TM 5-698-1

TECHNICAL MANUAL

RELIABILITY/AVAILABILITY OF ELECTRICAL & MECHANICAL SYSTEMS FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) FACILITIES

HEADQUARTERS, DEPARTMENT OF THE ARMY
14 MARCH 2003

REPRODUCTION AUTHORIZATION/RESTRICTIONS

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:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the Secretary of the Army

Distribution:

To be distributed in accordance with Initial Distribution Number (IDN) 344746, requirements for non-equipment TM 5-698-1.

☆ U.S. GOVERNMENT PRINTING OFFICE: 2003 496-806/85933

Technical Manual
No. 5-698-1

HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, *14 March 2003*

APPROVED FOR PUBLIC RELEASE: DISTRIBUTION IS UNLIMITED

RELIABILITY/AVAILABILITY OF ELECTRICAL & MECHANICAL SYSTEMS FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) FACILITIES

CONTENTS

CONTENTS

LIST OF TABLES

CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Purpose

The purpose of this technical manual is provide facility managers with the information and procedures necessary to baseline the reliability and availability of their facilities, identify "weak links", and to implement cost-effective means of improving reliability and availability.

1.2 Scope

The information in this manual reflects both the move to incorporate commercial practices and the lessons learned over many years of acquiring weapon systems "by the book." It specifically focuses on the availability of electrical and mechanical systems for command, control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) facilities and the role reliability plays in determining availability. The manual, in the spirit of the new policies regarding acquisition, describes the objectives of a sound strategy and the tools available to meet these objectives.

1-3. References

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

1-4. Definitions (Special Terms)

The three key terms used in this TM are availability, reliability, and maintainability. Additional terms and abbreviations used in this manual are explained in the glossary.

a. Availability. Availability is defined as the percentage of time that a system is available to perform its function(s). It is measured in a variety of ways, including Uptime/Uptime + Downtime (Total Time) and MTBF/MTBF+MTTR. Chapter 2 has a detailed discussion of availability.

b. Reliability. Reliability is concerned with the probability and frequency of failures (or more correctly, the lack of failures). A commonly used measure of reliability for repairable systems is the mean time between failures (MTBF). The equivalent measure for non-repairable items is mean time to failure (MTTF). Reliability is more accurately expressed as a probability over a given duration of time, cycles, etc. For example, the reliability of a power plant might be stated as 95% probability of no failure over a 1000-hour operating period while generating a certain level of power. Reliability is usually defined in two ways as shown in the following definitions. (Note that the electrical power industry has historically not used the definitions given here for reliability. The industry defines reliability as the percentage of time that a system is available to perform its function; i.e., availability. The relationship between reliability and availability is discussed in paragraph 1-6.)

(1) The duration or probability of failure-free performance under stated conditions.

(2) The probability that an item can perform its intended function for a specified interval under stated conditions. (For non-redundant items this is equivalent to the preceding definition (1). For redundant items this is equivalent to definition of mission reliability.)

c. Maintainability. Maintainability is defined as the measure of the ability of an item to be retained in or restored to a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. Simply stated, maintainability is a measure of how quickly and economically failures can be prevented through preventive maintenance or system operation can be restored following a failure through corrective maintenance. A commonly used measure of maintainability in terms of corrective maintenance is the mean time to repair (MTTR). Note that maintainability is not the same as maintenance. Maintainability is a design parameter, while maintenance consists of actions to correct or prevent a failure event.

1-5. Historical perspective

In measuring the performance of electrical and mechanical systems for C4ISR facilities, availability is of critical concern. The level of availability achieved in operation is determined by many factors, but arguably the two most important factors are reliability and maintainability. Reliability and maintainability (R&M) are two disciplines that have increased in importance over the past 30 years as systems have become more complex, support costs have increased, and defense budgets have decreased. Both disciplines, however, have been developing for much longer than 30 years.

a. Reliability. Reliability, for example, has been a recognized performance factor for at least 50 years. During World War II, 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: $R_S = R_1 \times R_2 \times \ldots \times R_n$.

b. Maintainability. Maintainability is perhaps less fully developed as a technical discipline than is reliability. Maintainability is a measure of the relative ease and economy of time and resources with which maintenance can be performed. Maintainability is a function of design features, such as access, interchangeability, standardization, and modularity. Maintainability includes designing with the human element of the system in mind. The human element includes operators and maintenance personnel.

1-6. Relationship among reliability, maintainability, and availability

Perfect reliability (i.e., no failures, ever, during the life of the system) is difficult to achieve. Even when a "good" level of reliability is achieved, some failures are expected. The effects of failures on the availability and support costs of repairable systems can be minimized with a "good" level of *maintainability*. A system that is highly maintainable can be restored to full operation in a minimum of time with a minimum expenditure of resources.

a. Inherent availability. When only reliability and corrective maintenance or repair (i.e., design) effects are considered, we are dealing with *inherent availability*. This level of availability is solely a function of the inherent design characteristics of the system.

b. Operational availability. Availability is determined not only by reliability and repair, but also by other factors related to preventative maintenance and logistics. When these effects of preventative maintenance and logistics are included, we are dealing with *operational availability*. Operational availability is a "real-world" measure of availability and accounts for delays such as those incurred when

spares or maintenance personnel are not immediately at hand to support maintenance. Availability is discussed in more detail in chapter 2.

1-7. The importance of availability and reliability to C4ISR facilities

C4ISR facilities support a variety of missions. Often these missions are critical and any downtime is costly, in terms of economic penalties, loss of mission, or injury or death to personnel. For that reason, availability is of paramount importance to C4ISR facilities.

a. Availability. Availability of a system in actual field operations is determined by the following.

(1) The frequency of occurrence of failures. These failures may prevent the system from performing its function (mission failures) or cause a degraded system effect. This frequency is determined by the system's level of reliability.

(2) The time required to restore operations following an system failure or the time required to perform maintenance to prevent a failure. These times are determined in part by the system's level of maintainability.

(3) The logistics provided to support maintenance of the system. The number and availability of spares, maintenance personnel, and other logistics resources combined with the system's level of maintainability determine the total downtime following a system failure.

b. Reliability. Reliability is a measure of a system's performance that affects availability, mission accomplishment, and operating and support (O&S) costs. Too often we think of performance only in terms of voltage, capacity, power, and other "normal" measures. However, if a system fails so often (i.e., poor reliability) that it's always being repaired, voltage, capacity, power, and capacity are irrelevant.

c. Reliability, trust, and safety. The importance of reliability is evident in our daily lives. When we begin a road trip in the family automobile, we do so with the assumption that the car will not break down. We are, perhaps unconsciously, assuming that the car has an inherent level of reliability. Similarly, we have a certain level of trust that the airliners in which we fly, the elevators we ride, and the appliances we purchase for our home will operate with little chance of failure. In dealing with systems and systems where failure can result in injury or death, the distinction between reliability and safety becomes blurred. Reliability does indeed affect safety, although safety is primarily concerned with preventing injury while reliability is primarily concerned with ensuring that a system does not fail to perform its function. While related and complementary, these two objectives are not identical.

d. Reliability and costs. Reliability also affects the costs to own and operate a system. Again using the example of the family automobile, the cost of ownership includes gas and oil, insurance, repairs, and replacement of tires and other "expendables." Reliability determines how often repairs are needed. The less often the car has a failure, the less it will cost to operate over its life. The reliability of any repairable system is a significant factor in determining the long-term costs to operate and support the system. For non-repairable systems, the cost of failure is the loss of the function (e.g., the missile misses its target, the fuse fails to protect a circuit, etc.).

e. The inevitability of failures. Regardless of how reliable a system may be, some failures will occur. An effective maintenance program applied to a system that has been designed to be maintainable is necessary to deal with the certainty of failure. For example, even when several redundant items are

installed to decrease the chance of a mission failure, when any one item fails, it must be repaired or replaced to retain the intended level of redundancy.

1-8. Improving availability of C4ISR facilities

The decision on which methods to use for improving availability depends on whether the facility is being designed and developed or is already in use.

a. Existing C4ISR facilities. For a facility that is being operated, two basic methods are available for improving availability when the current level of availability is unacceptable: (1) selectively adding redundant units (e.g., generators, chillers, fuel supply, etc.) to eliminate sources of single-point failure, and (2) optimizing maintenance using a reliability-centered maintenance (RCM) approach to minimize downtime. Of course, some combination of these two methods can also be implemented. The two methods will be discussed in more detail in chapter 3. A third method is available but is very expensive for existing facilities. That method is to redesign subsystems or to replace components and subsystems with higher reliability items. This method will be discussed in paragraph 1-8b, New C4ISR Facilities.

b. New C4ISR facilities. The opportunity for designing for high availability and reliability is greatest when designing a new facility. By applying an effective reliability strategy, designing for maintainability, and ensuring that manufacturing and commissioning do not negatively affect the inherent levels of reliability and maintainability, a highly available facility will result. Although the primary focus of this TM is on improving the availability of current facilities, a brief discussion of the approach used when designing a new facility is provided to give the reader an appreciation of an effective design and development program.

(1) A reliability strategy describes how an organization approaches reliability for all systems and services it develops and provides to its customers. The strategy can be considered as the basic formula for success, applicable across all types of systems and services. A reliability strategy that has proved successful in a variety of industries and in government is shown in figure 1-1.

(2) A reliability program is the application of the reliability strategy to a specific system or process. As can be inferred from figure 1-1, each step in the strategy requires the selection and use of specific methods and tools. For example, various methods can be used to develop requirements or evaluating potential failures.

(a) Developing Requirements. Translations, and analytical models can be used to derive requirements. Quality Function Deployment (QFD) is a technique for deriving more detailed, lower-level requirements from one level of indenture to another, beginning with customer needs. It was developed originally as part of the Total Quality Management movement. Translations are parametric models intended to derive design values of reliability from operational values and vice versa. Analytical methods include thermal analysis, durability analysis, predictions, etc.

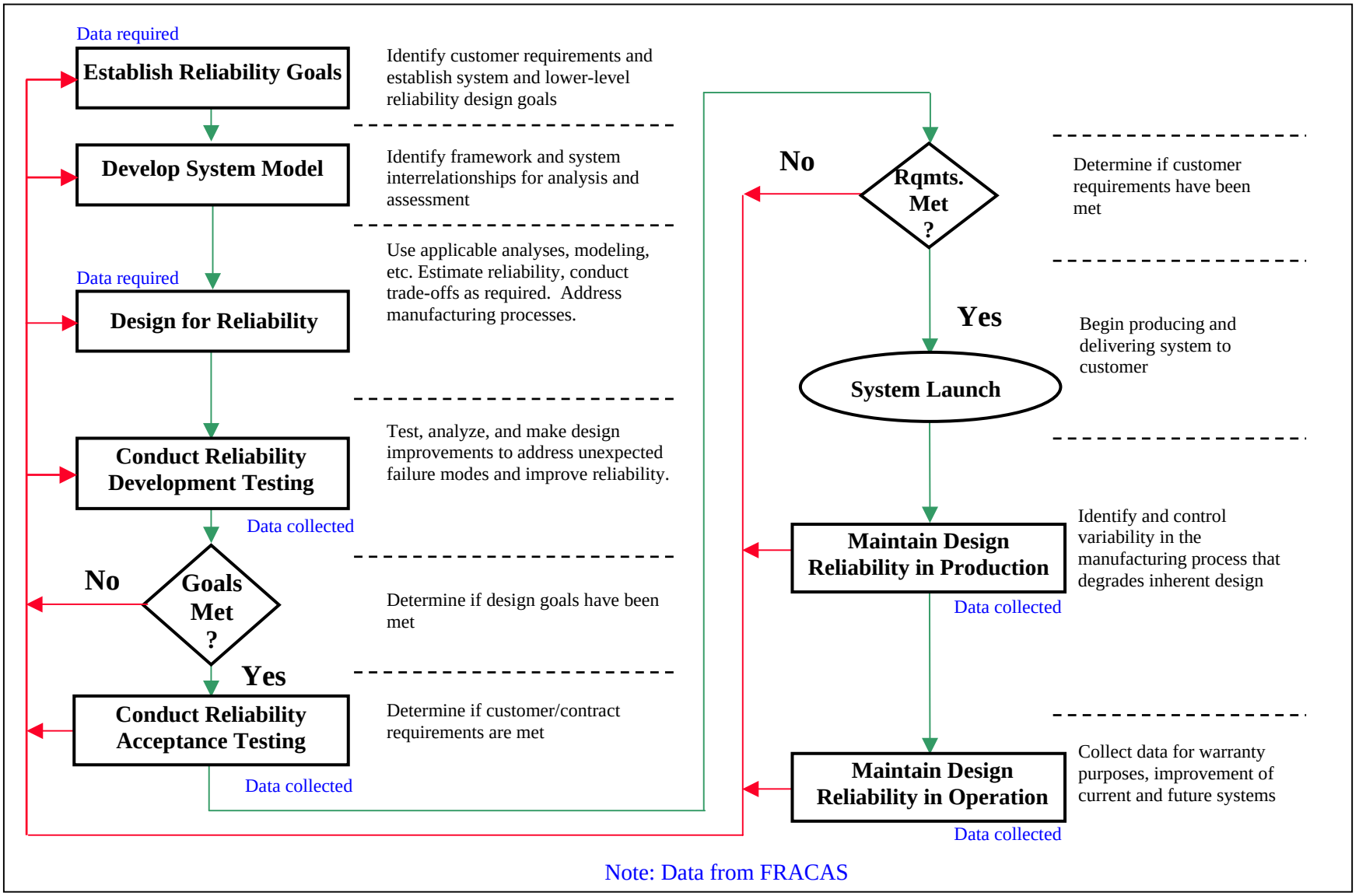


Figure 1-1. A sound reliability strategy addresses all phases of a system's life cycle.

(b) Evaluate possible failures. Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) are two different methods for evaluating possible failures. The reliability engineer must determine which one to use, or whether to use both. Chapter 3 will address these and other methods and how to determine which are applicable to a specific situation. Selecting the specific tasks to accomplish each step of the strategy results in a tailored system program. Table 1-1 shows some of the factors that must be considered in selecting tasks to implement the reliability strategy.

Table 1-1. Factors in selecting tasks for a specific program

Effectiveness and applicability of tasks vary depending on:

- Production runs (total population) – limits use of system-level statistical analysis
- Critical functions/cost of failure – may require exhaustive analysis
- Technology being used – may require new models
- Nature of development (i.e., evolutionary vs. revolutionary) – experience of much less value when breaking new ground

Selection of tasks is also a function of past experience, budget, schedule, and amount of risk you are willing to accept

(3) The entire effort of designing for reliability begins with identifying the customer's reliability requirements. These requirements are stated in a variety of ways, depending on the customer and the specific system. Table 1-2 lists some of the ways in which a variety of industries measure reliability. Note that in the case of the oil & gas and communications industries, availability is the real requirement. The reliability and maintainability requirements must then be derived based on the availability requirement.

Table 1-2. Typical reliability-related measures

Customer	System	Measure of Reliability
Airline	Aircraft	On-time departure
Consumer	Automobile	Frequency of repair
Hospital	Medical	Availability & Accuracy
Military	Weapon	Mission Success Probability
Highway Department	Bridge	Service Life
Oil & Gas	Subsea	Availability
Communications Organization	Utilities	Availability

CHAPTER 2

BASIC RELIABILITY AND AVAILABILITY CONCEPTS

2-1. Probability and statistics

This section provides the reader with an overview of the mathematics of reliability theory. It is not presented as a complete (or mathematically rigorous) discussion of probability theory and statistics but should give the reader a reasonable understanding of how reliability is calculated. Before beginning the discussion, a key point must be made. Reliability is a design characteristic indicating a system's ability to perform its mission over time without failure or to operate without logistics support. In the first case, a failure can be defined as any incident that prevents the mission from being accomplished; in the second case, a failure is any incident requiring unscheduled maintenance. Reliability is achieved through sound design, the proper application of parts, and an understanding of failure mechanisms. It is not achieved by estimating or calculating it. Estimation and calculation are, however, necessary to help determine feasibility, assess progress, and provide failure probabilities and frequencies to spares calculations and other analyses. With that in mind, let's first look at the theory of probability.

a. Uncertainty - at the heart of probability. The mathematics of reliability is based on probability theory. Probability theory, in turn, deals with uncertainty. The theory of probability had its origins in gambling.

(1) Simple examples of probability in gambling are the odds against rolling a six on a die, of drawing a deuce from a deck of 52 cards, or of having a tossed coin come up heads. In each case, probability can be thought of as the relative frequency with which an event will occur *in the long run*.

(a) When we assert that tossing an honest coin will result in heads (or tails) 50% of the time, we do not mean that we will necessarily toss five heads in 10 trials. We only mean that in the long run, we would expect to see 50% heads and 50% tails. Another way to look at this example is to imagine a very large number of coins being tossed simultaneously; again, we would expect 50% heads and 50% tails.

(b) When we have an honest die, we expect that the chance of rolling any possible outcome (1, 2, 3, 4, 5, or 6) is 1 in 6. Again, it is possible to roll a given number, say a 6, several times in a row. However, in a large number of rolls, we would expect to roll a 6 (or a 1, or a 2, or a 3, or a 4, or a 5) only 1/6 or 16.7% of the time.

(c) If we draw from an honest deck of 52 cards, the chance of drawing a specific card (an ace, for example) is not as easily calculated as rolling a 6 with a die or tossing a heads with a coin. We must first recognize that there are 4 suits, each with a deuce through ace (ace being high). Therefore, there are four deuces, four tens, four kings, etc. So, if asked to draw an ace, we know that there are four aces and so the chance of drawing any ace is 4 in 52. We instinctively know that the chance of drawing the ace of spades, for example, is less than 4 in 52. Indeed, it is 1 in 52 (only one ace of spades in a deck of 52 cards).

(2) Why is there a 50% chance of tossing a head on a given toss of a coin? It is because there are two results, or events, which can occur (assume that it is very unlikely for the coin to land on its edge) and for a balanced, honest coin, there is no reason for either event to be favored. Thus, we say the outcome is random and each event is equally likely to occur. Hence, the probability of tossing a head (or

tail) is one of two equally probable events occurring = 1/2 = 0.5. On the other hand, one of six equally probable events can result from rolling a die: we can roll a one, two, three, four, five, or six. The result of any roll of a die (or of a toss of a coin) is called a discrete random variable. The probability that on any roll this random variable will assume a certain value, call it x, can be written as a function, f(x). We refer to the probabilities f(x), specified for all values of x, as values of the probability function of x. For the die and coin, the function is constant. For the coin, the function is f(x) = 0.5, where x is either a head or tail. For the die, f(x) = 1/6, where x can be any of the six values on a die.

b. Probability functions. All random events have either an underlying probability function (for discrete random variables) or an underlying probability density function (for a continuous random variable).

(1) The results of a toss of a coin or roll of a die are discrete random variables because only a finite number of outcomes are possible; hence these events have an underlying probability function. When the probability of each event is equal, underlying probability function is said to be uniform.

(2) The number of possible heights for American males is infinite (between 5' - 8" and 6', for example, there are an infinite number of possible heights) and is an example of a continuous random variable. The familiar bell-shaped curve describes most natural events, such as the height of a person, intelligence quotient of a person, errors of measurement, etc. The underlying probability density function represented by the bell-shaped curve is called normal or Gaussian. Figure 2-1 shows a typical normal distribution. Note that the event corresponding to the midpoint of the curve is called the mean value. The mean value, also called the expected value, is an important property of a distribution. It is similar to an average and can be compared with the center of mass of an object. For the normal distribution, half the events lie below the mean value and half above. Thus, if the mean height of a sample of 100 Americans is 5' -9", we would expect that half the sample would be less than 69" inches tall and half would be taller. We would also expect that most people would be close to the average with only a few at the extremes (very short or very tall). In other words, the probability of a certain height decreases at each extreme and is “weighted” toward the center, hence, the shape of the curve for the normal distribution is bell-shaped.

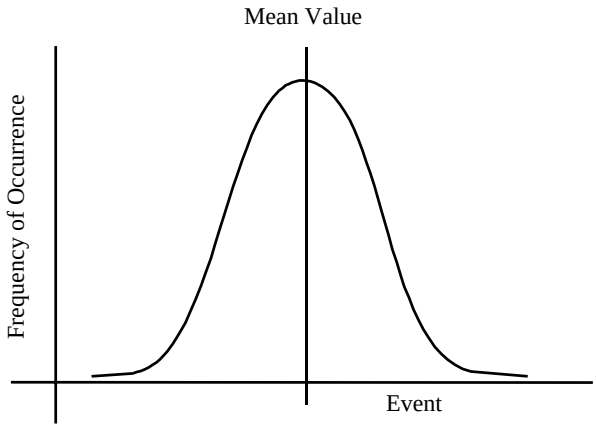


Figure 2-1. Typical normal distribution curve.

(3) The probability of an event can be absolutely certain (the probability of tossing either a head or a tail with an honest coin), absolutely impossible (the probability of throwing a seven with one die), or somewhere in between. Thus, a probability always can be described with equation 2-1.

$$0 \leq \text{Probability} \leq 1 \qquad \text{(Equation 2-1)}$$

(4) Determining which distribution best describes the pattern of failures for an item is extremely important, since the choice of distributions greatly affects the calculated value of reliability. Two of the continuous distributions commonly used in reliability are shown in table 2-1. Note that f(t) is called the probability density function. It is also referred to as the pdf. For reliability, we are usually concerned with the probability of an unwelcome event (failure) occurring.

Table 2-1. Commonly used continuous distributions

Distribution	Probability Density Function	Most Applicable to
Exponential	$f(t) = \lambda \exp(\lambda t)$	Electronic parts and complex systems
Weibull (2-parameter)	$f(t) = \frac{\beta}{\theta^{\beta}} t^{\beta-1} \exp\left[-\left(\frac{t}{\theta}\right)^{\beta}\right]$	Mechanical parts

(a) The underlying statistical distribution of the time to failure for parts is often assumed to be exponential. A glance at the equation of the probability density function explains why. It is easy to work with and has a constant mean, λ. Rather than assuming a distribution, one should determine the most appropriate one using various techniques discussed in chapter 3 for analyzing time-to-failure data.

(b) When the exponential distribution is applicable, the rate at which failures occur is constant and equal to λ. For other distributions, the rate at which failures occur varies with time. For these distributions, we cannot talk of a failure rate. Instead, we use the term Hazard Function, which is a function that describes how the rate of failures varies over time.

(c) Note that different types of parts (i.e., items that fail once and then are discarded and replaced with a new item) may have different underlying statistical distributions of the time to failure. The times to failure of electronic parts, for example, often follow the exponential distribution. The times to failure for mechanical parts, such as gears and bearings, often follow the Weibull distribution. Of course, the parameters for the Weibull for a gear most likely will be different from the parameters for a ball bearing. The applicability of a given distribution to a given part type and the parameters of that distribution are determined, in part, by the modes of failure for the part.

(d) By their very nature, systems consist of many, sometimes thousands, of parts. Since systems, unlike parts, are repairable, they may have some parts that very old, some that are new, and many with ages in between these extremes. In addition, each part type will have a specific distribution of times to failure associated with it. The consequence of these part characteristics together within a system is that systems tend to exhibit a constant failure rate. That is, the underlying statistical distribution of the time to failure for most systems is exponential. This consequence is extremely significant because many reliability prediction models, statistical demonstration tests, and other system analysis are predicated on the exponential distribution.

c. Determining failure rate or Hazard Function. How do we determine the failure rate (or Hazard Function) of a specific system or component? Two methods are used.

(1) In the first method, we use failure data for a comparable system or component already in use. This method assumes that the system in use is comparable to the new system and that the principle of transferability applies - this principle states that failure data from one system can be used to predict the reliability of a comparable system.

(2) The other method of determining failure rate or the Hazard Function is through testing of the system or its components. Although, theoretically, this method should be the "best" one, it has two disadvantages. First, predictions are needed long before prototypes or pre-production versions of the system are available for testing. Second, the reliability of some components is so high that the cost of testing to measure the reliability in a statistically valid manner would be prohibitive. Usually, failure data from comparable systems are used in the early development phases of a new system and supplemented with test data when available.

2-2. Calculating reliability

If the time, t, over which a system must operate and the underlying distributions of failures for its constituent elements are known, then the system reliability can be calculated by taking the integral (essentially the area under the curve defined by the pdf) of the pdf from t to infinity, as shown in equation 2-2.

$$R(t) = \int_t^{\infty} f(t)\, dt \qquad \text{(Equation 2-2)}$$

a. Exponential distribution. If the underlying failure distribution is exponential, equation 2-2 becomes equation 2-3.

$$R(t) = e^{-\lambda t} \qquad \text{(Equation 2-3)}$$

where:

λ is the failure rate (inverse of MTBF)
t is the length of time the system must function
e is the base of natural logarithms
R(t) is reliability over time *t*

(1) Figure 2-2 shows the curve of equation 2-3. The mean is not the "50-50" point, as was true for the normal distribution. Instead, it is approximately the 37-63 point. In other words, if the mean time between failures of a type of equipment is 100 hours, we expect only 37% (if t = MTBF = $1/\lambda$, then $e^{-\lambda t} = e^{-1} = 0.367879$) of the population of equipment to still be operating after 100 hours of operation. Put another way, when the time of operation equals the MTBF, the reliability is 37%.

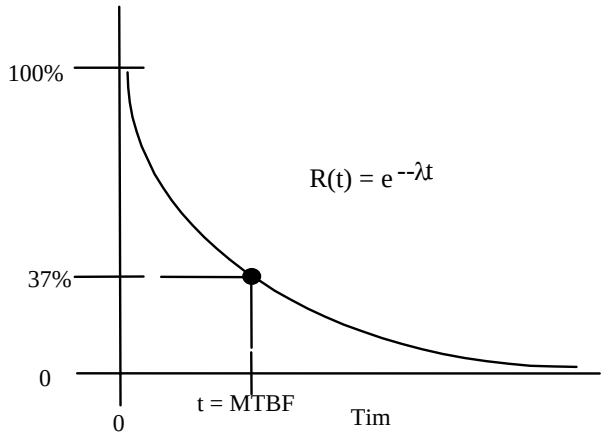


Figure 2-2. Exponential curve relating reliability and time.

(2) If the underlying distribution for each element is exponential and the failure rates, λ_i, for each element are known, then the reliability of the system can be calculated using equation 2-3.

b. Series Reliability. Consider the system represented by the reliability block diagram (RBD) in figure 2-3

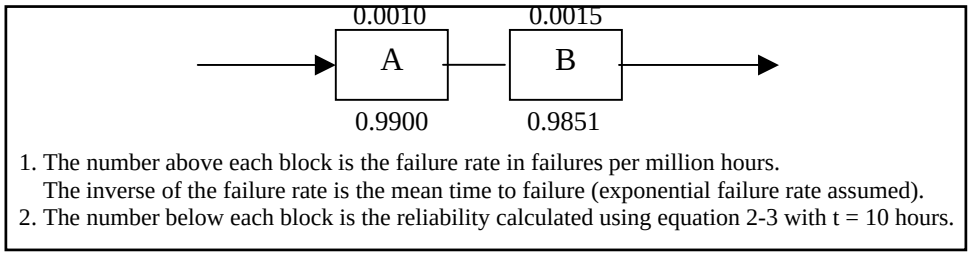


Figure 2-3. Example reliability block diagram.

(1) Components A and B in figure 2-3 are said to be in series, which means all must operate for the system to operate. Since the system can be no more reliable than the least reliable component, this configuration is often referred to as the weakest link configuration. An analogy would be a chain; the strength of the chain is determined by its weakest link.

(2) Since the components are in series, the system reliability can be found by adding together the failure rates of the components and substituting the result in equation 2-4. The system failure rate is 0.001000 + 0.001500 = 0.002500. The reliability is:

$$R(t) = e^{-0.0025x10} = 0.9753 \qquad \text{(Equation 2-4)}$$

(3) Alternatively, we could find the system reliability by multiplying the reliabilities of the two components as follows: 0.9900 x 0.9851 = 0.9753.

c. Reliability with Redundancy. Now consider the RBD shown in figure 2-4.

