proportions	$\overline{X}$ = Average number of units in a sample size with the attribute of interest
Rates 	$UCL = \overline{\mu} + \frac{3\sqrt{\mu}}{\sqrt{n}}$ $UCL = \overline{\mu} - \frac{3\sqrt{\mu}}{\sqrt{n}}$ Centerline = $\overline{\mu}$ $\overline{\mu}$ = Average rate n = Sample size	$\overline{\mu}$ could be the average number of defects per unit from experience, or the specified allowable defect rate

Table 5-2. Typical control charts (Cont'd)

Chart	Equation	Notes
Rates – Constant sample size  	$UCL = \overline{\mu} + 3\sqrt{\overline{\mu}}$ $UCL = \overline{\mu} - 3\sqrt{\overline{\mu}}$ $\overline{R}$ = Average rate per sample	$\overline{r}$ could be the average number of defects per unit from experience, or the specified allowable defect rate

(3) Process capability. The capability of a process is defined as the inherent variability of a process in the absence of any undesirable special causes. Special causes include part wear, environmental disturbances, loose fasteners, untrained workers, substandard materials, changes in shift or suppliers, etc. The process capability is the smallest variability of which the process is capable with variability due solely to common causes. A common cause is inherent process randomness. Typically, processes follow the Normal probability distribution (see table 5-3). When the Normal is applicable, a high percentage of the process measurements fall between ±3σ (plus or minus 3 standard deviations) of the process mean or center. That is, approximately 0.27% of the measurements would naturally fall outside the ±3σ limits, with the balance (approximately 99.73%) within the ±3σ limits. Since the process limits extend from ±3σ to ±3σ, the total spread amounts to about 6σ total variation. The two primary measures of process capability are shown in table 5-4.

Table 5-3. Normal distribution

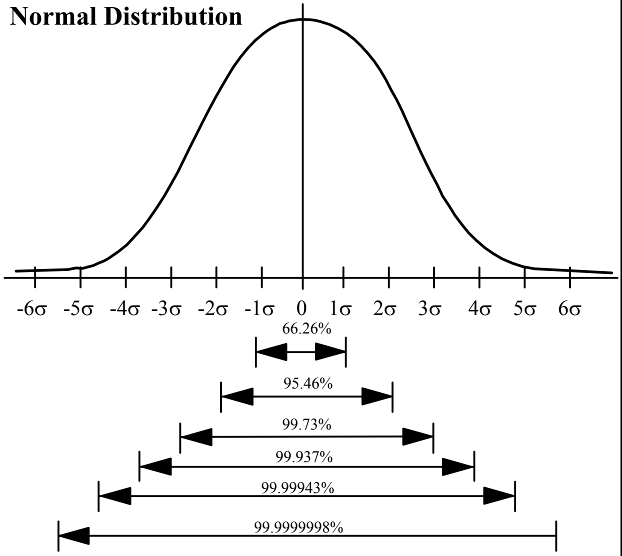
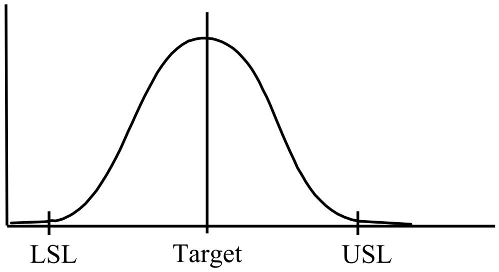
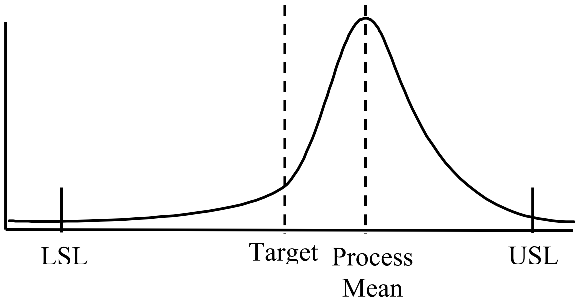
Tool	Equation
Normal Distribution  	$\sigma = \sqrt{\frac{\sum_{i=1}^{j}\left(\overline{X}_i - \overline{\overline{X}}\right)^2}{j-1}}$ $\overline{X}_i$ = mean of the i^{th} sample $\overline{X}_i$ $\overline{\overline{X}}$ = Mean of all samples j = Number of samples σ = standard deviation A fixed proportion of the product falls between any given values of σ. Hence, σ increases as variation increases

Table 5-4. Measures of process capability

Process Capability 	$Cp = \frac{USL - LSL}{6\sigma}$ USL = Upper specification limit LSL = Lower specification limit σ = Standard deviation $Cp < 1$ Generally considered poor $Cp = 1$ Generally considered marginal (99.7% in spec) $Cp \geq 1.3$ Generally considered good
Process Performance 	$Cpk = \frac{Min\ \{(USL - \mu);(\mu - LSL)\}}{3\sigma}$ Min {a;b) = Smaller of the two values USL, LSL, σ = As for Cp μ = Process mean $Cpk < 1$ Considered poor $Cpk = 1.5$ Considered excellent (Goal of "6σ" programs)

c. *Acceptance testing.* For products that are relatively expensive and complex, some form of product-level testing is desirable. The purpose of such testing is two-fold. First, it is better business to find a faulty product before shipping the product and having a customer find it. Second, by periodic tests, negative trends in product reliability can be detected and corrective action taken before too many products have been shipped. When tests are conducted for the latter purpose, the test used to demonstrate the product reliability during development (see Paragraph 4-7) can be repeated on a sample basis.

5-5. Conduct screening and testing

Screening eliminates unacceptable parts, thereby preventing them from being used in a finished system. Screening is one type of testing commonly conducted during testing. Another important type of testing often used during production is additional reliability testing.

a. *Burn-in.* Burn-in is one type of screening test. Burn-in is an attempt to eliminate early or infant failures. Using burn-in, we select the best items from a production run or lot, eliminating substandard or unacceptable ones. Ideally, we would have no unacceptable items – our design, quality control, and production control would maintain the variation in quality of individual items within acceptable limits. Even with the best controls, however, some quantity of unacceptable parts will exist due to our limited ability to design in and control reliability. Burn-in does not and cannot increase the inherent reliability of the system but controls the number of defective parts and items used in the system.

b. *Reliability testing.* Analyses and tests were used during design to achieve the required level of reliability and provide some measure of the inherent reliability. During production, especially long production runs, when changes can occur in even well-managed manufacturing, reliability is often used to ensure that no degradation in reliability due to manufacturing is occurring. The idea is to catch any negative trends before a large number of systems with inadequate reliability are delivered to the customer and take corrective action.

