Reliability:

A Practitioner's Guide

Release Conditions

Comments and/or questions can be addressed to:

Intellect
Russell Square House
10-12 Russell Square
London WC1B 5EE, UK
info@intellectuk.org

Relex Software Corporation
540 Pellis Road
Greensburg, PA 15601 USA
info@relexsoftware.com

Copies of this document may be purchased from:
http://www.intellectuk.org/relc
http://www.relexsoftware.com

Acknowledgements

The following Editorial Board members are thanked for their cooperation and assistance in the preparation of this guide. Without their time, efforts and knowledge, this document would never have been generated.

Dr. Bangalore Basker	BAE SYSTEMS
Paul Dibbens	AMS
Dr. Geoff Pullum	Consultant
Ron Sexton	MBDA
Robert Waltz	Smiths Detection

The topics treated in this guide were selected by a panel of eminent engineers representing the broad area of reliability engineering. The specialised chapters have been written or revised by many, often unnamed contributors, who are recognised experts in the reliability engineering field. Many contributors have been involved in major developments that have occurred in reliability. The result is guidance that is completely authoritative.

Because reliability engineering extends into many areas of design, the Editorial Board has found it necessary to limit coverage of many topics and to completely omit other topics, hoping one day it might be possible to fill some of the gaps. The chairman, Rob Sexton, expresses his pride and satisfaction in the quality of the authors' contributions and thanks them for their conscientious efforts.

Thanks are given to the UK Ministry of Defence for allowing the document RPM 80 to be used as a data source. Thanks are also given to Relex Software Corporation for assisting in the preparation and publishing of this guide. Special thanks to Dr. Suprasad Amari for his valuable comments and suggestions, and to Kathy Pippert for her patience, enthusiasm and good humour while serving as technical editor.

And, lastly, thanks are given to Dr. Roy Axford (ret.) at Intellect for initiating this publication and to Robert Limmergård at Intellect for his untiring efforts and perseverance as he encouraged and counselled all contributors to complete this major undertaking.

Contents

List of Figures

List of Tables

1. Introduction

General Introduction

This document was prepared with the aim of bringing up to date the disciplines associated with reliability prediction and analysis, and so overcome some of the problems associated with the techniques as performed over the last 20 years or so.

The opportunity has been taken to review those aspects of conventional reliability engineering and to provide a guide that can be used in a simple manner by those smaller companies that are required to provide larger customer organisations with reliability estimates and analyses for their equipment. It is also hoped that the techniques described herein will be of value to small- and medium-sized business enterprises when planning their own activities with respect to reliability. Reliable products enhance market position and protect company reputations.

The issue of this document has been timed to coincide with the spread of a new wave of thoughts and processes related to reliability engineering spreading from Europe to the rest of the world. It aims to support this wave of enthusiasm and to introduce a new and user friendly form of reliability prediction.

This document has been put together by a small team working under the auspices of Intellect with assistance from Relex Software Corporation, a worldwide leader in reliability analysis software tools. Supported by all Member Companies, this document updates an earlier UK Ministry of Defence document, RPM 80, which has been used worldwide.

The issue of this document is made even more important by the demise of many of the more traditional reliability prediction standards worldwide following the move towards commercial procurement of components and systems. There remains a need for companies to compete with one another in a reliability sense. Use of the reliability prediction and analysis techniques described in this document will allow them to compete from a common standpoint.

2. General Philosophy and Process of Reliability Prediction

Introduction

Reliability prediction is a continuing activity throughout the design and development of a project, from initial conception to production and beyond. The prediction methods that apply at any particular time may vary, but the general philosophy and principles remain common throughout. The primary objectives of this chapter are to:

- Describe the purposes of prediction and its application at different stages of a project.
- Consider the general philosophy and principles behind prediction methods.
- List the main activities comprising a prediction process.
- Indicate the main limitations of the general philosophy.

NOTE It is not the intention of this chapter to derive basic reliability expressions or to discuss probability and statistical theory. Information on these aspects is readily available in many standard textbooks.

Definitions

The definitions for those reliability terms most often used within this guide follow.

- **Reliability**.
  - The ability of an item to perform a required function without failure under stated conditions for a stated period of time.

    Or, as more commonly used in engineering applications:
  - The probability that an item can perform a required function under given conditions for a given time interval, $(t1, t2)$. This is normally denoted either by the letter R or by $R(t)$, with t denoting the interval $t1, t2$.

- **Failure**. The state of the item when it is unable to perform a required function. In the case of non-repairable items, it is the termination of the ability of an item to perform a required function.

  Note:
  1. After the occurrence of a failure, the item is in a faulty condition.
  2. An occurrence of a **failure** is an event (as distinguished from a **fault**, which is a state.
  3. This concept as defined does not apply to items consisting of software only.

- **(Instantaneous) Failure Rate**. The limit, if this exists, of the ratio of the conditional probability that the instant of time, t, of a failure of an item falls within a given time interval, (t, $t + \Delta\tau$), to the length of this interval, $\Delta\tau$, when $\Delta\tau$ tends to zero, given that the item is in an up state at the beginning of the time interval. This limit is normally denoted by $\lambda(t)$. Failure rates are often given in terms of failures per million hours (fpmh); however, some industries use an alternative measure of failures per 10^9 known as FITs (Failures in Time). Such failure rates are given in terms of failures per billion hours.

- **Mean Time To Restore**, **Mean Time To Recovery** or **Mean Time to Repair (MTTR)**. The expectation of the time to restore.

NOTE In this document, the term MTTR is frequently used. This is to maintain a measure of consistency with other work. The term **Mean Active Corrective Maintenance Time (MACMT)** may often be interchanged with **Mean Active Repair Time (MART)**.

Purposes of Prediction

The aim of prediction is to provide a quantitative forecast of the reliability that may be eventually achieved by any particular design. Prediction is therefore a fundamental activity in the overall design evaluation process. The prediction process does not in itself contribute directly to the reliability of a system, but the values produced constitute essential criteria for selecting courses of action that affect the reliability of a design.

Also, by carrying out prediction in a detailed and systematic manner, the process will help to identify potential reliability problems, including:

- Misinterpretation of requirements.
- Sources of unreliability.
- Design imbalance (from a reliability viewpoint).

Primary Purposes

The primary purposes of prediction are to:

- Evaluate whether or not a particular design concept is likely to meet a specified reliability requirement under defined conditions.
- Compare alternative design solutions.
- Provide inputs to related project activities, such as:
  - Design evaluation.
  - Trade-off studies.
  - Life cycle costs.
  - Spares provisioning.
  - Logistic and maintenance support studies.
- Assist in the identification and elimination of any potential reliability problems by imposing a systematic discipline that ensures all reliability aspects of a design are examined.
- Measure progress towards achieving the specified reliability requirements.

The prediction process is a continuing activity throughout a project, with the prediction being regularly updated as more design, test and evaluation data become available. The accuracy of any prediction depends largely upon the availability of detailed design and operating data. This is seldom available during the early stages of a project.

However, the requirement for prediction must be used to force detailed information to be made available as early as possible, particularly in critical areas, so that a more thorough and realistic pre-design assessment can be produced. Clearly, therefore, prediction must be a part of the design process and not simply a parallel activity.

Project Definition

During the feasibility and early project definition stages of a project, predictions obviously cannot be based on detailed design information. In spite of this, major decisions are made and large-scale funding is committed at this time. It is at this stage that accurate predictions would be most valuable.

It is an unfortunate fact, therefore, that the greatest uncertainty is attached to predictions during the early stages of design. Despite this, the best available methods must be employed to identify critical design areas as early as possible. Examples of such methods include comparison with similar equipment and generic parts count assessments. Such methods are described more fully in Chapter 3, “Reliability Prediction Methods”.

Design Stages

It is during the early and detailed design stages that reliability prediction has its widest application. As more design information becomes available (e.g., component lists, application stresses, environmental conditions, etc.), more detailed predictions can be made progressively and design areas associated with potential unreliability can be identified. Examples of prediction methods used at these stages include generic parts count and parts stress analysis. These methods are also described more fully in Chapter 3, “Reliability Prediction Methods”.

Development Stages

During the development stages, there are two main types of reliability prediction activity:

- The continual updating of theoretical predictions as design changes are introduced due to shortcomings revealed by development testing and by early reliability predictions themselves.
- Predictions based on the practical results from any reliability development testing, demonstration testing, etc.. Often a **reliability growth model** is used, which enables future reliability achievement to be predicted based on cumulative test results.

Important! *It is important to note that a theoretical prediction will generally reflect the reliability of “mature” equipment (i.e., after some years in service). A prediction based on a reliability growth model, however, reflects the number of design shortcomings still present in the design of the build standard under test or in early service life.*

In-Service Stages

During in-service stages, theoretical predictions must be carried out to assess the effects on reliability of design changes introduced as modifications. Predictions based on in-service results may also be used to assess when the design may achieve **maturity** and how the achieved reliability at that stage may compare with the requirements. Such predictions are normally based on an appropriate reliability growth model as indicated above.

General Philosophy of Prediction

Reliability can be defined in conceptual and quantitative terms:

- As a concept, reliability is the ability of an item to perform its specified function without failure under stated conditions for a stated period of time, number of cycles, distance or any other variate.
- As a quantitative measure, reliability is the probability that an item will perform its specified function for a specified interval under specified conditions.

NOTE In the previous definitions, an item is **any one of enumerated things**, without regard to size or complexity. An item may therefore be a complete system at one extreme or a single component at the other.

Four elements are involved either directly or indirectly in both of these definitions of reliability:

- Probability.
- Performance requirements.
- Time (or another variate).
- Conditions under which the item is used.

To predict reliability, therefore, relationships must be established between these four elements.

Failure Rate Variation with Time

For many items (e.g., non-repairable items or items which when repaired are restored to an **as new** condition), a generally accepted model for variation of failure rate with time is the familiar **bathtub** curve shown in Figure 2-1 and Figure 2-2.

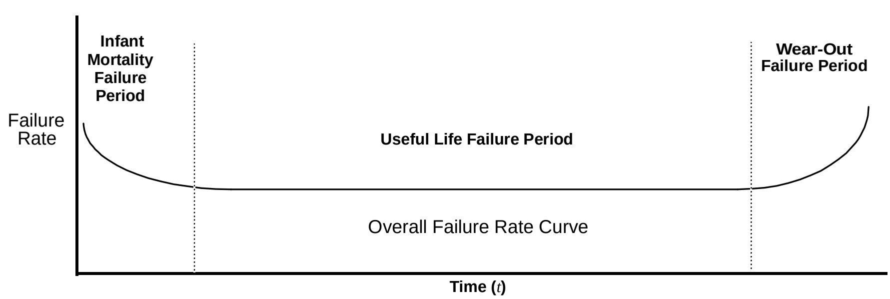


Figure 2-1. Bathtub Curve

The derivation of the bathtub curve is illustrated below. Initially, failures of an item placed in service are often seen to be dominated by 'quality' failures. These failures, which occur in what is known as the 'infant mortality' period, fade because they are fixed as they emerge. Later, as the system 'ages', the item enters a 'wear-out' period. The 'useful life' period, where there is often seen to be a 'constant' failure rate, lies between the infant mortality and wear-out periods.

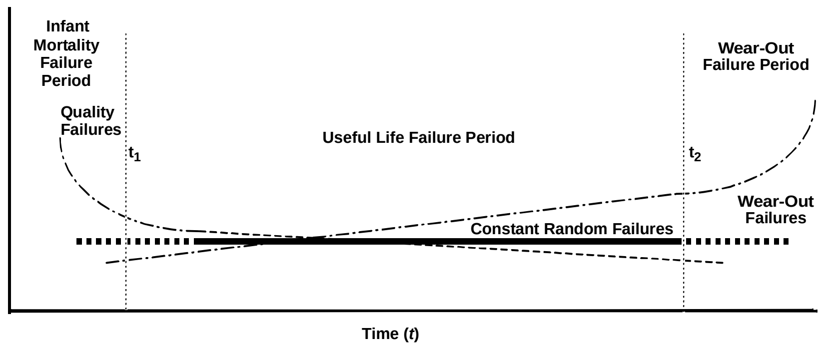


Figure 2-2. Derivation of Bathtub Curve

Infant Mortality Failure Period

In its early life, an item population exhibits a high failure rate, due mainly to manufacturing weaknesses, including:

- Poor joints and connections.
- Damaged components.
- Chemical impurities.
- Dirt and contamination.
- Assembly errors.

NOTE The failure rate decreases rapidly during the early life period and, at time t_1 say, stabilises at a certain value.

Normally, the quality weaknesses are revealed soon after the item is put to use. Therefore, as part of the quality control process, it is increasingly common for stress screening tests to be used to eliminate these weaknesses by simulating in the factory a period t_1 of use. However, stress screening is not always universally applied, and early life failures can cause problems in prediction because prediction generally claims to apply only to the useful life failure period.

Useful Life Failure Period

During the useful life failure period, t_1 to t_2, the failure rate remains substantially constant, and, although some failures may still arise from manufacturing weaknesses or wear-out, the majority of failures are caused by the operating stresses to which the item is subject in its particular application (e.g., temperature, electrical and environmental stresses) and occur randomly (without any time-dependent pattern). During this period, when the failure rate is considered to be constant, the negative exponential distribution describes the times to failure.

The useful life failure period is the interval of most interest from a reliability prediction standpoint because, if a rigorous reliability programme is applied throughout a project lifetime, it is assumed that:

- The majority of early life failures will normally be eliminated before an item enters service.
- An in-service maintenance policy will ensure that items are replaced **before** wear-out becomes a significant problem.

Important! *Note that, because of these assumptions, a prediction based on the exponential distribution will, in general, represent the reliability of a 'mature' design whose failure rate comprises mainly stress-related failures. Where the assumptions above are not given proper consideration, predictions will be substantially optimistic.*

Wear-Out Failure Period

During the wear-out failure period, the failure rate increases due mainly to deterioration of the item through prolonged exposure to operating and environmental stresses, which may include:

- Insulation breakdown.
- Wear or fatigue.
- Corrosion.
- Oxidation.

Normally, wear-out failures are avoided by replacing an item, either on the basis of fixed life replacement or **on-condition** monitoring. Even so, eventually the system becomes troublesome in use and is probably best replaced.

Derivation of Failure Rate Data

Prediction methods use unit or component failure rate data to produce a reliability characteristic or Mean Time To Failure (MTTF) value for the equipment being analysed. This data is usually derived from the following sources:

- In-house data derived from similar products.
- Manufacturers' data.
- Historical data from databases such as MIL-HDBK-217, Telcordia (formerly Bellcore), etc..

NOTE Appendix A, "Data Tables", contains failure rate data.

When To Carry Out Predictions

Reliability predictions should be carried out at all stages during the development of a project. By being continuously updated as the design progresses, reliability predictions can indicate whether the design reliability criteria are being met and also whether any elements that detract from the inherent reliability of the product have been eliminated.

The accuracy of reliability predictions depends largely upon the availability of detailed design and operating data. This information may not be available early in a design. However, the requirement for prediction must be used to force detailed information to be made available as early as possible, particularly in critical areas, so that a more thorough and realistic pre-design assessment can be produced. Predictions must therefore be an integral part of the design process from start to finish and not simply a parallel activity.

Reliability Function

Assuming that the conditions described in "Useful Life Failure Period" on page 2-7 apply so that the failure rate is constant, the relationship between reliability, failure rate and time is given by the expression:

Equation

$$R(t) = e^{-\lambda t} \qquad (2.1)$$

Where:

$R(t)$ = Reliability, i.e., the probability that an item will survive for time t under the specified operating conditions.

e = The base of the natural logarithms (approximately 2.7183).

λ = The item failure rate under the specified operating conditions of temperature, stress, environment, etc.. It is constant for at least time t .

t = The time that the item is at risk under the specified operating conditions. This is sometimes called the mission time.

Failure causes are not always dependent upon time and may depend upon particular events, such as switching, handling, etc.. In these cases, the relationship between reliability, failure probability and number of events is given by the expression:

Equation $$R(N) = (1 - \rho_E)^N \qquad (2.2)$$

Where:

$R(N)$ = Reliability, i.e., the probability that the item survives N events under specified operating conditions.

ρ_E = The probability that an event will be defective under specified operating conditions.

N = The number of events.

When $\rho_E \ll 1$, ρ_E can be thought of as a failure rate or better still as a percent defective:

$$(1 - \rho_E)^N \cong e^{-\rho_E N}$$

In general, the above assumption is valid for system prediction purposes and the following expression may be used:

Equation $$R(N) \cong e^{-\rho_E N} \qquad (2.3)$$

Where:

ρ_E = The expected number of failures per event under specified operating conditions.

N = The number of events.

Consider now the case when the specified time interval, t (for which the reliability of an item is to be predicted), is made up of a number of different time intervals, t_a, t_b, t_c, etc., each associated with different operating conditions. Then, from equation (2.1), the probability of failure in each time interval is given by:

$$R(t_a) = e^{-\lambda_a t_a}$$

$$R(t_b) = e^{-\lambda_b t_b}$$

Providing that $R(t_a)$, $R(t_b)$ and $R(t_c)$ can be considered independent of each other, they can be combined to give $R(t)$ as follows:

$$R(t) = R(t_a) \cdot R(t_b) \cdot R(t_c)$$
$$= [e^{-\lambda_a t_a}] \cdot [e^{-\lambda_b t_b}] \cdot [e^{-\lambda_c t_c}] \text{ or:}$$

Equation $$R(t) = e^{-(\lambda_a t_a + \lambda_b t_b + \lambda_c t_c)} \qquad (2.4)$$

Similarly, when the operational use of an item includes a number of independent events, the individual reliabilities given by equation (2.3) can be combined in a similar manner:

Equation $$R(M, N) = e^{-(\lambda_x M + \lambda_y N)} \quad (2.5)$$

Where M and N are events occurring at different times:

M = The number of events associated with *percent defective x*.

N = The number of events associated with *percent defective y.*

Finally, time-based and event-based probabilities can also be combined together if the operational use of an item involves both:

Equation $$R = e^{-(\lambda_a t_a + \lambda_b \lambda t_b + \lambda_x M + \lambda_y N)} \quad (2.6)$$

Relationship Between Components/Parts and System

In general terms, a **system** is a combination of items that are interconnected with each other to perform a specific operational function or functions. At its highest level, a system may consist of a number of individual pieces of equipment, each designed to perform a particular function as a self-contained unit; alternatively, at the lowest level of assembly, a system may be a combination of individual electronic components and/or mechanical parts providing an input function to the next higher level of assembly. Clearly, any combination of items between these two extremes may also form a system. Therefore, it is essential to define clearly the boundaries of the system under consideration. (This is described more fully in Chapter 3, “Reliability Prediction Methods”.)

Providing that a system is capable of performing its functions at some point in time, it will continue to have that capability until the operating characteristics of a component or part (or group of components/parts) changes to the extent that the specified function of the system is no longer achieved. The reliability of a system, therefore, depends upon:

- The number of components and parts.
- The way in which these components and parts are interconnected to perform the system functions.
- The reliabilities of the individual components.

To predict system reliability, the relationships between these factors must be established. Such relationships are described in the following section, “Reliability Block Diagrams”.

Reliability Block Diagrams

A Reliability Block Diagram (RBD) is a method of representing, in a single and visual way, the reliability relationships between the system and the items in the system. It can also be regarded as a model of a system failure/success definition. It does not necessarily relate to the physical connection of components or sub-units.

A system may require more than one RBD if it has to perform several functions or if it experiences several different operating states. In essence, the RBD must show the flow of inputs and outputs required for a particular function of the system being considered. It should be noted that the events modelled by RBDs must be totally independent of each other.

NOTE Other methods of establishing the reliability relationships between items, such as Fault Trees and Truth Tables, are not considered in this chapter. However, additional information on Fault Trees is presented in Chapter 5. (For additional information, also see Reference 1 in Appendix D, “Bibliography”.)

An example of an RBD is shown in Figure 2-3. For additional information, see Appendix B, “Preparation of Reliability Block Diagrams”.

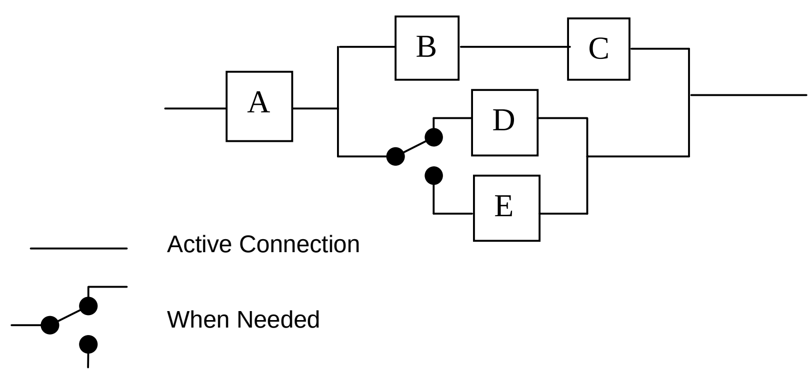


Figure 2-3. Example of an RBD

In Figure 2-3, it is assumed that both the system and its constituent items are in one of two states: either functioning correctly or failed. Hence each item may be looked on as a switch that is closed when the item is functioning and open when it has failed. The system will only function when a path exists between the input and output nodes. Thus, the system in Figure 2-3 will fail to function when at least:

- Item A has failed *OR*
- Item B or C has failed *AND*
  - Item D has failed *AND*
  - Item E has failed.

NOTE This can be written in Boolean notation in the form:

$$f = a + (b + c) \cdot e \cdot d$$

An RBD can always be constructed as connected groups of three types:

- Items in series (e.g., B and C in Figure 2-3).
- Items in parallel (or active) redundancy (e.g., B and D or C and D in Figure 2-3).
- Items in standby (or passive) redundancy (e.g., D and E in Figure 2-3).

NOTE From Figure 2-3, it can be seen that items A, B and C are sufficient to perform the desired system function. However, item D, which is operating simultaneously, is included in the system as an alternative means of helping to perform the system function. This is termed **parallel** (or **active redundancy**). Item E also provides an alternative, but remains inoperative until needed. This is termed **standby** (or **passive redundancy**).

Combining Reliabilities (No Repair)

Having established the functional relationship between the items in a system, the system reliability can be predicted by combining the reliabilities of the individual items.

Expressions for predicting the system reliabilities from the individual reliabilities of items in a system can be carried out in many ways. However, two particularly useful ways are based on the following:

- If X and Y are two independent events with probabilities $P(X)$ and $P(Y)$ of occurring, then the probability that both events will occur, $P(XY)$, is the product:

Equation $$P(XY) = P(X) \cdot P(Y) \quad (2.7)$$

- If two events X and Y are mutually exclusive (when one occurs the other cannot occur), the probability that either X or Y will occur is:

Equation $$P(X) + P(Y) \quad (2.8a)$$

- If the events X and Y are independent (not mutually exclusive), the probability that X or Y, or both X and Y, will occur is:

Equation $$P(XY) = P(X) + P(Y) - P(X) \cdot P(Y) \quad (2.8b)$$

Clearly, these rules may be extended to any number of events. However, the standby redundancy situation is an exception to the use of these rules. In a standby redundancy case, dependency must be considered because the failure time distribution of the standby element depends on the state of another element. RBDs cannot deal with sequential failures.