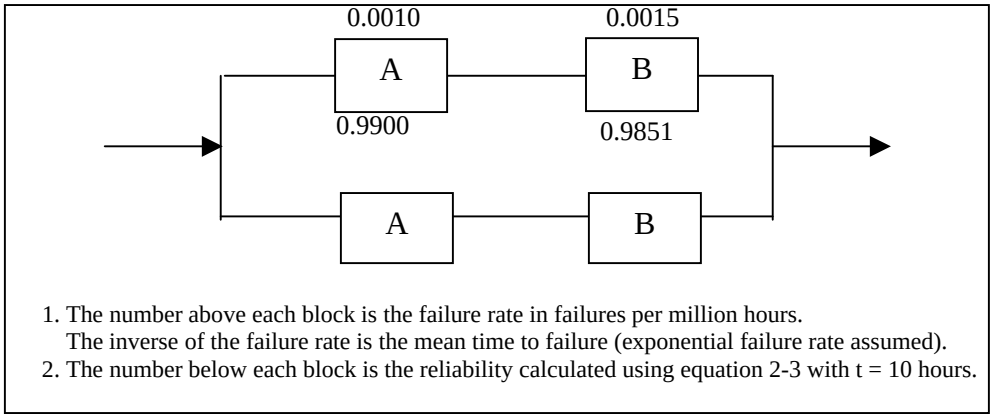


Figure 2-4. RBD of a system with redundant components.

(1) The system represented by the RBD in figure 2-4 has the same components (A and B) used in figure 2-3, but two of each component are used in a configuration referred to as redundant or parallel.

Two paths of operation are possible. The paths are: top A-B and bottom A-B. If either of two paths is intact, the system can operate. The reliability of the system is most easily calculated by finding the probability of failure (1 - R(t)) for each path, multiplying the probabilities of failure (which gives the probability of both paths failing), and then subtracting the result from 1. The reliability of each path was found in the previous example. Next, the probability of a path failing is found by subtracting its reliability from 1. Thus, the probability of either path failing is 1 - 0.9753 = 0.0247. The probability that both paths will fail is 0.0247 x 0.0247 = 0.0006. Finally, the reliability of the system is 1 - 0.0006 = 0.9994, about a 2.5% improvement over the series-configured system.

(2) Two components in parallel (redundant) may always be on and in operation (active redundancy) or one may be off or not in the "circuit" (standby redundancy). In the latter case, failure of the primary component must be sensed and the standby component turned on or switched into the circuit. Standby redundancy may be necessary to avoid interference between the redundant components and, if the redundant component is normally off, reduces the time over which the redundant component will be used (it's only used from the time when the primary component fails to the end of the mission). Of course, more than two components can be in parallel. Chapter 3 (3-1) discusses the various types of redundancy and how it can be used to improve the availability of current C4ISR facilities.

(3) Adding a component in parallel, i.e., redundancy, improves the system's ability to perform its function. This aspect of reliability is called functional or mission reliability. Note, however, that in figure 2-4, we have added another set of components that has its own failure rate. If we want to calculate the total failure rate for all components, we add them. The result is 5000 failures per million operating hours (0.005000). The failure rate for the series-configured system in figure 2-3 was 2500 failures per million operating hours. Although the functional reliability of the system improved, the total failure rate for all components **increased**. This perspective of reliability is called basic or logistics reliability. When standby redundancy is used, the sensing and switching components add to the total failure rate.

d. Logistics reliability. Whereas functional reliability only considers failures of the function(s), logistics reliability considers all failures *because some maintenance action will be required*. Logistics reliability can be considered as either the lack of demand placed on the logistics system by failures or the ability to operate without logistics. If standby redundancy is used with the redundant component not on, the apparent failure rate of that component will be less than that of its counterpart (because the probability it will be used is less than 1 and the time it will operate less than 10 hours), but the failure rate of the switching circuits must now be considered.

2-3. Availability

For a system such as an electrical power facility, availability is a key measure of performance. An electrical power facility must operate for very long periods of time, providing power to other systems, such as C4ISR, that perform critical functions. Even with the best technology and most robust design, it is economically impractical, if not technically impossible, to design power facilities that never fail over weeks or months of operation. Although forced outages (FAs) are never welcome and power facilities are designed to minimize the number of FAs, they still occur. When they do, restoring the system to operation as quickly and economically as possible is paramount. The maintainability characteristics of the system limit how quickly and economically system operation can be restored.

a. Reliability, maintainability, and availability. Consequently, reliability and maintainability (R&M) are considered complementary characteristics. Looking at a graph of constant curves of inherent availability (A_i), one can see this complementary relationship. A_i is defined by the following equation and reflects the percent of time a system would be available if delays due to maintenance, supply, etc. are ignored.

$$A_i = \frac{MTBF}{MTBF + MTTR} \times 100\% \qquad \text{(Equation 2-6)}$$

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

There are R&M trades. If the system never failed, the MTBF would be infinite and A_i would be 100%. Or, if it took no time at all to repair the system, MTTR would be zero and again the availability would be 100%. Figure 2-5 is a graph showing availability as a function of reliability and maintainability (availability is calculated using equation 1). Note that you can achieve the same availability with different values of R&M. With higher reliability (MTBF), lower levels of maintainability are needed to achieve the same availability and vice versa. It is very common to limit MTBF, MTTR, or both. For example, the availability requirement might be 95% with an MTBF of at least 600 hours and a MTTR of no more than 3.5 hours.

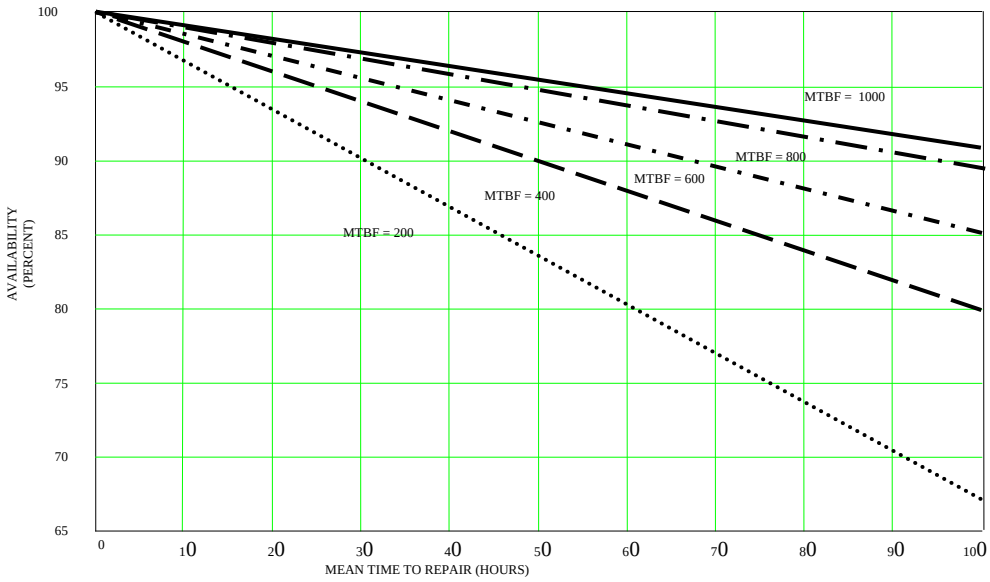


Figure 2-5. Different combinations of MTBF and MTTR yield the same availability.

b. *Other measures of availability*. Other measures of availability include operational availability, A_o, and measured availability, A.

(1) Operational availability includes maintenance and logistics delays and is defined using equation 2-7:

$$A_0 = \frac{MTBM}{MTBM + MDT} \qquad \text{(Equation 2-7)}$$

where MTBM is the mean time between all maintenance and MDT is the mean downtime for each maintenance action.

(2) Measured availability is defined in equation 2-8.

$$A = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime} = \text{Total Time}} \qquad \text{(Equation 2-8)}$$

where Uptime is the time during which the system is available for use and Downtime is the time during which the system is not available for use.

(3) Note that A_o and A_i are probabilistic measures, while A is a deterministic measure. MTBF and MTBM and MTTR and MDT are measures of reliability and maintainability (R&M), respectively, and are random variables. By designing for appropriate levels of R&M and conducting adequate statistically based tests, a high confidence in the availability can be obtained. That confidence can never be 100%. Measuring A is done by actually measuring the amount of time in a given time interval during which the system is "up" and then calculating the observed availability. For this measure of availability, the time interval for the measurement is extremely important. Its importance can be understood by considering an availability requirement of 95% with a maximum downtime of 10 hours. Table 2-2 shows the effect of varying intervals of time for measuring A.

Table 2-2. Effect of measurement interval on observed availability

Time Interval	Actual Downtime	Measured Availability	Maximum Downtime to Meet Requirement
1 hour	0.5 hour	50%	0.05 hour (3 minutes)
8 hours	1 hour	87.5%	0.4 hour (24 minutes)
24 hours	2 hours	91.67%	1.2 hours
240 hours	10 hours	95.83%	10 hours
7200 hours	10 hours	99.86%	10 hours

(a) Very short intervals make it increasingly difficult, if not impossible, to meet an availability requirement. It is very possible that a failure could occur in the first 8 hours of operation. If that were the case, the system would pass the 95% availability test only if the repair could be made in 3 minutes or less. For many systems, it may be impossible to correct any failure in 3 minutes or less. So even if it is unlikely that a failure will occur in the first hour of operation (i.e., the system is highly reliable), the probability of such a failure is not zero. If a failure occurs in the first hour and requires more than 3 minutes to repair, the system will have failed to meet an availability requirement of 95%. Yet, if the system is truly reliable, it may experience no more failures (and no more downtime) in the next 24 hours of operation, in which case the measured availability will be greater than the requirement.

(b) Since A_o, A_i, and A are not measured in the same way, it is extremely important in contracts to state, a priori, (e.g., in a step-by-step, deductive manner) how availability will be measured during acceptance or qualification testing.

2-4. Predictions and assessments

Predictions and assessments refer to the process of evaluating the reliability of a system, its weaknesses, and areas offering opportunities for improvement. Quantitative numbers are a usual byproduct of a prediction or assessment, and such numbers are necessary for calculating spares requirements, probability of success, and for other purposes. However, another very important result of a prediction or assessment is in identifying ways to improve the system.

a. Reliability Predictions. In a new development program, reliability predictions are a means of determining the feasibility of requirements, assessing progress toward achieving those requirements and

comparing the reliability impact of design alternatives. Predictions can be made through any appropriate combination of reliability models, historical data, test data, and engineering judgment. The choice of which prediction method to use depends on the availability of information, which in turn is a function of the point of the system life cycle at which the prediction is performed. Considerations in performing predictions are that correct environmental stresses are used, the reliability model is correct, the correct part qualities are assumed and that all operational and dormancy modes are reflected. Chapter 3 addresses the types of models commonly used.

b. Reliability Assessment. Predictions are one method of assessing the reliability of an item. At the onset of a new development program, the prediction is usually purely analytical. As the program progresses, other methods become available to improve or augment the analytical prediction. These methods include testing, design reviews, and other methods. For existing systems, reliability assessments include analyzing field data to determine the level of reliability being achieved and identify weaknesses in the design (i.e., opportunities for improvement).

(1) Table 2-3 lists some common techniques that can be used for assessing reliability and guidance for their use. Methods especially useful for existing systems are shown in bold. Some of these methods provide a numerical value that is representative of the system reliability at a point in time; all provide a valuable means of better understanding the design's strengths and weaknesses so that it can be changed accordingly.

(2) The assessment methods chosen should be appropriate for the system and require only a reasonable level of investment given the value of the results. The failure of some components, for example, may have little impact on either system function, or on its operating and repair costs. A relatively costly analysis may not be justified. For other systems, a thermal analysis may not be needed, given the nature of the system and its operating environment. When the consequences of failure are catastrophic, every possible effort should be made to make the system fail-safe or fault tolerant.

Table 2-3. Methods for assessing reliability

Method	Application
Accelerated Life Testing	Effective on parts, components or assemblies to identify failure mechanisms and life limiting critical components.
Critical Item Control	Apply when safety margins, process procedures and new technology present risk to the production of the system.
Design of Experiments (DOE)	Use when process physical properties are known and parameter interactions are understood. Usually done in early design phases, it can assess the progress made in improving system or process reliability.
Design Reviews	Continuing evaluation process to ensure details are not overlooked. Should include hardware and software.
Dormancy Analysis	Use for products that have "extended" periods of non-operating time or unusual non-operating environmental conditions or high cycle on and off periods.
Durability Analysis	Use to determine cycles to failure or determine wearout characteristics. Especially important for mechanical products.
Failure Modes, Effects and Criticality Analysis (FMECA)	Applicable to equipment performing critical functions (e.g., control systems) when the need to know consequences of lower level failures is important.
Failure Reporting Analysis and Corrective Action (FRACAS)	Use when iterative tests or demonstrations are conducted on breadboard, or prototype products to identify mechanisms and trends for corrective action. Use for existing systems to monitor performance.
Fault Tree Analysis (FTA)	Use for complex systems evaluation of safety and system reliability. Apply when the need to know what caused a hypothesized catastrophic event is important.
Finite Element Analysis (FEA)	Use for designs that are unproven with little prior experience/test data, use advanced/unique packaging/design concepts, or will encounter severe environmental loads.
Life Cycle Planning	Use if life limiting materials, parts or components are identified and not controlled.
Parts Obsolescence	Use to determine need for and risks of application of specific parts and lifetime buys
Prediction	Use as a general means to develop goals, choose design approaches, select components, and evaluate stresses. Equally useful when redesigning or adding redundancy to an existing system.
Reliability Growth Test (RGT)/Test Analyze and Fix (TAAF)	Use when technology or risk of failure is critical to the success of the system. These tests are costly in comparison to alternative analytical techniques.
Sneak Circuit Analysis (SCA)	Apply to operating and safety critical functions. Important for space systems and others of extreme complexity. May be costly to apply.
Supplier Control	Apply when high volume or new technologies for parts, materials or components are expected
Test Strategy	Use when critical technologies result in high risks of failure.
Thermal Analysis (TA)	Use for products with high power dissipation, or thermally sensitive aspects of design. Typical for modern electronics, especially of densely packaged products.
Worst Case Circuit Analysis (WCCA)	Use when the need exists to determine critical component parameters variation and environmental effects on circuit performance.

CHAPTER 3

IMPROVING AVAILABILITY OF C4ISR FACILITIES

3-1. Overview of the process

Facility managers are faced with the responsibility of providing the proper utilities (electrical, chilled water, steam, etc.) at the needed levels (power levels, voltage, pressure, etc.) to their customers when needed to support an end mission. The steps for improving the availability of a facility for two situations, new facilities in design and facilities already in use, are shown in table 3-1. Each step for each situation will be discussed in this chapter.

Table 3-1. The process for improving facility availability

New Facilities Being Designed	Facilities Already in Use
1. Determine system availability requirements	1. Determine system availability requirements
2. Derive reliability and maintainability requirements from availability requirement	2. Derive reliability and maintainability requirements from availability requirement
3. Develop "one-lines"	3. Develop "one-lines" of systems
4. Conduct analyses to predict availability, reliability, and maintainability and to determine weaknesses in design and redesign based on failure criteria and cost/benefit analysis	4. Collect data for availability assessment
	5. Assess availability, reliability, maintainability, and logistics performance being achieved for each system (this establishes the baseline performance)
	6. Identify shortfalls (differences between required level of performance and baseline performance)
5. Conduct testing to validate analytical results	7. Perform cost-benefit analysis to prioritize improvement efforts
6. Update assessment of availability, reliability, and maintainability based on test results	8. Design and develop system changes (using same process used for new facility design)
7. Revise design as necessary based on test results	9. Assess improvement in availability, reliability, and maintainability based on analyses and test
8. Construct facility and continuously assess performance and identify opportunities for improvement	10. Implement design changes
	11. Continuously assess performance and identify opportunities for improvement

3-2. New facilities in design

Since reliability and maintainability, and hence availability, are predominantly affected by design, it is essential that these system characteristics be addressed in the design of a new system. It is during design, that these characteristics can be most effectively and positively influenced at the least cost.

a. Determine system availability requirements. Establishing clear, comprehensive, and measurable requirements is the first and most important step in designing and developing systems that meet user needs. The design requirements must be derived from and, if met, allow the user needs to be met. User needs are often stated in non-design terms. For facilities, these might include operational availability, readiness, mean time between maintenance (where maintenance includes all maintenance actions, including those to repair operator-induced failures), and total downtime (including the time to order and ship parts if necessary). Designers must have requirements that they can control. For a facility, these may include inherent availability, mean time between design failures, and mean time to repair (includes only the actual "hands on" time to make a repair). The facility availability requirement should be included in the solicitation package (normally in the specification) for a new facility.

b. Derive reliability and maintainability requirements from availability requirement. Based on the user need (e.g., operational availability), the reliability and maintainability design requirements (e.g., mean time between failure and mean time to repair) must be derived. This derivation of lower-level requirements is usually done by the design organization and continues throughout the development effort until design requirements are available at the lowest level of indenture (subsystem, assembly, subassembly, part) that makes sense.

c. Develop "one-lines". Paragraph 4-5 discusses this method of representing a system.

d. Conduct Analyses. Conduct analyses to predict availability, reliability, and maintainability and to determine weaknesses in design and redesign based on failure criteria and cost/benefit analysis. Some of the pertinent analyses are summarized in table 3-2.

Table 3-2. Analyses helpful in designing for reliability

Analysis	Purpose	Application	When to perform
FEA	• Computer simulation technique for predicting material response or behavior of modeled device • Determine material stresses and temperatures • Determine thermal and dynamic loading	• Use for devices that: – Are unproven with little prior experience/data – Use advanced/unique packaging/design concepts – Will encounter severe environmental loads – Have critical thermal/mechanical constraints	In design phase when candidate devices can be selected using selection criteria
TA	• Calculate junction temperatures • Calculate thermal gradients • Calculate operating temperatures	• For integrated circuits • For electronics and electrical devices	• During circuit design • Prior to design of cooling systems
Dormancy Analysis	• Calculate failure rates of devices while dormant (e.g., storage)	• Use for devices identified to have periods of dormancy	• During design
FTA	• Top down approach to identify effects of faults on system safety or reliability • Address multiple failure	• Can be applied when FMECA too expensive • To address effects of multiple failures	• Early in design phase, in lieu of FMECA
FMECA	• Bottom up approach to identify single failure points and their effects • To assist in the efficient design of BIT and FIT • To establish and rank critical failures • To identify interface problems	• More beneficial if performed on newly designed equipment • More applicable to equipment performing critical functions (e.g., control systems)	• Early in design phase
SCA	• To identify failures not caused by part failures • To reveal unexpected logic flows that can produce undesired results • To expose design oversights that create conditions of undesired operation	• Mission and safety critical functions • Hardware with numerous interfaces • Systems with high testing complexities • Use selectively due to high cost of performing	• Later design stage but prior to CDR
WCCA	• To evaluate circuits for tolerance to "drift" • When time dependency is involved • To evaluate the simultaneous existence of all unfavorable tolerances • Single failures	• Assesses combined effect of parts parameters variation and environmental effects on circuit performance • Not often applied • Use selectively	• Later design stage as required

LEGEND: Finite Element Analysis (FEA); Thermal Analysis (TA); Fault Tree Analysis (FTA); Failure Modes, Effects and Criticality Analysis (FMECA); Sneak Circuit Analysis (SCA); Worst Case Circuit Analysis (WCCA)

e. Conduct testing to validate analytical results. No matter how diligent we are in developing the models and analytical tools used to design, we cannot account for all variations and factors. By testing a given design, we will uncover unexpected problems. These problems can include new types of failures, more frequent than expected failures, different effects of failures, and so forth. Problems discovered during test provide opportunities for improving the design and our models and tools.

f. Update assessment of availability, reliability, and maintainability based on test results. Based on the results of our testing, we should update the analytical assessments of reliability made earlier. Adding the results of testing provides higher confidence in our assessment than is possible using analytical results alone.

g. Revise design as necessary based on test results. If our updated assessment indicates we are falling short of our reliability (and availability) requirements, we must revise the design to improve the reliability. Even when our updated assessment indicates that we are or are close to meeting our requirements, we should consider making design changes based on cost-benefit considerations.

h. Construct facility and continuously assess performance and identify opportunities for improvement. Once we are satisfied that the reliability (and availability) requirements are satisfied by our facility design, the facility is constructed. We must ensure that the inherent levels of reliability are sustained over time, and collect information that can be used in the design of the next facility. To that end, we need to collect data and use the data to continuously assess the availability performance of the facility. This operational field data also should be archived for use in designing new facilities.

3-3. Facilities already in use

For facilities in use, the process for improving availability is somewhat different than that discussed for new systems. It is different for two major reasons. First, improvements must be made by modifying an existing design, which is usually more difficult than creating the original design. Second, the improvements must be made with as little disruption to the facility as possible, since it is supporting an ongoing mission. Although design changes are usually the primary focus of improvement efforts, changes in procedures or policy should also be considered. Not only are such changes usually much easier and economical to make, they may actually be more effective in increasing availability.

a. Determine system availability requirements. As was the case for a new system, the requirements must be known. For existing facilities, it may be difficult to find the original user needs or design requirements. Even when the original requirements can be determined, the current requirements may have changed due to mission changes, budget constraints, or other factors.

b. Derive reliability and maintainability requirements from the availability requirement. Whatever the operational requirements are, it is necessary to translate them into reliability and maintainability requirements.

c. Develop "one-lines" of systems. This step can be bypassed if "one-lines" were developed for the facility when it was developed and built and are still current.

d. Collect data for availability assessment. Ideally, a data collection system was implemented when the facility was first put into operation. If that is not the case, one must be developed and implemented at this point. The data to be collected includes failures, failure causes and mechanisms, repair times, and so forth.

e. Assess performance. Assess the availability, reliability, maintainability, and logistics performance being achieved for each system. Performing this step establishes the baseline performance for the facility.

f. Identify shortfalls. Shortfalls are the differences between the required level of performance and baseline performance.

g. Perform cost-benefit analysis to prioritize improvement efforts. Many potential improvements will be identified throughout the life of a facility. Those that are safety-related or are essential for mission success will always be given the highest priority. Others will be prioritized on the basis of the costs to implement compared with the projected benefits. Those that have only a small return for the investment will be given the lowest priority.

h. Design and develop system changes. The process for improving the availability, reliability, and maintainability performance of an existing facility is essentially the same as for designing new facility.

i. Assess improvement. Assess improvement in availability, reliability, and maintainability based on analyses and test. Before implementing any potential improvements, some effort must be made to ensure that the design changes must be validated. All too often, a change that was intended to improve the situation actually makes it worse. Through careful analyses and appropriate testing, one can determine that the proposed change actually results in some level of improvement.

j. Implement design changes. Those design changes that are validated as improving availability must be implemented in a way that minimizes the downtime of the facility. Perhaps they can be made during scheduled maintenance periods. Or perhaps there are times of the day, month, or year when downtime is less critical to the mission than at other times. Careful planning can minimize the impact on the mission. Also, the procedures, tools, training, and materials needed for the design change must be in place and validated prior to starting the facility modification.

k. Monitor performance. Continuously assess performance and identify opportunities for improvement. Continuous improvement should be the goal of every facility manager. As the facility ages, the cost-benefits of what were low-priority improvements may change, new problems may be introduced, and new mission requirements may arise. By collecting data and maintaining a baseline of the facility availability performance, the facility manager will be in a position to make future improvements as they become necessary or economical.

3-4. Improving availability through addition of redundancy

Redundancy is a technique for increasing system reliability and availability by making the system immune to the failure of a single component. It is a form of fault tolerance – the system can tolerate one or more component failures and still perform its function(s).

a. Types of Redundancy. There are essentially two kinds of redundancy techniques employed in fault tolerant designs, space redundancy and time redundancy. Space redundancy provides separate physical copies of a resource, function, or data item. Time redundancy, used primarily in digital systems, involves the process of storing information to handle transients, or encoding information that is shifted in time to check for unwanted changes. Space, or hardware, redundancy is the approach most commonly associated with fault tolerant design. Figure 3-1 provides a simplified tree-structure showing the various types of hardware redundancy that have been used or considered in the past.

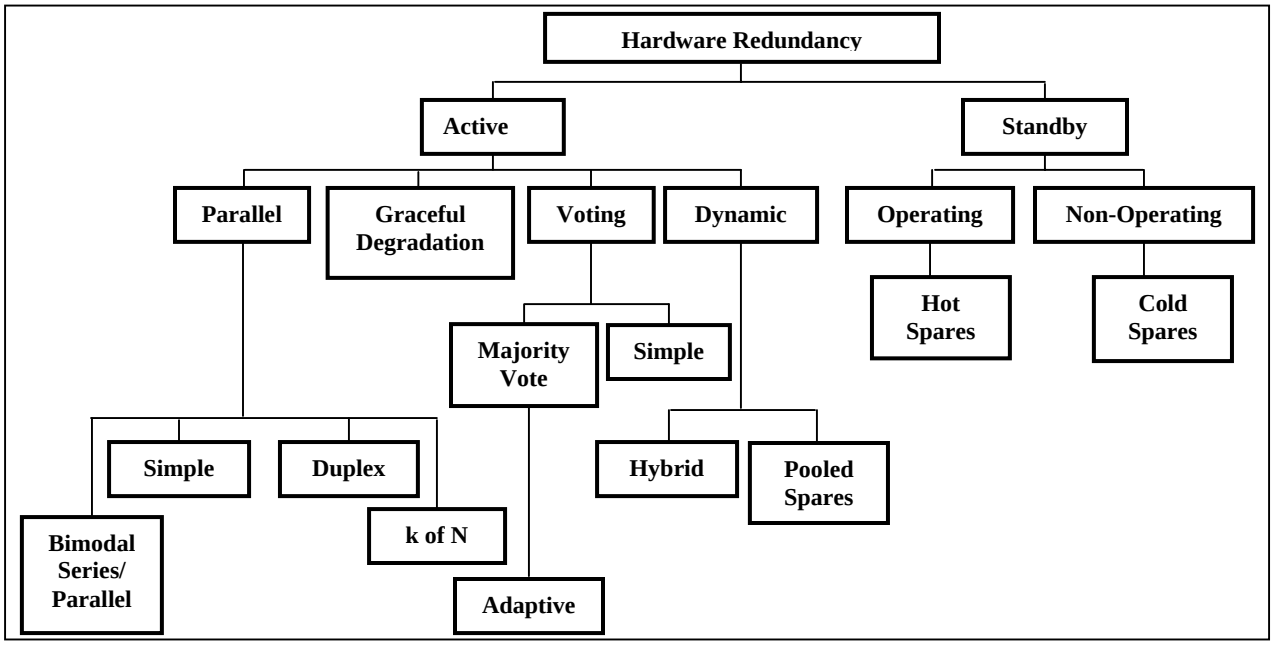


Figure 3-1. Types of redundancy.

b. Impact on Testability. Many of today's more sophisticated systems not only require an ability to detect faults but also to diagnose or isolate them. It may even be desirable for a system to have the ability to reconfigure itself to avoid system failure. Automated fault detection and isolation has therefore become an essential means of obtaining highly fault-tolerant systems. Because of this, the design of the diagnostic system, including any built-in-test (BIT) features and the overall testability of the design are important tradeoffs that need to be made as part of the fault tolerant design process. Table 3-3 presents a sample list of hardware fault tolerant design approaches, and their impact on diagnostic approaches and BIT.

Table 3-3. Diagnostic implications of fault tolerant design approaches

Fault Tolerant Design Technique	Description	Diagnostic Design Implications	BIT Implications
Active Redundancy, simple parallel	All parallel units are on whenever the system is operating. k of the N units are needed, where 0<k<N. External components are not required to perform the function of detection, decision and switching when an element or path in the structure fails. Since the redundant units are always operating, they automatically pick up the load for a failed unit. An example is a multi-engined aircraft. The aircraft can continue to fly with one or more engines out of operation.	Hardware/Software is more readily available to perform multiple functions.	N/A
Active Redundancy with voting logic	Same as Active Redundancy but where a majority of units must agree (for example, when multiple computers are used)	Performance/status-monitoring function assures the operator that the equipment is working properly; failure is more easily isolated to the locked-out branch by the voting logic.	N/A
Stand-by redundancy (Non-operating)	The redundant units are not operating and must be started if a failure is detected in the active unit (e.g., a spare radio is turned on when the primary radio fails).	Test capability and diagnostic functions must be designed into each redundant or substitute functional path (on-line AND off-line) to determine their status.	Passive, periodic, or manually initiated BIT.
Stand-by redundancy (Operating)	The redundant units are operating but not active in system operation; must be switched "in" if a failure is detected in the active unit (e.g., a redundant radar transmitter feeding a dummy load is switched into the antenna when the main transmitter fails).	N/A	Limited to passive BIT (i.e., continuous monitoring) supplemented with periodic BIT.