5-6. Production readiness

Being ready to start production on schedule can mean the difference between success and failure for many companies. Including manufacturing in the design process increases the probability of being ready to start production on schedule. Many factors determine readiness to start production. Table 5-5 lists some of the factors already discussed in this chapter with some key readiness questions.

Table 5-5. Some of the factors affecting production readiness

Factors	Key Questions
Processes	1. Are all processes developed and proved out? 2. Is there a plan for quality control, including statistical process control?
Manufacturing equipment	1. Is all manufacturing equipment in place and calibrated? 2. Has the equipment been proved out (e.g., pilot production)?
Personnel	1. Have the people with the requisite experience and skills been hired in the necessary numbers?
Training	1. Have the equipment operators and other manufacturing staff received the necessary training, earned any required certifications, and met any other requirements associated with the manufacture of the system?
Burn-in or screening	1. Have burn-in and screening plans been developed and checked for realism and practicality?
Suppliers	1. Are contracts in place with all suppliers? 2. Do the contracts include delivery, quality, and reliability requirements consistent with the system requirements?*
Packaging, Handling, and Transportation	1. Has the packaging been identified (standard packaging) or designed (custom packaging)? 2. Are plans in place to transport the system to the customer? If applicable, do the plans address transport of hazardous materials; any waivers to Federal, state, or local laws; or special arrangements (e.g., security)?

*Usually only for critical items – not for common items commercially available.

CHAPTER 6

RELIABILITY IMPROVEMENT

6-1. Data collection

In chapters 3 and 4, the importance and use of data during design was discussed. Collecting and analyzing data from development testing is an important part of the process of designing for and improving reliability. In chapter 5, we saw that the need for data does not end with the completion of design and development but is an important part of the overall quality control program. Data collection is also important during the life of a system.

a. *Importance of operational data use to the manufacturer*. For systems having some form of warranty, the manufacturer can use return data, to assess the economic viability of making changes to the design or manufacturing processes. Table 6-1 lists some of the ways in which the manufacturer can use data collected during the operational life of the system. Even when it is not economically advantageous to reduce the warranty claims for the current system, the data may show where changes should be made in the next system. Although it is relatively simple for the manufacturer to collect data during the warranty period, the effort becomes difficult and often impossible after the warranty expires. Often, it is only feasible to continue data collection when the manufacturer is providing maintenance or other logistics support over a system's life.

Table 6-1. Manufacturer's use of operational data

Type of Data	Use
Actual number of warranty returns versus expected number	Determine if potential reliability, operator, or maintenance problems exist, forecast actual warranty costs
Customer complaints	Qualitatively determine level of system performance
Repair data*	Determine nature of failures, frequency of repair
Failure analysis data*	Determine failure causes, refine or develop design requirements (standard practices), develop design, part selection, source, or other changes

*When the manufacturer is given access to such data by the customer or is providing the maintenance.

b. *Importance of operational data use to the customer.* The user is always interested in evaluating the performance of a system and in measuring the resources needed to operate and support the system. If the manufacturer or a third-party source is providing the logistics support (perhaps even operating the system), then the applicable service contract should include the requirement to collect data and use that data in managing the services being provided. The user has some of the same objectives as a manufacturer in collecting operating data but has some additional ones. Some of the ways in which the user can use data collected during the operational life of the system are listed in table 6-2.

Table 6-2. User's use of operational data

Type of Data	Use
Actual number of warranty returns versus expected number	Forecast impact of delivery schedules. Qualitatively determine level of system performance.
Repair data*	Determine nature of failures, frequency of repair.
Failure analysis data*	Determine failure causes, refine or develop design requirements (standard practices), develop design, part selection, source, or other changes.

*When the user is providing the maintenance.

6-2. Conduct trending

Once a system is fielded, it is important to collect performance data during its operational life. Such data can be used for a variety of purposes including detecting negative trends in reliability in sufficient time to take prompt corrective action. Although positive trends can occur, they are the exception – system reliability usually degrades over time.

a. *System failure behavior.* During their useful life, most systems tend to behave as if the times between system failures are exponentially distributed. This behavior results because a system is made up of many different types of parts and assemblies, each having its own failure characteristics. Due to the mix of failure modes and varying underlying failure distributions, a system has a constant rate of failure (and a constant mean time between failure, MTBF), unless the reliability is improving or degrading. The reliability improves when some action is being taken to decrease the number of failure per unit time. These actions can include design changes, improved maintenance training, and changes in operating procedures. Degradation of system reliability can occur for a variety of reasons, some of which are shown in table 6-3.

Table 6-3. Reasons why system reliability degrades over time

Reason	Discussion
Change in operating concept	If system is used in a manner different from that originally allowed for in the design, new failure modes can occur and the overall frequency of failures can increase. In such cases, corrective actions can be expensive or impractical. If the new operating concept is essential, decreased reliability may have to be accepted.
Change in operating environment	If a system is used in an environment different from that originally allowed for in the design, new failure modes can occur and the overall frequency of failures can increase. In such cases, corrective actions can be expensive or impractical. If the new operating concept is essential, decreased reliability may have to be accepted.
Inadequate training	If operating or maintenance training is inadequate, the number of failures induced by improper operation or maintenance usually increases. The corrective action is to improve the training.
Wearout	As systems age, the number of failures per unit time of parts having wearout characteristics, primarily mechanical parts, will increase. A preventive maintenance program to replace or overhaul such parts will prevent wearout from becoming a problem. Ideally, the preventive maintenance program is based on the reliability characteristics of the parts (i.e., a reliability-centered maintenance program).
Change in supplier	If a supplier chooses to stop manufacturing a part or material, goes out of business, or no longer maintains the necessary levels of quality, an alternate source of supply is needed. If reliability is not a major consideration in selecting the new supplier, system reliability may degrade.
Poor configuration control	Over a system's life, there is the temptation to reduce costs by substituting lower-priced parts and materials for those originally specified by the designer. Although the purchase price may be lower, life cycle costs will increase and the mission will suffer if the "suitable subs" do not have the necessary reliability characteristics. Strong configuration management and a change control process that addresses all factors, including reliability, are essential throughout the life of the system.
Manufacturing problems	Although the manufacturing processes may have been qualified and statistical process implemented at the start of production, changes can occur during the production line that degrade reliability. This possibility increases as the length of the production run increases. Constant quality control is essential.