Important! *This guide does not discuss common mode failures. Except in the case of standby redundancy, it is not necessary to assume constant failure rates in order that the expressions for combining reliabilities are valid. Expressions for combining reliabilities can become complicated. The aim here is simply to introduce general principles. Thus, the expressions are concerned only with simple series and redundancy configurations (see also Chapter 4, "Reliability Modelling") and do not relate to systems containing complex redundancy. As a general rule, a system should always be broken down into the simplest independent groups of items. The reliabilities of these groups can then be progressively combined to provide the system reliability.*

Series Group

Consider two items in a series configuration as shown in Figure 2-4.

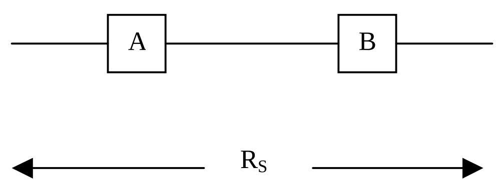


Figure 2-4. Series Configuration

Then, from equations (2.1) and (2.7):

$$R_S(t) = R_A(t) \cdot R_B(t)$$

$$= e^{-\lambda_A t} \cdot e^{-\lambda_B t} \text{ if failures rates are constant}$$

$$\therefore R_S(t) = e^{-(\lambda_A + \lambda_B)t}$$

Because this method can be extended to any number of items, the general expression for a series configuration is:

Equation $$R_S(t) = e^{-(\lambda_1 + \lambda_2 + \lambda_3 + \ldots + \lambda_N)t} \quad \text{(2.9)}$$

Parallel (or Active) Redundancy Group

The simplest case of a parallel redundant group is when it comprises two items, both of which can perform the specified function individually and independently as shown in Figure 2-5.

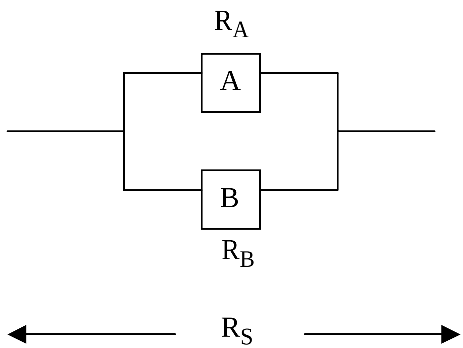


Figure 2-5. Parallel (or Active) Redundancy Configuration

Assuming that item failures are independent (i.e., failure in any one does not affect the behaviour of the other), then there are four possible system states as follows:

- Both A and B functioning → System functioning.
- A failed, B functioning → System functioning.
- A functioning, B failed → System functioning.
- Both A and B failed → System failed.

Because there is only one failure state, it is simpler to evaluate R_S on the basis of the probability of system failure (F_S). R_S is then given by $1 - F_S$. Then:

$$F_S = F_A \cdot F_B$$

$$= (1 - R_A) \cdot (1 - R_B)$$

$$= 1 - R_A - R_B + R_A R_B$$

$$R_S = 1 - F_S$$

$$= R_A + R_B - R_A R_B$$

Using equation (2.1):

$$R_S(t) = e^{-\lambda_A t} + e^{-\lambda_B t} - [e^{-\lambda_A t}][e^{-\lambda_B t}]$$

Equation $$\therefore R_S(t) = e^{-\lambda_A t} + e^{-\lambda_B t} - e^{-(\lambda_A + \lambda_B)t} \quad (2.10)$$

NOTE The system MTTF corresponding to equation (2.10) is given by:

$$MTTF_s = \frac{1}{\lambda_A} + \frac{1}{\lambda_B} - \frac{1}{(\lambda_A + \lambda_B)}.$$

However, the system failure rate, $\lambda_S(t)$, is not equal to $\frac{1}{MTTF_S}$. The quantity λ_S is in fact given by:

$$\lambda_S(t) = \frac{\lambda_A e^{-\lambda_A t} + \lambda_B e^{-\lambda_B t} - (\lambda_A + \lambda_B) e^{-(\lambda_A + \lambda_B)t}}{e^{-\lambda_A t} + e^{-\lambda_B t} - e^{-(\lambda_A + \lambda_B)t}}.$$

It is thus not independent of time.

Standby (or Passive) Redundancy Group

The simplest case of a standby redundant group is shown in Figure 2-6. It comprises one active item that performs the system function and one passive item that becomes active to perform the system function if the first item fails.

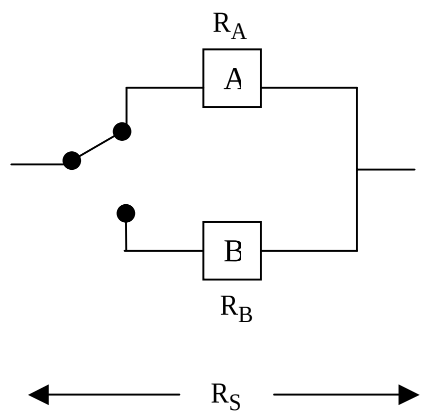


Figure 2-6. Standby (or Passive) Redundancy Configuration

The following are assumed:

- The active failure rate of B only applies when A has failed.
- Any switching device to bring B into use is failure-free.
- The passive failure rate of B is zero.
- Failure rates are constant.

Then, during a time interval, t, three possible outcomes exist:

- A survives for time $t \rightarrow$ System functions.
- A survives for time t_A and B survives for time $t - t_A \rightarrow$ System functions.
- Both A and B fail before $t \rightarrow$ System fails.

Although not derived here, it can be shown that, in this case, the system reliability, R_S, is given by the expression:

Equation

$$R_S(t) = \frac{\lambda_B \cdot e^{-\lambda_A t}}{\lambda_B - \lambda_A} + \frac{\lambda_A \cdot e^{-\lambda_B t}}{\lambda_A - \lambda_B} \qquad (2.11)$$

Where:

λ_A is the active failure rate of A.

λ_B is the active failure rate of B.

It can also be shown that if A and B are identical items:

$\lambda_A = \lambda_B = \lambda$

Then:

Equation

$$R_S(t) = e^{-\lambda t} \cdot (1 + \lambda t) \qquad (2.12)$$

Although the system reliability can still be calculated, where the redundancy is more complex and blocks appear more than once in an RBD, the use of Bayes theorem is required. This is considered further in “Bayes Theorem” on page 4-11.

Combining Reliabilities (Without Repair)

The general principles described in the foregoing sections apply only to systems that are not maintained (i.e., those which cannot be restored to a failure-free condition if they fail during any part of their operational duty cycle).

NOTE Operational duty cycles are explained on page 4-5.

For a repairable system, the methods of computing the probability (R) that the system functions as required must be modified to take into account the **maintainability** and hence the **availability** of the system.

NOTE In this context, **repairable** means repair during an operational duty cycle. (See “Reliability Evaluation when Redundant Sub-systems can be Repaired Before System Failure” on page 4-37.)

Maintainability and availability can be defined in quantitative terms as follows:

- **Maintainability**. The probability that an item can be restored to a serviceable condition within a specified period of time. A most useful measure of maintainability is the quantity Mean Down Time (MDT), which includes administrative and other logistic delays beyond the designer's control.
- **Availability (steady state)**. The proportion of an item's operational duty cycle during which the item is not engaged in any activity preventing its immediate use and is serviceable.

Thus, in the simplest terms, if reliability is identified in terms of MTTF and maintainability in terms of MDT, the intrinsic availability of a system (i.e., that which can be designed in) is given by:

Equation

$$\text{Availability (steady state)} \ (A) = \frac{MTTF}{MTTF + MDT} \quad \text{...} (2.13)$$

Important! *This expression is based on many assumptions, including:*

- *The system is operating continuously except when failed.*
- *Any failures are detected immediately upon occurrence.*
- *The operational duty cycle is large compared with the MTTF and MDT values so that the system can be considered to be in a steady state.*
- *Further failures do not occur during the repairs.*

In practice, the relationships between Availability, MTTF and MDT may be complex if the operational duty cycle is complex. However, this simple expression does serve to illustrate the principles associated with repairable systems.

When considering the probability that a repairable system functions as required, it is often convenient to introduce the concept of system success (SS) and to denote the associated probability as the product of two probabilities:

- *The probability that it is failure-free at some appropriate point within the operational duty cycle (steady state availability, A), and also*
- *The probability that the system survives the remainder of the operational duty cycle, given that it was failure-free at the appropriate point within the cycle (Reliability, $R(t)$).*

Example The missile launch and interception phase is a critical phase in the operation of a guided weapon system. Assume that the surveillance radar is a repairable component that operates continuously for some time prior to launch, and is required to operate throughout the launch and interception phase (time t). Assume also that the failure rate of the radar is constant throughout the duty cycle so that MTTF = 1/λ. Then:

- From equation (2.13), the probability that the radar is failure-free at launch is denoted by A (availability) and is given by:

  $$\frac{1/\lambda}{(1/\lambda + MDT)}$$

- Because the radar is effectively non-repairable during the launch and interception phase (they are too short), the probability that it survives this period is denoted by $R(t)$ (reliability) and is given by:

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

- The probability that the radar is not compromised by failure is denoted by SS (system success) and is thus the product of the above two expressions:

  $$SS = \frac{1}{1 + \lambda \cdot MDT} \cdot e^{-\lambda t}$$

Because MDT will be specified for the equipment concerned, SS can be predicted from this expression.

NOTE The foregoing is intended only to introduce the different philosophy that must be adopted when considering repairable systems.

Total System Reliability

Based on the RBD principles described in “Reliability Block Diagrams” on page 2-11, the functional relationships within each level of assembly, and also between each level of assembly, can be set down for a total system. A simple example is shown in Figure 2-7 on page 2-19.

Note that the levels to which relationships can be developed will vary according to the complexity of the system and the stage of the project. For example, for a complex system:

- During the conceptual and feasibility stages, data will probably be limited to system and sub-system levels.
- In the early design stage, data should be available at the unit level.
- As the detailed design is developed, data will become available at the module and component/part levels.

Having defined the functional relationships for a total system, reliability expressions such as those described in “Combining Reliabilities (No Repair)” on page 2-12 can be used to compute the reliabilities of individual elements within the system, and, progressively, to combine these reliabilities at the higher levels of assembly up to the total system level.

However, it must be noted that standard sources of failure rate data normally provide only **component** or **part** failure rates. Detailed prediction cannot therefore be carried out until the detailed design stage, when component and part population data become available. Before this stage, prediction depends on the use of broader and more comparative methods; for example, by comparison with some similar system or by the broad assessment of the numbers and types of components and parts that may be expected in the future design. (For additional information, see Chapter 3, “Reliability Prediction Methods”.)

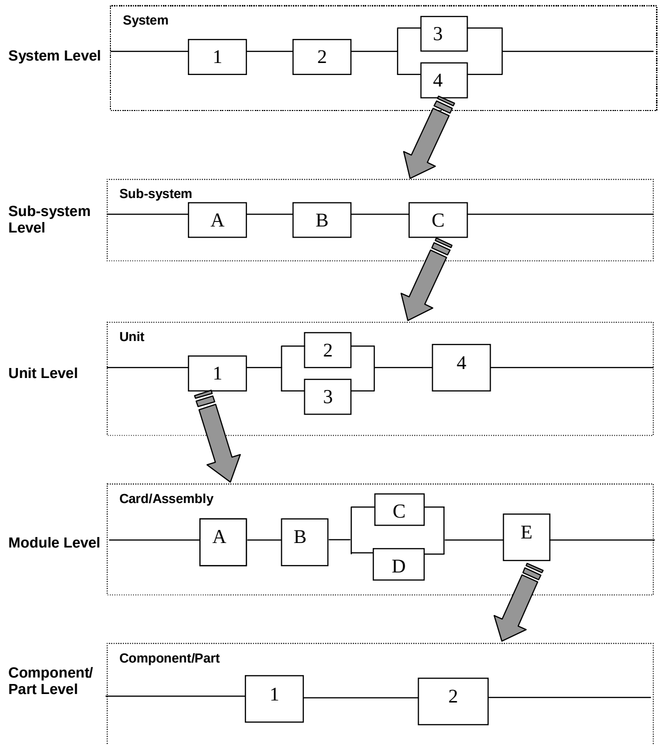


Figure 2-7. Example of a System

Outline of Prediction Process

Based on the considerations described in “General Philosophy of Prediction” on page 2-5, the reliability prediction process generally consists of activities that can be grouped under either **reliability modelling** or **reliability evaluation**.

Reliability Modelling

The activities for reliability modelling include:

- Define the system and its requirements.
- Establish system failure definitions.
- Define operating and maintenance conditions.
- Develop reliability models, (e.g., RBDs).

Reliability Evaluation

The activities for reliability evaluation include:

- Compile component and parts lists.
- Perform component stress analyses (i.e., the stresses associated with the intended application).
- Compute failure rates if constant (or probabilities of survival).
- Combine failure rates if constant (or probabilities of survival).
- Compute system reliability.

NOTE These activities are described more fully in later chapters.

Important! *The extent to which any of the above activities can be implemented will depend upon the data available at the particular time. In principle, however, each activity must be carried out as fully as possible whenever a prediction is attempted.*

Limitations of the Prediction Process

The main limitations of the practical prediction process stem from possible inaccuracies in reliability models, particularly with regard to the following assumptions:

- Constant failure rate during the useful life of an item.
- Independence of items within a system, thereby permitting use of the product rule for combining probabilities.

Important! *The implications of these factors are discussed in the following paragraphs. Other limitations include the lack of appropriate failure rate data, particularly in respect to advanced technology items and mechanical items, and difficulties of accurately modelling the true operating conditions.*

Constant Failure Rate

The assumption of constant failure rate is not essential to compute reliabilities and combine them as described in “General Philosophy of Prediction” on page 2-5. However, constant failure rate is necessary for the reliability distribution to be exponential.

The exponential distribution has an advantage over other statistical distributions in that it is described fully by the single parameter λ , or often by its reciprocal, MTBF, and the majority of standard failure rate data is presented as this single parameter. The added advantage of the exponential distribution is that reliability can be simply computed for series configurations using the sum of the individual item failure rates. (See equation (2.9) on page 2-13.)

In practice of course, the individual items that make up a system may not all have constant failure rates. Some may have reasonably constant failure rates (e.g., some electronic components), and others may have failure rates that increase to varying degrees with time (e.g., wear in mechanical items). Further, some items may not have failure rates in the conventional sense. For example, one-shot explosive devices are usually said to be time-independent.

Example

Consider now a system that is made up of items whose failure rates increase with time. Assume that the system is maintained so that:

- Individual items are replaced before the onset of severe wear-out failures, and in addition,
- Items are replaced as they fail.

The failure rate for new items is lower than for older ones. Thus, the failure rate of the system depends on the ages of the individual items. When all items are new, the system failure rate is low and increases as items age; but, whenever an item is replaced, it reduces the system failure rate. Thus, over a period of time, the system failure rate tends to oscillate, rising and falling in the form of a damped harmonic, and approaches a constant failure rate as illustrated in Figure 2-8.

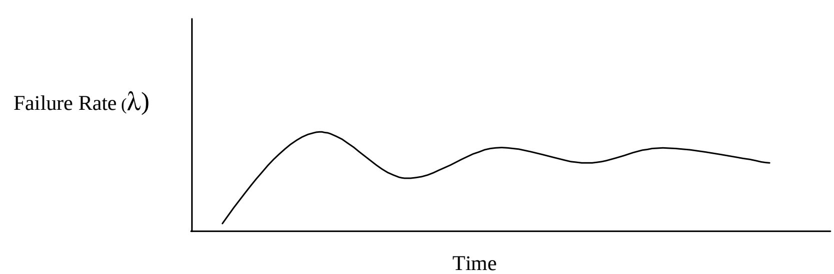


Figure 2-8. Variation of System Failure Rate with Time

From the above considerations, it can be seen that an assumption of constant failure rate is a reasonable basis for predicting the reliability of a complex repairable system in the long run even though all the individual items within the system may not exhibit constant failure rates. Clearly, however, the resulting prediction will be more approximate for systems comprising mainly items with time-related failure rates (e.g., mechanical systems) than for those with more constant failure rates (e.g., electronic systems).

It must also be recognised that the assumption of constant failure rate does not necessarily represent the same failure mechanisms in different types of items. For example, electronic component failures generally occur as a sudden breakdown whereas failures of mechanical parts occur through time-related failure mechanisms such as creep, corrosion, fatigue, wear, etc.. It is often the case that such failures may be foreseen and hence avoided.

Product Rule

The validity of the Product Rule is of particular significance when considering the use of redundancy to improve the reliability of a system. It is shown in "Parallel (or Active) Redundancy Group" on page 2-14 that if two independent items, A and B, are in parallel redundancy, then their combined reliabilities are given by:

$$R_{AB} = R_A + R_B - R_A \cdot R_B$$

Thus if:

$$R_A = R_B = R = 0.9$$

$$R_{AB} = R(2 - R) = 0.99$$

Important! *By putting the two items in parallel and using the Product Rule, a considerable gain in reliability has been achieved for independent items. In practice, however, it may sometimes be questionable whether such independence is really valid.*

Example Consider a situation where the two items are subject to a severe mechanical loading, such as shock through handling or transportation. Assuming that both items are of the same strength and are subject to the same loading, then, if the load exceeds the strength of one to produce failure, it will probably exceed the strength of the other. Such failures are termed **common mode**. In such cases, the Product Rule is invalid.

If both items fail together, then the system reliability (R_s)is the same as if it comprised only one item and would be equal to R . Therefore, if the items were in series, system reliability would be higher than indicated by the Product Rule (i.e., $R_s > R2$), and it would be lower than indicated by the Product Rule if the items were in redundancy (i.e., $R_s < (2R - R^2)$).

Thus, it can be seen that the methods for calculating reliability described in "Parallel (or Active) Redundancy Group" on page 2-14 depend crucially on the assumption of independence of failure occurrence. Where dependence exists, in the form of common mode failures for example, then calculations become more difficult, and in fact are the subject of much current research in the reliability field. As stated earlier in "Combining Reliabilities (Without Repair)" on page 2-16, such analysis is outside the scope of this guide.

NOTE The reader is also reminded that there are now two or more independent items to fail, and hence to maintain and so on. The apparent improvement in reliability comes with a cost.

3. Reliability Prediction Methods

Introduction

Reliability prediction depends essentially upon producing a model that represents the reliability relationships between items comprising a system (which is further described in Chapter 4, “Reliability Modelling”), and then evaluating the various elements within the model to provide a quantitative estimate of the system reliability and its constituent parts. This chapter describes methods that may be used to evaluate reliability at different stages of a project, depending upon the data available at the particular time. Frequent reference is made to the failure rate models described in Chapter 4, “Reliability Modelling”.

The methods that can be used during a project fall into two main categories as follows:

- Those which make use of previous experience, design data and standard failure rate data to give theoretical predictions of the reliability that a design may achieve when it reaches maturity (e.g., after being in service for two to three years). Such methods can be used before any hardware is produced. They include the Similar Equipment, Generic Parts Count, Parts Stress Analysis and Missile Prediction methods. These methods are described in subsequent paragraphs.
- Those which make use of the results of hardware testing to give practical estimates of the reliability that a design is achieving during development and predictions of probable achievement in the future. Methods of testing and mathematical techniques and models for analysing test results are described fully in Reference 1 in Appendix D, “Bibliography”, and are not considered further in this guide.

Reliability Prediction Basics

Reliability predictions fall into two categories:

- **Parts count**. Reliability prediction analyses carried out during the concept stages of a project when exact numbers and types of components are not known.

- **Parts stress**. Reliability prediction analyses carried out later in a project when parts lists are available and the results of component stress analyses are becoming available.

Reliability, R, has already been defined as the characteristic of an item expressed by a probability that it will perform a required function under stated conditions for a stated period of time. R is therefore a probability of failure, in that an item will operate for a stated period of time and then fail.

Now, assume the following:

- The item under consideration is a **series** system, i.e., the failure of one component will cause system failure.
- Each component failure is totally independent of another.

Then, from the Product Rule described on page page 2-22, the reliability of that system, R_S, will be given by:

$$R_S = \prod_{i=1}^{N} R_i$$

Where R_i is the reliability of each of its constituent components.

Now, introducing the time factor t:

$$R_S(t) = \prod_{i=1}^{N} R_i(t)$$

Where:

$R_S(t)$ = The probability that the system will not fail before time t.

$R_i(t)$ = The probability that the i th component of the system will not fail before time t.

Finally, assuming that the reliability of each component, $R_i(t)$, is exponentially (randomly) distributed with a constant failure rate of λ_i, then:

$$R_i(t) = exp(-\lambda_i t)$$

Therefore, the system reliability will be:

$$R_S(t) = \prod_{i=1}^{N} exp(-\lambda_i t)$$

In general, a reliability prediction considers the impact of each component on the overall design in order to determine the reliability of the overall product. This is achieved by summing the failure rates of all the constituent parts of that design. This includes all components, including connectors, interconnections (solder/crimp/welded joints, etc.) and printed circuit cards.

Hence:

$$\lambda_S = \sum_{i=1}^{N} \lambda_i$$

Where:

λ_S = The system failure rate.

λ_i = The failure rate of each of the independent components in the system.

The failure rate model for a component for an operational mode is:

$$\lambda_p = \lambda_B \cdot K_E \cdot K_S$$

Where:

λ_p = The predicted failure rate of the particular component under stated environmental, temperature and electrical stress conditions.

λ_B = The operational base failure rate of the component.

K_E = The environmental factor for the operational environment of the component.

K_S = The temperature and electrical stress factor for the component.

When an item comprises components in **series**, the predicted failure rate (λ_p) of the item can be obtained by summing the predicted failure rates of the individual components. Thus, the predicted operational failure rate of an item is given by:

$$\Sigma\ N \cdot \lambda_B \cdot K_E \cdot K_S$$

Similar Equipment Method

The primary objective of prediction during the early stages of a project (i.e., preliminary study, feasibility study, early project definition) is to provide quantitative estimates of reliability that can be used to:

- Compare design options.
- Establish realistic reliability targets.
- Identify areas of high risk.
- Provide inputs to trade off studies.

In general, such predictions will be concerned mainly with assessments at system and sub-system level and, because information is limited during early stages, will usually involve a considerable degree of engineering judgement.

Outline of Method

The Similar Equipment Method is based on comparison of a proposed design with similar designs for which reliability achievements are known. The best data for making such comparisons is that relating to similar products that:

- Originate from the same design resources, manufacturing facilities and specifications prepared and processed in the same way.
- Are used in similar environments.

The main steps in the method are as follows:

1. Define the proposed system design in terms of its main functions, characteristics, performance and operational requirements, related development time scale, etc., and develop a reliability model.
2. Identify similar equipment designs and their associated development/production histories, reliability achievements and operating environments.
3. Identify significant differences and adjust the relevant reliabilities to take account of such differences.
4. Evaluate and analyse the reliabilities of the proposed design.