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

(a) Maintain real-time status of the system's assets (on-line and off-line, or standby, equipment).

(b) Provide the operator with the status of available system assets.

(c) Maintain a record of hardware faults for post-mission evaluation and corrective maintenance.

(2) The essence of fault tolerance is that the system is able to perform its mission despite experiencing some failures. In systems where redundancy is used, this fault tolerance is achieved by one or more redundant units taking over the function previously being performed by another unit. When standby redundancy is used, the failed unit must be detected and the standby unit "brought on line." In still other cases, principally involving electronics, failures can be "repaired" by rerouting signals or functions to other units. These "repairs" can be done upon a failure or in anticipation of a failure. In such cases, the BIT should, in addition to the actions identified in paragraph 3-4b(1), maintain a record of any reconfiguration events that were required for system recovery during the mission.

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

c. Reliability's role in the fault tolerant design process. The role of the reliability engineer in regards to fault tolerant design requirements is to ensure that system reliability requirements are achievable for each of the fault tolerant design approaches being considered. Furthermore, to properly design a fault tolerant system, including a diagnostic scheme, the designer needs to understand the modes in which the system can fail, and the effects of those failure modes. This requires that a failure mode and effects analysis (FMEA) be performed, as a minimum. The FMEA will identify which faults can lead to system failure and therefore must be detected, isolated and removed to maintain system integrity. In general, the reliability design manager must ask a series of questions, as listed in table 3-4.

d. Fault tolerance and tradeoffs. The designer needs to consider each of the questions in table 3-4 and others as part of the overall fault tolerant design process. Other reliability tradeoffs to be considered involve analysis of the redundancy approaches being considered for the fault tolerant design. In addition to reliability concerns, fault tolerance also requires analysis of the impacts on maintainability and testability. As an example, consider figure 3-2. This figure illustrates a design vs. corrective maintenance tradeoff analysis performed early in the product development phase. In particular, the figure shows the tradeoff of restoration frequency versus the number of sensors being used to meet requirements. This program requires a time period for allocating a scheduled maintenance activity and a probability of less than one in 10 billion per flight hour that a total loss of the skewed sensor function would occur. The tradeoff is made between the number of sensors and the cost of unscheduled maintenance activity associated with each approach. Other tradeoffs, such as cost, power, weight, etc. are also necessary. In general, as in any design analysis support function, an analysis of the impacts on reliability, maintainability (including testability) and availability of a chosen fault tolerant design approach must be performed.

Table 3-4. Questions for the reliability design engineer related to fault tolerance

1. How do the system fault tolerance requirements impact the overall reliability, maintainability, and availability requirements? 2. Where should fault tolerant design methods be applied? • Which functions involve the most risk to mission success? • What is the effect of the operating environment • What maintenance strategy/policy needs to be considered? 3. What is the effect on maintainability and testability? 4. What are the constraints that affect fault tolerance? • Cost • Size & weight • Power • Interface complexity • Diagnostic uncertainties

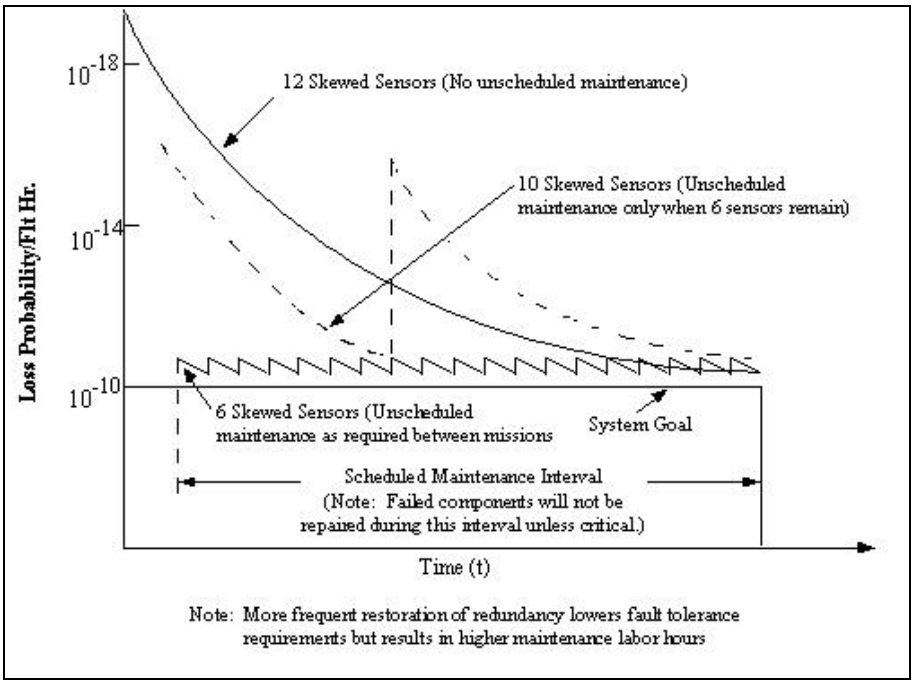


Figure 3-2. Effect of maintenance concept on level of fault tolerance.

e. General rules in applying redundancy. In applying redundancy to a C4ISR facility, the following general rules should be followed:

(1) Determine the weak links in the system to know where to add redundancy. These weak links may be portions of the system prone to single point failures or, where redundancy is already used, the reliability is still too low to meet availability requirements.

(a) As an example of applying rule (1), consider the simple system shown in figure 3-3. This system has five subsystems (lettered) with seven major components (numbered). The MTBF and MTTR for each component are shown. Using these figures, the overall system availability can be calculated using Monte Carlo simulation. The results of a Monte Carlo simulation of the system using RAPTOR yielded the results shown in table 3-5. The areas of weakness from a availability perspective can be determined from simply looking at the relative contribution to system unreliability as summarized in table 3-6. Note that subsystem C is the weakest link, even though it is not subject to a single point failure. Subsystem D is the next weakest link; it is subject to a single point failure. It may have been obvious that D, representing

a potential single point failure, is a weak link. It may not have been as obvious that C, even though it already incorporates redundancy, is a weak point. Looking at the relative availability of component 3, we see that it is much less reliable than the other components. Even dual redundancy is insufficient to compensate for the low MTBF. As this example shows, although it may be tempting to always add redundancy to those portions of a system subject to single point failures, it is sometimes more effective to add it elsewhere.

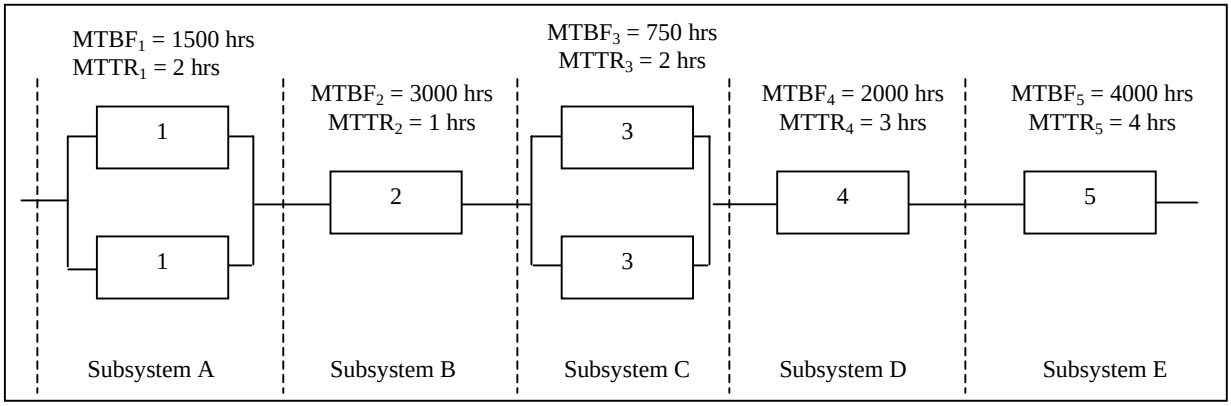


Figure 3-3. Analyzing the contributions to system reliability helps determine where redundancy is needed.

Table 3-5. Calculated availability of system in figure 3-3 using RAPTOR.

MTBM	Mean System Failures	MTTR	Availability (%)
258.77	1.0658	2.5695	99.7236

Notes: 1. For ease of calculation, the times to failure and the times to repair were assumed to be distributed exponentially.
2. 10,000 simulation trials were run using an operating time of 1,000 hours.

Table 3-6. Relative unreliability of subsystems (repairs ignored)

Subsystem	Reliability in 1000 hours	Expected Failures per 1000 Hours	% Contribution to System Unreliability	Contribution to System Unreliability Ranking
A	0.7632	0.2368	14.12	4
B	0.7165	0.2835	16.90	3
C	0.4577	0.5423	32.33	1
D	0.6065	0.3935	23.46	2
E	0.7788	0.2212	13.19	5
SYSTEM	0.1182	1.6773	-	-

(2) Add redundancy in a way that avoids undesirable interactions. Rule 2 implies that some components cannot be used in some forms of redundancy, depending on the failure modes, application, and other factors. The type of redundancy shown in figure 3-3 is active redundancy, in which all components are on all of the time that the system is operating. In some cases, such a redundant configuration would result in undesired interactions or interference among the redundant units. As will be seen later in this chapter, certain forms of redundancy are preferable to others in a given application.

(3) Adding redundancy increases support requirements and costs. Only use redundancy when availability is insufficient and no other technique will improve it. Rule 3 refers to the added costs incurred with redundancy. The most obvious increase is due to the fact that more components must be purchased and installed. An additional cost comes from an increased failure rate. The increase in complexity results in an increase in unscheduled maintenance. If nothing is done to

improve the reliability of the individual components in a system, but additional components are added to provide redundancy, the total failure rate of the components will increase. System reliability will improve but more component failures will occur. These failures will increase support requirements and costs. Redundancy also increases weight, space requirements, complexity, and time to design. Thus, safety and mission reliability is gained at the expense of adding an item(s) in the unscheduled maintenance chain. Only use redundancy when availability is insufficient and no other technique will improve it.

(a) The decision to use redundant design techniques must be based on analysis of the tradeoffs involved. Redundancy may prove to be the only available method, when other techniques of improving reliability, e.g., derating, simplification, better components, have been exhausted, or when methods of item improvement are shown to be more costly than duplications.

(b) When preventive maintenance is planned, the use of redundant equipment can allow for repair with no system downtime. Occasionally, situations exist in which equipments cannot be maintained, e.g., satellites; then redundant elements may be the best way to significantly prolong operating time.

(4) Ensure that any one redundant unit can be maintained without shutting down the other redundant units. Rule 4 requires that we ensure that any one redundant unit can be maintained without shutting down the other redundant units. Assume that two generators, for example, are sharing a load. If one fails and we must shut the other generator down to either gain access to or repair the failed generator, then we in effect have no redundancy. An implicit assumption in using redundancy is that availability increases because we can repair a failed component while the remaining redundant components continue to operate. If this assumption is violated, redundancy will not increase availability.

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

(1) Monte Carlo simulation and Markov techniques continue to be used as the primary means of analyzing highly sophisticated fault tolerant designs. These approaches have been modified to incorporate situations where the sequence of failure is important, where the failure is transient or intermittent, or where the response to failure (i.e., detection, isolation, recovery, and reconfiguration) is imperfect. In these situations, Markov methods continue to lead the way in evaluation methods. In general, the Markov approach, which is used to define the specific states that a system can occupy, has been used to incorporate fault handling and recovery. A major limitation to the Markov approach is that the number of system states that must be defined to comprehensively describe a large system and model the behavior of complex fault management schemes can become very large (approaching 10^5 for highly complex systems). A common solution to this problem is to partition the system into smaller systems, evaluate each partition separately, and then combine the results at the system level. However, such an approach is only exact when each partitioned subsystem's fault tolerant behavior is mutually independent of each other. If subsystem dependencies do exist, then an assumption of independence will result in only an approximate solution.

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

(a) Solving a fault-handling model in isolation and then reflecting its results in an aggregate model is, itself, an approximation technique. The assumptions necessary to determine a solution typically result in a lower bound (conservative) approximation of the system reliability.

(b) Separate fault-handling models have been assumed to be independent of system state. This requires that the same fault-handling model and choice of parameters be used irrespective of the system's level of degradation. This ignores the fact that for many systems the recovery process is faster if the number of active units is smaller or that the recovery process may be different, depending on the sequence of events in different subsystems.

(c) The common technique of partitioning the system into independent functional subgroups for computational ease is a potential source of error. The magnitude and direction of the error is a function of how truly independent/dependent the subgroups are of each other. If subgroups are assumed independent when in fact they are not, the effect is an overstatement of system reliability/availability. If subgroups are assumed completely dependent when some degree of independence exists, the effect is an understatement of the system's reliability/availability.

(d) Some models assume a constant instantaneous fault-protection coverage factor in lieu of a separate fault handling model. These fail to recognize that during time spent in the intermediate fault-handling states to detect, isolate, and recover/reconfigure, a second item failure could result in system failure. Further, as with fault handling models, these times are generally not constant, but depend on the current state of the system.

(e) Most models require the assumption that the system is perfect at the mission start. Therefore, they cannot evaluate the effects of latent defects (e.g., handling, manufacturing, transportation, and prior mission), nor assist in determining the testability payoff or requirements for detection and removing them before the start of the mission. Models with this limitation cannot be used to evaluate alternate maintenance concepts that include degradation between missions as an acceptable strategy.

(f) Some models require that spares be treated exactly like active units, irrespective of their actual utilization in the system mechanization. This requires that spares are assumed to be "hot" and have the same failure rates and failure modes as the active units. This assumption will cause the model to understate the system reliability in those situations where spares are "cold" or in "stand-by" and/or where their failure rates may be less that those of the active units.

(g) As indicated previously, some models require the assumption that item failure rates are constant throughout time. This will result in an overstatement of system reliability if the items have failure rates that increase with mission time. Some models remove this restriction and permit time-varying failure rates. However, the solution the algorithms employ requires the use of global time (as opposed to local time of entry into a state), thus precluding the use of the model for repairable systems and availability analysis.

3-5. Improving availability through reliability-centered maintenance (RCM)

All C4ISR facilities that are currently in operation require maintenance to continue to properly perform their functions and support their assigned missions. An effective and efficient maintenance program saves resources and maximizes availability. Reliability-Centered Maintenance (RCM) is an approach for developing an effective and efficient maintenance program based on the reliability characteristics of the constituent parts and subsystems, economics, and safety.

a. RCM introduction. Prior to the development of the RCM methodology, it was widely believed that everything had a "right" time for some form of preventive maintenance (PM), usually replacement or overhaul. Despite this commonly accepted view, the results indicated that in far too many instances, PM seemed to have no beneficial effects, and, in many cases, actually made things worse by providing more opportunity for maintenance-induced failures.

b. RCM overview. The RCM approach provides a logical way of determining if PM makes sense for a given item and, if so, selecting the appropriate type of PM. The approach is based on:

(1) RCM seeks to preserve system or equipment function, not just operability for operability's sake.

(2) RCM is more concerned on maintaining end system function than individual component function.

(3) Use reliability as the basis for decisions. The failure characteristics of the item in question must be understood to determine the efficacy of preventive maintenance.

(4) Consider safety first and then economics. Safety must always be preserved. When safety is not an issue, preventive maintenance must be justified on economic grounds.

(5) Acknowledge design limitations. Maintenance cannot improve the inherent reliability – it is dictated by design

(6) Treat RCM as a continuing process. The difference between the perceived and actual design life and failure characteristics is addressed through age (or life) exploration.

c. Preventive maintenance. RCM has changed the approach to preventive maintenance. The RCM concept has completely changed the way in which PM is viewed. It is now widely accepted that not all items benefit from PM, and it is often less expensive (in all senses of that word) to allow an item to "run to failure" rather than to do PM.

d. RCM definitions. The following definitions are commonly used in connection with RCM.

(1) RCM is a logical, structured framework for determining the optimum mix of applicable and effective maintenance activities needed to sustain the operational reliability of systems and equipment while ensuring their safe and economical operation and support.

(2) Maintenance is defined as those activities and actions that directly retain the proper operation of an item or restore that operation when it is interrupted by failure or some other anomaly. (Within the context of RCM, proper operation of an item means that the item can perform its intended function.

(3) Corrective maintenance is maintenance required to restore a failed item to proper operation. Restoration is accomplished by removing the failed item and replacing it with a new item, or by fixing the item by removing and replacing internal components or by some other repair action.

(4) Scheduled and Condition-based preventive maintenance conducted to ensure safety, reduce the likelihood of operational failures, and obtain as much useful life as possible from an item

e. Condition monitoring and analysis. Some impending failures can be detected using some form of condition monitoring and analysis, a type of preventive maintenance. Condition monitoring is defined as periodically or continuously checking physical characteristics or operating parameters of an item. Based on analyzing the results of condition monitoring, a decision is made to either take no action or to replace or repair the item. Condition monitoring can be performed through inspection, or by monitoring performance or other parameters,.

f. The RCM concept. RCM has two primary objectives: to ensure safety through preventive maintenance actions, and, when safety is not a concern, preserve functionality in the most economical manner. Preventive Maintenance (PM) is applicable only if it is both effective and economically viable. When safety is not a consideration and PM is either not effective or less economical than running to failure, only CM is required.

(1) PM can be effective only when there is a quantitative indication of an impending functional failure or indication of a hidden failure. That is, if reduced resistance to failure can be detected (potential failure) and there is a consistent or predictable interval between potential failure and functional failure, then PM is applicable.

(2) . The costs incurred with any PM being considered for an item must be less than for running the item to failure (economic viability). The failure may have operational or non-operational consequences. The two categories of cost included in such a comparison for these two failure consequences are (1) operational - the indirect economic loss as a result of failure and the direct cost of repair, and (2) non-operational - the direct cost of repair.

g. A product can fail in two basic ways. First, it can fail to perform one or more of the functions for which it was designed. Such a failure is called a functional failure. Second, a product can fail in such a way that no function is impaired. The failure could be something as simple as a scratch or other damage of the finish of the product. Or it could be that one of two redundant items, only one of which is required for a given function, has failed.

h. The three categories of failure consequences generally used in RCM analysis are Safety, Operational, and Economic. If a functional failure directly has an adverse affect on operating safety, the failure effect is categorized as Safety. When the failure does not adversely affect safety but prevents the end system from completing a mission, the failure is categorized as an Operational failure. When a functional failure does not adversely affect safety and does not adversely affect operational requirements, then the failure is said to have an Economic effect. The only penalty of such a failure is the cost to repair the failure.

3-6. Application of RCM to C4ISR facilities

For equipment used in facilities, condition monitoring, including inspections, overhauls, lubrication and servicing, and failure-finding tasks are all routinely part of an RCM-based

preventive maintenance program. C4ISR facilities potentially require all these tasks. More detailed information on applying RCM to C4ISR facilities will appear in TM 5-698-2 when written.

CHAPTER 4

ASSESSING RELIABILITY AND AVAILABILITY OF C4ISR FACILITIES

4-1. Purpose of the assessment

As systems become more and more complex, good methods for specifying and analyzing the systems and their sub-systems become more important. Reliability modeling (including prediction, evaluation, and control) is vital for proper design, dependable operation, and effective maintenance of systems. The popularity of designing redundancy into systems poses additional challenges to reliability professionals. For the various kinds of redundant systems, the reliability and availability are extremely sensitive to even small variations in certain parameters; thus, understanding and insight can be gained only by modeling. The purpose of this section is to provide the reader with an understanding of a type of modeling to assist in the decision making process for facility improvement. The Case Study provides an example of how much effort is necessary to baseline your facility and identify potential improvement areas. It is not specifically designed as an instructional document but more of a tutorial. The Case Study makes use of one software tool to quantify availability. In reality, the Case Study is an explanation of a specific type of modeling designed to predict facility performance, not necessarily simulate facility performance.

4-2. Approach

This modeling approach provides facility managers with a cost effective analysis for baselining their facilities and identifying areas of weakness. The results of the model will provide the basis for trade-offs for improving system availability. This chapter first provides the reader with basic concepts of modeling and identifies two approaches: empirical and statistical. Recommendations as to the type of model will be discussed along with a Case Study of an electrical system analysis utilizing a specific deterministic modeling program called GO.

4-3. General modeling concepts

The need to assess the reliability, availability, and maintainability of a system is becoming more important as organizations understand the potential effects of failures and downtime for the systems. Regardless of what product/service is being offered, or who the intended customer may be, it should be a reasonable assumption to state that the degree of product/service success is directly related to the ability of that product/service to meet or exceed customer expectations. Two popular means of assessing the reliability, availability, and maintainability of a system are empirical methods and statistically-based methods. When the statistically-based reliability characteristics (underlying distribution of failures and distribution parameters) of system modules are known, simulation is one way of using those characteristics to analyze system behavior.

a. Empirical prediction methods. For many types of parts, such as bearings and gears, engineers have noted a relationship between reliability and stress. For example, the bearing industry developed an empirical equation in the 1940s that relates fatigue life and bearing loading. The equation was developed using data analysis techniques such as regression analysis. The equations are valid only for the specific type of part for which they were developed and the

type of stress (e.g., fatigue failures). The equations are not statistically based and can provide only point estimates of reliability.

b. Statistically-based prediction models. By collecting data from a sample, either from a test or from field operation, a set of statistics can be derived. Based on the sample statistics, conclusions can be drawn regarding the population from which the sample was taken. When times to failure for parts are recorded, for example, Weibull analysis can be used to determine the statistical reliability function for the sample of parts. If the sample was representative of the population, we can infer the reliability characteristics of the population.

c. Simulation. Over the years, simulation has become a trusted tool in system design, development, implementation, and improvement. Simulation has proven to be versatile, as it can be applied from evaluating theoretical concepts to sustaining an examination of minor improvements to an existing, fully operational system.

(1) Webster's dictionary defines simulation as the following: "the imitative representation of the functioning of one system or process by means of another <a computer ~ of an industrial process>." This definition illustrates why simulation has historically proven to be agreeable to the reliability field, specifically the system parameters of reliability, maintainability, availability, system effectiveness, cost, and schedule.

(2) The eight-step process shown in table 4-1 should be adhered to during a simulation study (when applied to a reliability analysis). Validation is to be carried out throughout the eight-step process.

Table 4-1. Steps in performing a simulation.

Problem Definition: define simulation problem and its objectives.
Model Building: description of system's entities and their interaction.
Data Collection: quantify probability distributions for system's entities.
Program Code: select programming language to execute simulation (best to do before model is completed).
Verification: check that code is achieving expected results.
Experimental Design: determine initial conditions, simulation period and number of runs (must be statistically valid).
Implementation: run simulation and test its sensitivity to variations.
Documentation: document simulation study to verify problem definition objectives are reached (document enough for functional model in future).

4-4. Prediction

There are many valid reasons for predicting reliability. One purpose for reliability prediction is to assess the product design progress and to provide a quantitative basis for selection among competing approaches or components. In addition, prediction results can be used to rank design problem areas and assess trade study results. A combination of prediction methods should be used to assess progress in meeting design goals, achieving component or part derating levels, identifying environmental concerns, controlling critical items and determining end-of-life failure mechanisms. Predictions should be an ongoing activity that start with the initial design concept and the selection of parts and materials, and continue through the evaluation of alternate design approaches, redesigns, and corrective actions. Each iteration of prediction should provide a better estimate of product reliability as better information on the product design approach becomes

available. Later predictions, during the developmental phase, are used to evaluate life-limiting constraints, as well as identify design problem areas.

4-5. The GO method

The following sections outline vital information for an analyst utilizing the GO software tool. Paragraph 4-5a reviews the background of the GO software and 4-6b identifies a data source that can be used as an input to the tool. Paragraph 4-5c identifies the logic behind an analysis completed within GO, specifically the operators utilized as a representation of the components of a system. Next, paragraph 4-6 presents a case study, outlines the steps required to complete a GO analysis from identifying the one line diagram for the system to performing an analysis or troubleshooting the GO model. Paragraph 4-7 identifies the bibliographical sources utilized within this paper. Paragraph 4-8 defines important terms concerning the operators utilized within the GO software.

a. GO background. The estimation of product reliability requires judgment about its future. Such predictions are based primarily on modeling past experience and data. The GO software has proven to be a successful means of determining the availability and reliability of systems. GO was first introduced as a means of evaluating key reliability metrics of nuclear power facilities, but over the years it has proven to be a valuable tool in evaluating other systems.

(1) The GO software was originally designed to address the need of measuring the availability of nuclear facilities. The GO method, unlike fault tree analysis which focuses on a single system event and uses good/bad elements, is a comprehensive system analysis technique that addresses all system operational modes and is not restricted to two-state elements. GO is not a simulation package but a tool that utilizes the point estimates of component reliabilities to calculate desired system metrics. The GO procedure has been enhanced over the years to incorporate some special modeling considerations, such as system interactions and dependencies, as well as man-machine interactions. GO models are developed in a forward-looking manner following normal process flow or operational sequences. The models determine all system response modes (i.e. successes, failures, prematures, etc.).

(2) GO models consist of arrangements of GO operator symbols and represent the engineering functions of components, subsystems, and systems. The models are generally constructed from engineering drawings by replacing engineering elements (valves, motors, switches, etc.) with one or more GO symbols that represent system functions, logic, and operational sequences. The GO software uses the GO model to quantify system performance. The method evaluates system reliability and availability, identifies fault sets, ranks the relative importance of the constituent elements, and places confidence bounds on the probabilities of occurrence of system events reflecting the effects of data uncertainties.

(3) Key features of the GO method are:

- Models follow the normal process flow;
- Most model elements have one-to-one correspondence with system elements;
- Models accommodate component and system interactions and dependencies;
- Models are compact and easy to validate;
- Outputs represent all system success and failure states;
- Models can be easily altered and updated;
- Fault sets can be generated without altering the basic model;

- System operational aspects can be incorporated; and
- Numerical errors due to pruning are known and can be controlled.

(4) The GO procedure uses a set of standardized operators to describe the logic operation, interaction, and combination of physical equipment and human actions. The logic for properly combining the inputs for each GO operator is defined in a series of algorithms contained in the GO computer codes. These standardized operators are used to model commonly encountered engineering subsystems and components. A system is modeled by selecting the GO operators that characterize the elements of the system (i.e. represent the operational states that can be taken) and interrelating their inputs and outputs. The specific probabilities of component operation are defined separately as inputs to the computer code.

b. Input data sources to GO models. The U.S. Army Special Mission Office's Power Reliability Enhancement Program (PREP) sponsored a study of the reliability, availability, and maintainability characteristics of 234 power generation, power distribution, and heating, ventilation, and air conditioning (HVAC) items. This study will be summarized and published in the forthcoming Institute of Electric and Electronics Engineers (IEEE) Gold Book. The Reliability Analysis Center, a U.S. Department of Defense Information Analysis Center operated by IIT Research Institute, Rome, NY, began the work in October 1991 and delivered the final report in early 1994. (This study resulted in a publication within IEEE Transactions on Industry Applications in March/April 1999 entitled "Operational Maintenance Data for Power Generation Distribution and HVAC Components", and again in Jan/Feb 2001 entitled "Survey of Reliability and Availability of Power Distribution, Power Generation, and HVAC Components for Commercial, Industrial, and Utility Installations," which article will appear in its entirety as an appendix to the Gold Book). Items that were included in the study are gas turbine generators, diesel engine generators, switch-gear assemblies, cables, boilers, piping, valves, and chillers. This program was designed to determine the effects of "new technology" equipment (i.e. equipment installed after 1971) on availability. Information was obtained on a variety of commercial and industrial facility types (including office buildings, hospitals, water treatment facilities, prisons, utilities, manufacturing facilities, schools, universities, and bank computer centers), with varying degrees of maintenance quality. Data collection guidelines and goals were established to ensure that sufficient operational and maintenance data were collected for statistically valid analysis. Two keys to the data collection process were ensuring data completeness and accounting for maintenance policies.