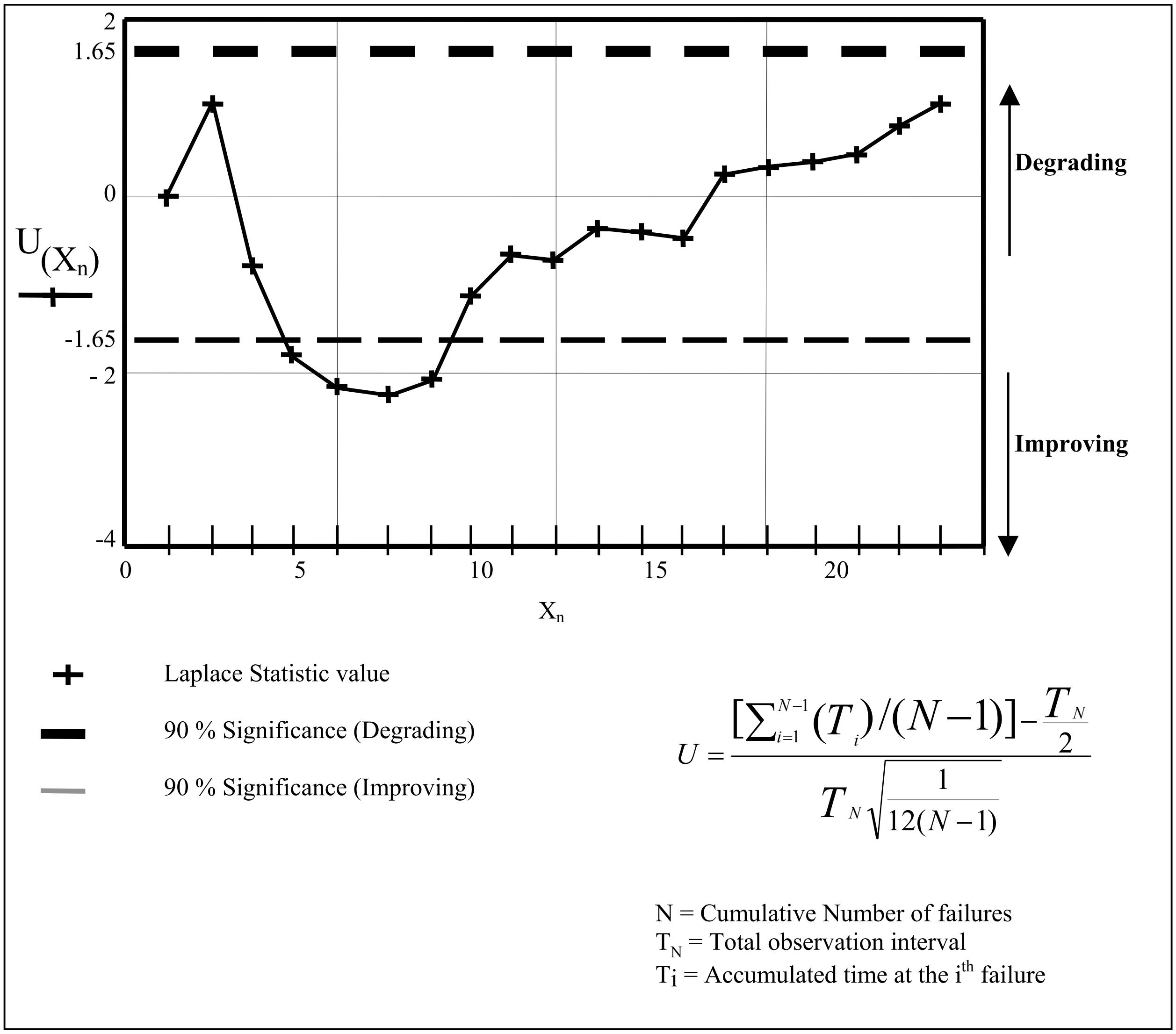
b. *Detecting trends in system reliability.* Although systems do tend to exhibit a constant MTBF during their useful lives, some statistical variation in the MTBF is to be expected. Whether the MTBF of a single system or a population of systems is being measured, the measured value will fluctuate. Some of this fluctuation is the result of statistical variation. Some fluctuation may result from operating at different times of the year or in different operating locations. For example, hydraulic seals may leak more during cold weather (winter) or when the temperatures are widely varying from day to day (possible in spring or fall). It is important to distinguish between such "normal" variation and a genuine negative trend. One tool for making this distinction is the Laplace statistic.

(1) The Laplace statistic, U, came from work done by the French mathematician Pierre-Simon Laplace. In 1778, he showed that U will be normally distributed with a mean of 0 and standard deviation of 1 when no trend is evident from the data with a given level of confidence. In the case of times to failure, if U is normally distributed with a mean of 0 and standard deviation of 1, the times between failures are exponentially distributed. Otherwise, a negative or positive trend exists. The presence or absence of a trend must be stated with a given level of confidence. That is, we cannot be 100% certain that a trend does or does not exist. Instead, we must accept some risk that we are wrong (i.e., we state there is a trend and there is not or we state that there is no trend and there really is).

(2) The following example illustrates how the Laplace statistic can be used to track system reliability and detect a trend. Suppose we have the failure data shown in table 6-4 for an electrical generation system. For each data point, the U statistic is calculated using the equation shown in figure 6-1 for failure truncation observations (i.e., the observations ended after a pre-determined number of failures) and plotted. (Note: if the observations ceased after a given time, a different equation would be used.) The values are shown in table 6-5. The control limits are based on the desired level of confidence. In this example, we used a confidence level of 90%. As long as the plotted values of U remain within the control limits, we can state with 90% confidence that there is no trend.