NOTE Each of these steps is considered in more detail in the paragraphs that follow.

System Definition and Model

The reliability of any item is influenced by a wide variety of factors, and it is essential that as many of these as possible are taken into account when comparing proposed and existing designs. While not in any order, the factors that should be considered and defined for the proposed system include:

- The purpose and functions of the system or systems.
- The main performance, safety and physical characteristics.
- The worst case reliability requirements.
- The operational and environmental conditions of use.
- The complexity and ‘state of the art’ involved.
- The design and development time scale and cost constraints.
- The facilities and resources available for reliability development testing.

- Whether the proposed design is a natural development of an existing design or is a new concept.
- Whether new manufacturing techniques are required.

This list is not intended to be exhaustive. Any additional factors that may assist in the comparison with similar designs should be noted during system definition. A reliability model should be developed to show the reliability relationships within the proposed system design. (See Chapter 4, “Reliability Modelling”.)

Similar Equipment Data

The data on mature equipments (with which the proposed design will be compared) must be as comprehensive as possible. The reliability that a particular piece of equipment is achieving in service must be determined, as well as the operational and environmental conditions of use associated with the reliability values. This is important because the same equipment can exhibit widely differing reliabilities in different environments and operating conditions. It is also important to establish, whenever possible, the development time scale and effort that was required to bring the reliability of a mature equipment to its current level. In general, data should include, where possible:

- The original reliability requirements.
- The extent of reliability design evaluation activities prior to hardware manufacture.
- The extent of reliability growth testing and the growth rate achieved during development.
- The rate at which design changes were schemed, manufactured and embodied for trial.
- Problem areas encountered during development and early in-service life.
- Analysis of main failure modes to avoid their recurrence.

The above data can then be used to assess the scale of the reliability programme associated with the reliability prediction.

Comparison of Data

The data on the mature equipments and the proposed design must be compared and significant differences must be identified. An engineering analysis of each of the differences must then be carried out, and the adjustment that should be made to the relevant reliability value must be assessed. Ground rules should be established, wherever possible, for making such assessments and should be stated in the analysis. For example, **state of the art** might be divided in four categories as follows:

- Current, well established technology.
- Known, advanced technology.
- Little experience, advanced technology.
- High risk, advanced technology.

Each of these categories might be given a **weighting** factor that could then be used to adjust reliability values.

It may not always be possible to define clear-cut categories for all the various data concerned, but it is most important that the reasoning behind all reliability weighting factors is clearly stated in the analysis.

Care must be taken to make due allowance for any differences in design, development and production resources. Clearly this will be more difficult if the mature equipment being used for comparison originated from different sources. This can lead to large errors in the prediction.

Due to the qualitative nature of the data comparison, the results may frequently depend upon the assumptions made. In general, therefore, reliability values should be assessed for both the **best case** and **worst case** assumptions.

Evaluation and Analysis

The results obtained from the data comparison should be used in the reliability model to evaluate the range of reliability values that the proposed design might be expected to achieve. The conditions associated with each value should be stated (e.g., the necessary reliability programme), and also the extent to which the predicted value depends upon any adjustments made during data comparison. Areas of high risk within the proposed design should be identified. Statements should be made on the nature of the risk and the feasibility of reducing that risk.

Generic Parts Count Method

The Generic Parts Count method is based on the principle that the reliability of any item depends upon the number of parts comprising the item, the failure rates of the individual parts and the environments in which the item is to be used. Basic assumptions of the method are that part failure rates are constant with time, and part failures are independent of each other. Part failure rates are calculated by multiplying **base** failure rates by an appropriate **environmental factor** (K_E).

NOTE The term **parts** is used here in its widest sense and includes electronic components, microelectronic devices, mechanical items, one-shot devices, etc..

The Generic Parts Count method can be used from that stage in a project at which part listings start to become available and onwards. Before detailed lists are available, the method can be applied using estimates of part populations based on previous experience; clearly, however, such an evaluation will provide only a broad estimate of reliability.

Outline of Method

The main steps in the Generic Parts Count method are as follows:

1. Define the proposed system and develop a reliability model.
2. For each block (or area) within the model:
    a. Determine the type and number of each generic part type.
    b. Calculate the failure rate of each generic part type for the appropriate operational conditions.
    c. Sum the failure rates to give the total failure rate for the block (or area). Evaluate the block (or area) reliability.
3. Combine the block (or area) reliabilities as shown by the reliability model to obtain the total system reliability.

NOTE Some blocks in the reliability model may represent items for which reliability is not time-dependent or is expressed as a probability of success. (See Chapter 4, “Reliability Modelling”.) These blocks must be evaluated separately.

The Generic Parts Count method is considered in more detail in the following paragraphs, and a completed example is given in Chapter 4, “Reliability Modelling”.

Worksheets

The method is best applied using worksheets that provide a clear presentation of the data used and aid the processing of the data. Two examples of worksheets are given in Figure 3-1 (Operational Mode) and Figure 3-2 (Non-operational Mode). They are for a hypothetical item using the data listed in Appendix A of this guide.

Note that these examples are shown only for guidance, and are presented separately for clarity in illustrating the detailed method. Other formats could be developed to embrace more than one set of conditions.

(1) Area of Evaluation

System: SRGA Weapon System
Sub-system: Control Unit
Item assessed: Computer
Reliability Block Diagram No: CU1

(2) Operational Conditions

Mode: Operational (Search Mode)
Reliability Time Interval (t): 336 hours (14 days)
Environment: Ground Mobile, G2

(3) Part Population

(4) Part Failure Rate (failures per 10^6 hours)

Parts Description	Qty N	Base Rate λ_B	Env Factor K_E	Predicted Rate $N\lambda_B K_E$	Percentage Contribution %
Capacitors, Tantalum, Solid	15	0.08	2.3	2.76	3.8
Transistors, Silicon, Signal, < 1W	50	0.05	4.4	11.00	15.2
Transistors, Silicon, High Power, > 5W	10	0.09	5.0	4.50	6.2
Diodes, Rectification, Low Power	20	0.12	2.5	6.00	8.3
Integrated Circuits, Digital, < 20 Gates	200	0.03	3.1	18.60	25.8
Resistors, Metal Oxide Film	230	0.02	4.0	18.40	25.5
Connections, Soldered, Hand	1000	0.004	1.0	4.00	5.6
Connections, Welded	2000	0.0017	1.0	3.40	4.7
Connector, Sealed (70 Pins)	1	0.025 x 70	2.0	3.50	4.9

(5) Predicted Item Failure Rate per 10^6 hours = $\Sigma N\lambda_B K_E$ = 72.16 100%

(6) Item Reliability $R(t) = exp(-\lambda t)$

$$R_{CU1} = exp(-72.16 \cdot 10^{-6} \cdot 336)$$
$$= exp(-0.02425)$$

$$R_{CU1} = 0.976046$$

Analyst: Date of Analysis:

Figure 3-1. Example of Generic Parts Count Worksheet (Operational Mode)

(1) Area of Evaluation					
System: SRGA Weapon System Sub-system: Control Unit Item assessed: Computer Reliability Block Diagram No: CU1					
(2) Operational Conditions					
Mode: Non-operational (Storage) Reliability Time Interval (t): 4368 hours (6 months) Environment: Ground Fixed Exposed Storage (GFE)					
(3) Part Population		(4) Part Failure Rate (failures per 10^6 hours)			
Parts Description	Qty N	Base Rate λ_B		Predicted Rate $N\lambda_b$	Percentage Contribution %
Capacitors, Tantalum, Solid	15	0.002		0.03	3.1
Transistors, Silicon, Signal, < 1W	50	0.003		0.15	15.7
Transistors, Silicon, High Power, > 5W	10	0.005		0.05	5.3
Diodes, Rectification, Low Power	20	0.0012		0.024	2.5
Integrated Circuits, Digital, < 20 Gates	200	0.003		0.60	62.9
Resistors, Metal Oxide Film	230	0.0002		0.046	4.8
Connections, Soldered, Hand	1000	0.00002		0.02	2.1
Connections, Welded	2000	0.00001		0.02	2.1
Connector, Sealed (70 Pins)	1	0.0002 x 70		0.014	1.5
Item Base Failure Rate = $\Sigma N\lambda_b$ =				0.954	100%

(5) Predicted Item Failure Rate $= (K_E \Sigma N\lambda_b = 2 \cdot 0.954)$

$= 1.908$ failures per 10^6 hours

(6) Item Reliability

$$R(t) = exp(-\lambda t)$$

$$R_{CU1} = exp(-1.908 \cdot 10^{-6} \cdot 4368336)$$

$$= exp(-0.02425)$$

$$R_{CU1} = 0.9917$$

Analyst: Date of Analysis:

Figure 3-2. Example of Generic Parts Count Worksheet (Non-operational Mode)

System Definition and Model

Define the system and develop a reliability model as described in Chapter 4, "Reliability Modelling". Each block in the RBDs must be identified by an appropriate reference number.

Area of Evaluation

State the area of the system, item to be evaluated and the appropriate block reference number (Figure 3-1 (1) and Figure 3-2 (l)).

Operational Conditions

By reference to the Operational Duty Cycles produced during system definition, define the reliability time interval being considered, the associated environment and whether the item is operational or non-operational during this period (Figure 3-1 (2) and Figure 3-2 (2)).

Parts Populations

Prepare a list of all parts used in the item being evaluated. Group parts by generic part type and record the Quantity (N) of each part type (Figure 3-1 (3) and Figure 3-2 (3)).

The parts listing on the worksheet should include all parts for which generic failure rate data is given in Appendix A, "Data Tables", as follows:

Table	Section Title and Page Number
Table A-2 through Table A-35	"Discrete Electronic and Electro-mechanical Components" on page A-1
Table A-36 and Table A-37	"Connectors" on page A-31
Table A-38 through Table A-47	"Microelectronic Devices (Excluding Hybrids)" on page A-32
Table A-56	"Mechanical Devices" on page A-47

Table 3-1. Generic Failure Rate Tables

Generic failure rate data is not given in this guide for hybrid devices. Such devices must be considered individually, and their failure rates estimated using the model given in Chapter 4, "Reliability Modelling". If all the necessary data is not available during the early design stages, reasoned approximations should be made.

Other guidelines to keep in mind follow:

- All joints and connections should be listed according to their type and should include the connections behind connectors.
- The complexity of microelectronic devices (ICs) should be stated (i.e., number of gates, bits, transistors) because generic failure rate data is related to complexity.
- Pyrotechnical and one-shot devices should not be included in the parts listing on the worksheet because their reliabilities are evaluated separately.

Item Failure Rates

Determine a **base** failure rate for each generic part type by referring to the relevant tables in Appendix A, “Data Tables”. For items in an operational mode (Figure 3-3), also determine an environmental factor appropriate to the operational environment. Calculate the failure rate contribution of each generic part type by multiplying the quantity (N) by the base failure rate (λ_b or λ_B) and the environmental factor (K_E) when the item is in the operational mode. Sum the failure rates to provide:

- The predicted failure rate for an item in the operational mode, i.e., $\Sigma N \lambda_B K_E$. (See Figure 3-1.)
- The predicted failure rate for an item in the non-operational mode, i.e., $\Sigma N \lambda_b$. Determine the **non-operational** environmental factor (K_E) for the particular environment from Table 3-2 and multiply by the base failure rate to obtain the predicted non-operational failure rate for the item, i.e., $K_E \ \Sigma \ N \ \lambda_b$. (See Figure 3-2.)

$$z = \frac{(t-\mu)}{\sigma} \qquad f(z) := \frac{1}{\sqrt{2\cdot\pi}} \cdot e^{\frac{-z^2}{2}}$$

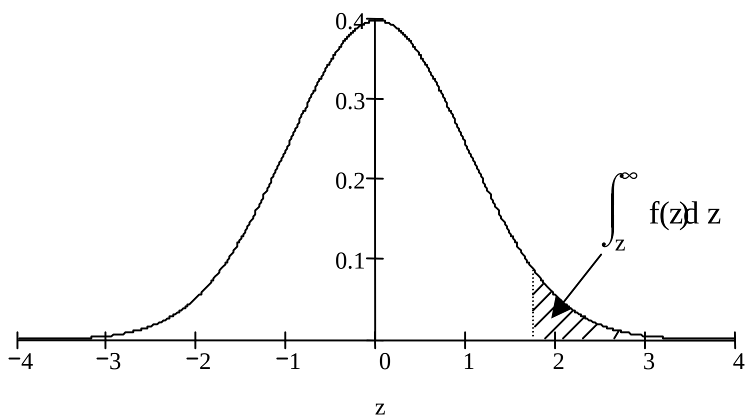


Figure 3-3. Evaluating Areas of the Normal Distribution

$\frac{(t-\mu)}{\sigma}$	.00	.01	.02	.03	.04	.05	.06	.07	.08	.09
0.0	.5000	.4960	.4920	.4880	.4840	.4801	.4761	.4721	.4681	.4641
0.1	.4602	.4562	.4522	.4483	.4443	.4404	.4364	.4325	.4286	.4247
0.2	.4207	.4168	.4129	.4090	.4052	.4013	.3974	.3936	.3897	.3859
0.3	.3821	.3783	.3745	.3707	.3669	.3632	.3594	.3557	.3520	.3483
0.4	.3446	.3409	.3372	.3336	.3300	.3264	.3228	.3192	.3156	.3121
0.5	.3085	.3050	.3015	.2981	.2946	.2912	.2877	.2843	.2810	.2776
0.6	.2743	.2709	.2676	.2643	.2611	.2578	.2546	.2514	.2483	.2451
0.7	.2420	.2389	.2358	.2327	.2296	.2266	.2236	.2206	.2177	.2148
0.8	.2119	.2090	.2061	.2033	.2005	.1977	.1949	.1922	.1894	.1867
0.9	.1841	.1814	.1788	.1762	.1736	.1711	.1685	.1660	.1635	.1611
1.0	.1587	.1562	.1539	.1515	.1492	.1469	.1446	.1423	.1401	.1379
1.1	.1357	.1335	.1314	.1292	.1271	.1251	.1230	.1210	.1190	.1170
1.2	.1151	.1131	.1112	.1093	.1075	.1056	.1038	.1020	.1003	.0985
1.3	.0968	.0951	.0934	.0918	.0901	.0885	.0869	.0853	.0838	.0823
1.4	.0808	.0793	.0778	.0764	.0749	.0735	.0721	.0708	.0694	.0681
1.5	.0668	.0655	.0643	.0630	.0618	.0606	.0594	.0582	.0571	.0559
1.6	.0548	.0537	.0526	.0516	.0505	.0495	.0485	.0475	.0465	.0455
1.7	.0446	.0436	.0427	.0418	.0409	.0401	.0392	.0384	.0375	.0367
1.8	.0359	.0351	.0344	.0336	.0329	.0322	.0314	.0307	.0301	.0294
1.9	.0287	.0281	.0274	.0268	.0262	.0256	.0250	.0244	.0239	.0233
2.0	.02275	.02222	.02169	.02118	.02068	.02018	.01970	.01923	.01876	.01831
2.1	.01786	.01743	.01700	.01659	.01618	.01578	.01539	.01500	.01463	.01426
2.2	.01390	.01355	.01321	.01287	.01255	.01222	.01191	.01160	.01130	.01101
2.3	.01072	.01044	.01017	.00990	.00964	.00939	.00914	.00889	.00866	.00842
2.4	.00820	.00798	.00776	.00755	.00734	.00714	.00695	.00676	.00657	.00639
2.5	.00621	.00604	.00587	.00570	.00554	.00539	.00523	.00508	.00494	.00480
2.6	.00466	.00453	.00440	.00427	.00415	.00402	.00391	.00379	.00368	.00357
2.7	.00347	.00336	.00326	.00317	.00307	.00298	.00289	.00280	.00272	.00264
2.8	.00256	.00248	.00240	.00233	.00226	.00219	.00212	.00205	.00199	.00193
2.9	.00187	.00181	.00175	.00169	.00164	.00159	.00154	.00149	.00144	.00139

Table 3-2. Standard Data Table for Evaluating Areas of the Normal Distribution

$\frac{(t-\mu)}{\sigma}$	.00	.01	.02	.03	.04	.05	.06	.07	.08	.09
3.0	.00135									
3.1	.00097		**Note:** For negative values of Z, the area is equal to one minus the area for the positive value of Z.							
3.2	.00069									
3.3	.00048									
3.4	.00034									
3.5	.00023									
3.6	.00016									
3.7	.00011									
3.8	.00007									
3.9	.00005									
4.0	.00003									

Table 3-2. Standard Data Table for Evaluating Areas of the Normal Distribution (Continued)

Appendix A, “Data Tables”, should normally be used as the source of failure rate data. When other sources are used, they should be recorded on the worksheets and approved by the contracting authority.

Item Reliability

Calculate the reliability of the item for the time interval concerned using the expression:

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

Where:

$R(t)$ = Reliability, i.e., the probability that an item will perform its required function for time t under the specified conditions.

e = The base of the natural logarithms (2.7183).

λ = The predicted failure rate of the item (Table 3-1).

t = The specified time interval at risk.

Examples are shown in the worksheets in Figure 3-1 and Figure 3-2.

Benefits and Limitations

Benefits

The main benefits of the Generic Parts Count method are:

- It allows prediction to be associated with the design process from its earliest stages and provides inputs to assist this process (e.g., comparison of alternative schemes, identification of critical areas, etc.).
- It is relatively quick and simple to apply, particularly if all parts in a system are in a series reliability configuration.

  Note: In the absence of detailed design data to establish precise reliability relationships, the result of assuming series configuration throughout would be a predicted reliability value which was, if anything, pessimistic.

- Where redundancy is present, the simple summation of part failure rates, ignoring redundancy, is useful because it provides the item defect rate.

Limitations

The main limitations of the Generic Parts Count method are:

- It assumes constant failure rate with time. Hence, the higher probabilities of failure during the early and wear-out failure periods are not considered.
- It relies on part failure rate data derived from a variety of sources. Such data is assumed to represent **average** conditions but these may vary widely.
- Failure rate data for mechanical parts is limited, and the method does not therefore take full account of the failure contribution of such parts.

Despite these limitations, it should be remembered that a primary objective of prediction is to provide a basis for **comparison** rather than an absolute reliability value. If the same baseline is used, the comparison will be valid.

Computer Aids

There are many computer programs available to assist in the evaluation of failure rates of components and systems.

Parts Stress Analysis Methods

The Parts Stress Analysis method is a refinement to the Generic Parts Count method in that it involves the same basic steps. Additionally, however, it requires evaluation of each part in terms of its mean operating stress levels in its intended application. This involves the use of detailed failure rate models as described in Chapter 4, “Reliability Modelling”. The Parts Stress Analysis method can be used from that stage in a project when detailed design data becomes available.

Outline of Method

The main steps in the Parts Stress Analysis method are as follows:

1. Define the proposed system and develop a reliability model.
2. For each block (or area) within the model:
   a. List each part comprising the item(s) represented by the block.
   b. Determine the mean operating stress levels for each part and hence the factors appropriate to its particular failure rate model. (See Appendix A, “Data Tables”.)
   c. Calculate the failure rate of each part using the appropriate model.
   d. Sum the failure rates to give the total failure rate for the block (or area). Evaluate the block (or area) reliability.
3. Combine the block (or area) reliabilities as shown by the reliability model to obtain the total system reliability.

NOTE Some blocks in the model may have to be evaluated separately, e.g., one-shot devices, items whose reliabilities are not time-dependent or constant with time, etc.).

General

The system must be defined and a reliability model developed as described in Chapter 4, “Reliability Modelling”. Worksheets should be devised to provide a clear presentation of the data used and to aid processing of the data. Examples of worksheets are given earlier in Figure 3-1 and Figure 3-2, and are used to illustrate the method.

Item Identity and Associated Operational Conditions

State the item to be evaluated and the appropriate block reference number (Figure 4-8). By reference to the operational duty cycles, define the time interval being considered, the associated environment and the operating mode of the item, e.g., full power, standby, etc. (Figure 4-1).

Parts Populations

List each part of the item being evaluated on a separate line of the worksheet, grouping them according to their functions. Note that all parts should be listed, except for small general service items (such as nuts, bolts, screws, washers, etc.). Joints and connections (including those behind connectors) should be listed as totals for a particular type, e.g., hand-soldered, crimped, etc..

Failure rate data may not be available for all parts listed on the worksheets but, by listing every part, the extent of such deficiencies can be assessed, if required.

Stress Analysis

Evaluate each listed part in its intended application, and record the engineering data required to determine the application factors in the relevant failure rate model.

Example The failure rate model for a resistor is as follows:

$$\lambda_p = \lambda_B \cdot K_E \cdot K_S$$

Where:

λ_p = The predicted failure rate of the particular component (in failures/10^6 component operating hours) under stated environmental, temperature and electrical stress conditions.

λ_B = The operational base failure rate of the component.

K_E = The environmental factor for the operational environment of the component.

K_S = The temperature and electrical stress factor for the component.

To determine K_S, the following engineering data is required:

- The temperature in which the resistor is required to operate.
- The rated power of the resistor.
- The mean operating power of the resistor in its intended application.

The stress ratio is:

$$\frac{\text{Mean operating power of the resistor in intended application}}{\text{Rated power of the resistor}}$$

This ratio and the temperature in which the resistor is required to operate enable the appropriate K_S value to be determined from the tables in Appendix A, “Data Tables”.

Microelectronic Devices (Excluding Hybrids)

This section describes the failure rate models to be used for predicting the failure rates of microelectronic devices under stated environmental and operating conditions. It also provides the base failure rates for various types of device and environmental and other factors for use in the models.

During the early stages of a project, the failure rate models may not be applicable due to lack of detailed information. Generic failure rate data for certain devices is therefore provided for use in such cases.

The data contained here also has application when predicting the failure rates of hybrid microelectronic devices. This particular application is discussed in "Hybrid Microelectronic Devices" on page 3-25.

Description of Terms

Terms which are used to describe microelectronic devices are explained below. The meanings are those which have been used throughout this guide.

- **Monolithic**. An integrated circuit in which the entire structure is obtained by processing a single chip of crystalline semi-conductor, i.e., a single chip device.
- i**Bipolar**. A technology using two polarities of carriers, holes and electrons. The active region is the base, several microns beneath the surface, between the emitter and the collector.
- **Unipolar (Metal oxide semi-conductor, MOS)**. A technology using one type of carrier only (holes in p channel MOS; electrons in n channel MOS). Surface effect devices where the active region consists of a channel induced at the silicon/silicon dioxide interface. MOS should be taken to include all metal oxide semi-conductor microcircuits fabricated on various substrates, e.g., PMOS, NMOS, CMOS and MNOS.
- **Small Scale Integration (SSI)**. Devices having complexities less than 10 gates (approximately 40 transistors).
- **Medium Scale Integration (MSI)**. Devices having complexities between 11 and 100 gates (approximately 44 to 400 transistors).
- **Large Scale Integration (LSI)**. Devices having complexities of 100 gates (approximately 400 transistors) or more.
- **Digital device**. A device that operates on the basis of discrete numerical techniques in which the variables are represented by coded pulses or states.
- **Linear (analogue) device**. A device that operates in such a way that the output response is a continuous function of the input signal.