(1) Data was categorized into different levels of data completeness to ensure that the final data collection included a fair data representation for each component, the data completion was quantified by four levels:

(a) Level 1 - Perfect Data: Data needed for a valid, complete reliability study, including a parts list, failure history data with time-to-failure statistics, parts description data, operational periods, and ten continuous years of recorded data. No engineering judgment or data extrapolation is required.

(b) Level 2 - Not Perfect Data: No serious flaws in data, but data collection process demanded additional time to ensure useful information was gathered.

(c) Level 3 - Verbal/Inspection Data: Serious gaps existed in data that required additional documentation and verification prior to its inclusion in the database. Senior maintenance personnel were interviewed to extract the necessary information to fill the data gaps.

(d) Level 4 - Soft Data: Data that relied on the memories of experienced maintenance personnel from the participating facility; it was often extracted from log books containing maintenance personnel entries, filing cabinets with work order forms, and repair records when outside repair support was needed. Engineering judgment was often required to determine numerous performance parameters.

(2) The data collection effort was planned to minimize the effects of maintenance policies and procedures on the calculated availability values by collecting data from a variety of locations with varying maintenance policies. Each facility's maintenance policy and procedure was categorized into one of three levels:

(a) Above average: The facility not only followed a scheduled, preventative maintenance policy that was equivalent or similar to the manufacturer's suggested policy, but also went beyond it, such as using redundant units, specialized equipment tests (thermograph, vibration analysis, oil analysis), complete spare parts kits for equipment, and so on.

(b) Average: Facility used either in-house maintenance crews performing scheduled, preventative maintenance according to the equipment manufacturer's suggested PM schedule or a combination of in-house maintenance crews and outside contractors. In either case, it was verified that they did follow a fairly rigid schedule.

(c) Below average: Facility's actual policy was less than average. It may have instituted a scheduled maintenance policy but not followed it or it may have had no maintenance policy. Symptoms such as leaky valves with rags tied around them, dirty air filters, squeaky bearings, loose belts, and general housekeeping because of unavailable manpower were typical signs that maintenance at a facility was less than desirable.

c. Input data sources to GO models. The IEEE Gold Book is another source of reliability information which has become the standard for reliability calculations over the years. Chapter 3 of the Gold Book summarizes years of survey information collected from a variety of users and manufactures. This data is compiled into a publication sold around the world. The data is presented in a variety of formats for the analyst discretion in utilizing the information. Reliability information as well as failure mode distribution can be found in chapter 3.

d. GO logic. The basic building block of a GO model is the node. Nodes can be either logical or physical, depending on their model function. Physical nodes correspond to actual pieces of equipment and have a reliability associated with them. They have either zero or one input signals (i.e. they may or may not be dependent on prior equipment for successful operation) with exactly one output signal. Logical nodes correspond to interconnections within the system or represent constraints imposed by mission requirements. Logical nodes have multiple inputs and may have multiple outputs to combine the physical nodes of the system. Examples of the operators found in the GO program are outlined in the following subsection.

e. GO operator types. Each of the following subsections presents all pertinent information for an operator type. Each type is presented with its usual name, symbol, the required operator data, the required kind data, the exact logical operation of the type, and comments. Prior to reviewing the description of the operator types that follow, the table of definitions that appears in appendix E should be read and understood. The following symbols are used consistently (other symbols will be defined as they are used):

S_1, S_2, … the identification number of an input (source, stimulus or input) signal

R_1, R_2, …the identification number of an output (result, response or output) signal

K the kind identification number
VS_i, VR_i the value (time) of signal S_i or R_i
P_1, P_2, … probability
∞ infinity or never

(1) When a type has only one input (output) the subscript on S(R) will be deleted.

(2) The operator and kind data are shown in the same order in which they must appear on data entries. We have generally separated the data items by a comma and a blank, but any combination of blanks and/or comma is permitted. Each record must end with a terminator (a dollar sign or slash depending upon the computer used). These terminators are not shown here.

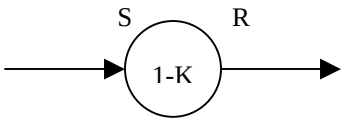
(3) Certain types (6, 7, and 9) have non-symmetric inputs (i.e. inputs are not interchangeable as in type 2 and 10). To differentiate between such inputs on the GO chart symbol we use a full arrowhead for the primary input and a half arrowhead for the secondary one or indicate the primary input by the letter "a" and the secondary one by the letter "b."

(4) The general order of operator data is: type, kind, number of inputs, inputs, number of outputs, outputs. The number of inputs and the number of outputs are omitted when the type definition requires a specific number (i.e. a type 1 always has one input and one output, therefore the two "1's" are not explicitly included in the data list).

(5) Types 2, 10, and 11 do not require kind data. The kind number in the operator data list is set to 0 for types 2 and 10 and is set equal to the value of the extra parameter for a type 11.

f. Type 1: Two state component

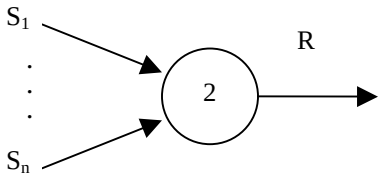
(1) GO symbol:



(2) Operator data: 1, K, S, R
(3) Kind data: K, 1, P_1, P_2
P_1: Component is good
P_2: Component fails
(4) Operation: VR = VS, if the component is good
= never, if the component is not good
(5) Comment: This type models any device which can assume one of the two states. The usual state interpretations are "good" and "bad."

g. Type 2: OR gate

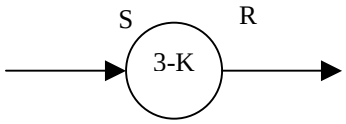
(1) GO symbol:



(2) Operator data: 2, 0, n, S_1, …, S_n, R
n: number of inputs, $2 \leq n \leq 10$
(3) Kind data: none
(4) Operation: VR = min {VS_1, …, VS_n}
(5) Comments:
(a) The name "OR gate" is used in the sense that R will occur as soon as S_1 or … or S_n occurs.
(b) Note that the kind number in the operator data is set to zero.

h. Type 3: Triggered generator

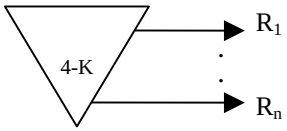
(1) GO symbol:



(2) Operator data: 3, K, S, R
(3) Kind data: K, 3, P_1, P_2, P_3
P_1: generator is good
P_2: generator fails
P_3: generator operates prematurely
(4) Operation: VR = 0, if the actuator prematures
= never, if the generator fails
= VS, if the generator is good
(5) Comment: This type is commonly used to model relay coils, accelerometers, etc.

i. Type 4: Multiple signal generator

(1) GO symbol:



(2) Operator data: 4, K, n, R_1, …, R_n
n: number of outputs, $1 \leq n \leq 10$
(3) Kind data: K, 4, n, m, V_{11}, …, V_{1n}, P_1

. . .
. . .
. . .
V_{m1}, …, V_{mn}, P_m

m: number of states for each signal (the total amount of kind data cannot exceed 100 items)
V_{ij}: the value of the i^{th} state of the j^{th} signal
P_i: the probability that the signals are in the i^{th} state

$$\sum P_i = 1.0$$

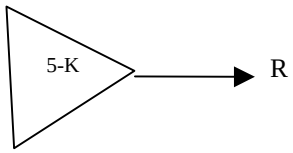
(4) Operation: $VR_1 = V_{11}$, $VR_2 = V_{12}$, …, $VR_n = V_{1n}$ with probability P_1

. . .
. . .
. . .
$VR_1 = V_{m1}$, $VR_2 = V_{m2}$, …, $VR_n = V_{mn}$ with probability P_m

(5) Comment: The type 4 operator generates two or more statistically dependent signals. It is a special case of the type 13 operator.

j. Type 5: Signal generator

(1) GO symbol:



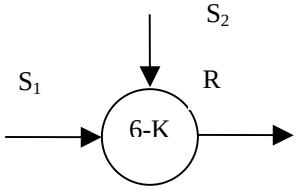
(2) Operator data: 5, K, R
(3) Kind data: K, 5, n, V_1, P_1, …, V_n, P_n
n: number of values for which a signal is to be generated
V_j: i^{th} value
P_i: probability for the i^{th} value

$$\sum_{i}^{n} P_i = 1$$

(4) Operation: VR = V_i with probability P_i, i = 1, …, n
(5) Comment: none

k. Type 6: Normally open contact

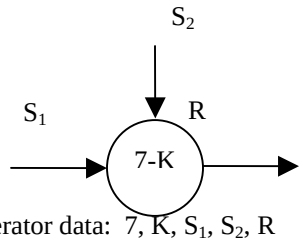
(1) GO symbol:



(2) Operator data: 6, K, S_1, S_2, R
(3) Kind data: K, 6, P_1, P_2, P_3
P_1: contact closes normally
P_2: contact fails to close
P_3: contact closes prematurely
(4)Operation: VR = max {VS_1, VS_2}, if the contact operates normally
= VS_1, if contact closes prematurely
= never, if contact fails
(5) Comment: none

l. Type 7: Normally closed contact

(1) GO symbol:



(2) Operator data: 7, K, S_1, S_2, R

(3) Kind data: K, 7, P_1, P_2, P_3

P_1: contact open normally

P_2: contact fails to open

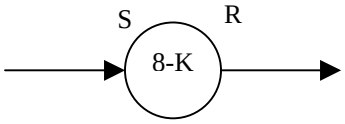
P_3: contact opens prematurely

(4) Operation: VR = VS_1, if the contact fails, or if $VS_2 > VS_1$ and the contact opens normally
= never, otherwise

(5) Comment: Note the convention that the simultaneous occurrence of S_1 and S_2 produce R at time never.

m. Type 8: Increment generator

(1) GO symbol:



(2) Operator data: 8, K, S, R

(3) Kind data: K, 8, n, D_1, P_1 …, D_n, P_n

N: number of possible increments, $1 \leq n \leq 48$

D_i: value of the i^{th} increment, $-\infty \leq D_i \leq \infty$

P_i: probability that the i^{th} increment occurs

$$\sum_{i}^{n} P_i = 1$$

(4) Operation: with probability P_i, i = 1, n

$VS + D_i$, if $0 \leq VX + D_i < \infty$

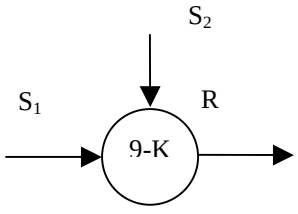
$VR = 0$, if $VS + D_i < 0$

∞, if $VS + D_i > \infty$

(5) Comments: The delay values can be negative as noted in the kind data.
The type 8 operator models component response delays.

n. Type 9: Function operator

(1) GO symbol:

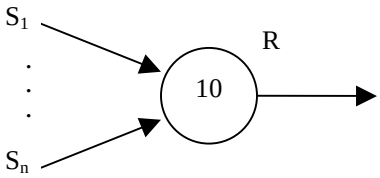


(2) Operator data: 9, K, S_1, S_2, R

(3) Kind data: K, 9, n, X_1, Y_1, …, X_n, Y_n
n: number of X_i, Y_i pairs
X_i, Y_i: ± time values. The set of pairs defines Y_i as a function of X_i (i.e., $Y_i = f(X_i)$). Both X_i and Y_i may lie in the range from –never to +never inclusive. Values of X_i within that range which are not explicitly included in the kind data have an associated Y_i of never.
(4) Operation: $VR = \max \{0, \min \{VS_1 + f(VS_2 - VS_1)\}\}$
(5) Comments: This type is "perfect" in the sense that there is always just one output term (with probability 1).
It is used to handle complex timing situations. It is somewhat difficult to get acquainted with but has proved to be of great value in many cases.

o. Type 10: AND gate

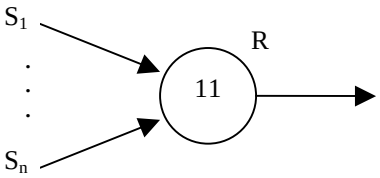
(1) GO symbol:



(2) Operator data: 10, 0, n, S_1, …, S_n, R
n: number of inputs, $2 \leq n \leq 10$
(3) Kind data: none
(4) Operation: $VR = \max \{VS_1, \ldots, VS_n\}$
(5) Comments: The name "AND Gate" is used in the sense that R will occur as soon as S_1 and … or S_n occurs. Note that the kind number in the operator data is set to zero.

p. Type 11: m-out-of-n gate

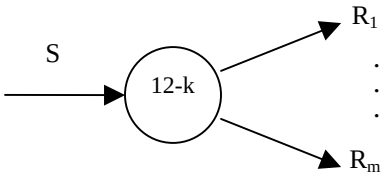
(1) GO symbol:



(2) Operator data: 11, m, n, S_1, …, S_n, R
n: number of inputs, $2 \leq n \leq 10$
m: gate parameters, $1 \leq m \leq n$
(3) Kind data: none
(4) Operation: Let V_1, V_2, …, V_n be the ordered set of values of VS_1, VS_2, …, VS_n (from smallest to largest). Then: $VR = V_m$
(5) Comments: Note that the kind number in the operator data is replaced with the gate parameter. If m = 1, this type is equivalent to a type 2; and if m = n, it is equivalent to a type 10.

q. Type 12: Path splitter

(1) GO symbol:



(2) Operator data: 12, K, S, m, R_1, …, R_m
m: number of outputs, $1 \leq m \leq 10$
(3) Kind data: K, 12, m, P_1, …, P_m
P_i: probability that i^{th} path is "selected"

$$\sum_{i}^{m} P_i = 1$$

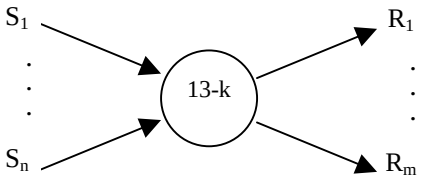
(4) Operation: m + 1 terms are produced. The first m of these are defined by:
VR_i = VS and VR_j = never for all $j \neq i$, with probability P_i, i = 1, …, m
And the m + 1^{st} is defined by:
VR_j = never for all j, with probability

$$1 - \sum_{i}^{m} P_i$$

(5) Comment: The m+1^{st} term does not occur if $\sum P_i = 1$.

r. Type 13: General purpose multiple input, multiple output operator

(1) GO symbol:



(2) Operator data: 13, K, n, S_1, …, S_n, m, R_1, …, R_m
n: number of inputs, $0 \leq n \leq 10$
m: number of outputs, $1 \leq m \leq 10$
(3) Kind data: K, 13, n, m, N

VS_{11} …$VS_{n1}m_1$
VR_1 … VR_mP_{11}
.
.
.
.
.
.
VR_1 … VR_m P_{m11}
VS_{1N} … $VS_{nN}m_N$
VR_1 … VR_m P_{1N}
.
.
.
VR_1 ... VR_m P_{mnN}

where:

n:	number of inputs, $0 \leq n \leq 10$
m:	number of outputs, $1 \leq m \leq 10$
N:	number of output time sets, $N \geq 1$, (if n = 0, N = 1)
Mi:	number of output terms for the i^{th} output time set
VS_{1i}, … VS_{ni}:	the ith input value comparison set (missing if n = 0)
P_{ij}:	probability of the i^{th} output term in the j^{th} output value set

$$\sum_{i=1}^{M_i} P_{ij} = 1,\ j = 1, ..., N$$

(4) Operation: If $n \neq 0$, the actual input values are compared with the N input value comparison sets. If a match is found, the corresponding joint output distribution is produced. If no match is found, all output values are set to never (with probability 1).
If n = 1, the signal joint output distribution is produced.

(5) Comments:

(a) The maximum amount of kind data is limited to 100 data items.

(b) For legibility the kind data should probably be laid out on several cards in the form indicated in c above rather than simply strung out item-by-item.

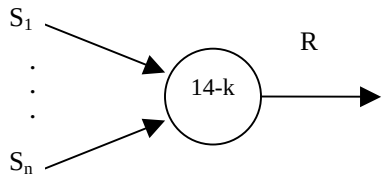
(c) In principle, any of the other GO types could be replaced by properly defined type 13's. However, the amount of kind data required for a complete definition is prohibitive in most cases. Consequently judicious use of the type 13 is indicated.

(d) Setting n (# of inputs) to zero gives us a signal generator which can produce several dependent signals (i.e., type 4) (as contrasted to several independent signals which would be produced by several type 5's).

(e) A type 13 can be easily used as a non-stochastic function device in which a single (multiple) output is defined as a function of a single (multiple) input.

s. Type 14: Linear combination generator

(1) GO symbol:



(2) Operator data: 14, K, n, S_1, …, S_n, R
n: number of inputs, $2 \leq n \leq 10$

(3) Kind data: K, 14, n, a_1, …, a_n, a_0
a_i: any real number

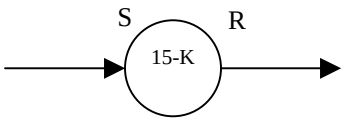
(4) Operation: Let A be the value of $a_0 + a_1 \times VS_1 + \ldots + a_n \times VS_n$ rounded to the nearest integer. Then:

VR = max 0, min A, never, if all $VS_i <$ never
VR = never, if any VS_i = never

(5) Comment: When using this type, signal values will usually be interpreted as amounts of some quantity rather than times.

t. Type 15: Time/probability gate-generator

(1) GO symbol:



(2) Operator data: 15, K, S, R

(3) Kind data: K, 15, V_1, V_2, V_3, V_4, P_1, P_2
V_1: output value if input is in gate (set to -1 if output value is to equal input value)
V_2: output value if input is not in gate
V_3, V_4: value gate values, $0 \leq V_3 \leq V_4 \leq$ never

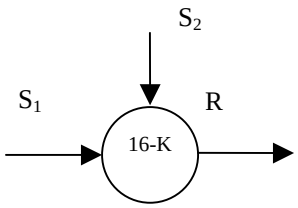
P_1, P_2: probability gate values, $0 \leq P_1 \leq P_2 \leq 1$

(4) Operation: Let V = V1, if $V1 \geq 0$
= VS, if V1 = -1
and PS = probability association with the input term
Then VR = V, if $V_3 \leq VS \leq V_4$ and $P_1 \leq PS \leq P_2$
= V_2, otherwise

(5) Comment: none

u. Type 16: Actuated normally open contact

(1) GO symbol:



(2) Operator data: 16, K, S_1, S_2, R

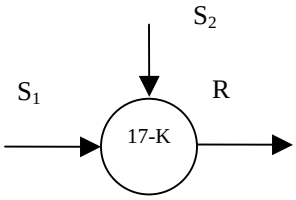
(3) Kind data: K, 16, P_1, P_2, P_3
P_1: contact operates normally
P_2: contact fails opened
P_3: contact fails closed

(4) Operation: VR = 0, if contact fails opened
= VS_1, if contact fails closed
= min {VS_1, VS_2}, if contact operates normally

(5) Comment: none

v. Type 17: Actuated normally closed contact

(1) GO symbol:



(2) Operator data: 17, K, S_1, S_2, R

(3) Kind data: K, 17, P_1, P_2, P_3
P_1: contact operates normally
P_2: contact fails closed
P_3: contact fails opened

(4) Operation: VR = ∞, if (a) contact normal and $VS_2 \geq VS_1$
(b) contact fails open and $VS_1 > 0$
(c) $VS_1 = 0$
= 0, if contact fails closed and $VS_1 > 0$
= VS_2, if $VS_1 = 0$ and $VS_2 < VS_1$ and contact normal

(5) Comment: Note the arbitrary convention that if $VS_1 = VS_2$, VR = ∞

w. Additional GO information. An understanding of the GO operator types and their algorithms is essential to modeling system availability or reliability appropriately. However, it is not necessary to be

thoroughly familiar with all of the operator types since some are used more frequently than others. There is a natural hierarchy of the operator types, based on ease of use and utility. Experience has shown that practically all modeling situations can be handled with the first two groups of operators. But special situations and the sophistication of the modeling may result in the use of operators from the third group (least used types). The hierarchy is:

(1) Most commonly used types: 1, 2, 5, 6, 10

(2) Often used types: 3, 7, 9, 11, 15

(3) Least used types: 4, 8, 12, 13, 14, 16, 17

4-6. GO model development

As previously discussed, the node is the basic building block to any GO model. The node can represent either the physical equipment of the system or the logical equipment that ties the system together. Unfortunately, there is no way to model control loops in which feedback signals propagate from downstream components to upstream components. If the items in the control loop affect reliability, the influence of those items must be reduced to a series operator. GO also requires that all nodes be independent, if two or more components are not independent, their dependency can be modeled as a logical combination of independent nodes. In the end, the GO model will resemble a tree of nodes. Signals flow down through the tree until they reach the bottom or output nodes, which have no nodes connected to their outputs.

a. Step 1: One line drawing creation/analysis. The first step to performing an analysis with GO is to examine the one line drawing that represents the system. Often, the one line drawing must be developed by the analyst. The one line drawing provides the analyst the path that must be modeled by GO to accurately represent the physical and logical equipment of the system. Figure 4-1 represents a one line drawing of the IEEE Gold Book Standard Network System. This system is supplied by two independent 15kV primary distribution feeders. There are four diesel engine generators at the facility where two of four generators are required to meet the network load demands at all times. The reliability indices of the load points in figure 4-1 (i.e. OUTPUTS A, B1, B2, C, D, E1, E2) will be evaluated by the Boolean Algebra reliability analytical methodology. The following reliability indices will be evaluated:

(1) Frequency of load point interruptions (interruptions per year).

(2) Annual duration of load point interruptions (hours per year).

(3) Average duration of load point interruptions (hours per interruption).

(4) Availability level of power supply to the load point.

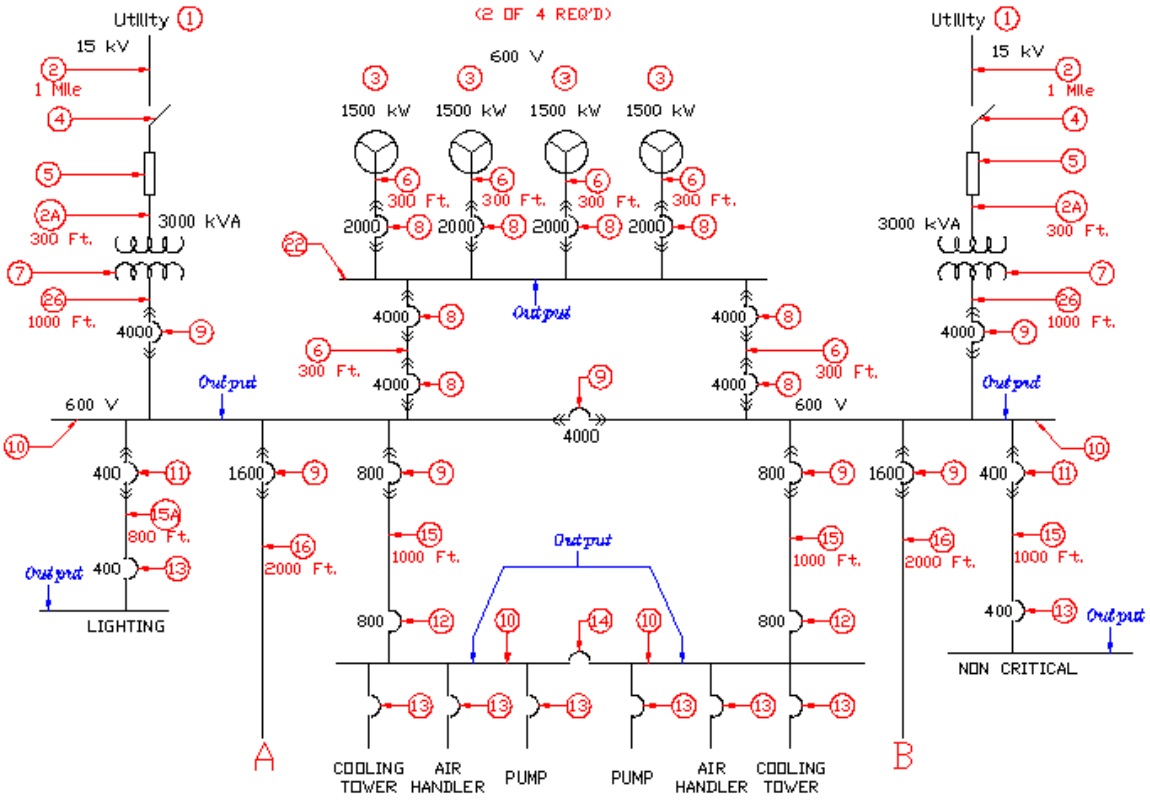


Figure 4-1. Single line diagram of IEEE Gold Book Standard Network.

b. Step 2: Parts identification. The next step is to develop a parts list of all the components found on the one line diagram. The analyst must identify the components compromising the system and identify them by functional categories. This way the reader can review the information in a logical process. Included in the parts list is the following information:

- Designation of the part identifying any alphanumeric reference on the one line diagram. This is the tie from the one line to the parts list.
- Description of the part including any qualifying information to ratings, size, normal operating position, etc.
- Identification of the Kind number that is a unique tracking identifier used in the GO model development.
- Reliability information including statistical numeric to develop the Inherent Availability information for the model.
- Data source category to track the different locations where the information originated.

(1) It is during this step that the analyst must determine what assumptions will be needed to complete the reliability analysis of the IEEE Gold Book Standard Network. The assumptions will allow the results that are obtained to be meaningfully compared with results obtained by using methodologies other than GO. The following assumptions were identified for any reliability methodology applied to the IEEE Gold Book Standard Network:

- Actual cable lengths are indicated on the drawings (see figure 4-1), modify failure rates accordingly. (For example, Cable Failure Rate per rated length X% of Actual Cable Length indicated on the drawing.)
- M denotes manual operation and is allocated 15 minutes for activation.
- 2 out of 4 generators are required.
- The UPS are redundant.
- The PDU transformers are redundant.
- Terminations, while normal for all systems, are omitted from the drawings. For this analysis terminations or splices are not included in the reliability calculations.
- Circuit breaker failure modes are assumed to be 50% open and 50% shorted.
- Constant failure rate is assumed.

(2) Table 4-2 identifies the pertinent statistical data used in the GO model to analyze the IEEE Gold Book Standard Network. The data is derived from the PREP database, which was discussed in paragraph 4-5b of this report, and supplemented by the IEEE Gold Book.