Table 6-4. Failure data for example

Failure No.	**Hrs. at Failure**	**Failure No.**	**Hrs. at Failure**	**Failure No.**	**Hrs. at Failure**
1	296	8	14971	15	22076
2	348	9	15056	16	23159
3	1292	10	17415	17	24589
4	2923	11	17473	18	24679
5	6405	12	19686	19	24764
6	10746	13	19692		
7	14934	14	21058		



$$U = \frac{\left[\sum_{i=1}^{N-1}(T_i)/(N-1)\right] - \frac{T_N}{2}}{T_N\sqrt{\frac{1}{12(N-1)}}}$$

N = Cumulative Number of failures
T_N = Total observation interval
T_i = Accumulated time at the i^{th} failure

Figure 6-1. Equation for U and plot of U values at 90% confidence for example.

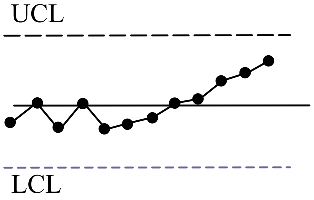
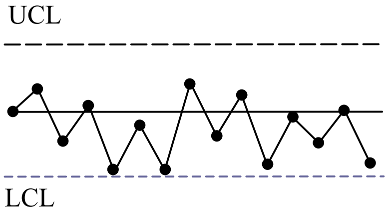
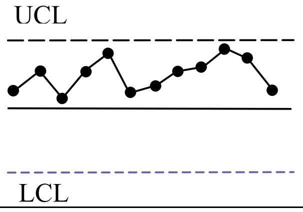
Table 6-5. Table of calculated values of U for example

Failure Number	U	Failure Number	U
1	0*	11	-0.18676
2	1.214426	12	-0.3403
3	-1.22854	13	0.172303
4	-1.67533	14	0.198925
5	-2.15012	15	0.325564
6	-2.24911	16	0.412416
7	-2.15835	17	0.38101
8	-1.35159	18	0.760795
9	-0.6759	19	1.118446
10	-0.75564		

*It is impossible to determine a trend with one data point, so U is 0.

(3) Even when the plotted values of U do not fall outside of the control limits, rules of thumb can be used to determine if a potential problem is indicated by the data. These rules of thumb are shown in table 6-6.

Table 6-6. Three possible signs of a problem when no points are outside of the upper control limit

Sign	Example	Discussion
7 consecutive points monotonically going in the "wrong" direction (toward the upper limit)		Statistical variation makes it highly unlikely that any of these three signs occur due to chance. In other words, it is likely that the sign occurs due to: ▪ A real degradation in reliability ▪ Irregularities in data reporting ▪ Unusual or improper actions by operators or maintainers ▪ Other changes Whenever any of these signs are observed or when the plot goes above the UCL, additional investigation should be conducted to determine the underlying root cause.
14 points alternating up and down		
10 consecutive points above the center line		

6-3. Identify needed corrective actions

When trending, field returns, and other user complaints indicate a problem in system performance, analysis is required to determine the root cause of the problem. As suggested earlier, the root causes may be the way the system is being maintained or operated, problems in the manufacturing process, or premature wearout. It is critical that the true cause be determined. Obviously changing the design is inappropriate if the true cause of the problem is an increase in induced failures due to inadequate training of maintenance personnel. Table 6-7 lists some of the potential causes of reliability degradation and the ways in which that degradation might be addressed. Corrective actions are taken only if safety is concerned or when the benefits outweigh the costs of implementing the corrective action.

Table 6-7. Causes of reliability degradation and potential corrective actions

Cause	Potential Corrective Actions
Premature wearout	Parts may have been inappropriately selected or applied; select higher reliability parts to replace the offending parts; evaluate effectiveness and frequency of preventive maintenance; select different supplier that provides higher reliability parts.
Unforeseen failure modes	Initial description of operating environment and stresses may have been incomplete or inaccurate; review original analyses and conduct additional analyses to determine if any design changes or changes in parts application or indicated.
Higher frequency of failures than forecasted	Initial description of operating environment and stresses may have been incomplete or inaccurate; review original analyses and conduct additional analyses to determine if any design changes or changes in parts application or indicated.
Inadequate training	Training may not have been developed or implemented properly; ensure training is effective and accurate; ensure all personnel, operational and support, receive necessary training before operating or working on the system; ensure all personnel stay up-to-date on system operation and maintenance.
Improper operation	Operating procedures may not have been developed properly, are out of date, or are not being followed; ensure procedures are accurate and up-to-date and all operators are following procedures.
Improper maintenance	Maintenance procedures may not have been developed properly, are out of date, or are not being followed; ensure procedures are accurate and up-to-date and all maintenance personnel are following procedures.

APPENDIX A

REFERENCES

Related Publications

Government Publications

MIL-HDBK-189, Reliability Growth Management, 24 October 2000.

MIL-HDBK-470A, Designing and Developing Maintainable Products and Systems, Volumes I and II, 4 August 1997.

MIL-HDBK-781A, Reliability Test Methods, Plans, and Environments for engineering Development, Qualification, and Production, 1 April 1996.

MIL-HDBK-217F, Reliability Prediction of Electronic Equipment, 28 February 1995.

MIL-HDBK-388, Electronic Reliability Design, 1 October 1998.

US Army TM 5-698-1, Reliability/Availability of Electrical & Mechanical Systems for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities.

US Army TM 5-698-2, Reliability-Centered Maintenance (RCM) for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities.

Non-Government Publications

Abernethy, Dr. Robert B., The New Weibull Handbook, 4th Edition, Abernethy, North Palm Beach, 1996.

ARINC Research Corporation, Product Reliability, Maintainability, and Supportability Handbook, Michael Pecht, Editor, CRC Press, 1995.

Blanchard, Benjamin, Systems Engineering and Analysis, 3rd Edition, Prentice-Hall, 1996.

Blanchard, Benjamin, Logistics Engineering and Management, 5th Edition Prentice-Hall, 1998.

Hoyland, A. and M. Rausand, System Reliability Theory: Models and Statistical Methods, John Wiley & Sons, 1994.

Meyer, Paul L., Introductory Probability and Statistical Applications, , Addison-Wesley, 1970.

Miller, Paul and Irwin Freund, Probability and Statistics for Engineers, 6th Edition, Prentice-Hall, 1999.

O'Connor, Patrick D.T., Practical Reliability Engineering, Halsted Printing, 4th Edition, 2002.

Reliability Analysis Center, Reliability Toolkit: Commercial Practices Edition,

Shooman, Martin L., Probabilistic Reliability An Engineering Approach, 2nd Edition, Krieger Publishing Company 1990.