- **Gate**. A device whose output level is determined by certain specific combinations of input levels, i.e., any one of the following functions: AND, OR, NAND, NOR, Exclusive OR and Inverter.
- **Bit**. An abbreviation of **binary digit**. A unit of capacity in a storage device. The capacity, in bits, of a storage device is the logarithm to the base 2 of the number of possible states of the device.

Failure Rate Mode General Expression

The Parts Stress Analysis models are based on the concept that the overall failure rate of an integrated circuit is the sum of two failure rate contributions:

- A contribution (C_1) due to failure mechanisms that are accelerated by temperature and electrical bias.
- A contribution (C_2) due to failure mechanisms that result from indirect mechanical stresses and also from indirect mechanical stresses such as those caused by thermal expansion.

C_1 and C_2 are termed **Complexity Failure Rates** because they are related to the complexity of any particular device. In effect, they represent the **base failure rate** of the device.

To adjust the two failure rate contributions (C_1 and C_2) for the particular conditions in which a device is to be applied, the base failure rates are weighted by factors, which are related to the operating conditions. The C_1 failure rate is adjusted by a temperature acceleration factor (K_T), which depends upon junction Temperature (T_j) and the C_2 failure rate by an environmental factor (K_E), which depends upon the particular operational environment in which the device is to be used.

Other considerations affecting the operational failure rate of a device are the number of active current-carrying pins and the quality screening and inspection process applied during manufacture. These are taken into account by means of further weighting factors, K_p and K_Q.

From the above considerations, the predicted failure rate (λ_p) of a microelectronic device is given by the general expression:

Equation

$$\lambda_p = (C_1 \cdot K_T + C_2 \cdot K_E) \cdot (K_p) \cdot (K_Q) \quad (3.1)$$

Where:

λ_p = The predicted operational failure rate (in failures/10^6 component operating hours) of a microelectronic device under stated environmental and operating conditions.

C_1 and C_1 = The operational base failure rates for the particular device.

K_T The temperature acceleration factor for the device.

K_E = The environmental factor for the operational environment of the device.

K_p = The active pin factor for the device.

K_Q = The quality factor for the screening level under which the device is procured.

Applicability of the General Expression

For prediction purposes, microelectronic devices can be divided into four main categories:

- Digital - Small and Medium Scale Integration (SSI/MSI).
- Digital - Large Scale Integration (LSI).
- Memories.
- Linear devices.

The general expression given at equation (3.1) can be applied to all the above categories except linear devices. For linear devices, the active pin factor is in effect unity (due to the low number of pins involved), and the model is thus:

Equation

$$\lambda_p = (C_1 \cdot K_T + C_2 \cdot K_E) \cdot K_Q \quad (3.2)$$

(linear devices)

Failure Rate Data and Factors

Generic failure rate data and environmental factors are given in Table A-38 and Table A-39 for use in the early design stages when detailed information may be insufficient to permit the use of failure rate models. Failure mode data is also included in these tables.

When using generic data, the predicted failure rate (λ_p) in the operational or non-operational mode is given by the expressions:

Equations

Operational mode:

$$\lambda_p = \lambda_B \cdot K_E \quad (3.3)$$

Non-operational mode:

$$\lambda_p = \lambda_b \quad (3.4)$$

Complexity Failure Rate Data and Model Factors

The failure rate data and the factors to be used in the models given in equations (3.1) and (3.2) above are listed in Table A-41 through Table A-47 inclusive. For ease of use, the failure rate models, factors and the data tables appropriate to each category of device are summarised in Table A-40. It should be noted that:

- For prediction purposes, SSI and MSI devices are grouped together because the same model and data apply to each.
- The Quality factor, K_Q (Table A-41), is keyed to the BS 9000 and BS CECC screening level against which a device is procured. This level, and also the manufacturer's name and product code, is given in PD 9002, "BS 9000 and BS CECC Qualified Products List".

Application of Models

To apply failure rate models, certain characteristics of the device under consideration must be determined. Examples of such characteristics include:

- The number of gates, circuit transistors or bits, as applicable.
- The type of logic (e.g., TTL, I2L or DTL).
- The junction temperature, T_j. Note that a method for estimating this parameter, when physical measurement is impracticable, is given in Table A-43.

Device characteristics can be obtained from manufacturers' data books and various other publications.

Examples of Application of Models

Four examples of the use of the failure rate models and the data tables follow.

Example **SSI/MSI Device**

Task: A TTL digital bipolar device with 10 gates and 16 package leads is being used in an **air protected** environment at $60°C$ ambient temperature. It was procured under BS 9000 screening level S2. Predict its failure rate.

Solution:

Step 1: Identify the appropriate failure rate model from Table A-40. Because the device has less than 100 gates, the SSI/MSI digital model applies. The failure rate is given by:

$$\lambda_p = K_Q \cdot K_p \cdot (C_1 \cdot K_T + C_2 \cdot K_E) \text{ failures per } 10^6 \text{ hours.}$$

Step 2: Determine the appropriate values of K_Q, K_E and K_T from Table A-41 through Table A-43 respectively:

- From Table A-41, $K_Q = 1.0$ (Screening level S2).
- From Table A-42, $K_E = 4.0$ (Air protected, Al).
- From Table A-43, Note 1, K_{T1} is the appropriate factor for the device (TTL digital bipolar).

From Table A-43, Note 3:

$$T_j = T + 10°C \text{ (No. of gates < 30)}$$
$$= 70°C$$
$$K_{T1} = 0.83$$

Step 3: Determine the appropriate values for C_1, C_2 and K_p. With 10 gates, the device is SSI/MSI and so, from Table A-47:

$$C_1 = 0.0061 \text{ and } C_2 = 0.0089$$
$$K_p = 1.0 \text{ (No. of package leads < 24)}$$

Step 4: Calculate λ_p by inserting the values derived above into the mode in Step 1:

$$\lambda_p = (1.0) \cdot (1.0) \cdot \{(0.0061) \cdot (0.83) + (0.0089) \cdot (4.0)\}$$
$$= 0.041 \text{ failures per } 10^6 \text{ hours}$$

Example **Linear Device**

Task: A monolithic linear bipolar device with 23 transistors is being used in a **ship protected** environment at $60°C$ ambient temperature. It was procured under BS 9000 screening level S2. Predict its failure rate.

Solution:

Step 1: From Table A-40, the failure rate model for linear devices is:

$$\lambda_p = K_Q \cdot (C_1 \cdot K_T + C_2 \cdot K_E) \text{ failures per } 10^6 \text{ hours.}$$

Step 2: The appropriate values of K_Q, K_E and K_T are:

- From Table A-41, $K_Q = 1.0$ (Screening level S2).
- From Table A-42, $K_E = 4.0$ (Ship protected, Sl).
- From Table A-43, Note 1, K_{T2} is the appropriate factor for the device.

From Table A-43, Note 3:

$$T_j = 60°C + 10°C \text{ (Transistors < 120)}$$
$$= 70°C$$
$$K_{T2} = 3.6$$

Step 3: From Table A-45, entering with 23 transistors:

$$C_1 = 0.0061 \text{ and } C_2 = 0.015$$

Step 4: Calculate λ_p by inserting the values derived above into the model in Step 1:

$$\lambda_p = (1.0) \cdot \{(0.0061) \cdot (3.6) + (0.015) \cdot (4.0)\}$$
$$= 0.082 \text{ failures per } 10^6 \text{ hours}$$

Example **LSI Device**

Task: A bipolar digital TTL LSI device is being used in a **ground fixed** environment at $40°C$ ambient temperature. The logic diagram of the device shows 128 package leads, 164 gates and 8 flip-flops (each flip-flop = 8 gates), making a total of 228 gates. It was procured under BS 9000 screening level S3. Predict its failure rate.

Solution:

Step 1: From Table A-40, the failure rate model for LSI devices is:

$$\lambda_p = K_Q \cdot K_p\{C_1 \cdot K_T + C_2 \cdot K_E\} \text{ failures per } 10^6 \text{ hours.}$$

Step 2: The appropriate values of K_Q, K_E and K_T are:

- From Table A-41, $K_Q = 2.5$ (Screening level S3).
- From Table A-42, $K_E = 1.0$ (Ground fixed, Gl).
- From Table A-43, Note 1, K_{T1} is the appropriate factor for digital TTL devices.

From Table A-43, Note 3:

$$T_j = 40°C + 25°C \text{ (Gates > 30)}$$
$$= 65°C$$
$$K_{T1} = 0.67$$

Step 3: From Table A-46, entering with 228 gates:

$$C_1 = 0.051 \text{ and } C_2 = 0.027$$
$$K_p = 1.2 \text{ (No. of package leads > 64)}$$

Step 4: Calculate λ_p by inserting the values derived above into the model in Step 1:

$$\lambda_p = (2.5)(1.2)\{(0.051)(0.67) + (0.027)(1.0)\}$$
$$= 0.184 \text{ failures per } 10^6 \text{ hours}$$

Example Memory

Task: A 512 bit Bipolar PROM using 16 package leads is being used in a **ground fixed** environment at $40°C$ ambient temperature. It was procured under BS 9000 screening level S4. Predict its failure rate.

Solution:

Step 1: From Table A-40, the failure rate model for memory devices is:

$$\lambda_p = K_Q \cdot K_p\{C_1 \cdot K_T + C_2 \cdot K_E\} \text{ failures per } 10^6 \text{ hours.}$$

Step 2: The appropriate values of K_Q, K_E and K_T are:

- From Table A-41, $K_Q = 5.0$ (Screening level S4).
- From Table A-42, $K_E = 1.0$ (Ground fixed, Gl).
- From Table A-43, Note 1, K_{T1} is the appropriate factor for memory devices.

From Table A-43, Note 3:

$$T_j = 40°C + 25°C \text{ (All memory devices)}$$
$$= 65°C$$
$$K_{T1} = 0.67$$

Step 3: From Table Table A-47, entering with 512 bits:

$$C_1 = 0.012 \text{ and } C_2 = 0.0045$$
$$K_p = 1.0 \text{ (No. of package leads < 24)}$$

Step 4: Calculate λ_p by inserting the values derived above into the model in Step 1:

$$\lambda_p = (5.0)(1.0)\{(0.012)(0.67) + (0.0045)(1.0)\}$$
$$= 0.063 \text{ failures per } 10^6 \text{ hours}$$

Hybrid Microelectronic Devices

A hybrid integrated circuit comprises a combination of two or more integrated circuit types, or one integrated circuit type and discrete components. This section describes the failure rate model to be used for predicting the failure rate of a hybrid device under stated environmental and operating conditions. However, because the model involves both discrete components and integrated circuits, it is also necessary to refer to the tables in Appendix A for discrete electronic and electro-mechanical components and for microelectronic devices.

This section describes the failure rate model for a hybrid device and provides failure rates and factors for those characteristics that are peculiar to a hybrid device. Other failure rates and factors that are part of the total model are contained in the tables found in "Discrete Electronic and Electro-mechanical Components" on page A-1 and the tables found in "Microelectronic Devices (Excluding Hybrids)" on page A-32. An example is given of the application of the model.

Failure Rate Model for a Hybrid Device

The failure rate model for a hybrid device is based on the concept that the overall failure rate of a hybrid device depends upon the following:

- The failure rate contribution of the individual integrated circuits and/or discrete components (λ_C) that form the hybrid device. Because the components of a hybrid device are relatively free of the many parasitic elements that may be associated with monolithic devices, the failure rates (λ_C) are adjusted by a **die correction factor**, K_G, depending upon the type of component concerned.
- The failure rate contributions of:
  - Each of the chip or substrate resistors, λ_r, depending upon the hybrid package temperature.
  - Each of the interconnections within the hybrid, λ_I, depending upon the type of connection and the package temperature.
  - The hybrid package, λ_S, depending upon the package temperature and seal perimeter.

  Each of the above failure rate contributions will further depend upon the intended operational environment of the device and its particular circuit function. Therefore, the failure rates are adjusted by an **environmental factor**, K_E, and a **circuit function factor**, K_F.
- The failure rate contributions derived from the above will also depend upon the mechanical complexity of the hybrid device as a whole and the screening process to which it is subjected during manufacture. Therefore, the failure rates are adjusted finally by a **density factor**, K_B, and a **quality factor**, K_Q.

From the above considerations, the predicted failure rate (λ_p) of a hybrid microelectronic device is given by the expression:

Equation

$$\lambda_p = \{\Sigma N_C \cdot \lambda_C \cdot K_G + (N_r \cdot \lambda_r + \Sigma N_I \cdot \lambda_I + \lambda_s)K_F \cdot K_E\} \cdot K_Q \cdot K_D \qquad (3.5)$$

Where:

λ_p = The predicted operational failure rate (in failures/10^6) of a hybrid microelectronic device under stated environmental and operating conditions.

N_C = The number of discrete components or integrated circuits of a particular type.

λ_C = The operational failure rate of the particular discrete component (Table A-2 through Table A-35) or integrated circuit (Table A-38 through Table A-47).

K_G = The die correction factor appropriate to the particular discrete component or integrated circuit (Table A-48).

N_r = The number of chip or substrate resistors.

λ_r = The **base** failure rate of the chip or substrate resistors (Table A-49).

N_I = The number of interconnections of a particular type.

λ_I = The **base** failure rate of the particular type of interconnection depending upon the package temperature (Table A-50).

λ_S = The **base** failure rate of the hybrid package depending upon the package temperature and seal perimeter (Table A-51).

K_F = The circuit function factor (Table A-52).

K_E = The environmental factor appropriate to the operational environment of the device (Table A-53).

K_Q = The quality factor appropriate to the screening level under which the device is procured (Table A-54).

K_D = The density factor appropriate to the mechanical complexity of the device (Table A-55).

Failure Rate Data and Factors

The failure rate data and factors which are peculiar to the hybrid failure rate model given in equation (3.5) are listed in Table A-48 through Table A-55. When calculating the operational failure rates (λ_C) of particular discrete components or integrated circuits, the methods and data given in Chapter 2, “General Philosophy and Process of Reliability Prediction”, and/or Chapter 4, “Reliability Modelling”, must be used as appropriate. However, the die correction factor, K_G, that must be applied to these failure rates is that given in Table A-48.

Number of Interconnections

The following points must be observed when counting the number of interconnections (N_I) to be used in the model:

- Each active (current-carrying) wire and each beam lead or solder blob should be counted as one interconnection.
- Redundant interconnections should be counted as only one interconnection.
- A bond should be considered bimetallic if any one of the bond interfaces involves more than one type of metal.
- Active die attach bonds (die to substrate bonds) should not be counted as interconnections.
- If an accurate count of interconnections cannot be obtained, the approximations in Table 3-3 may be made:

Component	Number of Interconnections
Each IC chip bonding pad	1
Each transistor	2
Each diode	1
Each capacitor	2
Each external lead	1
Each chip resistor	2

Table 3-3. Approximations for Number of Interconnections

Packages Enclosing More than One Substrate

When a hermetic package encloses more than one substrate, each substrate should be treated as a separate hybrid microcircuit. Each substrate should include its own density factor (K_D) and its own function factor (K_F), but only the substrate mounted on or serving as the package header should be allocated a package failure rate (λ_S). For all other substrates, $\lambda_S = 0$. The failure rate for the complete hybrid microcircuit package will be the sum of the failure rates for the individual substrates.

Multi-layered Metallisation

The model is valid for up to three layers of metallisation (i.e., metal connector paths on the semiconductor die).

Example of Application

An example of the use of the failure rate model for a hybrid device and the data tables follow.

Example **Hybrid Microcircuit Device**

Task: A hybrid microcircuit device is being used in a **ship protected** environment at a package temperature of $65°C$. The device has 28 gold/aluminium connections; 6 solder connections, 1 die linear with 16 transistors; 1 die linear with 24 transistors; 2 Si PNP transistors, power < 5w at 50% stress ratio; 4 Si diodes, power > 20w at 50% stress ratio; 4 capacitors, ceramic chip, 50% stress ratio; and 14 network, thick film resistors with 5-10% tolerance. The package is a hermetic flat pack with a seal length of 1.2 inches by 0.8 inches, and the substrate dimensions are 0.8 inches by 0.6 inches. The device is to be procured under BS 9000 screening level S2. Predict its failure rate.

Solution:

Step 1: The hybrid microcircuit device model applies. That is, from equation (3.5):

$$\lambda_p = \{\Sigma N_c \cdot \lambda_C \cdot K_G + (N_r \cdot \lambda_r + \Sigma N_I \cdot \lambda_I + \lambda_s)K_F \cdot K_E\} \cdot K_Q \cdot K_D$$

failures per 10^6 hours.

Step 2: Calculate $\Sigma N_c \cdot \lambda_C \cdot K_G$, which is the sum of the adjusted failure rates of the two linear die, the two transistors, the four diodes and the four capacitors:

Step 2.1: Linear Die 1 and 2

- Refer to Appendix A, “Data Tables”, and determine the model appropriate to the linear die, i.e., from Table A-40:
  $\lambda_C = K_Q(C_1 \cdot K_{T2} + C_2 \cdot K_E)$
- From the Appendix A tables, determine the appropriate base failure rates and factors for each die, as follows:

Table	Factor	Die 1	Die 2
Table A-41	K_G	1.0 (S2 Screening level)	1.0 (S2 Screening level)
Table A-44	C_1	0.0046 (16 Transistors)	0.0063 (24 Transistors)
Table A-44	C_2	0.012 (16 Transistors)	0.015 (24 Transistors)
Table A-42	K_E	4.0 (Ship protected)	4.0 (Ship protected)
Table A-43	K_{T2}	5.0 (Linear device $T_j = 75°C$)	5.0 (Linear device $T_j = 75°C$)

$$\therefore \text{Die 1} \quad \lambda_C = (1.0)\{(0.0046)(5.0) + (0.012)(4.0)\}$$
$$= 0.071 \text{ failures per } 10^6 \text{ hours}$$

$$\therefore \text{Die 2} \quad \lambda_C = (1.0)\{(0.0063)(5.0) + (0.015)(4.0)\}$$
$$= 0.915 \text{ failures per } 10^6 \text{ hours}$$

- From Table A-48:

  $K_G = 0.6$ for each device (both linear).

- There is one of each die so, in each case, $N_C = 1$. Therefore, from above, $N_C \cdot \lambda_C \cdot K_G$ for each die is:
  - Die 1 = $(1.0)(0.071)(0.6) = 0.0426$ failures per 10^6 hours
  - Die 2 = $(1.0)(0.0915)(0.6) = 0.0549$ failures per 10^6 hours

Step 2.2: Discrete Components

- Determine the model appropriate to discrete components, that is:

$$\lambda_C = \lambda_B \cdot K_E \cdot K_S$$

- From Appendix A tables, determine the appropriate base failure rates and factors for each type of component, as follows:

Value	Transistor	Diodes	Capacitors
λ_B	0.07	0.20	0.10
K_E	5.9 (Ship protected)	1.2 (Ship protected)	1.2 (Ship protected)
K_S	1.26 ($6°C$) (0.5 stress ratio)	0.67 ($65°C$) (0.5 stress ratio)	1.73 ($65°C$) (0.5 Stress ratio)
$\lambda_C = \lambda_B \cdot K_E \cdot K_S$	0.521	0.161	0.208

- From Table A-48, determine the K_G factor for each component type, i.e.:

	Transistors	Diodes	Capacitors
$K_G =$	0.40	0.20	0.80

- From above, $N_C \cdot \lambda_C \cdot K_G$ or each discrete component type is, as follows:

Component Type	N_C	λ_C	K_G	$N_C \cdot \lambda_C \cdot K_G$
Transistors	2	0.521	0.40	0.417
Diodes	4	0.161	0.2	0.129
Capacitors	4	0.208	0.80	0.666

Step 2.3: From Steps 2.1 and 2.2

$$\Sigma N_C \cdot \lambda_C \cdot K_G = 0.0426 + 0.0549 + 0.417 + 0.129 + 0.666$$
$$= 1.3095 \text{ failures per } 10^6 \text{ hours}$$

Step 3: Calculate $N_r\lambda_r$, which is the failure rate of the network resistors. For the number of network resistors, $N_r = 14$. From Table A-49 ($65°C$ package temperature), $\lambda_r = 0.00015$ failures per 10^6 hours.

$$\therefore N_r\lambda_r = (14)(0.00015)$$
$$= 0.0021 \text{ failures per } 10^6 \text{ hours}$$

Step 4: Calculate $\Sigma N_1\lambda_1$, which is the failure rate of the interconnections, using Table A-50.

Connection Type	N_1	λ_1	$N_1\lambda_1$
Gold/Aluminium	28	0.0013	0.0364
Solder	6	0.000871	0.0052

$$\therefore \Sigma N_r\lambda_r = 0.0416 \text{ failures per } 10^6 \text{ hours}$$

Step 5: Calculate λ_S, which is the package failure rate, using Table A-51.

$$\text{Seal perimeter} = (2 \cdot 1.2'') + (2 \cdot 0.8'')$$
$$= 4.0''$$
$$\text{Package temperature} = 65°C$$
$$\therefore \lambda_S = 0.0951 \text{ failures per } 10^6 \text{ hours}$$

Step 6: Determine the appropriate values for the factors K_F, K_E, K_Q and K_D.

- From Table A-52, $K_F = 1.25$ (linear hybrid device)
- From Table A-53, $K_E = 2.0$ (Ship protected, S1)
- From Table A-54, $K_Q = 1.0$ (Screening level S2)
- From Table A-55, Density $= \dfrac{\text{No. of Interconnections}}{\text{Substrate area} + 0.10}$

$$= \frac{34}{0.48 + 0.10} = 58.62$$
$$K_D = 1.34$$

Step 7: Calculate the predicted failure rate, λ_p, by substituting the results from Steps 2 through 6 in the failure rate model in Step 1.

$$\lambda_p = \{\Sigma N_c \cdot \lambda_C \cdot K_G + (N_r \cdot \lambda_r + \Sigma N_I \cdot \lambda_I + \lambda_s) \cdot K_F \cdot K_E\} \cdot K_Q \cdot K_D$$

failures per 10^6 hours

$$= (\{1.3095 + (0.0021 + 0.0416 + 0.0951)(1.25)(2.0)\} \cdot (1.0)(1.34))$$

$$= (1.3095 + 0.347) \cdot 1.34$$

$$\lambda_p = 2.220 \text{ failures per } 10^6 \text{ hours}$$

Failure Rates and K Factors

For each listed part, record the operational base failure rate of the part. Using the engineering data recorded on the worksheet and any other design or manufacturing considerations (e.g., quality screening policy), determine the K factors appropriate to the intended use of the part.

Calculate the predicted failure rate for each part by inserting the recorded values of base failure rates and K factors in the appropriate failure rate model for either operational or non-operational modes. (See Table A-57 and Table A-58.)