Table 4-2. Equipment availability data for Gold Book Standard Network configuration

Ref. #	Item Description	PREP Item #	Inherent Availability	MTTR (Hours)	Failure Rate (Failure/Year)	Calculated Availability
1	Single Circuit Utility Supply, 1.78 failures/unit years, A = 0.999705, Gold Book p. 107	NA	0.999705	1.32	1.956	?
2	Cable Arial, ≤ 15kV, per mile	32	0.99999022	1.82	0.047170	?
2A	Cable Arial, ≤ 15kV - 300 feet	32		1.82	0.002680	0.999999443
3	Diesel Engine Generator, Packaged, Stand-by, 1500kW	98	0.99974231	18.28	0.123500	?
4	Manual Disconnect Switch	187	0.9999998	1	0.001740	?
5	Fuse, 15kV	117	0.99995363	4	0.101540	?
6	Cable Below Ground in conduit, ≤ 600V, per 1000 ft	47	0.99999743	11.22	0.002010	?
6A	Cable Below Ground in conduit, ≤ 600V - 300 feet			11.22	0.000603	0.999999228
7	Transformer, Liquid, Non Forced Air, 3000kVA	208	0.99999937	5	0.001110	?
8	Ckt. Breaker, 600V, Drawout, Normally Open, > 600 Amp	68	0.99999874	2	0.005530	?
8A	Ckt. Breaker, 600V, Drawout, Normally Open, > 600 Amp	68		2	0.002765	0.999999369
9	Ckt. Breaker, 600V, Drawout, Normally Closed, >600 Amp	69	0.99999989	0.5	0.001850	?
9A	Ckt. Breaker, 600V, Drawout, Normally Closed, >600 Amp	69		0.5	0.000925	0.999999947
10	Switchgear, Bare Bus, 600V	191	0.9999921	7.29	0.009490	?
11	Ckt. Breaker, 600V Drawout, Normally Closed, < 600 Amp	67	0.99999986	6	0.000210	?
11A	Ckt. Breaker, 600V Drawout, Normally Closed, < 600 Amp	67		6	0.000105	0.999999928
12	Ckt. Breaker, 600V, Normally Closed, > 600 Amp, Gold Book p. 40	63	0.99998948	9.6	0.009600	?
12A	Ckt. Breaker, 600V, Normally Closed, > 600 Amp, Gold Book p. 40	63		9.6	0.004800	0.999994740
13	Ckt. Breaker, 3 Phase Fixed, Normally Closed, ≤ 600 Amp	61	0.99999656	5.8	0.005200	?
13A	Ckt. Breaker, 3 Phase Fixed, Normally Closed, ≤ 600 Amp, Gold Book p. 40	61		5.8	0.002600	0.999998279
14	Ckt. Breaker, 3 Phase Fixed, Normally Open, > 600 Amp	62	0.99998532	37.5	0.003430	?
14A	Ckt. Breaker, 3 Phase Fixed, Normally Open, > 600 Amp	62		37.5	0.001715	0.999992658
15	Cable, Above Ground, No Conduit, ≤ 600V, per 1000 ft.	20	0.99999997	2.5	0.000120	?
15A	Cable, Above Ground, No Conduit, ≤ 600V, per 1000 ft.	20		2.5	0.000096	0.999999973
16	Cable, Above Ground, Trays, ≤ 600V, per 1000 ft., Gold Book p.105		0.99999831	10.5	0.001410	?
	Cable, Above Ground, Trays, ≤ 600V, per 1000 ft., Gold Book p.105			10.5	0.002820	0.999996620
22	Switchgear, Insulated Bus, ≤ 600V		0.99999953	2.4	0.001700	0.999999534
26	Bus Duct, Gold Book p. 206, per Circuit foot		0.99999982	12.9	0.000125	0.999815959

c. Step 3: Logic model development. The third step in the development of the GO model is to produce a logical representation of the one line diagram. This model will provide the functional relationship to the system. Figure 4-2 shows the resulting Boolean Algebra model. In this process you will use the Kind number identified in the parts list from table 4-2 as a unique identifier. This unique identifier is then combined with the logical operators outlined in

paragraphs 4-5 through 4-5u to create a functional model. Functional paths are developed to show the operational characteristics of the system and these paths are identified with signal inputs and outputs.

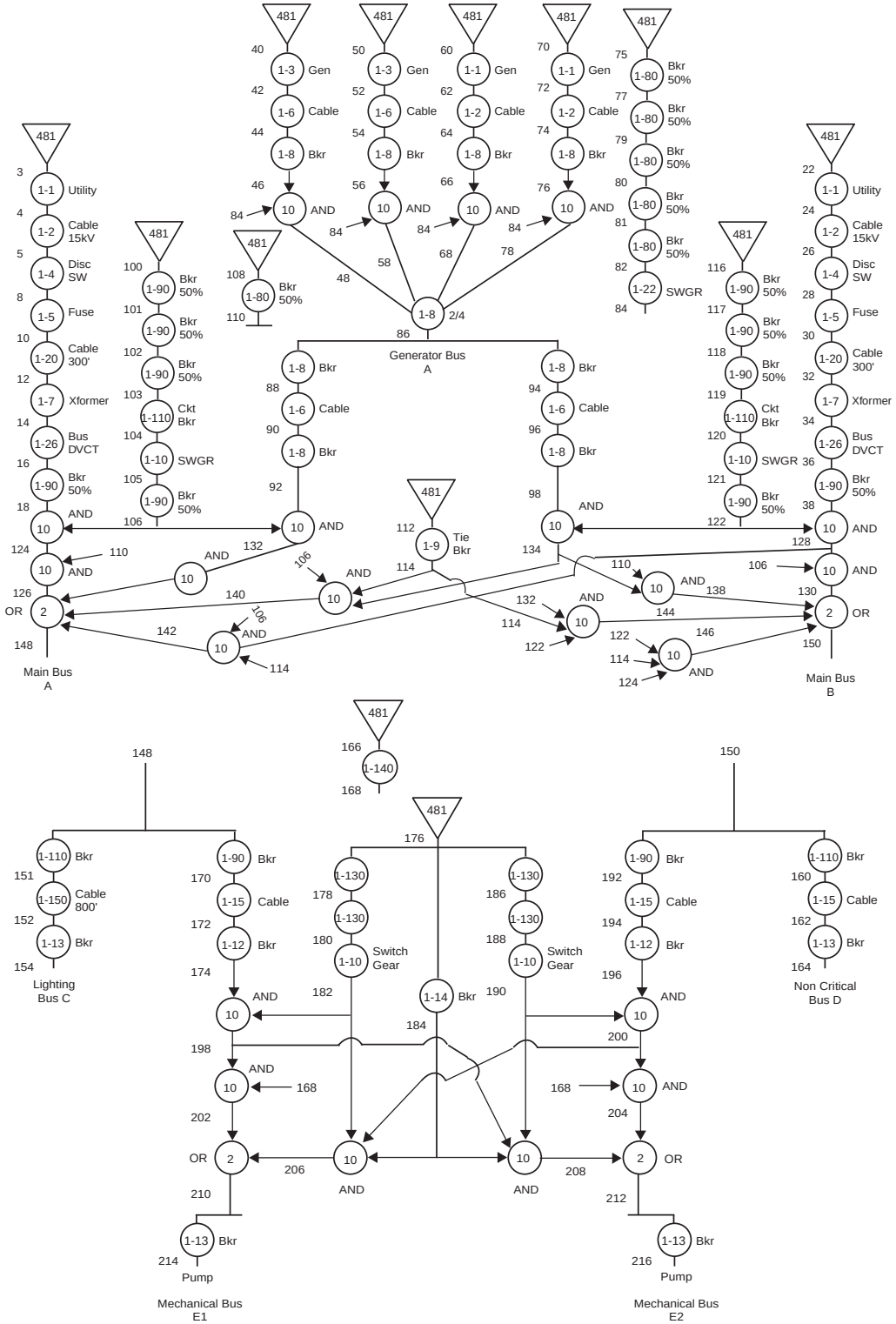


Figure 4-2. Boolean algebra diagram of the IEEE Gold Book Standard Network.

(1) Figure 4-2 illustrates the complete representation of the IEEE Gold Book Standard Network, but the following figures and description outline how the model was built. Figure 4-3 shows how the utility leg that appears on the left of figure 4-2 was created. This utility leg starts with a type 5 signal generator that is given a kind number of 481. The output signal of this perfect start is 2 which then becomes the input to the utility, modeled as a type 1 operator with a kind number of 1-1. The utility that emits a signal of 4 to the 15kV cable represented by another type 1 operator with kind number of 1-2. A 6 signal then connects the cable with a manual disconnect switch (type 1 operator, kind number 1-4) that outputs an 8 signal to a fuse (type 1 operator, kind number 1-5). Next, a 10 signal connects the fuse with another cable (type 1 operator, kind number 1-20) and emits a signal of 12 into a transformer (type 1 operator, kind number 1-7). The signal, 14, from the transformer then enters a bus duct (type 1 operator, kind number 1-26) continues as signal 16 into a circuit breaker (type 1 operator, kind number 1-9) before combination via an AND gate (type 10 operator, kind number 10) as signal 18. This path continues combining with other components of the system as it proceeds toward main bus A and beyond.

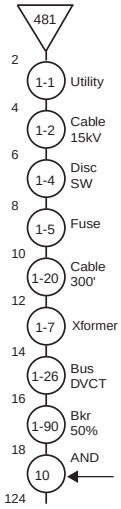


Figure 4-3. Utility 1 path to main bus A.

(2) Figure 4-4 describes the signal path at the top-center of figure 4-2 as the generators are combined via a 2 of 4 requirement. Four similar signal paths are started for each generator with perfect starts, type 5 operator with kind number of 481. The perfect starts output signals (40, 50, 60, and 70 respectively for each path) to the generators (type 1 operators, kind numbers 1-3). The generators then outputs signals (42, 52, 62, and 72 respectively) to cables (type 1 operators, kind numbers 1-6), the signal path (now as 44, 54, 64, and 74 respectively) continues into breakers (type 1 operators, kind number 1-8). At this point the signals, 46, 56, 66, and 76 are each combined via an AND gate with the switchgear and circuit breaker path of signal 84. Signal 84 is necessary to represent the capability of the breakers contributing to a bus shut down by passing the fault back to the generators. Fifty percent contribution to this failure mode of failure to open is estimated for this analysis. The AND gate output signals of 48, 58, 68, and 78 are then combined via a M out of N gate (type 11 operator, kind number 11) with the 2 of 4 requirement. The single output signal from the M out of N gate then enters the generator bus tiebreaker as signal 86, which splits to go down two different breaker paths that will create the tiebreaker effect as either side can be used to provide a signal to the components downstream. The steps identified to create the figures 4-3 and 4-4 can be used to model the remaining components and operators of the system.

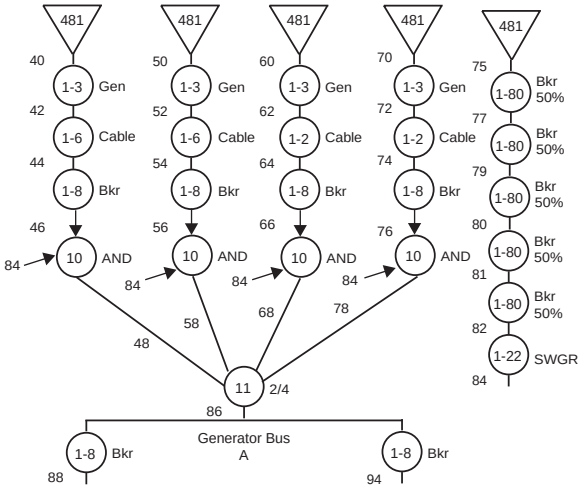


Figure 4-4. Paths to generator bus.

d. Step 4: Input file creation. The next step is to assemble the files that will be used as an input to the GO model. The GO software tool requires three main files that must be specifically configured to run in the program. These files are the model file, GO1.in file, the parts list file, GO2.in file, and the results file, GO3.in file. These files are normally created using the Notepad accessory on most computers.

(1) Utilizing the model developed in the previous step, a GO1 file is assembled based on the illustrated signal path of figure 4-2 with the identified Kind number representing the component. Operators are also inserted in the model path to represent the logical flow of operation. Table 4-3 contains the GO1 file that was developed to represent the IEEE Gold Book Standard Network. This file contains the components and operators representing the functional operation of the system. The last line of this file represents the desired output signals that an availability metric will be calculated (operator type of 0).

Table 4-3. GO1 model file

```
PREP Recommended Power Plant Model
 $param infin=1$
5 481 2                      $
1 1 2 4                      $
1 2 4 6                      $
1 4 6 8                      $
1 5 8 10                     $
1 20 10 12                   $
1 7 12 14                    $
1 26 14 16                   $
1 90 16 18                   $
5 481 22                     $
1 1 22 24                    $
1 2 24 26                    $
1 4 26 28                    $
1 5 28 30                    $
1 20 30 32                   $
1 7 32 34                    $
1 26 34 36                   $
1 90 36 38                   $
5 481 40                     $
1 3 40 42                    $
1 6 42 44                    $
1 8 44 46                    $
5 481 50                     $
1 3 50 52                    $
1 6 52 54                    $
1 8 54 56                    $
5 481 60                     $
1 3 60 62                    $
1 6 62 64                    $
1 8 64 66                    $
5 481 70                     $
1 3 70 72                    $
1 6 72 74                    $
1 8 74 76                    $
5 481 75                     $
1 80 75 77                   $
1 80 77 79                   $
1 80 79 80                   $
1 80 80 81                   $
1 80 81 82                   $
1 22 82 84                   $
10 0 2 46 84 48              $
10 0 2 56 84 58              $
10 0 2 66 84 68              $
10 0 2 76 84 78              $
11 2 4 48 58 68 78 86        $
1 8 86 88                    $
1 6 88 90                    $
1 8 90 92                    $
1 8 86 94                    $
1 6 94 96                    $
1 8 96 98                    $
```

Table 4-3. GO1 model file (continued)

```
5 481 100                    $
1 90 100 101                 $
1 90 101 102                 $
1 90 102 103                 $
1 110 103 104                $
1 10 104 105                 $
1 90 105 106                 $
5 481 108                    $
1 80 108 110                 $
5 481 112                    $
1 9 112 114                  $
5 481 116                    $
1 90 116 117                 $
1 90 117 118                 $
1 90 118 119                 $
1 110 119 120                $
1 10 120 121                 $
1 90 121 122                 $
10 0 2 18 106 124            $
10 0 2 124 110 126           $
10 0 2 38 122 128            $
10 0 2 110 128 130           $
10 0 2 92 106 132            $
10 0 2 98 122 134            $
10 0 2 110 132 136           $
10 0 2 134 110 138           $
10 0 3 134 106 114 140       $
10 0 3 128 106 114 142       $
10 0 3 132 114 122 144       $
10 0 3 114 122 124 146       $
2 0 4 126 136 140 142 148    $
2 0 4 130 138 144 146 150    $
1 110 148 151                $
1 150 151 152                $
1 13 152 154                 $
1 110 150 160                $
1 15 160 162                 $
1 13 162 164                 $
5 481 166                    $
1 140 166 168                $
1 90 148 170                 $
1 15 170 172                 $
1 12 172 174                 $
5 481 176                    $
1 130 176 178                $
1 130 178 180                $
1 10 180 182                 $
1 14 176 184                 $
1 130 176 186                $
1 130 186 188                $
1 10 188 190                 $
1 90 150 192                 $
1 15 192 194                 $
1 12 194 196                 $
10 0 2 174 182 198           $
10 0 2 190 196 200           $
10 0 2 198 168 202           $
10 0 2 168 200 204           $
10 0 3 182 184 200 206       $
10 0 3 184 190 198 208       $
2 0 2 202 206 210            $
2 0 2 204 208 212            $
1 13 210 214                 $
1 13 212 216                 $
0 18 38 126 130 148 150 128 124 210 212
86 154 164   $
```

(2) The GO2 file contains the reliability information that the GO1 file acts upon. For each Kind number defined in the GO1 file there is an availability metric representing the component's individual availability. The GO1 model assembles the individual availability information for each component with the logical operators to determine the overall system availability. Table 4-4 identifies the GO2 parts list file used to identify the individual availability data.

Table 4-4. GO2 parts list file

```
1   1     1 .999705     .000295     $Single Circuit Utility Supply, 1.78 failures/u
2   2     1 .999990218  .000009782  $Cable Aerial, <= 15kV, per mile
3   20    1 .999999443  .000000557  $Cable Aerial, <= 15kV, per mile, 300 ft.
4   3     1 .999742312  .000257688  $Diesel Engine Generator, Packaged,Stand-by, 15
5   4     1 .999999801  .000000199  $Manual Disconnect Switch
6   5     1 .999953634  .000046366  $Fuse,  15kV
7   6     1 .999997428  .000002572  $Cable Below Ground in conduit, <=600V, per 100
8   60    1 .999999228  .000000772  $Cable Below Ground in conduit, <=600V, per 100
9   7     1 .999999367  .000000633  $Transformer, Liquid, Non Forced Air, 3000kVA
10  8     1 .999998738  .000001262  $Ckt. Breaker, 600v, Drawout, Normally Open, >
11  80    1 .999999369  .000000631  $Ckt. Breaker, 600v, Drawout, Normally Open, >
12  9     1 .999999894  .000000106  $Ckt. Breaker, 600V, Drawout, Normally Closed,>
13  90    1 .999999947  .000000053  $Ckt. Breaker, 600V, Drawout, Normally Closed,>
14  10    1 .999992098  .000007902  $Switchgear, Bare Buss, 600V
15  11    1 .999999858  .000000142  $Ckt. Breaker, 600v Drawout, Normally Closed, <
16  110   1 .999999928  .000000072  $Ckt. Breaker, 600v Drawout, Normally Closed, <
17  12    1 .999989479  .000010521  $Ckt. Breaker, 600V, Normally Closed, >600 Amp,
18  120   1 .999994740  .000005260  $Ckt. Breaker, 600V, Normally Closed, >600 Amp,
19  13    1 .999996557  .000003443  $Ckt. Breaker, 3 Phase Fixed, Normally Closed,
20  130   1 .999998278  .000001722  $Ckt. Breaker, 3 Phase Fixed, Normally Closed,
21  14    1 .99998532   .00001468   $Ckt. Breaker, 3 Phase Fixed, Normally Open, >6
22  140   1 .999992658  .000007342  $Ckt. Breaker, 3 Phase Fixed, Normally Open, >6
23  15    1 .999999966  .000000034  $Cable, Above Ground, No Conduit, <= 600V, per
24  150   1 .999999973  .000000027  $Cable, Above Ground, No Conduit, <= 600V, per
25  16    1 .99999831   .00000169   $Cable, Above Ground, Trays, <= 600V, per 1000
26  160   1 .999996620  .000003380  $Cable, Above Ground, Trays, <= 600V, per 1000
27  22    1 .999999534  .000000466  $Switchgear, Insulated Buss, <=600V
28  26    1 .999815958  .000184042  $Bus Duct, Gold Book p.206, per Circuit foot, 1
29  480   1 .995000000  .005000000  $Manual Operator
30  481   5 1 0 1.0                 $Perfect Start
```

(3) The GO3 file identifies the parameters that govern the calculation of the availability results for the desired output signals. This file usually contains no data since its sole purpose is to define the results obtained from the executable files. Normally this file always contains the same information as illustrated in table 4-5.

Table 4-5. GO3 results file

```
GO-3 DATA
 $PARAM PMIN=1.e-13 $
```

e. Step 5: Performing analysis. There are three executable files that comprise the GO software, GO1.exe, GO2.exe, and GO3.exe. The first two executable files are used in conjunction with the GO1 and GO2 input files, respectively. These executable files will read the input files and develop the necessary output files leading up to the system availability analysis. The final executable file provides the system availability results when all files are executed successfully. This file contains the signal output(s) with their associated availability metric(s). Since GO is MS-DOS based program the executables and input files must be located within the same folder and the folder must be accessible while in a MS-DOS mode. The three executable files all write output text files into the folder where the input and executable files lie (output files are named "t1," "t2," and "t3" to coincide with their respective executable file). The following

example, see figure 4-5, will illustrate how an analysis is performed (in this case the executable and input files are located on the C:\ drive in a folder labeled "GO").

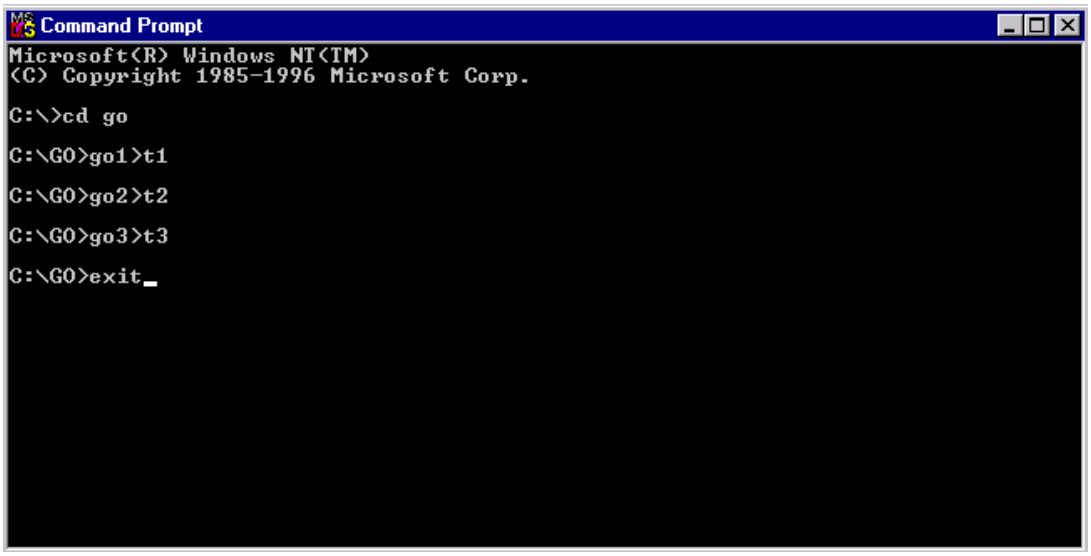


Figure 4-5. MS-DOS screen while performing analysis.

(1) Figure 4-5 was taken just prior to returning to the MS Windows environment from the MS-DOS window. As illustrated in the figure, the steps taken to run the availability analysis consist of:

- Opening folder where executable and input files exist (cd go).
- Run input model GO1 to output model t1 (go1>t1).
- Execute input model GO2 to output model t2 (go2>t2).
- Run results file, GO3, to output model t3 (go3>t3).
- Exit MS-DOS to return to MS Windows environment.

(2) The output files, t1 and t2, for the GO1 model file and GO2 parts list file contain all the information from the input files plus additional information that GO uses to analyze the system. The t1 file also includes information regarding each signal called out within the model, which is used to identify the logic of the model and determine if signals have an output, if not they are added to final signal list that was identified at end of GO1 model file. The t2 output file identifies the parts list from GO2 and identifies how many of each operator and kind type are called out in the GO1 model file.

(3) The t3 output file contains the results of the GO analysis with each output signal given an availability metric. This output file is shown in table 4-6.

Table 4-6. GO results output file

```
GO-3 DATA

OPERATOR FILE -

PREP Recommended Power Plant Model     KIND FILE ---- GO2 Input
-----------------------------------------------------------------

TOTAL PROBABILITY =  .9999999999871
TOTAL ERROR =        .0000000000129

INDIVIDUAL SIGNAL PROBABILITY DISTRIBUTIONS

VAL.        148
----   -------------
  0   .9999912359880
  1   .0000087639992

VAL.        150              210              212
----   -------------    -------------    -------------
  0   .9999912359883   .9999886527944   .9999886527944
  1   .0000087639989   .0000113471928   .0000113471928

VAL.         86              154              164
----   -------------   -------------    -------------
  0   .9999963789276   .9999876940199   .9999876870202
  1   .0000036210596   .0000123059672   .0000123129669
```

f. Step 6: Troubleshooting. Unfortunately, GO models rarely yield the desired availability results on the first attempt to perform the analysis. Therefore, analysts will need to understand the potential pitfalls associated with the GO software and the input files required to perform the analysis. Following are many of the known pitfalls associated with a GO availability analysis.

(1) All executable files (GO1.exe, GO2.exe, and GO3.exe) and GO input files (GO1.in, GO2.in, and GO3.in) must be located in the same folder and be accessible from the MS-DOS environment on the computer.

(2) The contents of the GO1 and GO2 input files must be meticulously entered to ensure model is accurately portrayed. See table 4-7.

Table 4-7. Accurately entering GO1 and GO2 files

In the case of GO1 this means making sure that the operator types, kind numbers, and signals are entered correctly. • Special attention should be given to ensure that all signals that are output signals of one component are the input signal of the next component or operator in series unless it is to be included as a final signal. • Unless using a generator operator an input signal can not be referred to unless already defined as the output signal of another operator. • A check should be made to verify that signals are not re-used in the model also. • The order of information for this file is the operator type to the far left followed by a space, then the kind number, another space, the input signal, another space, the output signal, another space, and the description beginning with a $ sign. The previous description is for type 1 Operators only, refer to paragraph 4.1 for alternative operators. • The maximum number of final signals that can be analyzed are 16. • The signal number can not exceed 8999.
GO2 requires a standard format with the following guidelines. • The kind numbers line up on the far left with a certain number of spaces between the kind number and operator type (6 for single digit kind numbers, 5 for double digits, etc.), then one space to 9 decimal availability values for kind numbers followed by two spaces and 9 decimal unavailability values, and finally two spaces until the description portion that begins with a $ sign. The previous description is for type 1 Operators only, refer to paragraph 4.1 for alternative operators. • The availability and unavailability metric can not start with a 0 prior to the decimal. • These availability and unavailability metrics must add up to 1.000000000.

(3) If a problem arises during the analysis usually an error message will occur following the step that is being completed. Table 4-8 lists these error messages.

Table 4-8. Analysis error messages

Run-time error F6501: READ(OPGO1.XXX)," followed by "- end of file encountered," on the next line for errors within the GO1 input file as the GO1 executable is being run to t1 file. Run-time error F6600: WRITE(internal)," followed by "- internal file overflow," on the next line for errors within the GO2 input file.

(4) The best means of identifying a problem is to examine the output files, t1, t2, and t3. First examine the output file corresponding to the last step that was being performed when the error appeared and work back through other files (i.e. if GO2.exe encountered an error examine t2 then t1 files). If the corresponding executable ran successfully there will be a note at the bottom of the output file stating "GO# FINISHED" (the # corresponds to the output file being examined). If an error occurred it will state "SUICIDE BECAUSE OF ERRORS," followed by "FATAL ERROR: …..SUICIDE….," two lines later and the error messages shown in table 4-9 will commonly be found within the output files.

Table 4-9. Error messages

"**** SIGNAL X REUSED," followed by "------ERROR------" in the next line of the t1 file, this message reflects the identification of a signal number as an output signal for more than one area of the model.
"**** INPUT SIGNAL X HAS NOT BEEN ENTERED," followed by "------ERROR------" in the next line, this error message appears in the t1 file. This message identifies that an input signal was called out in the model even though it has not been previously modeled as an output signal for another component within the model.
"**** THERE ARE TOO MANY FINAL SIGNALS," appears in the t1 file as signals not used as inputs to other operators are added to final signal list. This message is yielded when more than 16 final signals are identified (either within the last line of GO1 input file or by GO software when GO1 file is executed and all end signals become final signals).
"**** PROBABILITY SUM IS X," within the t2 file signifies that the reliability/unreliability or availability/unavailability numeric combinations specified for an operator does not add up to 1.

APPENDIX A

REFERENCES

REQUIRED PUBLICATIONS

Non-Government

Institute of Electrical and Electronics Engineers
445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, www.ieee.org

"Operational Maintenance Data for Power Generation Distribution and HVAC Components," IEEE Transactions on Industry Applications, March/April 1999 (cited in paragraph 4-5b).

"Survey of Reliability and Availability Information for Power Distribution, Power Generation, and HVAC Components for Commercial, Industrial, and Utility Installations," IEEE Transactions on Industry Applications, January/February 2001 (cited in paragraph 4-5b).

Coyle, Timothy, Arno, Robert G., and Hale, Peyton S., "GO Reliability Methodology Applied to Gold Book Standard Network," IEEE Transactions on Reliability, IEEE, 2002 [cited in paragraphs 4-5b, 4-5c, 4-6a, figure 4-1, 4-6b(1), 4-6b(2), 4-6c(1), table 4-2, 4-6d(1), and table 4-3].

RELATED PUBLICATIONS

Government Publications

MIL-HDBK-189
Reliability Growth Management

MIL-HDBK-781
Reliability Test Methods, Plans and Environments for Engineering Development, Qualification & Production

Non-Government Publications

Abernethy, Dr. R.B., "The New Weibull Handbook," Gulf Publishing Co., Houston, TX, 1994.

AIAG MFMEA-1 (Automotive Industry Action Group, Machinery Failure Mode & Effects Analysis), www.aiag.com, Potential Failure Mode & Effects Analysis for Tooling & Equipment.

Blanchard, Benjamin S. and Wolter J. Fabrycky, Systems Engineering and Analysis, Prentice-Hall, Inc., January 1998.

Burkhard, Alan H., "Deterministic Failure Prediction," 1987 Proceedings Annual Reliability and Maintainability Symposium, IEEE, 1987.

Carter, A.D.S., Mechanical Reliability , John Wiley & Sons, 1986.

IEC Electronics Corporation, www.iec-electronics.com, IEC 60300-1, Dependability Programme Management - Part 1: Dependability Programme Management.IEC 60300-2, Dependability Management - Part 2: Dependability Programme Elements and Tasks and IEC 60300, Part 3-11, "Dependability Management – Part 3: Application Guide – Section 11: Reliability Centered Maintenance.