Reliability Analysis Center, Mechanical Applications in Reliability Engineering, 1993.

Reliability Analysis Center, Practical Statistical Tools for the Reliability Engineer, 1999.

Reliability Analysis Center, Reliability Toolkit: Commercial Practices Edition, 1995.

APPENDIX B

AVAILABILITY

B-1. Availability as a function of reliability and maintainability

The effects of failures on availability can be minimized with a "good" level of maintainability. Consequently, reliability and maintainability are said to be complementary characteristics. This complementary relationship can be seen by looking at a graph of constant curves of inherent availability (A_i). A_i is defined by the following equation and reflects the percent of time a product would be available if no delays due to maintenance, supply, etc. were encountered:

$$A_i = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \qquad \text{(Equation 1)}$$

where MTBF is mean time between failure and MTTR is mean time to repair

If a product never failed, MTBF would be infinite and A_i would be 100%. Or, if it took no time to repair the product, MTTR would be zero and again the availability would be 100%. Figure B-1 is a graph showing curves of constant availability calculated using equation 1. Note that you can achieve the same availability with different values of R&M. As reliability decreases, higher levels of maintainability are needed to achieve the same availability and vice versa.

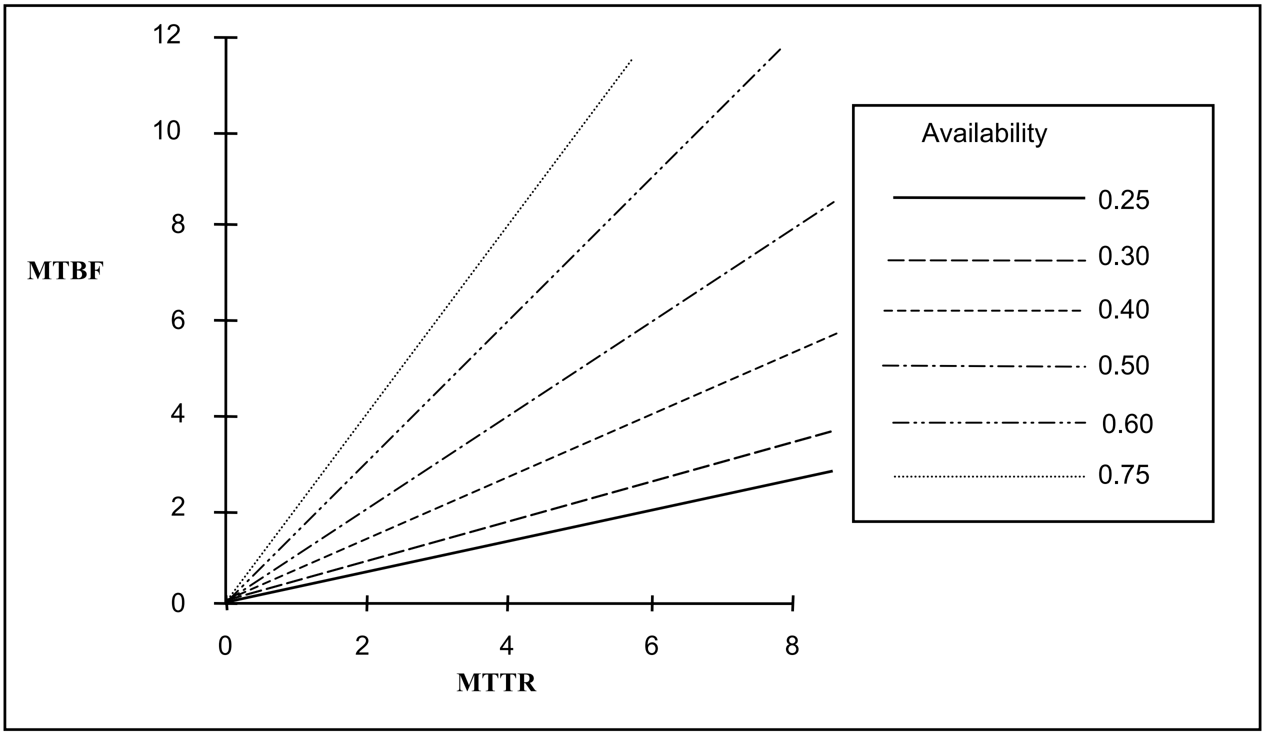


Figure B-1. Different combinations of MTBF and MTTR yield the same availability.

a. *Trade space.* This relationship between reliability and maintainability means that trades can be made to achieve the same level of availability. The range of allowable values of two or more parameters that satisfies some higher-level requirement is called trade space. If designers are having a particularly difficult time achieving a certain level of reliability, they can compensate by achieving a higher level of maintainability. Of course, the customer's top-level requirement had to have been availability. If reliability were the top-level requirement, then that is the level needed.

b. *Maximum repair time*. Even if a customer specifies availability as the top-level requirement, they may not be able to tolerate downtimes in excess of some value. In that case, in addition to specifying availability, the customer will specify a maximum time to repair. However, since time to repair is a variable, it is impossible to guarantee an absolute maximum. Therefore, a commonly used maintainability parameter is $M_{Max}(\varphi)$, where φ is a stated level of confidence. Thus, a requirement of $M_{Max}(95)$, = 6 hours means that 95% of all repairs must take less than 6 hours.

B-2. Availability as a function of logistics

Even if all reliability and maintainability requirements are met, it is possible that the availability achieved in actual use will be less than needed. The reason that this can occur is that when a failure does occur and spares are needed to make the repair, it is possible that the spares will not be available. Alternatively, the required maintenance personnel may not be available to make the repair, or they may not be adequately trained to make the repair in the optimum time. Consequently, the level of availability achieved in the field is a function not only of reliability and maintainability but also of logistics. Finally, availability is affected by all maintenance, preventive as well as corrective. So actual availability must take into consideration all maintenance performed. Thus, we must define availability in the field differently from Inherent Availability. This aspect of availability is called Operational Availability (A_o). A_o is estimated using the following equation:

$$A_o = \frac{\text{MTBM}}{\text{MTBM} + \text{MDT}} \text{ x } 100\% \qquad \text{(Equation 2)}$$

where MTBM is mean time between all maintenance and MDT is mean downtime

APPENDIX C

EXAMPLES OF RELIABILITY PREDICTION METHODS

C-1. Introduction

The following examples of reliability prediction methods have been simplified by omitting some mathematical constraints. For example, it is assumed that the elements are independent (that is, if the failure of one has no effect on another). The examples, however, are valid and should give the reader a feeling for the process of combinatorial reliability calculations.