Sum the predicted failure rates of the individual parts to give the predicted failure rate of the item.

Failure rate models, data and K factors are described fully in Appendix A tables as follows:

Table	Section Title and Page Number
Table A-2 through Table A-35	"Discrete Electronic and Electro-mechanical Components" on page A-1
Table A-36 and Table A-37	"Connectors" on page A-31
Table A-38 through Table A-47	"Microelectronic Devices (Excluding Hybrids)" on page A-32
Table A-48 through Table A-55	"Microelectronic Hybrid Devices" on page A-42
Table A-56	"Mechanical Devices" on page A-47

Table 3-4. Generic Failure Rate Tables

The data tables in Appendix A should normally be used as the source of failure rate data. When other sources are used, they should be recorded on the worksheets and approved by the contracting authority.

Item Reliability

Calculate the reliability of the item for the time interval concerned using the expression:

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

This method is described in “Item Reliability” on page 3-13.

Benefits and Limitations

Benefits

The main benefits of the method for a hybrid device are:

- It uses detailed design data and takes account of the various operating, environmental and manufacturing conditions that affect failure rates. It thereby ensures that detailed design improvements are properly reflected in the reliability predictions.
- It assists the design process by highlighting overstressed parts and marginal stress levels in the design. This reduces the risk of unreliability through inadequate design by ensuring that all parts operate within their specified rated capabilities. Thermal evaluation ensures that the design configuration provides adequate heat dissipation characteristics.
- It ensures that reliability considerations are an integral part of the design process.

Limitations

The main limitations of the method for a hybrid device are:

- Despite the detailed nature of the method, it will still only provide a broad estimate of in-service reliability due to the difficulties in modelling failure rates and reliability accurately. These difficulties are common to all reliability prediction methods.
- The limitations which apply to the Generic Parts Count method described on page page 3-6 also apply here.

Despite these limitations, the method provides a valuable aid to the design process, from a reliability standpoint. It provides quantitative measures for comparison and aids decision making.

Computer Aids

A number of computer programs are available to assist in the evaluation of parts-stress reliability predictions.

Reliability Prediction for Items Prone to Wear-Out

The foregoing reliability prediction methods are based on the assumption that failure rates are constant, and hence that a preventative maintenance policy will be applied to ensure that items subject to wear-out are replaced before significant failures occur due to wear-out. However, if such a policy is in any doubt, the reliability of such items must be evaluated separately, as described below, and taken into account in the overall prediction for a system.

Items in the system that could be required to function beyond one third of their estimated mean life should be identified. Their reliabilities should be evaluated for the time interval (τ) of interest, bearing in mind that such reliabilities will be **age dependent**. In other words, a system comprising items subject to wear-out will have a probability of surviving a mission of duration τ, depending on the age T of the system at the beginning of the mission.

The probability of failure-free operation from **new** to age T is $R(T)$. So, the probability of surviving a further time τ (given that the system has survived from new to T), is $R(T, \tau)$. However, the probability of surviving from new to $T + \tau$ is simply $R(T + \tau)$. It thus follows that $R(T + \tau) = R(T, \tau) \cdot R(T)$, from which we see that:

$$R(T, \tau) = \frac{R(T + \tau)}{R(T)}$$

Based on the assumption that times to wear-out failure can be represented by the normal distribution, the numerator of the above expression is:

$$\frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_{\frac{T + \tau - \mu}{\sigma}}^{\infty} exp\left(\frac{-z^2}{2}\right) dz$$

And, the denominator is:

$$\frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_{\frac{T - \mu}{\sigma}}^{\infty} exp\left(\frac{-z^2}{2}\right) dz$$

Note: If T, μ, σ and τ can be quantified, numerical values for the above integrals can be obtained using standard (cumulative) Normal probability tables.

Thus, $R(T, \tau, \mu, \sigma)$ is given by:

$$R(T, \tau, \mu, \sigma) = \frac{\frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_{\frac{T + \tau - \mu}{\sigma}}^{\infty} exp\left(\frac{-z^2}{2}\right) dz}{\frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_{\frac{T - \mu}{\sigma}}^{\infty} exp\left(\frac{-z^2}{2}\right) dz}$$

In the above:

$R(T, \tau, \mu, \sigma)$ = The probability of survival for time τ from age T.

z = $\frac{(t - \mu)}{\sigma}$

σ = The standard deviation of the distribution.

τ = A variable denoting mission time.

μ = The mean life of the item.

Note that $z = 0$ when $t = \mu$; therefore, negative values of z refer to times (t) prior to the mean (μ).

It is interesting to observe that whenever mission times start from **new** ($T = 0$), the equation for reliability becomes:

$$R(T, \tau, \mu, \sigma) = \frac{\frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_{\frac{\tau - \mu}{\sigma}}^{\infty} exp\left(\frac{-z^2}{2}\right) dz}{\frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_{\frac{-\mu}{\sigma}}^{\infty} exp\left(\frac{-z^2}{2}\right) dz}$$

Observe that the limits for z in the numerator correspond to time $t = \tau$ to infinity and in the denominator to time $t = 0$ to infinity. The denominator therefore can be regarded as a normalising factor to take into account that negative values of t do not exist so that the times to failure for systems subject to wear-out follow a **truncated** normal distribution.

Prior to hardware testing, values of estimated mean life (μ) and assumed standard deviation (σ) should be used in the above expression. Values of standard deviation generally lie between one-sixth and one-third of the mean life value, and so an average standard deviation should be assumed equal to one-quarter of the estimated mean life value.

Figure 3-4 shows, as an example, the failure-time density functions applicable to an item with a mean life (μ) of 300 hours, for standard deviation value (σ) equal to 50 hours ($\frac{\mu}{6}$), 75 hours ($\frac{\mu}{4}$) and 100 hours ($\frac{\mu}{3}$).

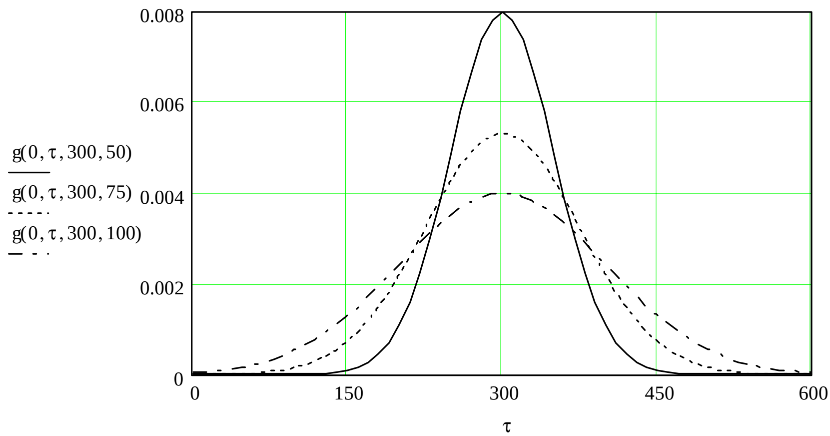


Figure 3-4. Variation in Density Function with Standard Deviation (Plotted for a Mean Life Equal to 300 Hours)

It can be seen that as the standard deviation increases, wear-out failures are more widely distributed about the mean life time. Hence, the larger the standard deviation, the earlier wear-out failures begin to affect reliability. The reliability associated with failure-time density function can be determined by integration, because:

$R(t) = \int_t^{\infty} f(\tau) d\tau$ so that $R(0) = 1$ where $f(\tau)$ denotes the truncated normal pdf.

Figure 3-5 shows a plot of this reliability function for each density function plotted in Figure 3-4. It should be noted that wear-out failures are negligible up to $t = 30$ hours (i.e., one-tenth of the estimated mean life μ). Providing the standard deviation applicable to the item's life is $< \mu/6$, wear-out failures can be assumed negligible up to $t = 150$ hours (i.e., one-half of the estimated mean life μ).

The predicted reliabilities of wear-out items, derived as shown in Figure 3-5, should be combined with the reliability values for constant failure rate items according to the relationships shown in the system reliability model.

Reliability $R(t) = \int_t^{\infty} f(\tau)\,d\tau$

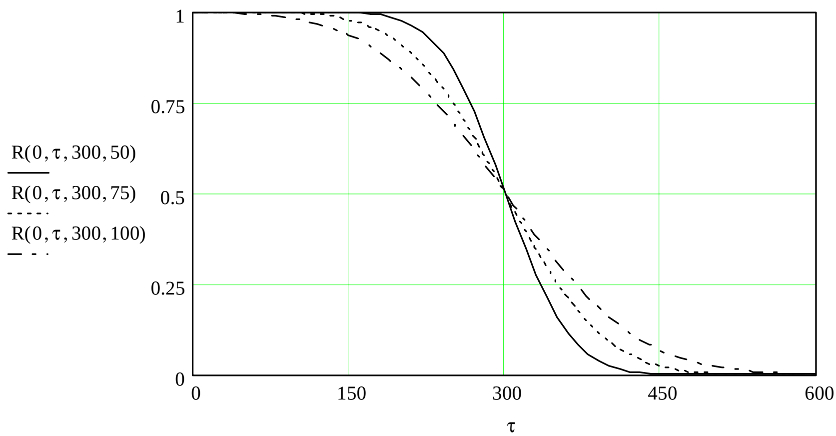


Figure 3-5. Variation in Reliability with Standard Deviation (Plotted for a Mean Life Equal to 300 Hours)

Figure 3-6 shows, as another example, the failure-time density functions applicable to an item with a mean life (μ) of 100 hours, for standard deviation value (σ) equal to 50 hours ($\frac{\mu}{6}$), 75 hours ($\frac{\mu}{4}$) and 100 hours ($\frac{\mu}{3}$).

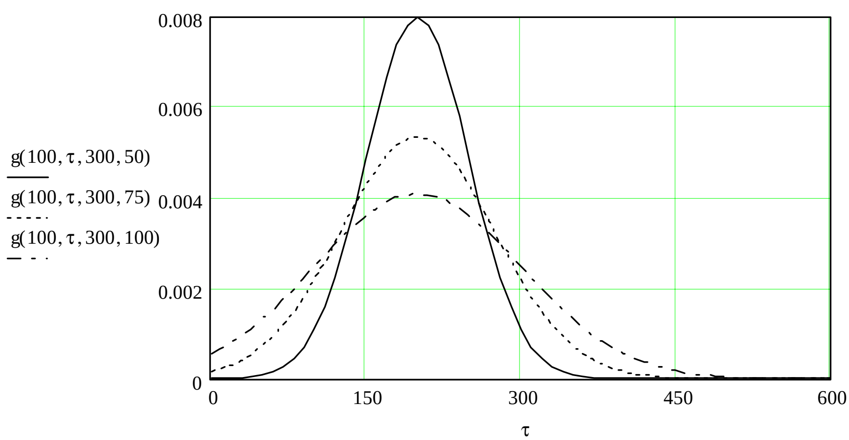


Figure 3-6. Variation in Density Function with Standard Deviation (Plotted at Age 100 Hours for a Mean Life Equal to 300 Hours)

The predicted reliabilities of wear-out items, derived as shown in Figure 3-7, should be combined with the reliability values for constant failure rate items according to the relationships shown in the system reliability model.

Reliability $R(t) = \int_t^{\infty} f(\tau)d\tau$

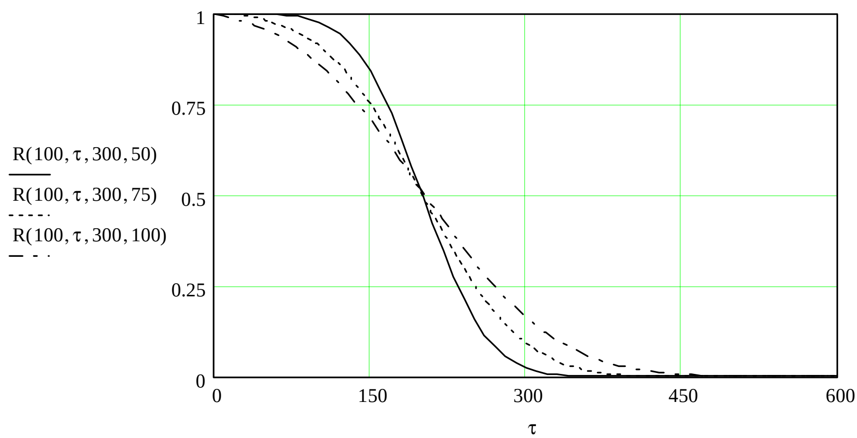


Figure 3-7. Variation in Reliability with Standard Deviation (Plotted at Age 100 Hours for a Mean Life Equal to 300 Hours)

Prediction Theory for Connectors

This section describes the failure rate model to be used for predicting the failure rate of connectors under stated environmental and operating conditions. It provides operational base failure rates for various types of connectors and environmental and other factors for use in the model, and also non-operational base failure rates. The model and data are derived from those detailed in MIL-HDBK-217.

Failure Rate Model - Operational Mode

This model is based on the concept that the failure rate of a pair of mated connectors in the operational mode depends on the number of active pins (or contacts), the operational environment in which it is being used and also upon the frequency of **making and breaking** (cycling) the male and female halves. The failure rate model for a pair of mated connectors is:

Equation

$$\lambda_p = \lambda_B \cdot K_E \cdot K_P + N_P \cdot \lambda_{cyc} \quad (3.6)$$

Where:

λ_p = The predicted operational failure rate (in failures per 10^6 hours) of a pair of mated connectors under stated environmental and operating conditions.

λ_B = The operational base failure rate of the particular type of connector in the **ground fixed** environment (Table A-1).

K_E = The environmental factor appropriate to the operational environment of the connector (Table A-1).

K_p = The active pin (or contact) factor appropriate to the number of active pins (N) in the connector (Table A-37).

N_P = The number of active pins (or contacts) in the pair of connectors.

λ_{cyc} = The cycling failure rate appropriate to the number of cycling operations per 1000 operating hours (Table A-36).

NOTE For a single connector (e.g., a test connector in the unmated mode), λ_p should be divided by two.

Failure Rate Model - Non-operational Mode

The predicted failure rate (λ_p) of a connector in the non-operational mode is given by:

$$\lambda_p = \lambda_b \cdot K_p$$

Where:

λ_b = The non-operational base failure rate of the connector (Table A-1).

K_p = The active pin (or contact) factor (Table A-37).

NOTE For a single connector, λ_p should be divided by two. Note also that a non-operational K_E factor is not included in the equation because an overall factor is applied at equipment/assembly level. (See Chapter 4, “Reliability Modelling”.)

Failure Rate Data and Factors

Non-operational base failure rates (λ_b) and operational base failure rates (λ_B) for four types of connectors are listed in Table A-1. This table also lists the operational environmental factors (K_E) appropriate to the various ground (G1 and G2), ship (S1 and S2) and air (A1 and A2) environments.

Active Pin Factors (K_p) and Cycling Failure Rates (λ_{cyc}) are listed in Table A-37 and Table A-36 respectively. Note that when the number of cycling operations is less than 10 per 1000 operating hours, the cycling rate is negligible and taken as zero.

Example of Application of Model

An example of the use of the failure rate model and the data tables follow.

Example **Edge Connector**

Task: An edge connector using 85 active pins is being used in an **air protected** (A1) environment. It is estimated that it will be disconnected and reconnected 25 times per 1000 operating hours. Predict the operational failure rate of the connector.

Solution:

Step 1: From equation 3.5, the failure rate model for connectors is:

$$\lambda_p = \lambda_B \cdot K_E \cdot K_P + N_P \cdot \lambda_{cyc}$$

Step 2: The appropriate values of λ_B, K_E, K_P and λ_{cyc} are:

- From Table A-1, $\lambda_B = 0.03$.
- From Table A-1, $K_E = 2.0$ (Air protected, Al).
- From Table A-37, $K_P = 19.39$.
  (85 active pins, N_P)
- From Table A-36, $\lambda_{cyc} = 0.00125$.

Step 3: Calculate λ_p by inserting the values derived above into the model in Step 1:

$$\begin{aligned}\lambda_p &= 0.03(2.0)(19.39) + (85 \cdot 0.00125)\\ &= 1.16 + 0.11\\ &= 1.27 \text{ failures per } 10^6 \text{ hours}\end{aligned}$$

Reliability Prediction for One-Shot Devices

A **one-shot device** is defined as an item that is required to perform its function once during normal operational use. In general, such items will be destroyed during their normal operation (e.g., motors, fuzes, warheads, etc.) and will therefore be **no-test** items. Also, one-shot devices are required to operate for only a relatively short time.

For these reasons, it can be assumed for prediction purposes that failure of any one-shot device is independent of time and can be expressed as a fixed probability of occurrence, (P_F). Reliability (i.e., probability of successful operation) is then given by ($I - P_F$). Data for various one-shot devices is given in Appendix A, “Data Tables”.

When using the prediction methods described in previous paragraphs, one-shot devices must be identified separately, and their reliabilities derived from the data given in Appendix A. These reliabilities should then be combined with the reliabilities of other items in the design, according to the system reliability model.

If data is not given in Table A-59, estimates of reliability should be made by comparison with similar items, and these values used until more specific data becomes available, (e.g., from testing programmes).

NOTE The data given in Appendix A is related to a temperate climate. The possible effects of more severe environmental conditions should be assessed, as necessary, by the analyst, using the best available information. The sources of such information, and any alternative data used in the prediction, should be recorded.

The reliability required from one-shot devices is generally high. It is most important, therefore, that their design and manufacturing processes are evaluated in as much depth as possible, using both quantitative and qualitative analysis techniques. These are described more fully in Reference 1, which is described in the “Bibliography” on page D-1.

4. Reliability Modelling

Introduction

The aim of this chapter is to provide an understanding of reliability modelling as it applies to the modelling process. It is not the intention to give exhaustive descriptions of the more sophisticated modelling techniques that may be obtained from the references and other literature. Its intent is rather to describe the more common techniques that may be used and essential features that must be taken into account.

The purpose of reliability modelling is to generate a mathematical picture of a system in the environment in which the system is to be used. It is important, before modelling begins, that both the system and the environment in which it is to be operated are understood. The consequences of system failure and the ability to repair the system should also be considered.

In particular, it should be noted that in this chapter, little consideration is given to the modelling of systems in which redundant sub-systems are repaired prior to system failure. In other words, each component or non-redundant sub-system is assumed to have an infinite repair time (zero repair rate). Thus, when such a component or sub-system fails, it remains in this state until the system of which it is a part is completely repaired or replaced in its entirety. In effect, this form of maintenance strategy typifies **one-shot** devices such as fire extinguishers, undersea cables, weapons systems and the like. For a brief summary of procedures to be adopted for modelling systems in which redundant sub-systems are repaired prior to system failure, see “Reliability Evaluation when Redundant Sub-systems can be Repaired Before System Failure” on page 4-37.

This chapter develops the principles outlined in Chapter 2, “Reliability Prediction Methods”, and describes:

- The purpose of reliability modelling.
- System definition.
- Construction of reliability models.
- General expressions for use in prediction.

The methods described in this chapter can be applied generally to most types of equipment (bearing in mind the comments made in the introductory paragraphs). However, beginning on page 4-32, a Guided Weapon System (GWS) example is used to illustrate these methods because such systems often consist of a variety of equipment, each with differing operating and maintenance conditions.

Purpose of Modelling

The purpose of reliability modelling is to express the specified requirements, functions, and operating and maintenance conditions for a system in such a way that the reliabilities of the items comprising the system can be assessed and combined to predict the system reliability, indicate shortcomings and assess logistic implications.

To be effective, models must represent, as closely as possible, the various features of a system and the conditions in which it is expected to operate. The most useful models, however, are those which strike a good balance between an accurate representation of a real-life situation and the need to provide results in a reasonable time, with due regard to the quality and quantity of input data and the required accuracy of the results. It is often better to make approximations based on reasoned assumptions than to attempt to use sophisticated mathematical techniques that are inconsistent with the quality of input data. Always remember that, although prediction is a quantitative process, its primary objective is to identify weak design areas for improvement. Thus, the emphasis is often on the **comparison** of values rather than the absolute values themselves.

It should be remembered that, in addition to the above, a reliability model is really a model of the system failure definition. In other words, there can be as many reliability models for a particular system as there are system failure definitions. For example, if a two-speaker stereo system was considered to have failed when stereo sound could not be heard from both speakers, then the reliability model would consist of blocks representing the speakers in a series configuration. However, if system failure was defined as a total loss of sound, then, for the same system, the speakers would appear in a parallel configuration. Thus, a key starting point in reliability modelling is to construct a set of system failure definitions. This is intuitive because to state that a system had a mean time to failure one year would be meaningless unless what is meant by system failure was clearly defined.

No one would presumably doubt that a transport vehicle had failed if the engine failed to start, or, despite all efforts, the vehicle could not be moved. It would be hoped that the mean time to failure for such a definition of failure would be acceptably large. However, if system failure was defined as the inability to travel faster than 70 mph, then the corresponding mean time to failure would likely be much shorter.

System Definition

Reliability models are central to the entire design process. Therefore, they must be based on a thorough understanding of the proposed system design and the requirements that the design must satisfy. System definition involves making studies of documents ranging from staff requirements to circuit diagrams, working closely with design staff and carrying out detailed engineering analyses to determine functional dependencies within the design. Necessary data may not always be clearly specified, and assumptions may have to be made. However, such assumptions must always be recorded and agreed to by both customer and supplier.

Compared to only a few years ago, the analysis of reliability models, even using powerful analytical techniques, now presents little difficulty in the light of techniques that have been developed and, in many cases, this analysis is supported by commercially available software packages. Ensuring that the models produced results that actually represent reality is where there still is, or can be, a considerable amount of difficulty.

The objective of system definition is to bring together all available information relating to the system and its components and to record in an ordered manner:

- The specified operational requirements and any constraints, for the system.
- The proposed system configuration, including the functional relationships between items comprising the system and failure criteria.
- The operating and maintenance conditions that apply to the system.

These aspects are considered more fully in the following paragraphs. It must be emphasised that, in practice, the various factors are all closely interrelated and must be considered as a whole.

During the detailed design stage of a project, data should be available to define a system down to the component/part level, and this must be done because most tables of base failure rates (e.g., see Appendix A, “Data Tables”) provide data only at this level. Clearly, during earlier project stages, system definition will be restricted to higher levels of assembly but the same general principles for gathering data and analysing the system will apply. System definition involves much detailed and time-consuming work, which may be done by many different people. Therefore, a reference or coding method that readily identifies any particular item within the system hierarchy must be adopted so that data can be cross-referenced easily and accurately.