Institute of Electrical and Electronics Engineers
445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, www.ieee.org

ANSI/IEEE 762 - Standard Definitions for Use in Reporting Electric Generating Unit Reliability, Availability, and Productivity.

Heidtmann, Klaus D., "Deterministic Reliability-Modeling of Dynamic Redundancy," IEEE Transactions on Reliability, Volume 41, Number 3, IEEE, September 1992.

Ireson, W.G., Handbook of Reliability Engineering and Management, McGraw-Hill, 1988.

Kapur, K.C. and L.R. Lamberson, Reliability in Engineering Design, John Wiley & Sons, 1977.

Kececioglu, D, Reliability Engineering Handbook, 2 Vols., Prentice-Hall, 1991.

Moubray, John, Reliability-Centered Maintenance II, Industrial Press, New York, NY, April 1997.

NASA, National Aeronautics and Space Administration, www.nasa.gov

National Aeronautics and Space Administration, "Reliability Centered Maintenance Guide for Facilities and Collateral Equipment," December 1996.

Nelson, Dr. Wayne, Accelerated Testing; Statistical Models, Test Plans and Data Analysis, John Wiley & Sons, 1990.

Nowlan, F.S. and H.F. Heap, "Reliability-Centered Maintenance," DoD, 1978, available from Maintenance Quality Systems, LLC, 1127-F Benfield Blvd, Suite F, Millersville, MD 21108-2540, www.mqsllc.com.

O'Connor, P.D.T., Practical Reliability Engineering, John Wiley & Sons.

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

Reliability Analysis Center, 201 Mill Street Rome, NY 13440, www.rac.iitri.org.

Reliability Analysis Center, Fault Tree Application Guide, 1990.

Reliability Analysis Center, Failure Modes Effects and Criticality Analysis, 1993.

Reliability Analysis Center, Reliability Toolkit: Commercial Practices Editions, 1994

Smith, Anthony M., Reliability-Centered Maintenance, McGraw Hill, New York, NY, September1992

Society of Automotive Engineers, 755 W. Big Beaver, Suite 1600, Troy, MI 48084, www.sae.org.

SAE JA1000: Reliability Program Standard.

SAE JA1000/1: Reliability Program Standard Implementation Guide.

Society of Automotive Engineers, "Evaluation Criteria for Reliability-Centered Maintenance (RCM) Processes," JA1011, August 1999.

Society of Automotive Engineers, "A Guide to the Reliability-Centered Maintenance (RCM) Standard," JA1012, Draft, June 2000.

Talmor, Michael, and Arueti, Shimshon, "Reliability Prediction: The Turnover Point," 1997 Proceedings Annual Reliability and Maintainability Symposium, IEEE, 1997.

Wang, Wendai, and Kececioglu, Dimitri B., "Confidence Limits on the Inherent Availability of Equipment," 2000 Proceedings Annual reliability and Maintainability Symposium, IEEE, 2000.

Wadsworth, H.M., Handbook of Statistical Methods for Engineers and Scientists, McGraw Hill, 1989.

APPENDIX B

THE MATHEMATICS OF RELIABILITY

B-1. Introduction to the mathematics of reliability

This appendix provides the reader with an overview of the mathematics of reliability theory. It is not presented as a complete (or mathematically rigorous) discussion of probability theory but should give the reader a reasonable understanding of how reliability is calculated. Before beginning the discussion, a key point must be made. Reliability is a design characteristic indicating a product's ability to perform its mission over time without failure or to operate without logistics support. In the first case, a failure can be defined as any incident that prevents the mission from being accomplished; in the second case, a failure is any incident requiring unscheduled maintenance. Reliability is achieved through sound design, the proper application of parts, and an understanding of failure mechanisms. **It is not achieved by estimating it or calculating it**. Estimation and calculation are, however, necessary to help determine feasibility, assess progress, and provide failure probabilities and frequencies to spares calculations and other analyses. With that in mind, let's first look at the theory of probability.

B-2. Uncertainty - at the heart of probability

The mathematics of reliability is based on probability theory. Probability theory, in turn, deals with uncertainty. Probability had its origins in gambling. Some gamblers, hoping to improve their luck, turned to mathematicians with questions like what are the odds against rolling a six on a die, of drawing a deuce from a deck of 52 cards, or of having a tossed coin come up heads. In each case, probability can be thought of as the relative frequency with which an event will occur *in the long run*. When we assert that tossing an honest coin will result in heads (or tails) 50% of the time, we do not mean that we will necessarily toss five heads in 10 trials. We only mean that in the long run, we would expect to see 50% heads and 50% tails. Another way to look at this example is to imagine a very large number of coins being tossed simultaneously; again, we would expect 50% heads and 50% tails.

a. Events. Why is there a 50% chance of tossing a head on a given toss of a coin? It is because there are two results, or events, that can occur (assume that it is very unlikely for the coin to land on its edge) and for a balanced, honest coin, there is no reason for either event to be favored. Thus, we say the outcome is random and each event is equally likely to occur. Hence, the probability of tossing a head (or tail) is the probability one of two equally probable events occurring = 1/2 = 0.5. Now consider a die. One of six equally probable events can result from rolling a die: we can roll a one, two, three, four, five, or six. The result of any roll of a die (or of a toss of a coin) is called a discrete random variable. The probability that on any roll this random variable will assume a certain value, call it x, can be written as a function, f(x). We refer to the probabilities f(x), specified for all values of x, as values of the probability function of x. For the die and coin, the function is constant. For the coin, the function is $f(x) = 0.5$, where x is either a head or tail. For the die, $f(x) = 1/6$, where x can be any of the six values on a die.

b. Probability functions. All random events have either an underlying probability function (for discrete random variables) or an underlying probability density function (for a continuous random variable). The results of a toss of a coin or roll of a die are discrete random variables because only a finite number of outcomes are possible; hence these events have an underlying probability function. The possible height of a male American is infinite (between 5' - 8" and 6', for example, there are an infinite number of heights) and is an example of a continuous random variable. The familiar bell-shaped curve describes most natural events, such as the height of a man, intelligence quotient, errors of measurement,

etc. The underlying probability density function represented by the bell-shaped curve is called normal or Gaussian. Figure B-1 shows a typical normal distribution.

c. Mean value. Note that the event corresponding to the midpoint of the curve is called the mean value. The mean value, also called the expected value, is an important property of a distribution. It is similar to an average and can be compared with the center of mass of an object. For the normal distribution, half the events lie below the mean value and half above. Thus, if the mean height of a sample of 100 male Americans is 5' -9", half the sample will be less than 69" inches tall and half will be taller. We would also expect that most men will be close to the average with only a few at the extremes (very short or very tall). In other words, the probability of a certain height decreases at each extreme and is "weighted" toward the center; hence, the shape of the curve for the normal distribution is bell-shaped.

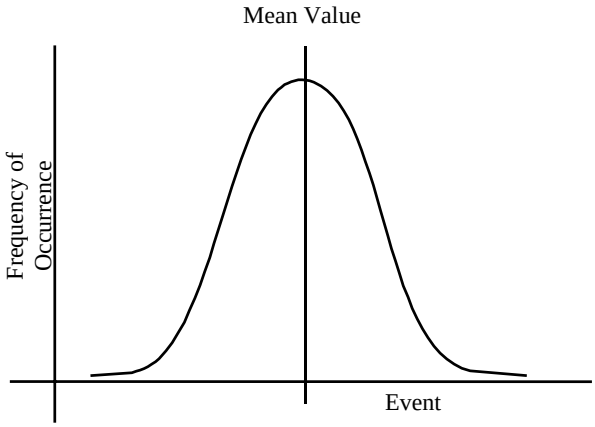


Figure B-1. Typical normal distribution curve.

d. Range of values of probability. The probability of an event can be absolutely certain (the probability of tossing either a head or a tail with an honest coin), absolutely impossible (the probability of throwing a seven with one die), or somewhere in between. Thus, a probability always can be described with equation B-1.

$$0 \leq \text{Probability} \leq 1 \qquad \text{(Equation B-1)}$$

B-3. Probability and reliability

Just as probability is associated with gambling events and naturally occurring phenomena (e.g., height of humans), it is associated with the times to failure. Since there can be an infinite number of points on a time line, time is a continuous random variable and probability density functions are used.

a. Use of the exponential distribution in reliability. Often, the underlying statistical distribution of the time to failure is assumed to be exponential. This distribution has a constant mean, λ. A reason for the popularity of the exponential distribution is that a constant failure rate is mathematically more tractable than a varying failure rate.

(1) Equation B-2 is the typical equation for reliability, assuming that the underlying failure distribution is exponential.

$$R(t) = e^{-\lambda t} \qquad \text{(Equation B-2)}$$

where:

λ is the failure rate (inverse of MTBF)
t is the length of time the product must function
e is the base of natural logarithms
R(t) is reliability over time *t*

(2) Figure B-2 shows the curve of equation B-2. The mean is not the "50-50" point, as was true for the normal distribution. Instead, it is approximately the 37-63 point. In other words, if the mean time to failure of an item is 100 hours, we expect only 37%* of the population of equipment to still be operating after 100 hours of operation. Put another way, when the time of operation equals the mean, the reliability is 37%.

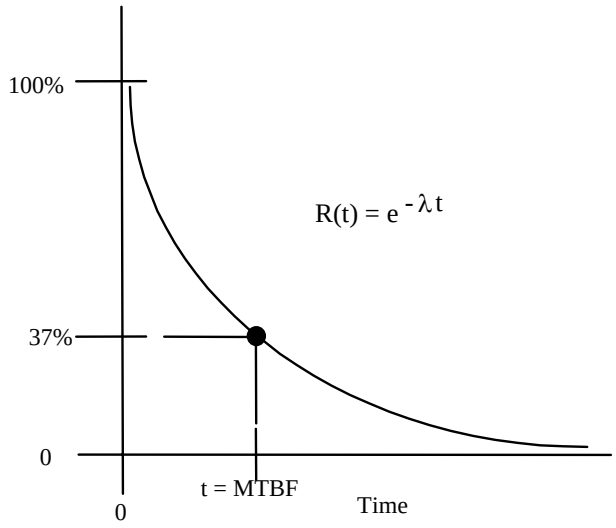


Figure B-2. Exponential curve relating reliability and time.

b. Other probability density functions used in reliability. As already stated, the popularity of the exponential distribution is its simplicity and ease of use. Unfortunately, the exponential does not accurately describe the time to failure for many parts (items that fail once and are not usually repaired, such as resistors, bearings, belts and hoses, seals, etc.). Since the failure rate, λ, is a constant, it implies that the probability of failure for a new part is the same as for an old part. But we know that many parts wear out with use or as they age. Obviously, the probability of failure increases with age for these parts. Accordingly, many other probability distributions are used to describe the time to failure of parts. The most versatile of these is the Weibull.

(1) The Weibull distribution is defined by equations B-3 and B-4 (equation B-3 is for the two-parameter Weibull and equation B-4 is for the three-parameter Weibull).

$$F(t) = 1 - e^{-(t/\theta)^{\beta}} \qquad \text{(Equation B-3)}$$

$$F(t) = 1 - e^{-[(t-t_0)/\theta]^{\beta}} \qquad \text{(Equation B-4)}$$

* If $t = MTBF = 1/\lambda$, then $e^{-\lambda t} = e^{-1} = 0.367879$.

(2) The Weibull distribution can provide accurate estimates of reliability with few samples, renders simple and useful graphical results, provide clues to physics of failure, and can represent many distributions. When β is equal to 1, the Weibull is exactly equal to the exponential distribution. When, β is 3.44, the Weibull is approximately the normal distribution.

c. Applicability of the exponential to systems. Although the exponential is often inappropriate for parts (i.e., items that fail once and are discarded), it is often applicable to systems. The reason is that systems are made of many parts, each with different failure characteristics. As parts fail, they are replaced. After some time, the system has parts of varying "ages". The net result is that the times between failures of the system are exponentially distributed. This behavior of system is described by Drenick's Theorem.

B-4. Failure rate data

How do we determine the failure rate of a specific product or component? Two methods are used.

a. Method 1 - Comparable product. In the first method, we use failure rate data for a comparable product(s) already in use. This method has two underlying assumptions. First, the product in use is comparable to the new product. Second, the principle of transferability applies. The principle of transferability states that (failure rate) data from one product can be used to predict the reliability of a comparable product.

b. Method 2 – Testing. The other method of determining failure rate data is through testing of the product or its components. Although, theoretically, this method should be the "best" one, it has two disadvantages. First, predictions are needed long before prototypes or pre-production versions of the product are available for testing. Second, the reliability of some components is so high that the cost of testing to measure the reliability in a statistically valid manner would be prohibitive. Usually, failure rate data from comparable products are used in the early development phases of a new product and supplemented with test data when available.

B-5. Calculating reliability

If the time, t, over which a product must operate and its failure rate, λ, are known, then the reliability of the product can be calculated using equation B-2. If the information is known for individual subsystems or components, then the reliability of each can be calculated and the results used to calculate the reliability of the product. For example, consider the product represented by the reliability block diagram (RBD) in figure B-3.

a. Series calculation. Components A, B, and C are said to be in series, which means all three must operate for the product to operate. Since the components are in series, we could find the reliability of each component using equation B-2 and multiply them as follows: 0.9900 x 0.9851 x 0.9925 = 0.9680. Alternatively, the product reliability can be found by simply adding together the failure rates of the components and substituting the result in equation B-4. The product failure rate is 0.001000 + 0.001500 + 0.000750 = 0.003250. The reliability is:

$$R(t) = e^{-0.003250 \times 10} = 0.9680$$

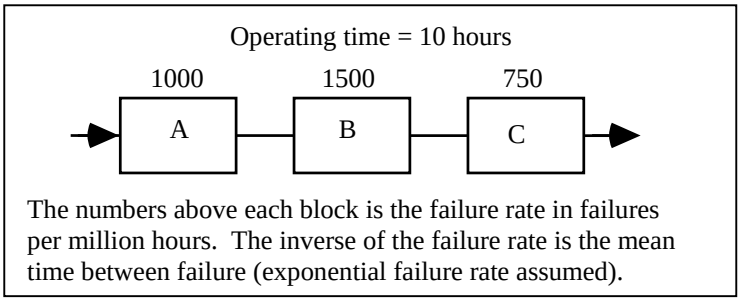


Figure B-3. Example reliability block diagram.

b. Redundancy. Now consider the RBD shown in figure B-4. The system represented by the RBD in figure B-4 has two components marked B, in a configuration referred to as redundant or parallel. Two paths of operation are possible. The paths are: A, top B, and C; and A, bottom B, and C. If either of two paths is intact, the product can operate.

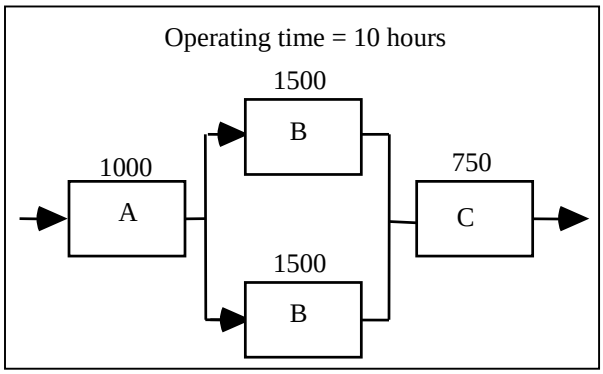


Figure B-4. RBD of a system with redundant components.

(1) The reliability of the product is most easily calculated by finding the probability of failure (1-R(t)) for each path, multiplying the probabilities of failure (which gives the probability of both paths failing), and then subtracting the result from 1. The reliability of each path was found in the previous example. Next, the probability of a path failing is found by subtracting its reliability from 1. Thus, the probability of either path failing is 1 - 0.9680 = 0.0320. The probability that both paths will fail is 0.032 x 0.032 = 0.001. Finally, the reliability of the product is 1 - 0.001 = 0.9989, about a 3.2% improvement over the series-configured product.

(2) Two components in parallel (redundant) may always be on and in operation (active redundancy) or one may be off or not in the "circuit" (standby redundancy). In the latter case, failure of the primary component must be sensed and the standby component turned on or switched into the circuit. Standby redundancy may be necessary to avoid interference between the redundant components and, if the redundant component is normally off, reduces the time over which the redundant component will be used (it's only used from the time when the primary component fails to the end of the mission). Of course, more than two components can be in parallel.

B-6. Calculating basic versus functional reliability

Reliability can be viewed from two perspectives: the effect on system performance and the effect on logistics costs.

a. Functional reliability. In the previous examples, we have seen how adding a component in parallel, i.e., redundancy, improves the system's ability to perform its function. This aspect of reliability is called functional reliability.

b. Basic reliability. Note that in figure B-4, we have added another component that has its own failure rate. If we want to calculate the total failure rate for all components, we add them. The result is 4750 failures per million operating hours (0.004750). The failure rate for the series-configured product in figure B-3 was 3,250 failures per million operating hours. Although the functional reliability of the system improved, the total failure rate for all components **increased**. This perspective of reliability is called basic or logistics reliability. Whereas functional reliability only considers failures of the function(s), logistics reliability considers all failures *because some maintenance action will be required*. Logistics reliability can be considered as either the lack of demand placed on the logistics system by failures or the ability to operate without logistics. If standby redundancy is used with the redundant component not on, the apparent failure rate of that component will be less than that of its counterpart (because the probability it will be used is less than 1 and the time it will operate less than 10 hours), but the failure rate of the switching circuits must now be considered. The logistics reliability for the system with active redundancy in figure B-4 is 0.9536 over a ten-hour period.

APPENDIX C

POINT ESTIMATES AND CONFIDENCE BOUNDS

C-1. Introduction to point estimates and confidence bounds

Predicting reliability and maintainability is necessary because both characteristics are very difficult to measure, especially early in a development program. Some experts even deny that they can be measured at all. Without going into the philosophical and mathematical theories on which these experts base this denial, suffice it to say that predictions continue to be used in most every product development program.

a. What is a prediction? Mathematically speaking, predictions are *estimates* of the true values of the parameters of any probability distribution. R&M, at least in part, are probability concepts. Reliability can be stated as the probability that a product will operate successfully under given conditions. Maintainability can be stated as the probability of completing a repair within a certain time under given conditions. If we observed the results of operating an entire population of a product in a given year, we could divide the number of failures by total attempted operations and determine the reliability of the product in that year *after the fact*. This "measurement" is not made to try and tell us what will happen next year or what would have happened in the year in question had only half the products been operated - it is not a prediction. Probability, on the other hand, is that branch of mathematics that allows statements to be made about a population based only on a sample of the population or when we try to predict *before the fact* the outcome of events. These predictions are estimations of the "truth."

b. Types of estimates. Two kinds of estimation can be made: point estimates and interval estimates.

(1) *Point estimates*. A point estimate is, as implied by the title, a single number that is an estimate of the distribution parameter in which we are interested. For example, on the basis of analysis or test, we might estimate the reliability to be 95%. How much confidence do we have in the estimate? It depends on the information used to make the estimate. If we used only analytical methods of arriving at the estimate (i.e., no actual testing performed), it would depend on how much the new product resembled the old product(s) from which the data used in the analysis were derived. If we had one test that was the basis for the estimate, we could be 50% sure that the true reliability is higher or lower than our estimate. Finally, if we test 100 products (out a larger total population), it seems intuitive that we could be more confident in our estimate than when we tested only one product.

(a) As our sample size increases, we can make estimates in which we can have a higher confidence. Unfortunately, the subject of confidence is a bit more complex than that. For example, take the case where we have a sample of 100 products to test. Suppose that 10 failures occur. We could estimate the reliability to be 10/100 or 90%. We could also estimate it as 85% or 75%. How can that be? Well, the 90% figure is a point estimate in which we can be 50% confident. If we want to be more confident, say 95% confident that the true value is equal to or higher than the estimate, *our estimate must be more conservative*.

(b) The reader might wonder what is wrong with just using a point estimate. Nothing is "wrong" with using a point estimate. But a point estimate isn't discriminating; it tells us nothing about the risk involved with the estimate. And there is always the risk that our estimate of reliability is optimistic, i.e., too high (customers don't care, at least in theory, if it's too low, i.e., conservative). Consider the example estimates in table C-1. From the table, one can understand why a point estimate is not discriminating! Most people would more readily accept the point estimate made using 1000 products than that made with only 10.

Table C-1. Point estimates for different sample sizes

Size of Sample (or number of tests)	Number of Failures	Point Estimate of Reliability
10	1	90%
100	10	90%
1000	100	90%

(2) *Interval estimates*. An interval estimate is one in which we calculate a range of values and can state the probability of the true value of the parameter being estimated being contained in the interval. The lower and upper values of the interval are called lower and upper confidence limits, respectively. The confidence level is the probability that the range or interval of values actually includes the true value of reliability. A confidence bound can be two-sided or one-sided. A two-sided bound can be compared to a tolerance. Most of us are familiar with a measurement that is stated, for example, as 12 feet ± 0.01 feet. A two-sided bound on a reliability estimate of 95% might be ±2.1%, at 95 confidence. In other words, we are 95% confident that the interval of 92.9% to 97.1% includes the true reliability. We may, however, only be interested in the lower limit. A one-sided confidence bound would be stated as, for example, "we are 95% confident that the true reliability is greater than 90%." In this case, we are not worried about how much higher it may be. If we are trying to determine if a contractor has met (or exceeded) the reliability requirement, the one-sided confidence bound is sufficient. If we want to plan a spares buy based on the reliability of the product, the two-sided bound should be used.

c. Estimation and confidence are topics filling entire chapters of textbooks. The discussion herein is necessarily simplified and abbreviated. For a more rigorous and mathematically accurate treatment of estimation and confidence, the reader is directed to "Practical Statistical Analysis for the Reliability Engineer (SOAR-2)," The Reliability Analysis Center, Kieron A. Dey, 1983. (Available from the Reliability Analysis Center: 1-800-526-4802), or "Methods for Statistical Analysis of Reliability and Life Test Data," Nancy R. Mann, Ray E. Schafer, and Nozer D. Singpurwalla, John Wiley and Sons, Inc., Somerset, NJ, 1974, or any good text on probability and statistics.

APPENDIX D

FACTORS INFLUENCING FIELD MEASURES OF RELIABILITY

D-1. Design reliability versus field reliability

The reliability achieved by diligent attention to failure modes and mechanisms during design and manufacture is defined as design reliability. The reliability actually observed during operation of the system in its intended environment is defined as field reliability.

a. Design reliability. Design reliability is by definition the level of reliability inherent in the system as designed and manufactured. All failures are due to inherent weaknesses in the design, flaws in the materials, or defects from the manufacturing processes. The level of design reliability achieved is determined through analysis and test. Although in applying analytical methods and in testing the system (the "actual" system or prototypes), the design and development team attempts to simulate the actual operating environment, it is difficult if not impossible to account for some aspects of operation.

b. Field reliability. Field reliability is the measure a customer or user of a system uses. Whenever a system fails to perform its function(s) or requires maintenance, the customer will count such events as failures, regardless of the cause. Inherent weaknesses in the design, flaws in the materials, and defects from the manufacturing processes will cause such failures, but so will maintenance errors, improper operation, and changes in operating concept. In addition, if the operating environment is substantively different from that defined during design, more failures or failure modes may occur than were addressed during design and manufacturing. Consequently, field reliability can never be higher than design reliability and is usually lower.

D-2. Accounting for the differences

We can account for the differences between design and field reliability. We can do so in two ways: the way we design and develop procedures, and the way in which we develop design requirements.

a. Design and procedure. Recognizing that humans make mistakes, we can apply design techniques that minimize the chance of human error. For example, we can design mating parts to mate in only one way, preventing maintenance personnel from making an incorrect connection. We can design displays that are easy to read and use conventional symbols. We can design controls using standard orientation (e.g., turn right to shut off a valve). In a similar manner, we can write procedures that are clear, concise, and logical. Such attention to the human element during design can minimize the opportunity for human error.

b. Design requirements. If the customer needs a field reliability of 1000 hours Mean Time Between Failures (MTBF) for a system, we cannot use 1000 hours as our design requirement. If we did so, and missed one failure mode due to our inexact understanding of the operating environment, we would not meet the field reliability requirement. We must, therefore, design to a higher level. Of course, we should not set an arbitrarily high design reliability requirement. To do so would drive up costs unnecessarily. A commonly used approach for setting the design reliability requirement is to use past experience. If experience with previous systems indicates

that the field reliability runs 10%-15% lower than what was measured during design and manufacture, then, as a rule of thumb, the design reliability requirement for new systems should be 12% higher than the field reliability requirement. For example, if the design reliability for past systems was 1,000 hours MTBF and the observed field reliability was only 850 hours (15% less), and the field reliability requirement for a new system is 1,000 hours, the design reliability requirement must be about 11.8% higher or 1,180 hours. If we achieve this level of design reliability, then we can expect our filed reliability to be 1180 - (15% x 1180) = 1,003 hours.

APPENDIX E

REDUNDANCY AS A DESIGN TECHNIQUE

E-1. Introduction to redundancy as a design technique

Redundancy can be defined as the existence of more than one means for accomplishing a given task. In general, all means must fail before there is a system failure. In chapter 2, we calculated the reliability of a redundant system. We will now provide a more detailed explanation of the calculations involved.

a. Simple parallel system. Consider the system with two parallel elements shown in figure E-1, with A having a reliability R_A and B having a reliability R_B. Define the probability of no failure as p and the probability of failure as q. Then $p + q = 1$ and the probability of system failure, Q, would be $q_A\ q_B$. (figure E-2 summarizes the characteristics of simple parallel active redundancy.)

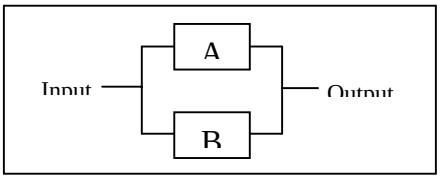


Figure E-1. Simple parallel network.

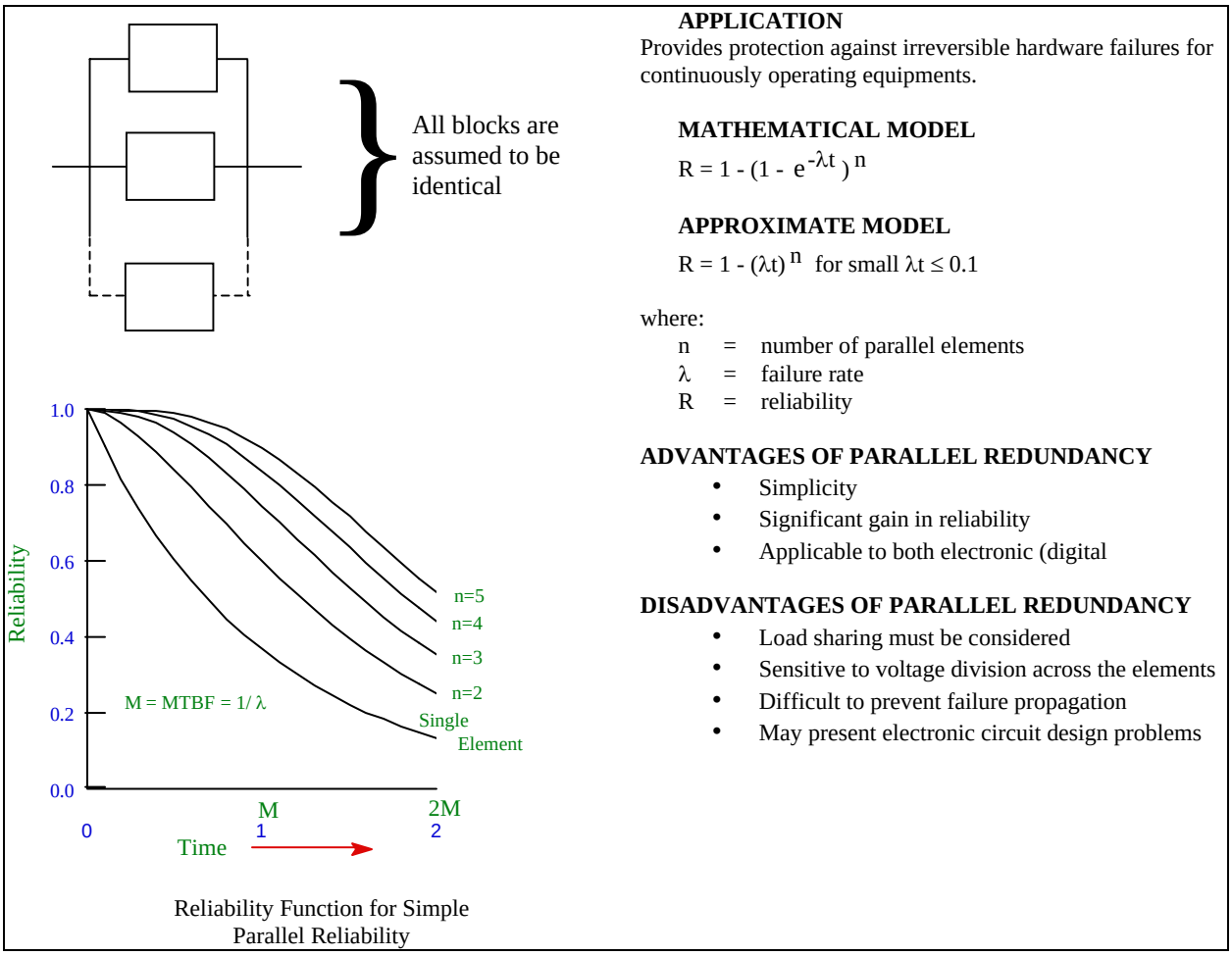


Figure E-2. Summary of simple parallel redundancy.