C-2. Failure rate example

Figure C-1 shows a series system with four independent parts. The failure rate, λ_i, of each part is indicated below the element. The failure rate of this series system, λ_{System}, is equal to the sum of the individual failure rates (the mean time to failure is the inverse of the failure rate):

$$\lambda_{\text{System}} = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4$$

$$= 10.1 + 5.6 + 1.1 + 15.5$$

$$= 32.3 \text{ (failures per million operating hours)}$$

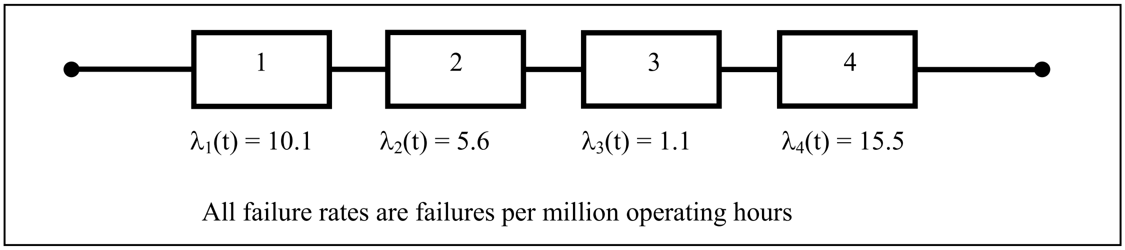


Figure C-1. The failure rate of this series system is $\lambda_{System} = 32.3$ *failures per million operating hours. The mean time to failure is* $1/\lambda_{System} = 30{,}960$ *hours.*

C-3. Similarity analysis

A new system being developed will consist of a signal processor, a power supply, a receiver transmitter, and an antenna, all in a series configuration. The antenna and power supply are off-the-shelf items that are used in a current system. The reliability of each of these items for an operating period of 150 hours is 0.98 and 0.92, respectively. The signal processor will be a new design incorporating new technologies expected to provide a 20% improvement over previous signal processors. The prior generation of signal processors has exhibited failure rates ranging from 1 to 3 failures per 10,000 operating hours. The receiver transmitter is a slightly modified version of an existing unit that has achieved an MTBF of 5,000 hours for the past year. The new system will be used in a slightly harsher environment (primarily higher temperatures) than its predecessor and will operate for 150-hour missions.

a. The observed reliabilities of the antenna and power supply can be used because they are for 150-hours, the length of a mission for the new system. However, since the environment is slightly harsher, the reliabilities are degraded by 5% to 0.93 and 0.87, respectively.

b. The failure rate for the new signal processor is estimated using a conservative value for its predecessor of 3 failures per 10,000 hours. This value is adjusted to address the harsher environment by increasing it by 5% to 3.2

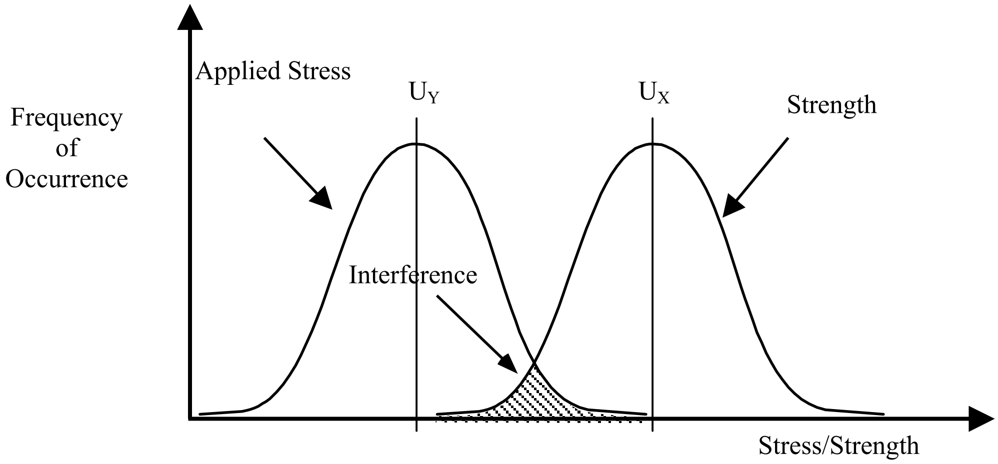
failures per 10,000 hours. Since a constant failure rate is being used, it is assumed that the underlying pdf is the exponential. The reliability of the new signal processor for 150-hours is estimated as $e^{-(0.00032 \times 150)} = 0.95$.

c. The old receiver transmitter has an MTBF of 5,000 hours, which is equivalent to a failure rate of 0.0002 failures per hour. We degrade this by 5% to account for the more severe environment and use a failure rate of 0.00021. The reliability of the modified receiver transmitter is $e^{-(0.00021 \times 150)} = 0.97$.

d. The reliability of the new system is estimated to be 0.93 x 0.87 x 0.95 x 0.97 = 0.75.

C-4. Stress-strength interference method

Figure C-2 shows the curves for the stress and strength distributions for a mechanical part used in a given application. In this case, both stress and strength are Normally distributed. For two Normal curves, the area of interference is called Z, the Standardized Normal Variant. If we have the values for the means and variances of the stress and strength, we can calculate Z and look up the probability (the area of interference) in probability tables.



$$Z = \frac{U_x - U_y}{\sqrt{\sigma_x^2 + \sigma_y^2}}$$

Where:

U_x = Mean strength
U_y = Mean stress

σ_x^2 = Strength variance

σ_y^2 = Stress variance

Z = Standardized Normal Variant from probability tables

Figure C-2. Example of the stress-strength interference method when both stress and strength are Normally distributed.