Operational Requirements and Constraints

The specified operational requirements and constraints provide the baseline against which the proposed design must be compared. Customer requirements must be studied and all data relevant to reliability must be extracted. If there are any ambiguities or inconsistencies related to reliability, then these must be clarified with the appropriate authorities as soon as practicable so that time and effort is not wasted. Reliability modelling must be based on an agreed interpretation of the requirements. In particular:

- The purpose and functions of the system should be described. If a system has more than one functional mode of operation (e.g., an aircraft, a search and tracking radar, etc.), the requirements in each mode should be identified separately. Requirements for alternative modes (i.e., redundancy) or standby modes of operation should also be identified.
- The main performance, safety and physical characteristics should be listed in order of importance. Acceptable limits of satisfactory performance should be stated so that failure criteria can be established, and any acceptable performance degradation that still allows a limited operational capability should also be defined. The latter is often important when performing a Failure Mode and Effects Analysis (FMEA), which is described in Chapter 6. Any physical constraints (e.g., size, weight, etc.) may be important, for example, when considering the scope for redundancy, or when assessing the severity of handling as a failure cause.
- Requirements for the specified reliability characteristics (reliability, Mean Time To Failure [MTTF], availability, failure rate, etc.) should be stated and quantified along with the time period, or other variables for which the requirement applies. If reliability requirements are specified individually for major sub-systems (rather than as an overall system requirement), the relevant data for each sub-system should be assembled accordingly.
- The specified conditions of use for the system (and sub-systems, if appropriate) should be stated, including operating states, environments, time intervals, maintenance policies, etc.. The sequence of use conditions during the period for which reliability is to be assessed is termed the **operational duty cycle**, and is described more fully in “Operational Duty Cycle” on page 4-5.

System Configuration and Failure Criteria

The major sub-systems that comprise the proposed system design should be identified and their functional relationships established with respect to the system functions. If the functional configuration of the system can vary during operational use, then each configuration must be identified separately. The system performance requirements should be detailed and the conditions that constitute a system failure defined. If a particular failure condition applies only to a limited part of the operational duty cycle as described in the next section, then this should be noted.

For modelling purposes, the functional relationships within a system must be developed through successive levels of the assembly to the component/part level. For a large system, it is generally best to establish the relationships between the major sub-systems first, and then to consider each sub-system individually.

Functional block diagrams (or other similar methods) should be used to show the functional relationships within a system in a concise and visual manner. Descriptive notes should be made on the diagrams to provide more detailed information that cannot be portrayed directly by the diagram. A complex system may need a large number of functional block diagrams to describe it, and so diagrams must be clearly referenced so that they can be easily cross-referenced.

Operational Duty Cycle

The conditions under which an item is used will influence its failure rate and hence its reliability. Therefore, the sequence of operating states, environments, time intervals, maintenance and other events to which an item is subject must be defined for the period during which reliability is to be assessed. This is termed the **Operational Duty Cycle**; essentially, it defines the types and periods of risk to which an item is exposed.

Operating States

The operating and dormant phases of use must be identified because device failure rates differ widely depending on whether an item is active or inactive, and whether it is likely to be affected by the frequency of switching on and off. Also, when an item is operating, its failure rate will depend upon the ratio of the applied stress to the design (or rated) stress; therefore, the precise operating conditions must be defined whenever a detailed parts stress analysis is to be carried out. For additional information, refer to “Parts Stress Analysis Methods” on page 3-15.

Environments

The environments appropriate to each operating or dormant phase of use must be determined because device failure rates vary according to the environment. Note that the term “environment” is used here in its broadest sense to mean qualitative operational locations (e.g., ship storage, air carriage, etc.) rather than detailed quantitative physical or climatic conditions (e.g., temperature $20°C$, humidity 90%, etc.). The environmental categories are described in Table A-57 in Appendix A, “Data Tables”.

Time Intervals and Events

The probability of failure of an item may depend upon the time for which it is at risk (e.g., continuous running equipment) or on the conditions associated with a particular event (e.g., shock through handling, high stress transients through switching, etc.). Each must be identified separately because different reliability expressions will apply. Note that the operating failure rates for the components/parts listed in Appendix A, “Data Tables”, are applicable mainly to time-related, rather than event-related, applications.

Maintenance Conditions

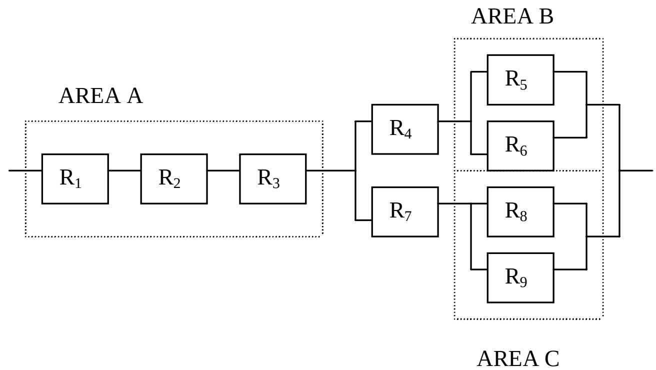
Maintenance conditions must be defined because they may have a significant influence on the reliability assessment and also affect availability. For example, the time for which an item is at risk will depend upon whether or not it is tested, the frequency of testing and the test effectiveness.

Identifying the Duty Cycle

The following procedure should be followed when identifying duty cycles:

1. Determine the operational duty cycle for the system.
2. From consideration of the system duty cycle and the functions of the sub-systems, determine the duty cycle for each sub-system.
3. For each sub-system, determine the operational duty cycle of each item comprising the particular sub-system. Highlight any item whose duty cycle differs from that of its parent sub-system, and define the duty cycle for that particular item.

Generally, it is convenient to show the duty cycles in the form of a diagram like that shown in Figure 4-1.

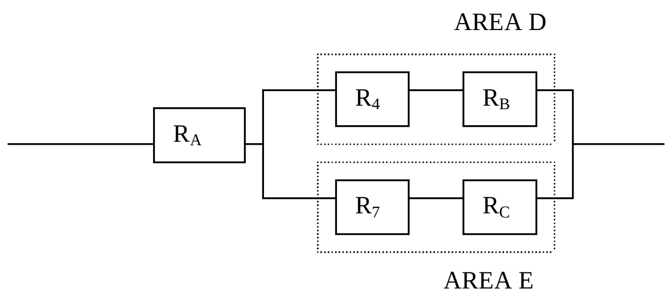


Step 1. Determine Reliability expressions for Areas A, B and C, i.e.:

$$R_A = R_1 \cdot R_2 \cdot R_3$$

$$R_B = R_5 + R_6 - R_5 \cdot R_6$$

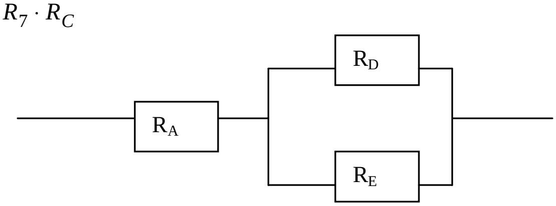
$$R_C = R_8 + R_9 - R_8 \cdot R_9$$



Step 2. Determine Reliability expressions for Areas D and E, i.e.:

$$R_D = R_4 \cdot R_B$$

$$R_E = R_7 \cdot R_C$$



Step 3. Combine Reliability expressions for Areas A, D and E to give System Reliability, i.e.:

System Reliability, $R_S = R_A \cdot (R_D + R_E - R_D \cdot R_E)$

$$\text{or } R_S = (R_1 \cdot R_2 \cdot R_3) \cdot [(R_4) \cdot (R_5 + R_6 - R_5 \cdot R_6) + (R_7) \cdot (R_8 + R_9 - R_8 \cdot R_9) - (R_4) \cdot (R_7) \cdot (R_5 + R_6 - R_5 \cdot R_6) \cdot (R_8 + R_9 - R_8 \cdot R_9)]$$

Figure 4-1. Example Derivation of a Reliability Model

Reliability Model Construction

To construct a reliability model for a system, the reliability relationships between the items comprising the system must first be established. A common method of representing such reliability relationships within a system is a Reliability Block Diagram (RBD). An RBD is a logic chart and is described in "Reliability Block Diagrams" on page 2-11 and below.

Reliability Block Diagrams (RBDs)

A complex system will require a large number of RBDs to describe it, and the first step is to develop an RBD at the system level as follows:

- By reference to the data assembled during System Definition, specify the functions of the system and the operating states (e.g., standby, full power, etc.).
- Specify the minimum requirements for the system to operate successfully in terms of the functions of the system.
- Draw a system RBD in terms of the system functions.
- Specify the sub-systems that are required to perform the system functions.
- Draw a system RBD in terms of the sub-systems and simplify as necessary.

Once an RBD has been constructed to show the reliability dependencies at the system level, a similar procedure should be followed to construct RBDs for each sub-system at successive levels of assembly down to the level at which reliabilities, or failure rates, can be estimated from the component/part data. This process is illustrated in Figure 4-2.

RBDs must always be as explicit as possible and should contain all pertinent information. This may not always be possible simply by the arrangement of blocks and interconnecting lines. Appropriate notes should be made on the diagrams as necessary. For example:

- Types of redundancy should be described, when not evident from the diagram.
- If the failure of a redundant element degrades performance or places additional stress on items in alternative paths, this should be noted.
- If the operating or maintenance conditions appropriate to a particular block are different from associated blocks (see "Operational Duty Cycle" on page 4-5), this should be highlighted (e.g., an item which may be replaced or repaired during the operational period).

The overall aim must be to record all data that may influence the reliability analysis and calculations.

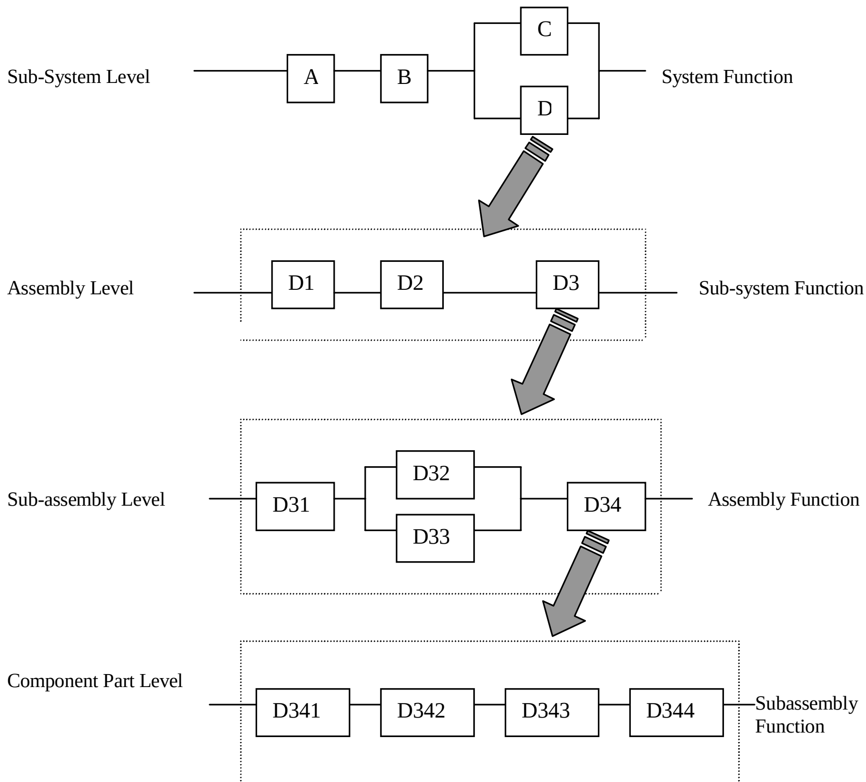


Figure 4-2. Development of Reliability Block Diagrams Within a System

The following points should be noted when constructing RBDs at system, sub-system and lower assembly levels:

- More than one RBD may be necessary to depict differing operational objectives or alternative functional modes.
- Elements of an RBD should contain only items that have the same operational duty cycle.
- When constructed to its lowest level, the blocks comprising an RBD should contain only series equivalent elements or have known reliability characteristics established from previous analysis.
- If an element has more than one failure mode, separate RBDs must be drawn using each failure mode.
- When functional relationships between elements cannot be represented by straightforward series, active redundant or standby redundant configurations, the

group of elements concerned must be isolated and highlighted for special consideration. In general, reliability evaluation of such groups can be made using Bayes Theorem, which is described on page 4-11.

When developing RBDs, it is not always a matter of simple inspection to determine the conditions that represent successful operation of a system (the system up states), or alternatively the system down states. In these cases, techniques such as Truth Tables or Boolean algebra should be used as described in Reference 1. For additional information, see the “Bibliography” on page D-1.

System Reliability Model

A reliability model for a group of items is derived by combining the reliabilities of the individual items according to set rules for combining probabilities. The two most common groups of items are:

- **Series configuration**. All items must operate successfully for the group to be successful. Here the group reliability is the product of the reliabilities of the individual items if they are independent, that is:

  $$R_G = R_1 \cdot R_2 \cdot R_3 \cdot \ldots \cdot R_N$$

- **Parallel (Active) Redundancy configuration**. In its simplest form, all items must fail for the group to fail. Here, the group reliability is equal to one minus the product of the unreliability of individual blocks if they are independent, that is:

  $$R_G = 1 - \{(1 - R_1) \cdot (1 - R_2) \cdot (1 - R_3) \cdot \ldots \cdot (1 - R_N)\}$$

Further expressions that can be used for other configurations (including M/N and Standby Redundancy) are given later in this chapter.

To construct a system reliability model, the RBDs must be studied and the reliabilities of individual blocks combined according to the appropriate rules. This is straightforward when the blocks are independent and in a series or simple redundancy configuration. For more complex systems, however, it is generally better to sub-divide the system into convenient areas that can be evaluated separately and then brought together to provide the system reliability. This is particularly so when blocks are in more complex redundancy configurations because these must be solved by progressive re-grouping, which allows standard expressions to be used. A simple example of the way in which this may be done is shown in Figure 4-2.

Common rules for combining reliabilities follow:

- When preparing an RBD, it is important to be aware of common shared items. A common example is shown on the next page.
- When preparing an RBD, the lowest level block would normally be associated with the system’s maintenance philosophy, i.e., those items that are replaced during maintenance.

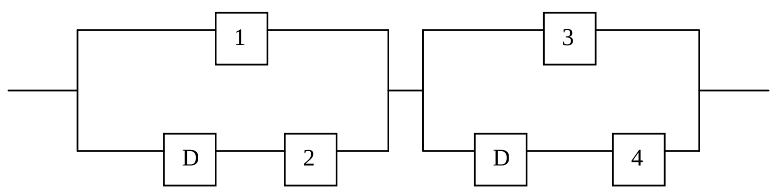
Bayes Theorem

If the functional relationships within a group of elements are more complex than simple series or redundant configurations, then the previous guidelines for combining reliabilities may be invalid. In such cases, suitable reliability expressions may often be determined by using derivatives of Bayes Theorem.

The following two examples illustrate the use of the theorem to derive reliability expressions.

Example **Power Supply**

Step 1: Consider the group of items represented by Reliability Block Diagram 1 below, where D is a power supply common to items 2 and 4 only.



Reliability Block Diagram 1

Step 2: For two events, A and B, a formula derived from Bayes Theorem is:

$$P(A) = P(A \backslash B) \cdot P(B) + P(A \backslash \bar{B}) \cdot P(\bar{B})$$

Where:

$P(A)$ = The probability of event A occurring.

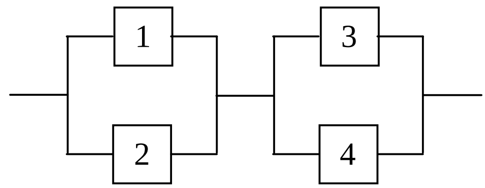
$P(A \backslash B)$ = The probability of event A occurring given that event B occurs.

$\bar{B}$ = The probability of event B not occurring.

A = The probability of system success.

B = The probability of item D operating successfully.

Step 3: Then, $P(A \backslash B)$ is the probability that the group shown in Reliability Block Diagram 2 below does not fail because this is the system RBD given that D does not fail:

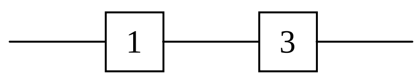


Reliability Block Diagram 2

Thus:

$$P(A \backslash B) = (R_1 + R_2 - R_1 \cdot R_2)(R_3 + R_4 - R_3 \cdot R_4)$$

Step 4: $P(A \backslash \bar{B})$ is the probability of the system being successful given that D fails. For this, items 1 and 3 must operate successfully. The system RBD, given that D fails, is thus:



Reliability Block Diagram 3

Thus:

$$P(A \backslash \bar{B}) = R_1 \cdot R_3$$

Step 5: If the reliability of item D is R_D, then:

$$P(B) = R_D$$

$$P(\bar{B}) = 1 - R_D$$

Step 6: $P(A)$ is equivalent to the system reliability. Thus, substituting the above results in the expression in Step 2:

System Reliability =

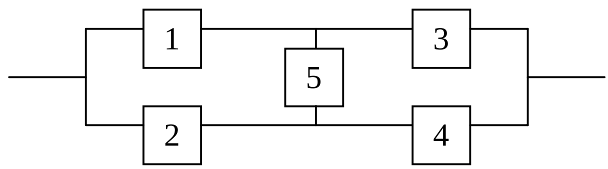
$$(R_1 + R_2 - R_1 \cdot R_2)(R_3 + R_4 - R_3 \cdot R_4)(R_D) + (R_1 \cdot R_3)(1 - R_D)$$

Example **Conditional System Operation**

Task: Consider the group of items represented by Reliability Block Diagram 1 below, where the system will operate successfully providing at least one of the following conditions are met:

- Items 1 and 3 are operational.
- Items 2 and 4 are operational.
- Items 1, 5 and 4 are operational.
- Items 2, 5 and 3 are operational.

Step 1: Derive the reliability model for the system:



Reliability Block Diagram 1

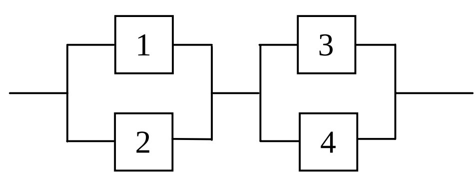
Step 2: Let:

A = System success.

B = Item 5 operating successfully.

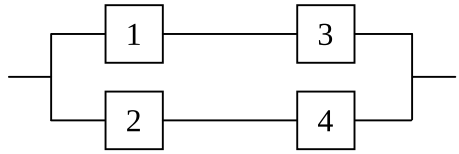
Then, following similar procedures to those described in Example 1, the following expressions can be derived:

$P(A \backslash B)$ =



$(R_1 + R_2 - R_1 \cdot R_2)(R_3 + R_4 - R_3 \cdot R_4)$

$$P(A\backslash\bar{B}) =$$



$$(R_1 \cdot R_3) + (R_2 \cdot R_4) - (R_1 \cdot R_3 \cdot R_2 \cdot R_4)$$

$$P(B) = R_5$$

$$P(\bar{B}) = 1 - R_5$$

Step 3: Thus, system reliability, R_S, is given by:

$$R_S = (R_1 + R_2 - R_1 \cdot R_2)(R_3 + R_4 - R_3 \cdot R_4)(R_5) + \\ (R_1 R_3 + R_2 \cdot R_4 - R_1 \cdot R_3 \cdot R_2 \cdot R_4)(1 - R_5)$$

Reliability Model Analysis

In this document, the term **reliability** is used in two quite different senses. It has been used in a qualitative sense to mean the effectiveness or goodness of the system and also in a quantitative sense to mean the probability of failure-free operation for a specified period of time. In the latter sense, it is one of a set of what might be termed **reliability characteristics** of a system, with other reliability characteristics being Mean Time To Failure (MTTF), Mean Time To First Failure (MTTFF), failure rate, availability and so on. In this section, a method is given for obtaining system MTTF and failure rate from system reliability.

System MTTF and Failure Rates with No Maintenance

Whenever an expression for system reliability can be obtained, a corresponding value for system MTTF can also be obtained. This is done by using the relationship:

Equation

$$MTTF = \int_0^{\infty} R(t)dt \quad \text{(4.1)}$$

where the integral ranges from t (mission time) = zero to infinity. For systems having a **constant failure rate** λ_S, the expression for system reliability, $R_S(t)$, is given by:

Equation $R_S(t) = exp(-\lambda_S t)$ .... (4.2)

so that $MTTF = \int_0^{\infty} R(t)dt$ is simply $1 / \lambda_S$.

However, if λ_S is not constant, then MTTF does not equal $1 / \lambda_S$.

As an example of a non-constant failure rate system, consider a system comprising two sub-systems that are parallel in terms of reliability (Figure 4-3).

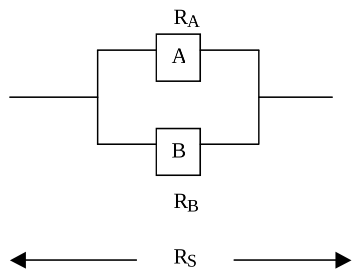


Figure 4-3. Parallel (or Active) Redundancy Configuration

The reliability of this system is given by:

$R_S = R_A + R_B - R_A R_B$ (See “Parallel (or Active) Redundancy Group” on page 2-14.)

Provided that the **sub-system** failure rates are constant, the system MTTF is given by integrating equation 2.10 in Chapter 2, “General Philosophy and Process of Reliability Prediction”, from $t = 0$ to infinity. We thus obtain:

Equation $MTTF_S = \frac{1}{\lambda_A} + \frac{1}{\lambda_B} - \frac{1}{\lambda_A + \lambda_B}$ .... (4.3)

This quantity depends only on failure rates and not on time. The system failure rate, λ_S, on the other hand is given by:

Equation $\lambda_S = \frac{\lambda_A \cdot exp(-\lambda_A \cdot t) + \lambda_B \cdot exp(-\lambda_B \cdot t) - (\lambda_A + \lambda_B) \cdot exp[-\lambda_A + \lambda_B \cdot t]}{exp(-\lambda_A \cdot t) + exp(-\lambda_B \cdot t) - exp[-\lambda_A + \lambda_B \cdot t]}$ .... (4.4)

Or, if all of the failures are equal:

Equation $\lambda_S = 2 \cdot \lambda \cdot \frac{1 - exp(-\lambda \cdot t)}{2 - exp(-\lambda \cdot t)}$ .... (4.5)

Note that both the above expressions for λ_S involve the variable t (time).

Taking as an example $\lambda = 1000$ fits (1 fit = 1 failure per 10^9 component hours), a plot of λ_S against time takes the form illustrated in Figure 4-4.