(1) Since reliability + unreliability = 1, the reliability, or probability of no failure, is given by $R = 1 - Q = 1 - q_A\, q_B$.

(2) If A has a reliability of 0.9 and B a reliability of 0.8, their unreliabilities q_A and q_B would be $q_A = 1 - 0.9 = 0.1$ and $q_B = 1 - 0.8 = 0.2$ and the probability of system failure would be $Q = (0.1)(0.2) = 0.02$. Hence the system reliability would be $R = 1 - Q = 0.98$, which is a higher reliability than either of the elements acting singly. Again, it should be pointed out that while redundancy reduces mission failures, it increases logistics failures.

(3) In general, with n elements in parallel, the overall probability of failure at time t is $Q(t) = q_1(t) \cdot q_2(t) \cdot \ldots \cdot q_n(t)$ and the probability of operating without failure is given by $R(t) = 1 - Q(t) = 1 - q_1(t) \cdot q_2(t) \cdot \ldots \cdot q_n(t)$. Because $q_i(t) = 1 - R_i(t)$ for each component, the latter equation can also be given as

$$R_{System}(t) = 1 - [\,1 - R_1(t)]\,[\,1 - R_2(t)] \ldots [\,1 - R_n(t)]$$

(4) When each of the component reliabilities is equal, the previous equations reduce to

$$Q(t) = [q(t)]^n$$

$$R_{System}(t) = 1 - [q(t)]^n = 1 - [1 - R(t)]^n$$

b. Interactions. So far it has been assumed that parallel components do not interact and that they are active all the time (or they may be activated when required by ideal failure sensing and switching devices). Needless to say, the latter assumption, in particular, is difficult to meet in practice. Therefore, the potential benefits of redundancy cannot be realized fully.

c. Basic formulas. Most cases of redundancy encountered will consist of various groupings of series and parallel elements. Figure E-3 typifies such system. The basic formulas previously given previously and in chapter 2 can be used to solve the overall system reliability R_S as equal to 0.938.

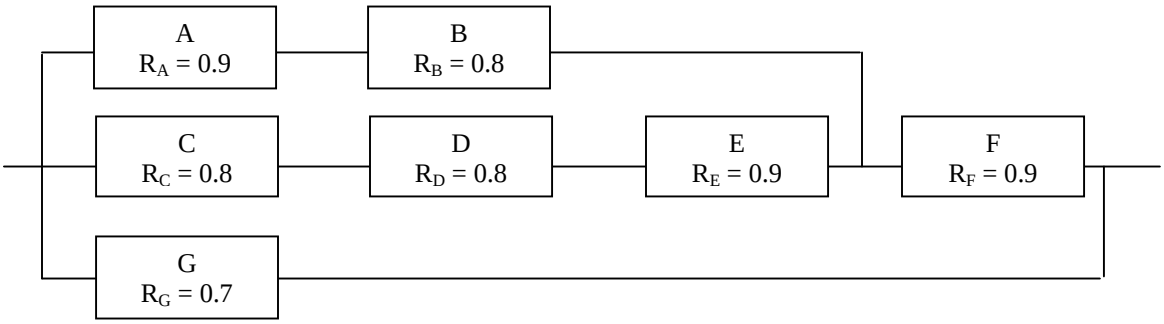


Figure E-3. Series-parallel redundancy system.

d. Levels of redundancy. Redundancy may be applied at the system level (essentially two systems in parallel) or at the subsystem, component, or part level within a system. Figure E-4 is a simplified reliability block diagram drawn to illustrate the several levels at which redundancy can be applied. System I is shown with its redundant alternative II, at the system level. II is in turn built up of redundant subsystems or components (B and C) and redundant parts within subsystems (b_1 and b_2 within subsystem B). From the reliability block diagram and a definition of block or system success, the paths that result in successful system operation can be determined. For example, the possible paths from input to output are [A, a, b_1, C_1], [A, a, b_1, C_2], [A, a, b_2, C_1], [A, a, b_2, C_2], and [I]. The success of each path may be computed by determining an assignable reliability value for each term and applying the multiplicative theorem. The computation of system success (all paths combined) requires a knowledge of the type of redundancy to be used in each case and an estimate of individual element reliability (or unreliability).

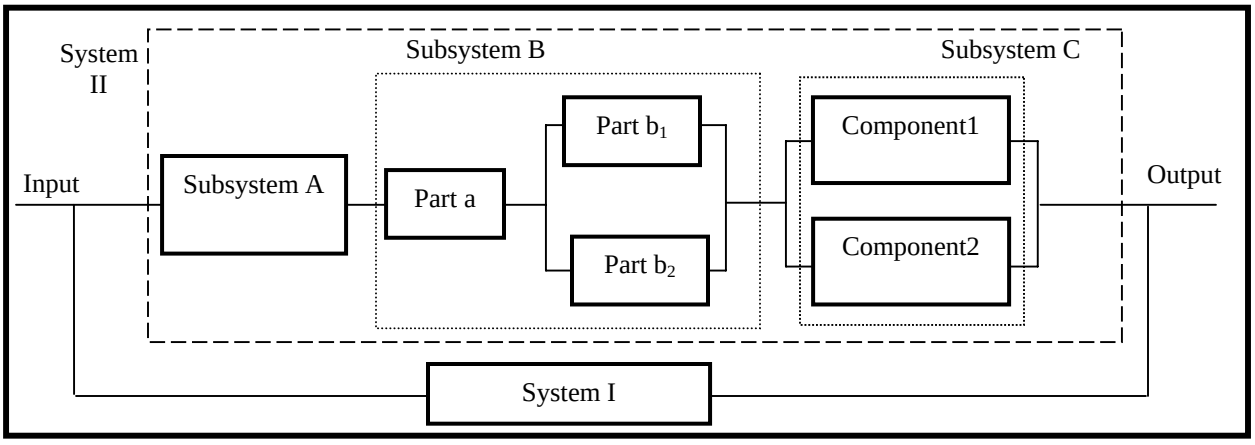


Figure E-4. Reliability block diagram depicting redundancy at the system, subsystem, component, and part levels.

e. Probability notation for redundancy computations. Reliability of redundancy combinations is expressed in probabilistic terms of success or failure -- for a given mission period, a given number of operating cycles, or a given number of time independent "events," as appropriate. The "MTBF" measure of reliability is not readily usable because of the non-exponential nature of the reliability function produced by redundancy. Reliability of redundancy combinations that are "time dependent" is therefore computed at a discrete point in time, as a probability of success for this discrete time period. The notation shown in figure E-5 is applicable to all cases and is used throughout this section.

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

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

p = probability of success or reliability of an element

q = probability of failure or unreliability of an element

For probability statements concerning an event:

P(A) = probability that A occurs

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

For the probabilities:

$R + Q = 1$

$p + q = 1$

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

Figure E-5. Probability notation for redundancy computations.

f. Redundancy combinations. The method of handling redundancy combinations can be generalized as follows.

(1) Parallel elements, series units. If the elements are in parallel and the units in series (figure E-6), first evaluate the redundant elements to get the unit reliability. Then find the product of all unit reliabilities to obtain the block reliability. In the redundancy combination shown in figure E-6, Unit A has

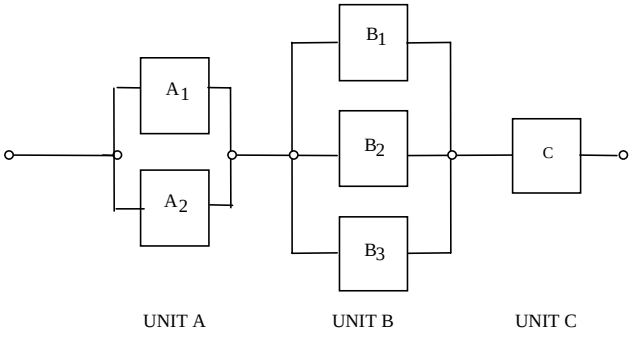


Figure E-6. Series-parallel configuration.

two parallel redundant elements, Unit B has three parallel redundant elements, and Unit C has only one element. Assume that all elements are independent. For Unit A to be successful, A_1 or A_2 must operate; for Unit B success, B_1, B_2 or B_3 must operate; and C must always be operating for block success. Translated into probability terms, the reliability of figure F-6 becomes:

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

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

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

where:

$$q_i = 1 - p_i$$

(2) *Series elements, parallel units.* If the elements are in series and the units or paths are in parallel (figure E-7), first obtain the path reliability by calculating the product of the reliabilities of all elements in each path. Then consider each path as a redundant unit to obtain the block reliability. Often there is a

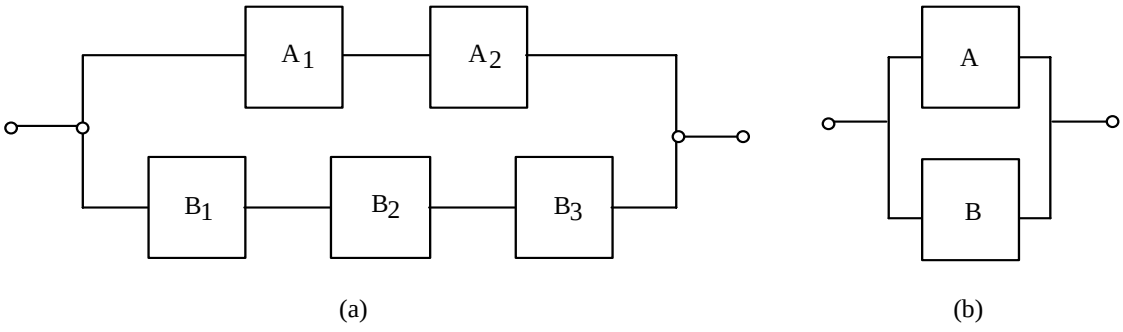


Figure E-7. Parallel-series configuration.

combination of series and parallel redundancy in a block as shown in figure E-7a. This arrangement can be converted into the simple parallel form shown in figure E-7b by first evaluating the series reliability of each path using the following equations (the terms on the right hand side represent element reliability):

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

$$p_B = p_{b_1} p_{b_2} p_{b_3}$$

The block reliability can then be found from:

$$R = 1 - (1 - p_A) \cdot (1 - p_B)$$

$$= 1 - q_A q_B$$

g. Redundancy in time dependent situations. The reliability of elements used in redundant configurations is usually time dependent. If the relation between element reliability and time is known,

inclusion of the time factor does not change the basic notation and approach to redundancy computation outlined above.

(1) Example of redundancy in time dependent situations. As an example, assume two active independent elements in parallel. System reliability is given by:

$$R = 1 - (1 - p_a)(1 - p_b) = 1 - 1 + p_a + p_b - p_a p_b$$

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

(2) Expressing reliability over a period of time. The former equation is applicable for one time interval. To express reliability over a segment of time, the reliability of each element must be expressed as a function of time. Hence,

$$R(t) = p_a{}^{(t)} + p_b{}^{(t)} - p_a{}^{(t)}\, p_b{}^{(t)}$$

where:

$R(t)$ = system reliability for time t, $t > 0$

and $p_a{}^{(t)}, p_b{}^{(t)}$ = element reliabilities for time t

(3) When the exponential applies. The failure pattern of some components is described by the exponential distribution:

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

where:

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

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

$$R(t) = p_a{}^{(t)}\, p_b{}^{(t)} = e^{-\lambda_a t}\, e^{-\lambda_b t} = e^{-(\lambda_a + \lambda_b)t}$$

(5) System reliability function for redundant element systems. The system reliability, R(t), function for elements in series with constant failure rates is exponential. With redundant elements present in the system, however, the system reliability function is not itself exponential. This is illustrated by two operative parallel elements whose failure rates are constant. From:

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

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

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

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

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

or, if the failure rates of both elements are equal,

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

and

$$MBTF = \frac{3}{2\lambda} = \frac{3}{2}\theta$$

(7) Three elements in parallel. For three independent elements in parallel, the reliability function is:

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

and

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

$$\frac{1}{\lambda_b - \lambda_c} + \frac{1}{\lambda_a + \lambda_b + \lambda_c}$$

(8) Reliability function for three elements in parallel. For three independent elements in parallel when $\lambda_a = \lambda_b = \lambda_c = \lambda$, the reliability function is:

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

and

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

(9) General rule. In general, for n active parallel elements, each element having the same constant failure rate, λ,

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

and

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

h. Types of redundancy. There are two basic types of redundancy: active and standby.

(1) Active redundancy. External components are not required to perform the function of detection, decision and switching when an element or path in the structure fails. The redundant units are always operating and automatically pick up the load for a failed unit. An example is a multiengine aircraft. The aircraft can continue to fly with one or more engines out of operation.

(2) Standby redundancy. External elements are required to detect, make a decision and switch to another element or path as a replacement for a failed element or path. Standby units can be operating (e.g., a redundant radar transmitter feeding a dummy load is switched into the antenna when the main transmitter fails) or inactive (e.g., a backup generator is turned on when the primary power source fails).

(3) Other forms of redundancy. Table E-1 summarizes a variety of redundancy techniques. The most important of these are discussed later in this appendix.

Table E-1. *Redundancy techniques*

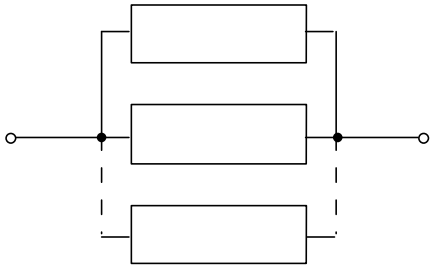
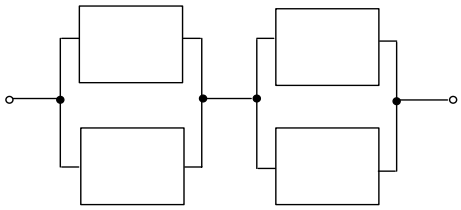
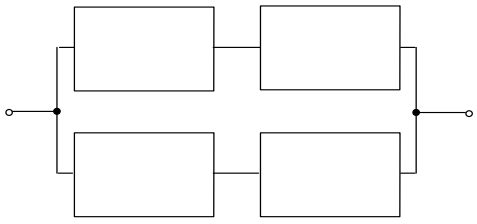
Simple Parallel Redundancy (Active Redundancy) 	In its simplest form, redundancy consists of a simple parallel combination of elements. If any element fails open, identical paths exist through parallel redundant elements.
(a) Bimodal Parallel/Series Redundancy  (b) Bimodal Series/Parallel Redundancy 	A series connection of parallel redundant elements provides protection against electrical shorts and opens. Direct short across the network due to a single element shorting is prevented by a redundant element in series. An open across the network is prevented by the parallel element. Network (a) is useful when the primary element failure mode is open. Network (b) is useful when the primary element failure mode is short.

Table E-1. Redundancy techniques (Cont'd)

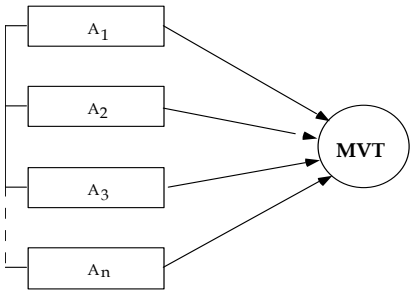
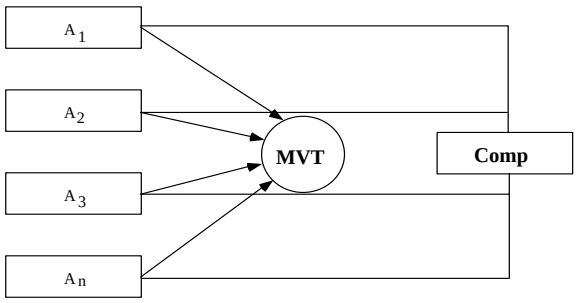
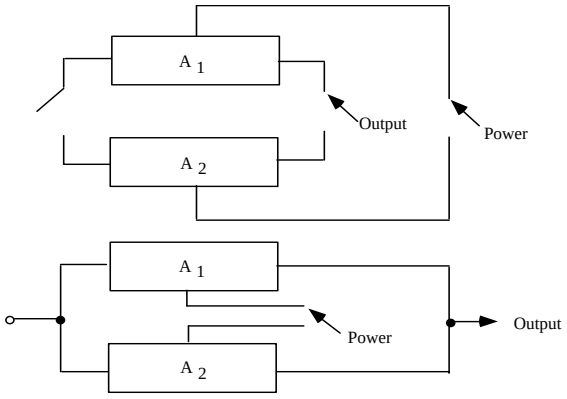
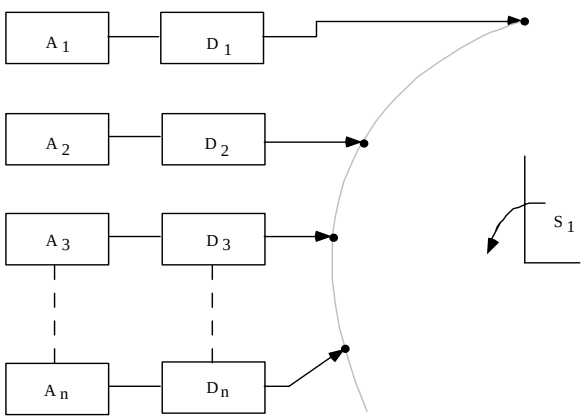
Majority Voting Redundancy 	Decision can be built into the basic parallel redundant model by inputting signals from parallel elements into a voter to compare each element's signal with the signals of the other elements. Valid decisions are made only if the number of useful elements exceeds the failed elements.
Adaptive Majority Logic 	This technique exemplifies the majority logic configuration discussed previously with a comparator and switching network to switch out or inhibit failed redundant elements.
Standby Redundancy 	A particular redundant element of a parallel configuration can be switched into an active circuit by connecting outputs of each element to switch poles. Two switching configurations are possible. The elements may be isolated by the switch until switching is completed and power applied to the element in the switching operation. All redundant elements are continuously connected to the circuit and a single redundant element activated by switching power to it.

Table E-1. Redundancy techniques (Cont'd)

Operating Standby Redundancy 	In this application, all redundant units operate simultaneously. A sensor on each unit detects failures. When a unit fails, a switch at the output transfers to the next unit and remains there until failure.

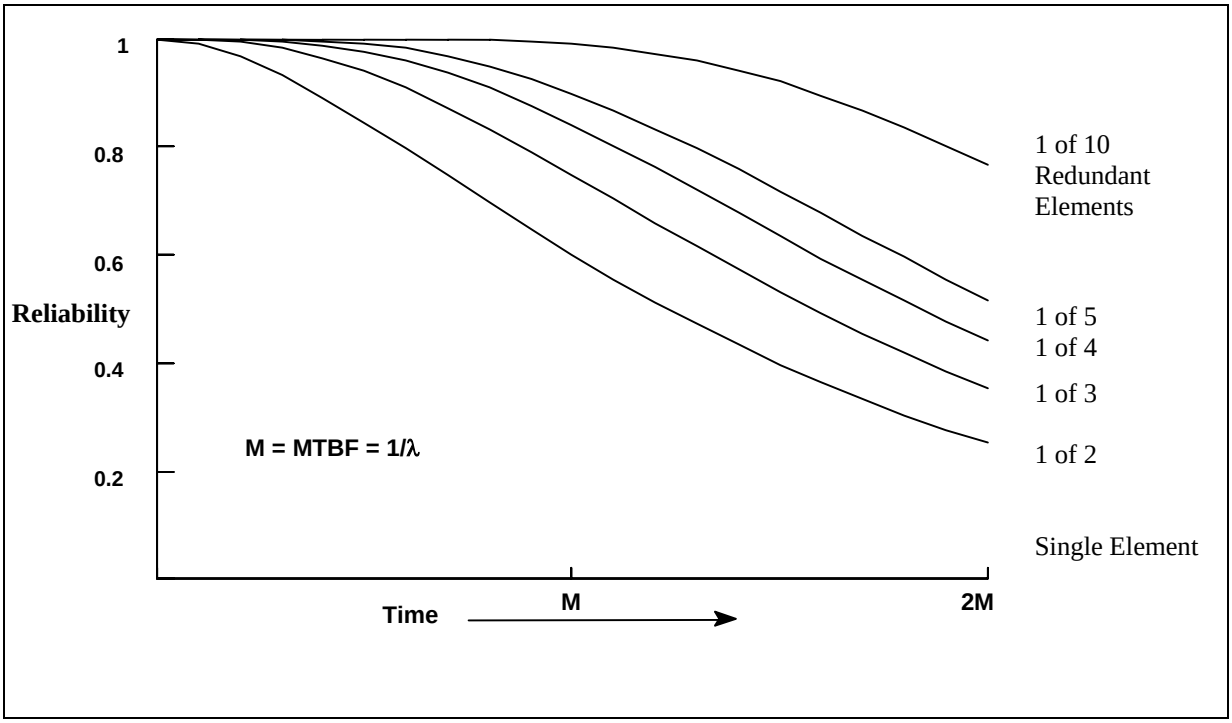
i. Limited benefits of redundancy. In general, the reliability gain for additional redundant elements decreases rapidly for additions beyond a few parallel elements. As illustrated by figure E-8 for simple parallel redundancy, there is a diminishing gain in reliability and MTBF as the number of redundant elements is increased. As shown for the simple parallel case, the greatest gain achieved through addition of the first redundant element is equivalent to a 50% increase in the system MTBF.

(1) Redundancy may not help. The reliability of certain redundant configurations may actually be less than that of a single element due to the serial reliability of switching or other peripheral devices needed to implement the particular redundancy configuration. Care must be exercised to ensure that reliability gains are not offset by increased failure rates due to switching devices, error detectors and other peripheral devices needed to implement the redundancy.

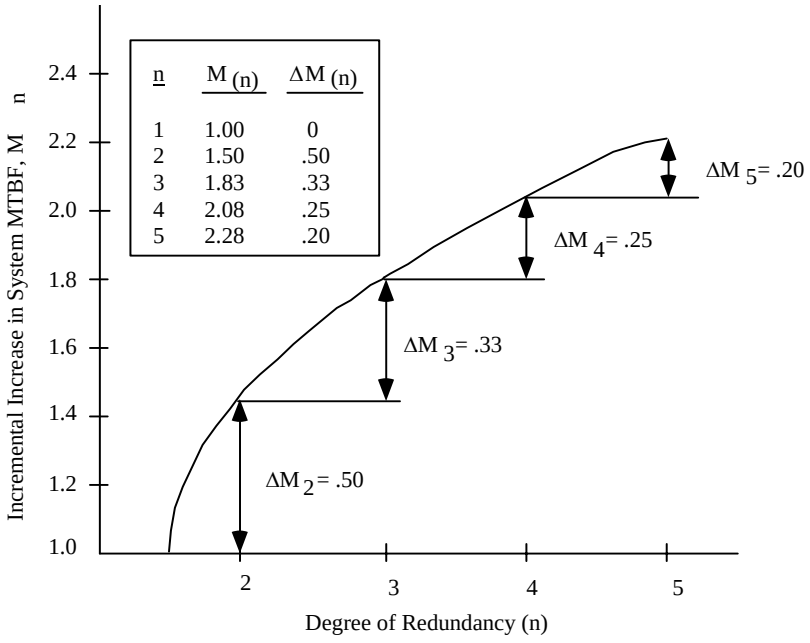
(2) Increasing the effectiveness of redundancy. The effectiveness of certain redundancy techniques (especially standby) can be enhanced by repair. Standby redundancy allows repair of the failed unit (while operation of the good unit continues uninterrupted) by virtue of the switching function built into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

(3) An example. An illustration of the enhancement of redundancy with repair is shown in figure E-9. The increased reliability brought about by incorporation of redundancy is dependent on effective isolation of redundant elements. Isolation is necessary to prevent failure effects from adversely affecting other parts of the redundant network. In some cases, fuses or circuit breakers, overload relays, etc., may be used to protect the redundant configuration. These items protect a configuration from secondary effects of an item's failure so that system operation continues after the element failure. The susceptibility of a particular redundant design to failure propagation may be assessed by using an FMEA. The

particular techniques addressed there offer an effective method of identifying likely fault propagation paths.



a. Simple active redundancy where one of n elements is required.



b. Incremental increase in system MTBF for n active elements.

Figure E-8. The gain in reliability decreases as the number of active elements increases.

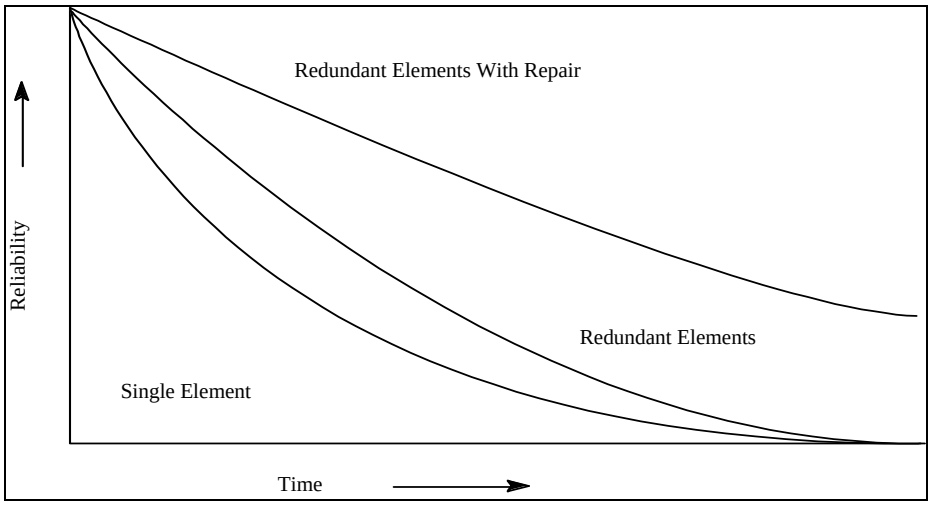


Figure E-9. Reliability gain for repair of simple parallel element at failure.

j. Redundancy in protective circuits. Redundancy may be incorporated into protective circuits[1] as well as the functional circuit that it protects. Operative redundancy configurations of protection devices (e.g., fuse, circuit breaker) can be used to reduce the possibility that the "protected" circuit is not completely disabled should the protective circuit device open prematurely or fail to open due to overcurrent.