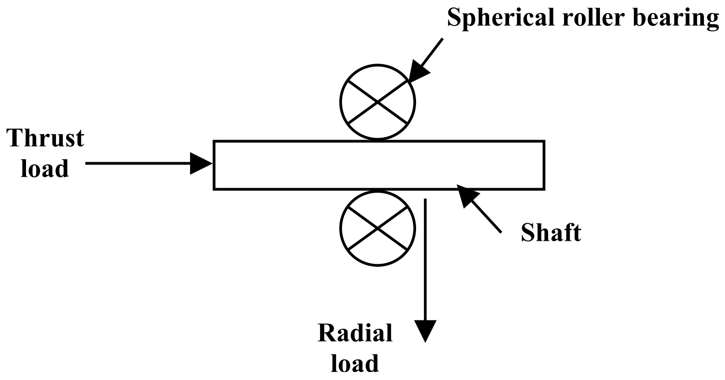
a. Assume the mean strength is 50,000 psi and the variance of the strength distribution is 40,000 psi^2. Assume the mean stress is 30,000 psi and the variance of the stress distribution is 22,000 psi^2. Using these values, we calculate Z = 2.54.

b. From a probability table, we find that a value of 2.54 for Z corresponds to a probability of 0.00554, or 0.544% probability of failure (unreliability).

c. The reliability is 1 - Interference = 1 - 0.00554 = 0.99445 or 99.445%.

C-5. Empirical model

Figure C-3 shows a spherical roller bearing that supports a rotating shaft. The empirical model for predicting the B_{10} fatigue life of bearings was given in table 3-1 and is shown again in figure C-3. Recall that the B_{10} life is the life at which 90% of a given type of bearing will survive.



$P = XR + YT$

where: R = Radial load (LBS)
T = Thrust load (LBS)
X and Y = Radial and thrust factors

BEARING TYPE	X_1	Y_1	X_2	Y_2
Single-row ball	1.00	0.00	0.56	1.40
Double-row ball	1.00	0.75	-.63	1.25
Cylindrical roller	1.00	0.00	1.00	0.00
Spherical roller	1.00	2.50	0.67	3.70

The set of X_1 Y_1 or X_2 Y_2 giving the largest equivalent load should be used

$$B_{10} = \left(\frac{C}{P}\right)^{K} \text{x } 10^{6} \text{ revolutions}$$

Figure C-3. Calculating the B_{10} life for a spherical roller bearing.

a. Assume that the radial load is 1,000 lbs. and the thrust load is 500 lbs. As stated in the figure, we calculate the resultant load, P, by first using the factors X_1 and Y_1 and then X_2 and Y_2 and using the largest result. For a spherical roller bearing, $P_1 = 1 \text{ x } 1{,}000 + 2.5 \text{ x } 500 = 2{,}250$, and $P_2 = 0.67 \text{ x } 1{,}000 + 3.7 \text{ x } 500 = 2{,}520$. The largest result of these two calculations, 2,520 lbs. will be used.

b. Recall that the values of C and K come from the bearing manufacturer's literature. For the example, K = 10/3 and C = 3,000 lbs. Substituting in the empirical bearing fatigue life equation, we find that the B_{10} life is 1.8 million revolutions.

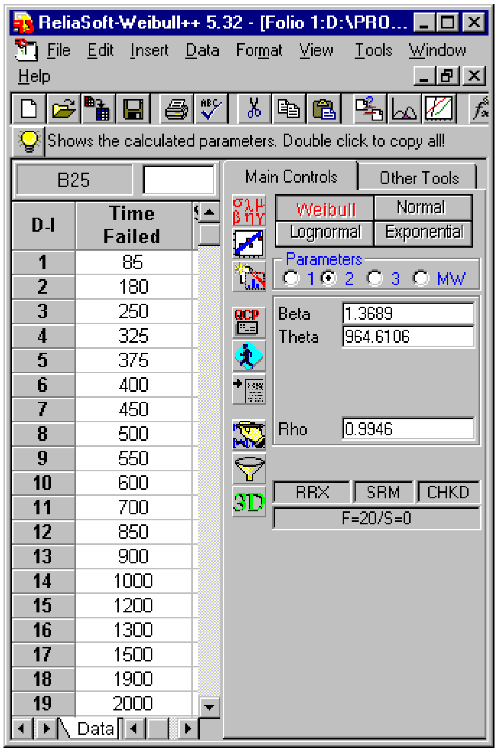
C-6. Failure data analysis

In this example, we have tested 20 valves until all failed. The times to failure, in cycles, are shown in table C-1. We can use Weibull analysis to determine the reliability of the valves at any point in time (number of cycles); in this case, at 100 cycles. A variety of software packages are commercially available for performing Weibull analysis.

Using one of these software packages, Weibull++™ by ReliaSoft ™ Corporation, we find that the reliability of this type of valve, when operated for 100 cycles is 90%. Figures C-4 and C-5 show the input page and graph for the analysis using the software.

Table C-1. Times to failure (cycles) for 20 valves

85	180	250	325
375	400	450	500
550	600	700	850
900	1000	1200	1300
1500	1900	2000	2550



Shows the calculated parameters. Double click to copy all!

B25

D-I	Time Failed
1	85
2	180
3	250
4	325
5	375
6	400
7	450
8	500
9	550
10	600
11	700
12	850
13	900
14	1000
15	1200
16	1300
17	1500
18	1900
19	2000

Parameters ○ 1 ● 2 ○ 3 ○ MW

Beta 1.3689
Theta 964.6106
Rho 0.9946

F=20/S=0

Figure C-4. Input page from Weibull++ ™ for failure data analysis example.

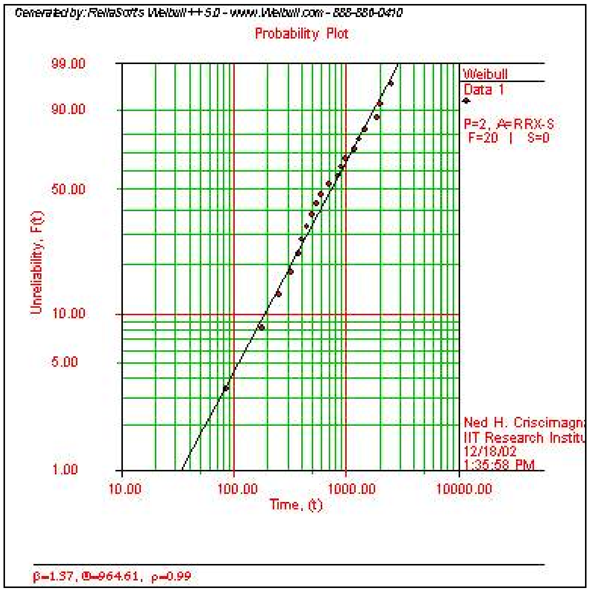


Figure C-5. Graph of Weibull plot from Weibull++ ™ for data analysis example.