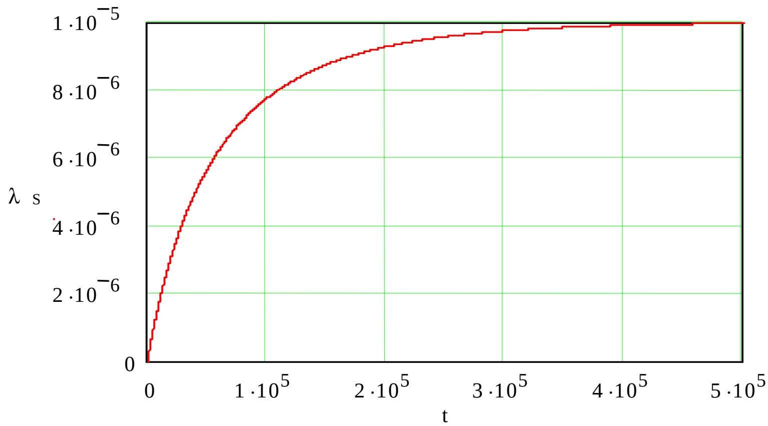


Figure 4-4. Variation of Failure Rate with Time

System MTTF and Failure Rates with Maintenance

If a system comprised of two sub-systems in active redundancy (see Figure 4-3) is inspected every T time units and if, at the time of inspection, one of the sub-systems is discovered to have failed and is immediately replaced, then the system mean time to failure ($MTTF_S$) instead of being given by equation (4.1) will be given by:

Equations

$$MTTF_S = \frac{\int_0^T R_S(t)dt}{1 - R_S(T)} \quad \text{.......(4.6)}$$

which, when both **sub-systems** have equal, constant failure rates, becomes:

$$MTTF_S := \frac{1}{2} \cdot \frac{(exp(-\lambda \cdot T) - 3)}{[(exp(-\lambda \cdot T) - 1) \cdot \lambda]} \quad \text{.......(4.7)}$$

If a plot is made of the variation of $MTTF_S$ with T, it is found that a graph of the following form is obtained:

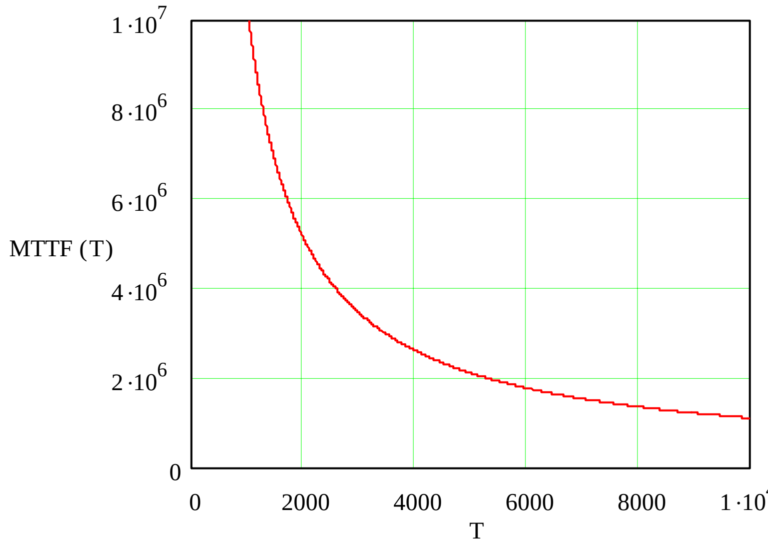


Figure 4-5. Variation of MTTFs with Time

From the above, the enormous benefit that can arise as the inspection interval T is decreased can be seen. In fact, as T approaches zero, the value of $MTTF_S$ approaches infinity.

It should be noted that equation (4.7) is generally valid, but for the special case where $R_S(t) = exp(-\lambda t)$ (no maintenance), $MTTF_S$ as given by equation (4.7) simplifies to $1/\lambda$.

Scenario Modelling

Reliability prediction is a precise but inexact science. Software tools implementing the formulae defined in MIL-HDBK-217, for example, are capable of producing very precise results whose accuracy must always be treated with informed scepticism. There are undoubtedly strengths and weaknesses associated with this type of prediction.

Strengths

The strengths of this type of prediction are:

- It can be used throughout the design process, in its parts count form initially, followed by parts stress, to enable the technical risk of design decisions to be minimised at the earliest opportunity.
- It lends itself well to comparing options and performing trade-off analyses.

- It provides consistency and repeatability.
- It is a well-established methodology, supported by proven proprietary software tools available from diverse vendors.
- Despite its weaknesses, which are listed below, this type of prediction provides a mechanism for the fair comparison of alternatives and/or competing equipment suppliers.

Weaknesses The contrasting weaknesses of this type of prediction are:

- Its lack of absolute accuracy.
- Its assumption that failure rate is constant with time.
- Its ability to consider only series configurations.
- Its inability to address many factors, including:
  - Inadequate design.
  - Manufacturing defects.
  - Software.
  - Power on/off cycling.
  - Environmental flux.
  - Physical disruption.
  - Human interference.

Note: More recent reliability prediction calculation models may address some of the above factors.

It has been said that *"Reliability prediction is about as accurate as weather forecasting; the only thing you can be absolutely sure of is that it's wrong."* At first glance this may seem a pretty damning statement; but, in the context of the proper use of reliability prediction, absolute accuracy is largely irrelevant.

It is essential to realise that the result of a reliability prediction is just a guess; an educated one maybe, but a guess nonetheless. The important factor is that the results are repeatable, and the inaccuracy is consistent across alternative proposed design solutions such that informed decisions may be made with regard to choice of options. It is worth digesting the opening paragraphs of the *Reliability Prediction Manual for Guided Weapon Systems* (Rex, Thompson and Partners on behalf of the MoD(PE); 1980) at this point:

“Reliability prediction is a forecasting technique by which the potential reliability achievement of a ‘mature’ system can be estimated during its design and development phases, and criteria established to aid decision making during those phases. The particular methods, which can be used at various stages during a project, depend upon the details of system design which are available, and the data that are relevant from previous experience. The true benefits of reliability prediction lie in the disciplines imposed by systematic and detailed analysis of the proposed design and its specified requirements, and the engineering interpretation of the predicted figures rather than in the absolute values themselves. In general, failure rate or MTBF predictions are likely to be optimistic and a prediction lying within a factor of two of the eventual achievement can be considered as good agreement. Despite the limitations which may be associated with any type of forecast, the prediction process provides the means to compare alternative design solutions against a common base-line, to identify reliability shortcomings which can be improved or corrected and highlight areas where trade-off studies or decisions may be required.”

So, although reliability prediction tools are capable of generating very precise results (to several decimal places), we must not allow ourselves to be tricked into believing that this must mean that they are very accurate results. Precision does not equate to accuracy.

If the above is true for predictions of inherent reliability, then the problems associated with the translation from predicted inherent to expected operational are far more complex and severe. Once deployed in the field, the subject equipment is exposed to many reliability threatening factors, although in this context we are actually referring to observed or perceived reliability rather than the inherent reliability of the original predictions.

These prediction techniques were derived from the assumptions that failures occur in a random manner with respect to the time domain and that the failure rate of individual components is constant. This concept provides a framework for collection and analysis of component failure rate data and for feedback of this data into the reliability prediction models. The effects of some operating stresses and environmental conditions on component failure rates were recognised early in the development of prediction techniques and have been incorporated into the currently accepted failure rate models where possible.

Most of this data was collected at the component level during life tests with no power on/off cycling and very little cyclic electrical, mechanical or thermal stress. As a result, cyclic effects that are significant in many equipment applications have not been adequately reflected in the data and thus are not explicitly represented in component failure rate models. This omission is the main reason that many reliability predictions for complex electronic equipment differ markedly from the values subsequently observed or perceived during service use.

Analysis

Many studies have been carried out to display the effects of operational scenario on the achieved reliability of complex electronic systems, and many attempts have been made to empirically derive correction factors that can be applied to the results of predictions. Although the derived mathematical models differ in form and correction factors, the research leading to their derivation shares a common thread.

The generally accepted belief is that the damaging effects of cyclic operations can be attributed to a complex combination of electrical and thermal stress, moisture ingress, physical shock, airborne corrosive agents and transient power surges. There is also empirical evidence to suggest that the way these factors combine may produce a progressively degenerative effect that systematically reduces a system's ability to withstand the increased stress of cyclic operation.

Before an attempt to derive some meaningful correction factors can be made, those parameters that are fixed in the prediction process but subject to significant variation in service must first be identified. Varying the baseline temperature used for the prediction can mitigate thermal effects and account for major environmental differences.

Mission profile is the main area not addressed. Both the number of missions and the mission duration are normally assumed to be constant for a prediction. Indeed, most models assume constant operation. An attempt must therefore be made to correct for:

- Variation from the 100% usage factor.
- The number of power on/off cycles.
- Variation in mission duration.

MIL-HDBK-217 assumed that the constant random failure rate is modified by the effect of on/off cycling to some extent, but by far the most significant is the effect of mission duration. For a given number of power cycles the increase in failure rate will be relatively constant, whereas the calculated reliability will vary with mission duration.

Example **Failure Rate Variations Due to Mission Duration Versus Calculated Reliability**

Step 1: Assume 10 missions during which there are a total of 6 failures, 5 attributed to the constant random failure rate and 1 attributed to the increased power cycling. Experience shows that the failure rate does not vary significantly with mission duration but calculated reliability certainly does:

- If each mission is of 24 hours duration, then:

$$MTBF = \frac{(24\text{ hours} \cdot 10)}{6} = 40\text{ hours}$$

- If each mission is of 500 hours duration, then:

$$MTBF = \frac{(500\text{ hours} \cdot 10)}{6} = 833\text{ hours}$$

Step 2: When lower one-sided statistical confidence limits using the Chi-squared distribution are applied, this difference becomes even more pronounced:

- If each mission is of 24 hours duration, then:
  - 90% lower, one-sided confidence gives 23 hours.
  - 80% lower, one-sided confidence gives 26 hours.
  - 70% lower, one-sided confidence gives 30 hours.
- If each mission is of 500 hours duration, then:
  - 90% lower, one-sided confidence gives 475 hours.
  - 80% lower, one-sided confidence gives 551 hours.
  - 70% lower, one-sided confidence gives 616 hours.

Much work has been carried out in this area, and one example is documented by the Reliability Analysis Centre, Rome Laboratory, Griffiss Air Force Base, New York. (RADC-TR-89-299: Reliability and Maintainability Operational Parameter Translation II). The model developed for ground-based equipment is:

$$MTBF_C = MTBF_P^{0.6} \cdot R_C$$

Where:

$MTBF_C$ = The corrected value of operational reliability.

$MTBF_P$ = The predicted inherent reliability.

R_C = The reliability correction factor (4.8 for mobile systems and 27 for fixed systems).

Empirical testing of this model against real-world observations has shown it to be reasonably representative; but, in many cases, it is still too coarse, having only two possible outcomes, as can be seen in the next example.

Example **Real-World Scenarios**

MIL-HDBK-217 parts stress prediction carried out for $30°C$ in a **ground fixed** environment gives an MTBF of 600 hours. This equipment is deployed in three distinctly different scenarios and is exhibiting a similar number of different levels of reliability performance.

Scenario 1: Training Role (Potentially Mobile)

Power Cycles:	> 250 per annum
Average Mission:	8 hours
Operational Time:	2000 hours
Duty Cycle:	22.8%
Failures:	6
Achieved MTBF:	333 hours

Scenario 2: Gap Filler Role (Mobile)

Power Cycles:	> 120 per annum
Average Mission:	10 hours
Operational Time:	1200 hours
Duty Cycle:	13.7%
Failures:	6
Achieved MTBF:	200 hours

Scenario 3: Fully Operational Role (Fixed Site)

Power Cycles:	> 10 per annum
Average Mission:	1000 hours
Operational Time:	8500 hours
Duty Cycle:	97.0%
Failures:	8
Achieved MTBF:	1062 hours

Using the RAC parameter translation models:

- For scenarios 1 and 2, the result is 223 hours.
- For scenario 3, the result is 1235 hours.

General Expressions for Use in Modelling

General expressions that can be used to calculate these parameters for various item configurations are given in Table 4-1 through Table 4-8. The derivation of the expressions is described in various reliability engineering textbooks.

Note that expressions that are based on RBD analysis are often only valid under certain restrictive assumptions, e.g., independence of blocks, no queuing for repair, etc.. Modelling techniques that may be used to overcome such restrictions are described elsewhere.

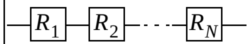
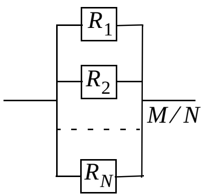
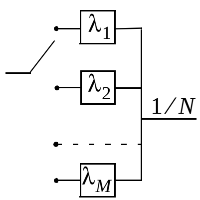
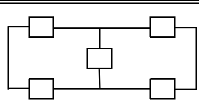
Reliability Block Diagram (RBD)	System Reliability (R_S)	Conditions		
 **Series System**	$R_S = R_1R_2R_3\ldots R_N = \prod_{i=1}^{N} R_i$	N Unequal blocks		
	$R_S = R^N$	N Equal blocks		
 **Active Redundancy**	$R_S = 1 - \prod_{i=1}^{N}(1-R_i)$	$M = 1, N$ general	Unequal Blocks	
	$R_S = R_1R_2R_3 + R_1R_2(1-R_3) + R_1R_3(1-R_2) + R_2R_3(1-R_1)$	$M = 2, N = 3$		
	$R_S = 1-(1-R)^N$	$M = 1, N$ general	Equal Blocks	
	$R_S = \sum_{i=0}^{N-M} {}^{N}C_i R^{(N-i)}(1-R)^i$ or alternatively $R_S = 1 - P_F = 1 - \sum_{i=N-M}^{N} {}^{N}C_i R^{(N-i)}(1-R)^i$ where ${}^{N}C_i = \frac{N!}{(N-i)!i!}$	M and N general See also Table 4-2 for $N \le 6$.		
 **Standby Redundancy**	$R_S(t) = \frac{\lambda_2 e^{-\lambda_1 t}}{\lambda_2-\lambda_1} + \frac{\lambda_1 e^{-\lambda_2 t}}{\lambda_1-\lambda_2}$	$M = 1$ $N = 2$	Unequal Blocks	$R_S(t)$ is the probability of the system surviving time t. Block active times to failure are negative exponentially distributed. Passive failure rates & switching failure rates are assumed to be zero.
	$R_S(t) = \frac{\lambda_2\lambda_3 e^{-\lambda_1 t}}{(\lambda_2-\lambda_1)(\lambda_3-\lambda_1)} + \frac{\lambda_1\lambda_3 e^{-\lambda_2 t}}{(\lambda_1-\lambda_2)(\lambda_3-\lambda_2)} + \frac{\lambda_1\lambda_2 e^{-\lambda_3 t}}{(\lambda_1-\lambda_3)(\lambda_2-\lambda_3)}$	$M = 1$ $N = 3$		
	$R_S(t) = e^{-\lambda t}\sum_{i=0}^{N-1}\frac{(\lambda t)^i}{i!}$	$1, N$ general	Equal Blocks	
	For systems like this, and others which are not like the above, Bayes Theorem may be used. (Refer to “Bayes Theorem” on page 4-11.)			
The reliability of systems that have RBDs that comprise combinations of the above block groups may be calculated by successive groupings. (Refer to “Bayes Theorem” on page 4-11.)				

Table 4-1. Reliability Expressions for Missions Without Repair

N \ M	1	2	3	4	5
2	$1-Q^2$				
3	$1-Q^3$	R^3+3R^2Q			
4	$1-Q^4$	$1-(4RQ^3+Q^4)$	R^4+4R^3Q		
5	$1-Q^5$	$1-(5RQ^4+Q^5)$	$R^5+5R^4Q+10R^3Q^2$	R^5+5R^4Q	
6	$1-Q^6$	$1-(6RQ^5+Q^6)$	$1-(15R^2Q^4+6RQ^5+Q^6)$	$R^6+6R^5Q+15R^4Q^2$	R^6+6R^5Q
$Q = 1-A$. The above expressions contain the least possible number of terms. Q = unavailability and A = availability.					

Table 4-2. Reliability Expressions for *M/N* Active Redundancy (Equal Blocks, No Repair)

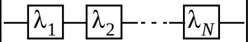
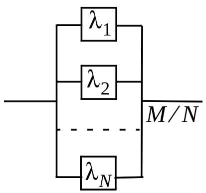
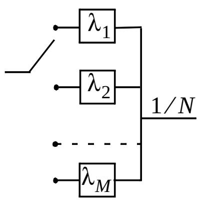
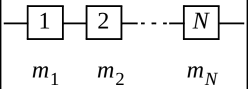
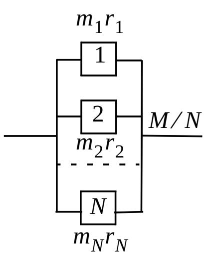
Reliability Block Diagram (RBD)	System MTTF	Conditions		
 Series System	$MTTF = \frac{1}{\lambda_S} = \frac{1}{\sum_{i=1}^{N} \lambda_i}$	N Unequal blocks		Block active times to failure are negative exponential distribution.
	$MTTF = \frac{1}{\lambda_S} = \frac{1}{N\lambda}$	N Equal blocks		
	$MTTF = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$	$M = 1$ $N = 2$	Unequal Blocks	
	$MTTF = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_3} - \frac{1}{\lambda_1 + \lambda_2} - \frac{1}{\lambda_2 + \lambda_3} - \frac{1}{\lambda_3 + \lambda_1} + \frac{1}{\lambda_1 + \lambda_2 + \lambda_3}$	$M = 1$ $N = 3$		
	$MTTF = \frac{1}{\lambda_1 + \lambda_2} + \frac{1}{\lambda_1 + \lambda_3} + \frac{1}{\lambda_2 + \lambda_3} - \frac{2}{\lambda_1 + \lambda_2 + \lambda_3}$	$M = 2$ $N = 3$		
Active Redundancy	$MTTF = \frac{1}{\lambda}\left[\frac{1}{N} + \frac{1}{(N-1)} + \frac{1}{(N-2)} + \ldots + \frac{1}{M}\right]$	N and M general See also Table 4-4 for $N \le 6$.	Equal Blocks	
	$MTTF = \sum_{i=1}^{N} \frac{1}{\lambda_i} = \sum_{i=1}^{N} m_i$	Unequal Blocks	$M = 1$ N general	$\lambda_i = \frac{1}{m_i}$
Standby Redundancy	$MTTF = \frac{N}{\lambda} = N \cdot m$	Equal Blocks		Any failure time distribution.
For more complex groupings, successive groupings are not permitted in order to calculate system MTTF because the assumptions of constant failure rates will be violated when redundancy is involved.				

Table 4-3. MTTF Expressions for Missions Without Repair

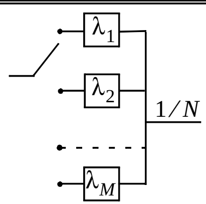
N \ M	1	2	3	4	5
2	$\frac{3}{2\lambda}$				
3	$\frac{11}{6\lambda}$	$\frac{5}{6\lambda}$			
4	$\frac{25}{12\lambda}$	$\frac{13}{12\lambda}$	$\frac{7}{12\lambda}$		
5	$\frac{137}{60\lambda}$	$\frac{77}{60\lambda}$	$\frac{47}{60\lambda}$	$\frac{9}{20\lambda}$	
6	$\frac{147}{60\lambda}$	$\frac{29}{20\lambda}$	$\frac{57}{60\lambda}$	$\frac{37}{60\lambda}$	$\frac{11}{30\lambda}$
λ = Active failure rate of a block, which is assumed constant.					

Table 4-4. MTTF Expressions for *M/N* Active Redundancy (Equal Blocks, No Repair)

<table>
<tr><th>Reliability Block Diagram (RBD)</th><th>System MTBF (m_S)</th><th colspan="3">Conditions</th></tr>
<tr><td rowspan="2">

Series System</td><td>$m_S = \frac{1}{\sum_{i=1}^{N} \lambda_i}$</td><td colspan="3">Unequal blocks</td></tr>
<tr><td>$m_S = \frac{1}{N\lambda} = \frac{m}{N}$</td><td colspan="3">Equal blocks, each with MTBF = m</td></tr>
<tr><td rowspan="4">

Active Redundancy</td><td>$m_S = \frac{A_S}{A_1Q_2\lambda_1 + A_2Q_1\lambda_2}$</td><td>$M = 1$
$N = 2$</td><td rowspan="3">Unequal Blocks</td><td rowspan="4">A is calculated in Table 4-7.

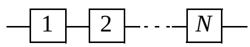
$Q = 1 - A$</td></tr>
<tr><td>$m_S = \frac{A_S}{Q_1Q_2A_3\lambda_3 + Q_1A_2Q_3\lambda_2 + A_1Q_2Q_3\lambda_3}$</td><td>$M = 1$
$N = 3$</td></tr>
<tr><td>$m_S = \frac{A_S}{K}$ where
$K = A_1A_2Q_3(\lambda_1 + \lambda_2) + A_1A_3Q_2(\lambda_1 + \lambda_3) + A_2A_3Q_1(\lambda_2 + \lambda_3)$</td><td>$M = 2$
$N = 3$</td></tr>
<tr><td>$m_S = \frac{A_S m}{M\,{}_NC_M A^M Q^{N-M}}$ where ${}^NC_M = \frac{N!}{(N-M)!M!}$</td><td>$M$ and N general</td><td>Equal Blocks
See also Table 4-6 for $N \le 6$.</td></tr>
<tr><td>

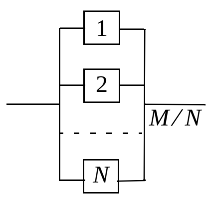
Standby Redundancy</td><td>$m_S = \sum_{i=2}^{N} \frac{m^{i-1}(N-1)!}{r^{i-2}(N+1-i)!}$</td><td colspan="3">$1/N$ case, with equal blocks, each having exponentially distributed active failure and repair times. Passive and switching failure rates are assumed to be zero.</td></tr>
<tr><td colspan="5">More complex systems than the above can be analysed by successive grouping.</td></tr>
<tr><td colspan="5">Key: m and r denote MTBF and MTTR respectively. $\lambda = \frac{1}{m}$ and $\mu = \frac{1}{r}$. The distribution of failure and repair times is not constrained, except for standby redundancy.</td></tr>
</table>

Figure 4-5. MTBF Expressions for Repairable Systems in the Steady State

N \ M	1	2	3	4	5
2	$\frac{A_S m}{2AQ}$				
3	$\frac{A_S m}{3AQ^2}$	$\frac{A_S m}{6A^2Q}$			
4	$\frac{A_S m}{4AQ^3}$	$\frac{A_S m}{12A^2Q^2}$	$\frac{A_S m}{12A^3Q}$		
5	$\frac{A_S m}{5AQ^4}$	$\frac{A_S m}{20A^2Q^3}$	$\frac{A_S m}{30A^3Q^2}$	$\frac{A_S m}{20A^4Q}$	
6	$\frac{A_S m}{6AQ^5}$	$\frac{A_S m}{30A^2Q^4}$	$\frac{A_S m}{60A^3Q^3}$	$\frac{A_S m}{60A^4Q^2}$	$\frac{A_S m}{30A^5Q}$
$Q = 1 - A$. A is calculated as in Table 4-7. Q = unavailability and A = availability.					