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

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

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

(1) Partial redundancy example 1. A generator has three filters. The generator will operate if at least two filters are operational, that is, if k = 2 or k = 3. The probability of each channel being successful is equal to p; then

$$R = P(2, 3 \mid p) + P(3, 3 \mid p)$$

$$R = \binom{3}{2} p^{2} (1-p) + \binom{3}{3} p^{3} (1-p)^{0}$$

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

$$R = 3p^2 (1 - p) + p^3$$

$$R = 3p^2 - 2p^3$$

(2) Partial redundancy example 2. Use of the binomial formula becomes impractical for hand calculation in multi-element partial redundant configurations when the values of n and k become large.[2] In these cases, the normal approximation to the binomial may be used. The approach can be best illustrated by an example. A transmitting array is designed using 1000 RF elements to achieve design goal performance for power output and beam width. A design margin has been provided, however, to permit a 10% loss of RF elements before system performance becomes degraded below the acceptable minimum level. Each element is known to have a failure rate of 1000×10^{-6} failures per hour. The proposed design is illustrated in figure E-10, where the total number of elements is n = 1000; the number of elements required for system success is k = 900; and, the number of element failures permitted is r = 100. It is desired to compute and plot the reliability function for the array.

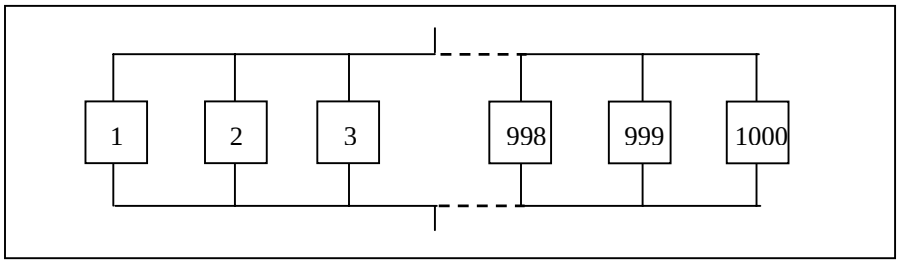


Figure E-10. Partial redundant array.

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

$$R_s t = \sum_{x=0}^{r} \binom{n}{x} p^{n-x} q^x$$

$$= \sum_{x=0}^{100} \binom{1000}{x} \left(e^{-\lambda t}\right)^{n-x} \left(1 - e^{-\lambda t}\right)^x$$

where:

$q = 1 - e^{-\lambda t}$

$p = e^{-\lambda t}$

x = number of failures

λ = element failure rate

(b) The binomial summation can be approximated by the standard normal distribution function using table E-2 to compute reliability for the normalized statistic z.

[2] See any good textbook on probability and statistics.

Table E-2. Reliability calculations for example 2

Time, t	z	F(z) = $R_s(t)$
90	1.570	0.9420
95	0.989	0.8389
105	0.000	0.5000
110	-0.420	0.3370
120	-1.300	0.0970
130	-2.030	0.0210

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

where:

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

(c) By observation, it can be reasoned that system MTBF will be approximately 100 hours, since 100 element failures are permitted and one element fails each hour of system operation. A preliminary selection of discrete points at which to compute reliability might then fall in the 80- to 100-hour bracket. Table E-3 shows the calculations.

Table E-3. MTBF calculations for example 2

At 80 Hours:

$$q = 1 - e^{-\lambda t} = 1 - e^{-(1000 \cdot 10^{-6} \cdot 80)} = 0.077$$

$$p = e^{-(1000 \cdot 10^{-6} \cdot 80)} = 0.923$$

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

$$\sigma = \sqrt{npq} = \sqrt{1000(0.077)(0.923)} = \sqrt{71.07} = 8.4$$

$$x = 100$$

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

$R_s(80) = F(z_{80}) = F(+2.74) = 0.997$, from standard normal tables

At 100 Hours:

$$\mu = nq = 1000\,(1 - e^{-1000 \cdot 10^{-6} \cdot 100}) = 95$$

$$p = e^{-1000 \cdot 10^{-6} \cdot 100} = 0.905$$

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

$$x = 100$$

$$z_{100} = \frac{100 - 9.5}{9.3} = 0.54$$

$R_s(100) = F(z_{100}) = F(+0.54) = 0.705$

These points are then used to plot the reliability function for the array, shown in Figure E-11. Also shown in the figure are curves for r = 0, 50, and 150.

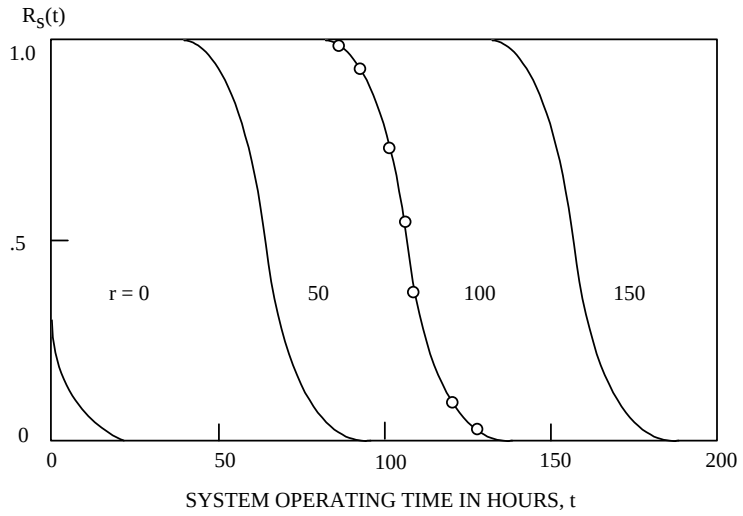


Figure E-11. Reliability functions for partial redundant array of figure E-10.

m. Operating standby redundancy. Until now we have assumed that switching devices were either absent or failure free. We now deal with cases whose redundant elements are continuously energized but do not become part of the system until switched in after a primary element fails. We will consider two modes of failure that can be associated with the switching mechanism: Type 1 - The switch may fail to operate when it is supposed to; and Type 2 - The switch may operate without command (prematurely). In the discussions that follow, q_s = probability of a Type 1 failure, and q'_s = probability of a Type 2 failure. Note that the probability of switching failures must be considered in modeling redundancy with switching. The consideration of such failures can be complex. If the switching reliability is high in comparison with element reliability (i.e., switch failure rate is one-tenth that of the element failure rate), it is often possible to simplify the model with an acceptable loss of accuracy by ignoring switch failures.

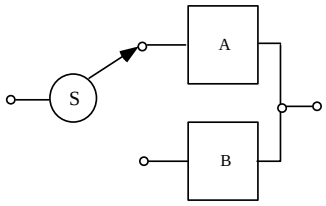
(1) Two parallel elements. Consider the system in figure E-12. There are three possible states that could lead to system failure. In state 1, A fails, B succeeds, and the switch fails (Type 1 failure). In state 2, A succeeds, B fails, and the switch fails (Type 2 failure). In state 3, A fails and B fails. The calculations for the system reliability are shown in the figure.

(2) Three Parallel Elements. Figure E-13 illustrates this type circuit. It operates as follows: If A fails, S switches to B. If B then fails, S switches to C. Enumerating all possible switching failures shows two kinds of Type (1) failure and four kinds of Type (2) failure as shown in the figure.

n. Voting Redundancy. Figure E-14 shows three elements, A, B, and C, and the associated switching and comparator circuit which make up a voting redundant system. The circuit function will always be performed by an element whose output agrees with the output of at least one of the other elements. At least two good elements are required for successful operation of the circuit. Two switches are provided so that a comparison of any two outputs of the three elements can be made. A comparator circuit is required that will operate the two switches so that a position is located where the outputs again agree after one element fails.

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

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



The unreliability of the system, Q, is

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

The reliability of the system, R, is

$$R = 1 - Q = 1 - (p_a\ p_q\ q'_s + q_a\ p_b\ q_s + q_a\ q_b)$$

Example: Assume

$$q_a = q_b = 0.2 \text{ and } q_s = q'_s = 0.1$$

Then

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

$$= (0.8)(0.2)(0.1) + (0.2)(0.8)(0.1) + (0.2)(0.2) = 0.072$$

$$R = 1 - Q = 1 - 0.072 = 0.928$$

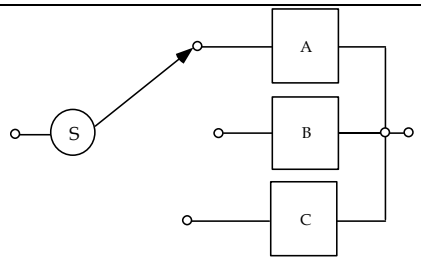
If we are not concerned with Type (2) failures, $q'_s = 0$, and the unreliability is

$$Q = q_a\ p_b\ q_s + q_a\ q_b$$

$$= (0.2)(0.8)(0.1) + (0.2)(0.2) = 0.056$$

$$R = 1 - 0.056 = 0.944$$

Figure E-12. Redundancy with switching.



Type (1) Switching Failures:

- q_{s_1} - A fails, S does not switch to B.
- q_{s_2} - A fails, S switches to B, B fails, S fails to switch to C.

Type (2) Switching Failures:

- q'_{s_3} - A succeeds, but S switches to B.
- q'_{s_4} - A succeeds, S switches to B, B fails, S does not switch to C.
- q'_{s_5} - A succeeds, S switches to B, B succeeds, S switches to C.
- q'_{s_6} - A fails, S switches to B, B succeeds, S switches to C.

Figure E-13. Three-element redundant configuration with switching.

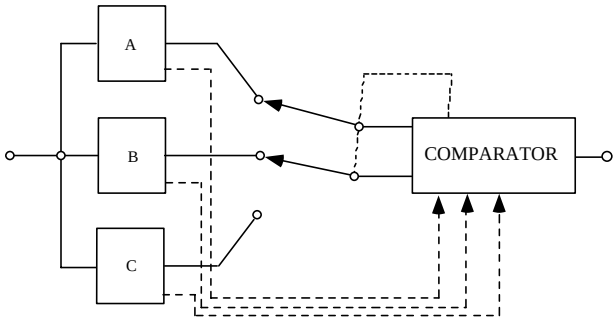


Figure E-14. Three-element voting redundancy.

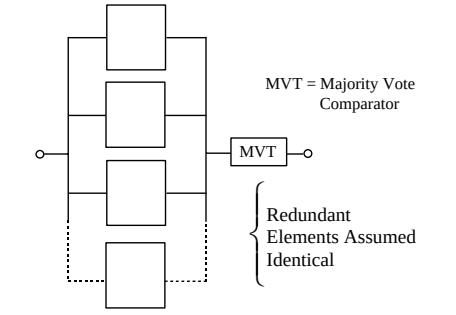
(2) Imperfect switching. If failure free switching cannot be assumed, conditional probabilities of switching operation have to be considered. To simplify the discussion, consider the probability of the comparator and switches failing in such a manner that the switches remain in their original positions.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

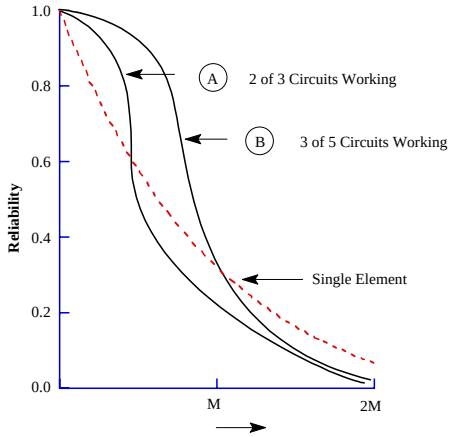
$$R = p_a\, p_b + (p_a\, p_c + p_b\, p_c - 2p_a\, p_b\, p_c)(1 - q_s)$$

(3) Example. Here is an example of a voting redundant system (information and expressions for the general majority voting case are given in figure E-15). Let all three elements have the same probability of success, 0.9, i.e., $p_a = p_b = p_c = 0.9$. Assume that the comparator switch has a probability of failing (q_s) of 0.01.

$$R = 9^2 + \left[0.9^2 + 0.9^2 - 2(0.9)^3 \right] [1 - 0.01]$$

$$R = 970$$





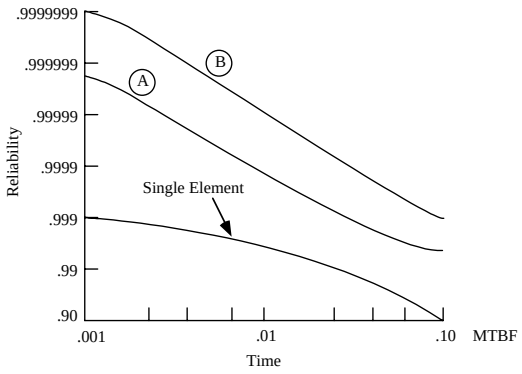
Reliability Function for Majority Voting Redundancy

ADVANTAGES

- Can be implemented to provide indication of defective elements
- Can provide a significant gain in reliability for short mission times (less than one MTBF)

DISADVANTAGES

- Requires voter reliability be significantly better than that of element
- Lower reliability for long mission time (greater than one MTBF)



Reliability For Mission Time Less Than One MTBF

APPLICATION

Generally used with logic circuitry for either continuous or intermittent operation. This technique with minor modification, may be put in the form of adaptive majority logic or gate connector redundancy

MATHEMATICAL MODEL

$$R = \left[\sum_{i=0}^{n} \binom{2n+1}{i} \left(1 - e^{-\lambda t}\right) e^{-\lambda t(2n+1-i)} \right] e^{-\lambda_m t}$$

Figure E-15. Majority voting redundancy.

o. Inactive standby redundancy. In a system with redundant elements on an inactive standby basis (not energized), no time is accumulated on a secondary element until a primary element fails. For a two-element system, the reliability function can be found directly as follows. The system will be successful at time t if either of the following two conditions holds (let A be the primary element): A is successful up to time t. or A fails at time $t_1 < t$, and B operates from t_1 to t.

(1) The exponential case. For the exponential case where the element failure rates are λ_a and λ_b, the reliability of the standby pair is given by the following equation.

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

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

(2) MTBF. The mean-time-to-failure of the system just described is

$$MTBF = \frac{\lambda_a + \lambda_b}{\lambda_a \lambda_b}$$

$$\theta_a + \theta_b$$

$$= 2\theta, \text{ when } \theta_a = \theta_b = \theta$$

(3) Multiple elements. For n elements of equal reliability, it can be shown that,

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

where:

r is the number of failures

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

(4) Inactive standby redundancy as a function of mission time. Figure E-16 is a chart relating system reliability to the reliability of individual operating standby redundant parallel elements as a function of mission time, t/θ. By entering the chart at the time period of interest and proceeding vertically to the allocated reliability requirement, the required number of standby elements can be determined.

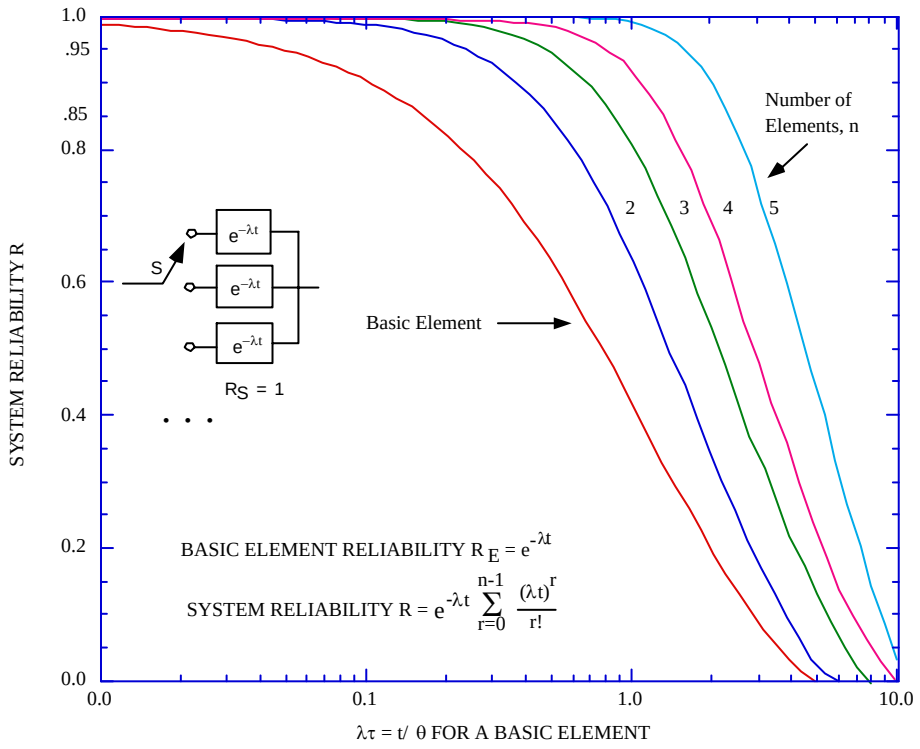


Figure E-16. System reliability for n standby redundant elements.

(5) Example of inactive standby redundancy. A critical element within a system has a demonstrated MTBF, θ = 100 hours. A design requirement has been allocated to the function performed by this element of R_s = 0.98 at 100 hours. This corresponds to a 30-to-1 reduction in unreliability compared with that which can be achieved by a single element. In this case, n = 4 will satisfy the design requirement at t/θ = 1. In other words, a four-element standby redundant configuration would satisfy the requirement. Failure rates of switching devices must next be taken into account.

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

(1) Conditional events. Figure E-17 illustrates an example of conditional or dependent events. Assume elements A and B are both fully energized, and normally share or carry half the load, L/2. If either A or B fails, the survivor must carry the full load, L. Hence, the probability that one fails is dependent on the state of the other, if failure probability is related to load or stress. The system is operating satisfactorily at time t if either A or B or both are operating successfully.

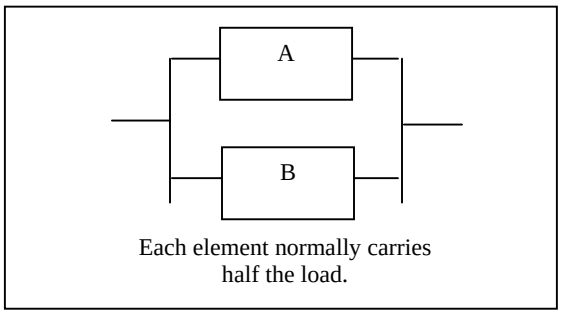


Figure E-17. Load sharing redundant configuration.

(a) Figure E-18 illustrates the three possible ways the system can be successful. The bar above a letter represents a failure of that element. A primed letter represents operation of that element under full load; absence of a prime represents operation under half load. If the elements' failure times are exponentially distributed and each has a mean life of θ under load L/2 and $\theta' = \theta/k$ under load L where $k \geq 0$, block reliability and system mean life are given by:

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

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

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

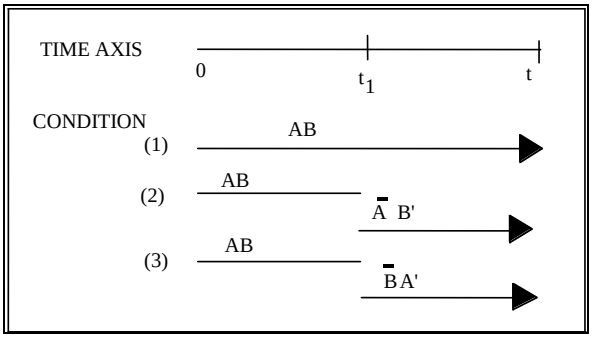


Figure E-18. Success combinations in two-element load-sharing case.

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

(1) Redundancy is not free. Since cost, weight, and complexity factors are always involved, the minimum amount of redundancy that will produce the desired reliability should be used. Thus efforts should be concentrated on those parts of the system that are the major causes of system unreliability.

(2) Example. Assume that we have two elements, A and B, with reliabilities over a certain time period of 0.95 and 0.50, respectively. If A and B are joined to form a series non-redundant circuit, its reliability is

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

(a) If we duplicate each element, as in figure E-19a,

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

(b) Duplicating element B only, as in figure E-19b,

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

(c) Obviously, duplicating element A contributes little to increasing reliability. Triplication of B gives the configuration shown in figure E-19c and $R_3 = 0.95 [1 - (0.5)^3] = 0.831$, which is a 75% increase in the original circuit reliability as compared to the 58% increase of R_1.

(d) If complexity is the limiting factor, duplicating systems is generally preferred to duplicating elements, especially if switching devices are necessary. If another series path is added in parallel, we have the configuration in figure E-19d, and $R_4 = 1 - (1 - 0.475)^4 = 0.724$, which is only slightly less than R_1. If switches are necessary for each redundant element, R_4 may be the best configuration. A careful analysis of the effect of each element and switch on system reliability is a necessary prerequisite for proper redundancy application.

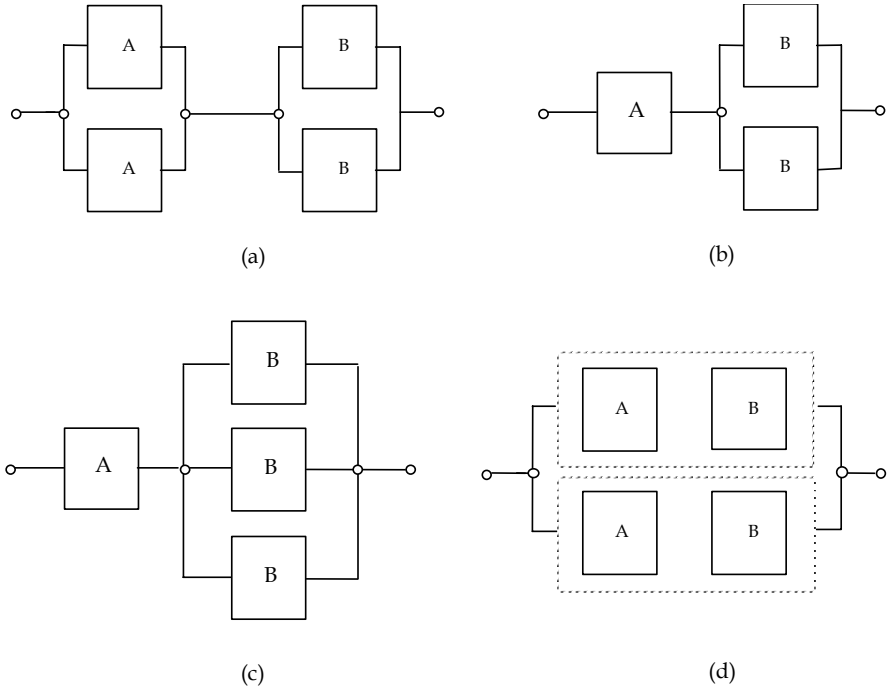


Figure E-19. Possible alternative redundant configurations for optimization example. Baseline is a series system with two elements, A and B.

GLOSSARY

Glossary

-A-

ALLOCATION. The apportionment of "system-level" R&M requirements to lower levels of indenture. The system is defined as the item being developed. In the case of an aircraft, the R&M requirements could be allocated to major subsystems (e.g., propulsion), then to components within that subsystem (e.g., turbofan engine), then to sub-components (e.g., the rotor), and so on. If the item in development were the engine, then the engine R&M requirements would be allocated to lower equipment indentures within the engine.

AVAILABILITY. A measure of the degree to which an item is in an operable and commitable state at the start of a mission when the mission is called for at an unknown (random) time. (Item state at start of a mission includes the combined effects of the readiness-related system reliability and maintainability parameters, but excludes mission time.) (MIL-STD-721C, now canceled). In its simplest definition, availability is uptime divided by downtime. In terms of reliability (MTBF or and maintainability (Mean Time to Repair or Mean Downtime), inherent and operational availability are defined as:

A_O. Operational Availability. The percentage of time that a system is available for use based on its operational reliability and maintainability, and logistics factors, such as delay times. Usually defined by the following steady-state equation:

$$A_o = \frac{MTBM}{MTBM + MDT}$$

A_i. Inherent Availability. The percentage of time that a system is available for use based only on its inherent reliability and maintainability characteristics. Usually defined by the following steady-state equation:

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

-B-

BASIC RELIABILITY. A measure of a system's ability to operate without logistics support. All failures, whether the mission is or can be completed, are counted.

-D-

DOWNTIME. That element of time during which an item is in an operational inventory but is not in condition to perform its required function.

-F-

FAILURE. The event, or inoperable state, in which any item or part of an item does not, or would not, perform as previously specified.

FAILURE ANALYSIS. Subsequent to a failure, the logical systematic examination of an item, its construction, application, and documentation to identify the failure mode and determine the failure mechanism and its basic course.

FAILURE MECHANISM. The physical, chemical, electrical, thermal or other process which results in failure.

FAILURE MODE. The consequence of the mechanism through which the failure occurs, i.e., short, open, fracture, excessive wear.

FAILURE MODE AND EFFECTS ANALYSIS (FMEA). A procedure for analyzing each potential failure mode in a product to determine the results or effects thereof on the product. When the analysis is extended to classify each potential failure mode according to its severity and probability of occurrence, it is called a Failure Mode, Effects, and Criticality Analysis (FMECA).

FAILURE, RANDOM. A failure, the occurrence of which cannot be predicted except in a probabilistic or statistical sense. It must be noted that every failure occurs for a reason. The randomness addresses the time at which a failure will occur.

FAILURE RATE. The total number of failures within an item population, divided by the total number of life units expended by that population, during a particular measurement period under stated conditions.

FAULT. Immediate cause of failure (e.g., maladjustment, misalignment, defect, etc.).

FAULT TREE ANALYSIS. An analysis approach in which each potential system failure is traced back to all faults that could cause the failure. It is a top-down approach, whereas the FMEA is a bottom-up approach.

FIELD RELIABILITY. The reliability achieved in actual use. Field Reliability includes the combined effects of item design, installation, quality, environment, operation, maintenance, and repair.

-I-

INHERENT AVAILABILITY (A_i). A measure of availability that includes only the effects of an item design and its application, and does not account for effects of the operational and support environment.

INHERENT AVAILABILITY (A_i). A measure of availability that includes only the effects of an item design and its application, and does not account for effects of the operational and support environment. Sometimes referred to as "intrinsic" availability.

-M-

MEAN DOWNTIME (MDT). The average time a system is unavailable for use due to a failure. Time includes the actual repair time plus all delay time associated with a repair person arriving with the appropriate replacement parts.

MEAN TIME BETWEEN FAILURE (MTBF). A basic measure of reliability for repairable items. The mean number of life units during which all parts of the item perform within their specified limits, during a particular measurement interval under stated conditions.

MEAN TIME TO REPAIR (MTTR). A basic measure of maintainability. The sum of corrective maintenance times at any specific level of repair, divided by the total number of failures within an item repaired at that level, during a particular interval under stated conditions.

-R-

REDUNDANCY. The existence of more than one means for accomplishing a given function. Each means of accomplishing the function need not necessarily be identical. (MIL-STD-721C, now canceled). The two types of redundancy are:

ACTIVE REDUNDANCY. That redundancy wherein all redundant items are operating simultaneously.

STANDBY REDUNDANCY. That redundancy wherein the alternative means of performing the function is not operating until it is activated upon failure of the primary means of performing the function.

RELIABILITY. (1) The duration or probability of failure-free performance under stated conditions. (2) The probability that an item can perform its intended function for a specified interval under stated conditions. (For non-redundant items this is equivalent to definition (1). For redundant items this is equivalent to definition of mission reliability.) (MIL-STD-721C, now canceled)

RELIABILITY-CENTERED MAINTENANCE (RCM). A disciplined logic or methodology used to identify preventive and corrective maintenance tasks to realize the inherent reliability of equipment at a minimum expenditure of resources.

-U-

UPTIME. The time during which a system is in condition to perform its required functions.

GO definitions:

Active Signals: The number of signals which make up the joint distribution at any point in the quantification of the GO model.
Infinity: The largest value that a signal in a specific data set may be assigned. Often equated with complete failure of a component or system.
Kind: Set of parameters (usually probabilities) that, with the operator type, defines the component function and probability characteristics.
Kind Data: The set of numbers, state values, and probabilities representing component reliability data and system success criteria.
Operator: Fundamental element of a GO model. It represents an algorithm for a component for creating one or more new signals.
Operator Data: The set of numbers describing the system model structure.
Perfect Operators: Operators that have only one assigned state are called perfect.
Premature: Successful component function prior to the normal operation time due to certain component failure modes.
Pruning Value: The probability value to which each new term of the distribution is compared so that terms less than the pruning value can be eliminated.
Signal: A random variable created by an operator. The output signal values and their probabilities are determined by the operator type, kind data, and input signal values.
System States: Integer values representing modes of system and component operation.
Type: Operator classification by "Type" of algorithm which defines the operator outcome for all possible input combinations.