GLOSSARY

ACTIVE REDUNDANCY: Two or more components in a parallel combination where all are powered and active simultaneously. Only one component needs to function for the system (or next higher assembly) to function.

ASSESSMENT: Current evaluation of a component's or system's reliability. A prediction.

AVAILABILITY: A measure of the percentage of time that an equipment or system is operationally ready. Usually defined in terms of MTTR and MTBF (MTTF) as:

$$A(t) = [MTBF\ (MTTF)] / [MTTR + MTBF\ (MTTF)]$$

BURN-IN: Eliminating early failures by operating the product (l00% sampling). Ideally done in an environment similar to the operational environment.

CONFIDENCE LEVEL/INTERVAL: A statistical measure of the uncertainty associated with an estimate. For example, an estimate of MTBF is 103 hours. Using statistical techniques (such as the chi-square method) we obtain a 95% confidence interval of 100.1 to 105.9. That is, 95% of the time, the actual MTBF will be between 100.1 and 105.9 hours. The confidence interval depends on sample size and variance.

FAILURE RATE: Defined as the number of failures per unit time. Mathematically, the failure rate (also called the hazard function) is

$$z(t) = f(t) / R(t)$$

Where R(t) is the reliability function and f(t) is the underlying probability distribution. For the exponential distribution

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

Thus the failure rate, when the exponential distribution describes the time to failure, is constant.

FMEA: Failure Modes and Effects Analysis. An analysis to determine the ways in which failure can occur and the effect of the failure on the system and/or other equipment.

FOT&E: Follow-On Operational Test and Evaluation. Operational testing of a system conducted in an operational environment. Generally occurs after IOT&E is completed and is done on production items.

HARDWARE RELIABILITY: The inherent reliability of an individual piece of equipment, usually an LRU. Measured in terms of MTBF or MTTF. System hardware reliability is the overall hardware reliability, also measured in terms of MTBF or MTTF.

HI-REL: High Reliability. Usually used to describe piece parts that have been produced to an extremely demanding specification.

IOT&E: Initial Operational Test and Evaluation. Early operational testing of a system conducted prior to a production decision. Normally conducted on pre-production items in a less than perfectly realistic environment.

ITEM: Used interchangeably in this document with product or equipment. Usually refers to the individual article rather than the inclusive class or kind of product.

LAPLACE STATISTIC. A statistic used to determine if a data set indicates a positive or negative trend, at a given level of confidence.

LCC: Life Cycle Cost. The total cost of a system from its inception to its retirement. Usually defined as including four major cost categories: development, production, operation, and support.

LRU: Line Replaceable Unit. An equipment usually removable as an entity at the aircraft or operating site. Includes items such as a radio receiver, hydraulic pump, or inertial platform.

LSC: Logistic Support Cost. The cost of a support category such as spares, maintenance, or ground support equipment.

MEAN: Also called the expected value of a random variable, the mean is defined as follows: Let X be a continuous random variable with a probability density function = f. The expected value of X is:

$$E(X) = \int_{x} xf(x)dx$$

The mean, or expected value, is analogous to the concept of center of mass in mechanics.

MISSION RELIABILITY: The probability that a system will complete its intended mission. Hardware failures that do not hinder the success of the mission (e.g., due to redundancy) are not counted against mission reliability.

MTBF: Mean Time Between Failures. The expected value, or mean, of the time between failures of an item. For the case where the exponential distribution is used, the MTBF is the inverse of the failure rate. MTBF is used only for reparable equipment/systems and can also be used to describe the overall system hardware reliability.

MTTF: Mean Time to Failure. Has the same meaning as MTBF except it is used for equipment/systems where renewal (repair or replacement) does not occur. It is numerically equal to the MTBF only for a single parameter distribution.

MTTR: Mean Time to Repair. The expected value, or mean, of the time required to repair an equipment/system.

OPERATIONAL RELIABILITY: The reliability of a system or equipment after it is put in operation.

PAG: Parts Advisory Group. A group of managers and specialists who advise on the selection of parts for a program.

PARALLEL COMBINATION: The combining of two or more items in such a way that only one is required for operation – thus, the parallel combination is characterized by alternate paths of operation.

PCB: Parts Control Board. A board of managers and specialists who control the selection of parts for a program.

PPL: Preferred Parts List. A list of parts that have proved themselves and are approved for use.

PROBABILITY DISTRIBUTION: A formula that describes the probabilities associated with the values of a discrete random variable.

PRODUCT: An equipment, item, or hardware contracted for by a customer. Usually used to describe the inclusive class or kind of item, equipment, etc., rather than each individual entity.

QA: Quality Assurance. A program that provides for the integrity of a design through inspection and control of drawings, manufacturing, shipping, handling, and materials.

REDUNDANCY: A design technique that provides alternate paths of operation through parallel combination of equipment.

RELIABILITY PREDICTION: An estimate of reliability based on information that includes historical data, piece parts count, complexity, and piece part failure rates.

RIW: Reliability Improvement Warranty. A contractual provision that incentivizes the contractor to reduce support costs by improving reliability.

SCREENING: A series of tests intended to weed out items that are not within certain limits of performance.

SERIES COMBINATION: The combining of two or more items in such a way that all must operate for the system to operate -there is only one path of operation.

STANDBY REDUNDANCY: Two or more components in a parallel combination where only one is functioning at any time. The other components are disconnected and power is applied prior to or simultaneously with switching.

SUCCESS: Achievement of an objective or completion of a function or set of functions.

SWITCH: A device that selects one component in a parallel or redundant configuration as the functioning component. Used for standby redundancy. Incorporates such provisions as logic circuits and fault detection.

The proponent agency of this publication is the Chief of Engineers, United States Army. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQUSACE, (ATTN: CEMP-SP), Washington, DC 20314-1000.

By Order of the Secretary of the Army:

JOHN M. KEANE
General, United States Army
Acting Chief of Staff

Official:
Joel B. Hudson
JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army

Distribution:

To be distributed in accordance with Initial Distribution Number (IDN) 344775, requirements for non-equipment TM 5-698-3.

☆ U.S. GOVERNMENT PRINTING OFFICE: 2003 496-806/95455