Table 4-6. MTBF Expressions for *M/N* Active Redundancy (Equal Blocks, Repairable)

<table>
<tr><th>Reliability Block Diagram (RBD)</th><th>System Availability (A_S)</th><th colspan="2">Condition</th></tr>
<tr><td rowspan="2">

Series System</td><td>$A_S = \prod_{i=1}^{N} A_i$</td><td colspan="2">$N$ Unequal Blocks</td></tr>
<tr><td>$A_S = A^N$</td><td colspan="2">N Equal Blocks</td></tr>
<tr><td rowspan="2">

Active Redundancy</td><td>$A_S = 1 - \prod_{i=1}^{N} (1 - A_i)$</td><td>$M = 1$
N general</td><td>Unequal Blocks</td></tr>
<tr><td>$A_S = 1 - (1 - A)^N$</td><td>$M = 1$
N general</td><td>Equal Blocks</td></tr>
<tr><td colspan="4">Note: For series and active redundancy configurations, the expressions for A_S are comparable with those for R_S. Further expressions for A_S can therefore be derived from Tables 4-1 and 4-2 by substituting A_S and A_1 for R_S and R_1 respectively.</td></tr>
<tr><td colspan="4">Standby Redundancy</td></tr>
<tr><td colspan="4">Computer models will normally be necessary to calculate the availability of a standby redundancy group. For the $1/N$ case, however, A_S can be calculated from:

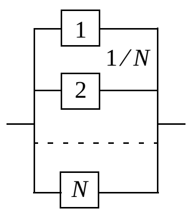
$A_s = \frac{m_s}{m_s + r_s}$ where m_s is system MTBF (see Table 4-5) and r_s is system MTTR (see Table 4-8)

This expression is applicable only when items are identical, passive and switching failure rates are zero and item failures are distributed exponentially with respect to their active time.</td></tr>
</table>

Table 4-7. Availability of Repairable Systems in the Steady State

<table>
<tr><th>Reliability Block Diagram (RBD)</th><th>System MTTR (r_s)</th><th>Condition</th></tr>
<tr><td colspan="3">In general, it is recommended that system MTTR (r_s) be calculated from the expression:

$$r_s = \frac{m_s(1 - A_S)}{A_S}$$

Where A_S and m_s are calculated as described in Tables 4-7 and 4-5 respectively. However, for $1/N$ active or standby redundancy, r_s may be calculated simply and directly as below.</td></tr>
<tr><td rowspan="2">

Active or Standby Redundancy</td><td>$$r_s = \frac{1}{\sum_{i=1}^{N} \frac{1}{r_1}}$$</td><td>Unequal Blocks
MTTR of $i^{th} = r_I$</td></tr>
<tr><td>$$r_s = \frac{r}{N}$$</td><td>Equal Blocks
Each with MTTR = r</td></tr>
</table>

Table 4-8. MTTR Expressions for Repairable Systems in the Steady State

Examples of Reliability Modelling

This simplified example is intended to illustrate the reliability modelling process at system/sub-system level. The subject of the example is a hypothetical Guided Weapon System (GWS) that, in general terms, is required to be a land-based, mobile system to search for, detect, track, intercept and destroy airborne targets.

Step 1: Define the Operational Requirements and Constraints

Assume that, from the study of the customer documents, the requirements and constraints area as follows:

- Operational. With any 24-hour battlefield day, to be capable of:
  - 14 hours at alert state with one target engagement of 2 minutes.
  - 10 hours at non-alert state, including one redeployment involving 2.5 hour cross-country movement.
- Maintenance:
  - Missile to be no-test and capable of 5 years storage before firing.
  - Launcher not repairable during alert state.
  - Radar to be repairable on site, with mean time to repair not exceeding 20 minutes.
- Reliability. A probability of at least 97.5% that successful intercepting of a target is not prevented by a system hardware failure (including the missile and its flight) during a 24-hour battlefield day.

Step 2: Define the system functions, configuration and failure criteria.

- The function F of the system is to intercept and destroy enemy targets. This overall function is comprised of three main elements:
  - Target Search and Detection (Fl).
  - Target Tracking and Pre-launch Guidance Commands (F2).
  - Launch Commands and Target Interception (F3).
- The proposed design consists of a Search Radar (SR), a Control Unit (CU), a Tracker Radar (TR) an alternative Manual Sight (MS) and two Launchers (Ll and L2), with each Launcher containing two Missiles (Ml, M2 and M3, M4). The Search Radar operates continuously during an alert state and passes search data to the Control Unit. When a target is detected, the Tracker Radar is brought into operation and provides pre-launch guidance information via the Control

Unit to the two Launchers and their Missiles. The Manual Sight provides an alternative method to tracking targets. A functional block diagram of the system is shown in Figure 4-6.

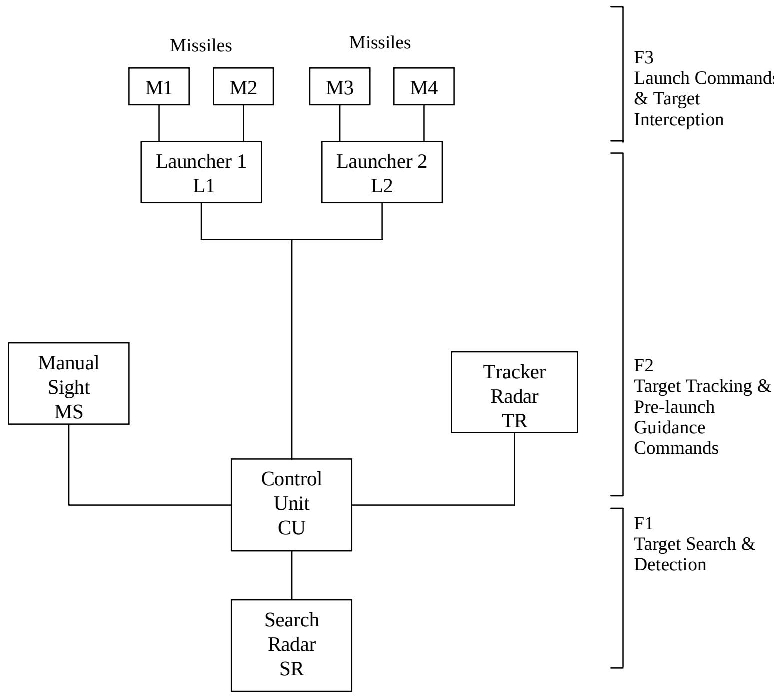


Figure 4-6. Functional Block Diagram of Hypothetical Guided Weapon System (GWS)

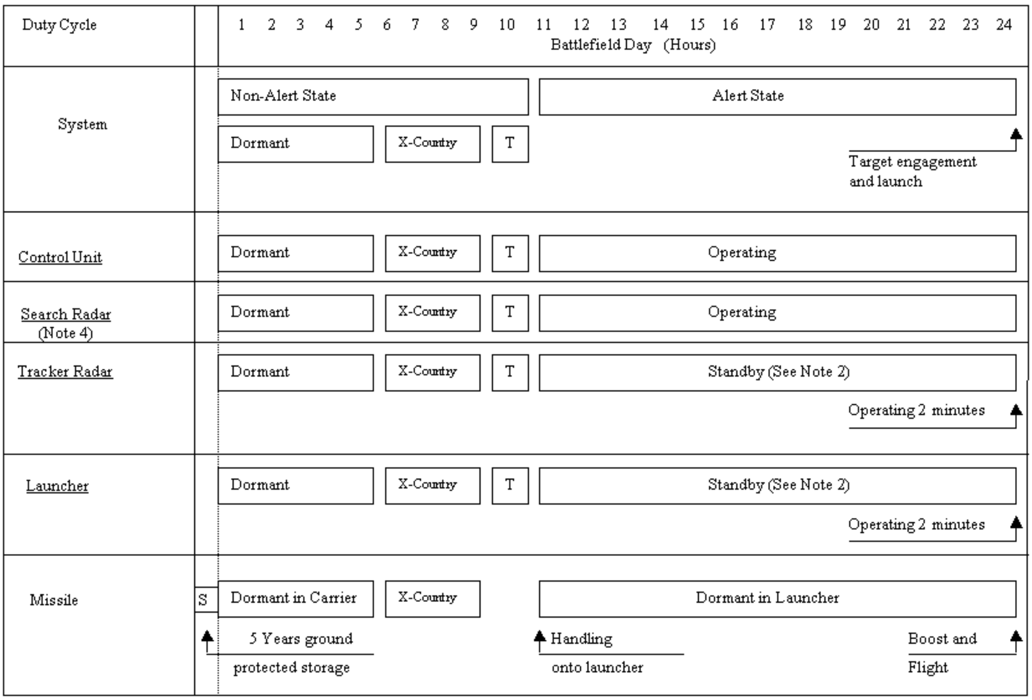
- The sub-systems associated with the system functions are as follows:

Function	Performed By
F1	SR and CU
F2	CU, TR, MS, L1/2
F3	CU, L1/2, M1/2/3/4

A system failure is defined as any failure in the system hardware that prevents the successful interception of a target. Thus, failure to perform any one of the three system functions (Fl, F2 and F3) constitutes a system failure.

Step 3: Define Operational Duty Cycles.

From consideration of the requirements detailed in Step 1, the operational duty cycles for the system and sub-systems are as shown in Figure 4-7.



Note 1: T = Setting up tests, involving 15 minutes operating and 1 switching cycle.

Note 2: Standby means that the equipment is **warmed up** and ready for immediate use but is not fully operational.

Note 3: Environments. The **Ground Mobile** environmental category applies throughout all cycles, except for Missile storage, boost and flight.

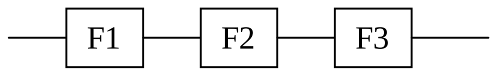
Note 4: Repairable on site during the Alert state; Mean Time To Repair (MTTR) not exceeding 20 minutes.

Figure 4-7. Examples of Operational Duty Cycles for Hypothetical Guided Weapon System (GWS)

Note: The cycles are related to a 24-hour battlefield day because this is the time interval specified for the reliability requirement. However, the duty cycle for the missiles must also include the requirement for up to 5 years storage prior to their operational use.

Step 4: Construct Reliability Block Diagrams (RBDs).

The minimum requirements for the system to operate successfully are that all three functions, Fl, F2 and F3 must be performed. Thus, successful operation of the system can be represented by:



- The sub-systems required to perform functions F1, F2 and F3 successfully are as follows:

Function	**Performed By**	**Figure**
F1	SR and CU	Figure 4-8a
F2	TR and CU and L1 or L2 or MS and CU and L1 or L2	Figure 4-8b
F3	CU and L1 and M1 or M2 or CU and L2 and M3 orM4	Figure 4-8c

The RBDs for each of these functions are shown in Figure 4-8. Note that ‘and’ equates to a series configuration and ‘or’ to a parallel configuration.

- Because Fl, F2 and F3 must all be performed successfully for the system to perform its functions successfully, the individual RBDs can be combined in series to give the RBD for the system as shown in Figure 4-8d.

Step 5: Construct the Reliability Model for the System/Sub-System Level.

Using the grouping procedure illustrated in Figure 4-1, the reliability model for the system, in terms of the reliabilities of the sub-systems, is as follows:

$$
\begin{aligned}
R_S = {} & (R_{SR})(R_{CU})(R_{TR} + R_{MS} - R_{TR} \cdot R_{MS}) \cdot [(R_{L1})(R_{M1} + R_{M2} - R_{M1} \cdot R_{M2}) \\
& + (R_{L2})(R_{M3} + R_{M4} - R_{M3} \cdot R_{M4}) \\
& - (R_{L1})(R_{L2})(R_{M1} + R_{M2} - R_{M1} \cdot R_{M2})(R_{M3} + R_{M4} - R_{M3} \cdot R_{M4})]
\end{aligned}
$$

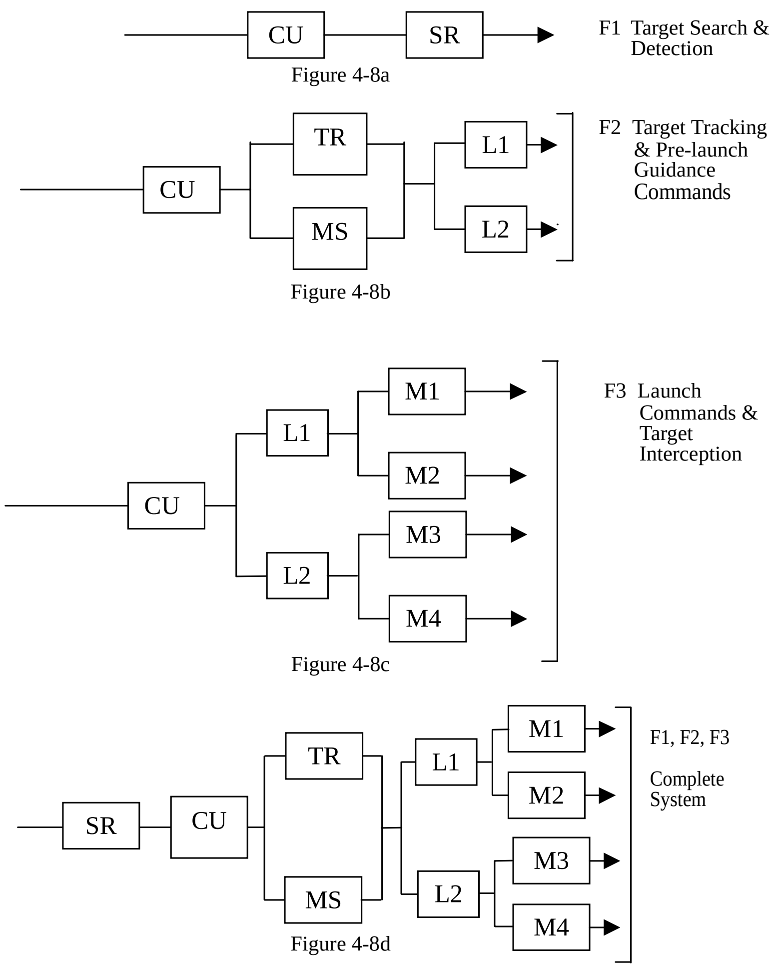


Figure 4-8. Reliability Block Diagram for Hypothetical Guided Weapon System (GWS)

Reliability Evaluation when Redundant Sub-systems can be Repaired Before System Failure

As pointed out on page 4-1, little consideration has been given so far to the modelling of systems in which redundant sub-systems are repaired prior to system failure. This omission will now be addressed, but only insofar as a brief summary of some of the associated formulae and conditions of use will be given. This topic can become quite complex from an analytical point of view; however, no attempt will be made here to give any proofs because they are covered extensively in reliability engineering literature.

Firstly, consider a two sub-system active redundant system; then, consider a system comprising one active sub-system and one cold standby sub-system.

NOTE The use of the word **cold** indicates that the standby is not energised (and hence for this example cannot fail) until it is required to be used.

For convenience, we will assume both sub-systems have the same failure rate (λ) and repair rate (μ). Assume also that both λ and μ are constant with time and that $\lambda \ll \mu$. The reciprocals of theses quantities are the Mean Time to Failure (MTTF or θ) and Mean Time to Repair (MTTR or τ) respectively.

Reliability Parameters - Active Redundancy

This section provides parameters for active redundancy.

Reliability

The quantity reliability, $R_S(t)$, is given by the expression:

Equation

$$R_S(t) = \frac{s_1 \cdot e^{s_2 \cdot t} - s_2 \cdot e^{s_1 \cdot t}}{s_1 - s_2} \quad \text{(4.8a)}$$

where s_1 and s_2 (both negative quantities) are roots of the equation:

$$s^2 + (\mu + 3\lambda)s + 2\lambda^2 = 0$$

It should be noted that since $\mu \gg \lambda$, one of the roots (s_1, say) is numerically very much greater than the other; so, equation (a) can, to a good approximation, be written in the form:

Equation

$$R_S(t) \approx e^{s_2 \cdot t} \approx e^{-2 \cdot \frac{\lambda^2}{\mu} \cdot t} \quad \text{(4.8b)}$$

MTTF$_S$

The quantity MTTF (θ) can be obtained from equation (4.8a) using the relationship expressed in “System MTTF and Failure Rates with No Maintenance” on page 4-14, i.e.:

Equation

$$\theta_S = \int_0^\infty \frac{s_1 \cdot e^{s_2 \cdot t} - s_2 \cdot e^{s_1 \cdot t}}{s_1 - s_2} dt = -\left[\frac{s_1 + s_2}{s_1 \cdot s_2}\right] = \frac{3 \cdot \lambda + \mu}{2 \cdot \lambda^2} \quad \text{(4.9a)}$$

which, because $\mu \gg \lambda$, can to a good approximation, be written in the form:

Equation

$$\theta_S \approx \frac{\mu}{2\lambda^2} \approx \frac{\theta^2}{2\tau} \quad \text{(4.9b)}$$

However, if $\mu = 0$, equation (4.9a) becomes $\theta_S \approx \frac{3}{2 \cdot \lambda}$, a fundamental result.

NOTE This result can also be obtained by integrating the right-hand side of equation 2.10 from $t = 0$ to $t = \infty$ and letting $\lambda_A = \lambda_B = \lambda$.

Reliability Parameters - Cold Standby

This section provides parameters for cold standby.

Reliability

Once again, the quantity for system reliability is given by the expression:

$$R_S(t) = \frac{s_1 \cdot e^{s_2 \cdot t} - s_2 \cdot e^{s_1 \cdot t}}{s_1 - s_2}$$

However, this time, s_1 and s_2 are roots of the equation:

$$s^2 + (\mu + 2\lambda)s + \lambda^2 = 0$$

It should be noted that since $\mu \gg \lambda$, one of the roots (s_1, say) is again numerically very much greater than the other; so, the above equation can, to a good approximation, be written in the form:

Equation

$$R_S(t) \approx e^{s_2 \cdot t} \approx e^{-\frac{\lambda^2}{\mu} \cdot t} \quad \text{(4.10)}$$

MTTF$_S$

This quantity, MTTF (θ), can be obtained from equation (4.8a) using the relationship:

Equation

$$\theta_S = \int_0^{\infty} \frac{s_1 \cdot e^{s_2 \cdot t} - s_2 \cdot e^{s_1 \cdot t}}{s_1 - s_2} dt = -\left[\frac{(s_2 + s_1)}{s_2 \cdot s_1}\right] = \frac{2 \cdot \lambda + \mu}{\lambda^2} \quad \text{(4.11a)}$$

which, because $\mu \gg \lambda$, can to a good approximation, be written in the form:

Equation

$$\theta_S \approx \frac{\mu}{\lambda^2} \approx \frac{\theta^2}{\tau} \quad \text{(4.11b)}$$

However, if $\mu = 0$, equation (4.11a) becomes $\theta_S \approx \frac{2}{\lambda}$.

NOTE This result can also be obtained by integrating the right-hand side of equation 2.12 from $t = 0$ to $t = \infty$.

Cautionary Remarks

Cautionary remarks about both active and standby redundant systems follow.

Active Redundant Systems

From the above expressions, it would appear that the improvement gained as a result of being able to repair redundant sub-systems while the system is operating is truly enormous. For example, consider a system comprising two identical, constant failure rate sub-systems in active redundancy. Suppose the MTTF and Mean Time To Repair (MTTR) of each sub-system are 1000 hours and 0.5 hours respectively. Then, the MTTF of the system, instead of being 1500 hours as it would be if repair were not possible while the system was operating, would become one million hours when the MTTR of each sub-system is 0.5 hours. (See equation (4.9b).)

This is an ideal theoretical situation based on the assumption that when one of the redundant sub-systems fails, an alarm is raised and within a mean time of half an hour, (in this example), the failed sub-system is fully working again. In practice however, there is a chance (measured by what is referred to as **degree of coverage**) that when one sub-system fails, it remains in a failed state (referred to as a **dormant fault**) until the other sub-system fails, in which case the system as a whole fails. It turns out that even if there is the slightest chance of a dormant fault, the theoretically attainable value of MTTF is reduced considerably. Other factors that can considerably reduce the benefits of redundancy, irrespective of whether repair is involved, are **common cause** and **common mode** failures. These topics are covered extensively in reliability engineering literature.

Standby Redundant Systems

Most of what is said concerning active redundant systems holds true for stand-by systems as well. For the latter, however, there is an additional mechanism by which the theoretically achievable system reliability parameters can be severely compromised: namely the failure of the switch-over mechanism to operate successfully when required to do so (and to some extent the failure of the switch-over mechanism to remain inactive when required to be so).

It is the existence of the control and switch-over mechanism that can often make a stand-by system less reliable than its active counterpart. Note that for the non-repairable case, the MTTF of a two sub-system active redundant system is 1.5 times the MTTF of the individual sub-systems; but for a standby system, the multiplier is 2 and not 1.5. Thus the standby system appears to be superior; however, this may not be true in practice on account of any unreliability of the control and switch-over mechanism.

Approximation Methods

Provided $\mu \gg \lambda$, the formulae needed to evaluate systems containing redundant sub-systems that can be repaired before the system as a whole fails can be quite simple and easy to use.

The first thing to note is that the general expression for the failure rate of a two-unit active redundant system (using the notation given in "Reliability Parameters - Active Redundancy" on page 4-37) is given by:

Equation

$$\lambda(t) = \frac{exp(s_2 \cdot t) - exp(s_1 \cdot t)}{s_2 \cdot exp(s_1 \cdot t) - s_1 \cdot exp(s_2 \cdot t)} \cdot s_1 \cdot s_2 \quad \text{(4.12a)}$$

When $\mu \gg \lambda \ldots s_1 \gg s_2$, the failure rate given above becomes equal to the constant value $-s_2$, (s_1 and s_2 are negative quantities), i.e.:

$\lambda_S(t) \approx \frac{2\lambda^2}{\mu}$, which is more conveniently written in the form:

Equation

$$\lambda_S(t) \approx 2\lambda^2\tau \text{ where } \mu = \frac{1}{\tau} \text{ just as } \lambda = \frac{1}{\theta} \quad \text{(4.12b)}$$

This last equation is an extremely useful and well-known result. Other useful results involving two simultaneous failures in a parallel (reliability-wise) system of units may be obtained from it. For example, for a system comprising three units in parallel where two are required for system success, the corresponding expression for system failure rate is:

Equation

$$\lambda_S \approx 2\lambda^2\tau \cdot 3 \quad \text{(4.12c)}$$

where the multiplier 3 accounts for the fact that there are three ways of selecting two units from three. For the case where, in a system comprising 10 units, 8 units are required for system success, any combination of 3 (or more) failing together would result in system failure.

For such a system, the failure rate would be given by:

Equation

$$\lambda_S = 3\lambda^3\tau^2 \cdot 120 \quad \text{(4.12d)}$$

where $3\lambda^3\tau^2$ is the (constant) failure rate of a three-unit active parallel system (1 out of 3 needed), and the factor 120 is the number of ways of selecting 3 units from 10.

From the above, it should be apparent that provided each block constituting even the most complicated of block diagrams has an $MTTF \gg MTTR$ $(\theta \gg \tau)$, then the failure rate of the system for which the block diagram represents a particular system failure definition, can be written down by inspection of the diagram without the need for any difficult calculations at all. This is more simple than analysing the **non-repairable** counterpart.

Example Suppose a failure definition for a particular system is represented by the RBD below:

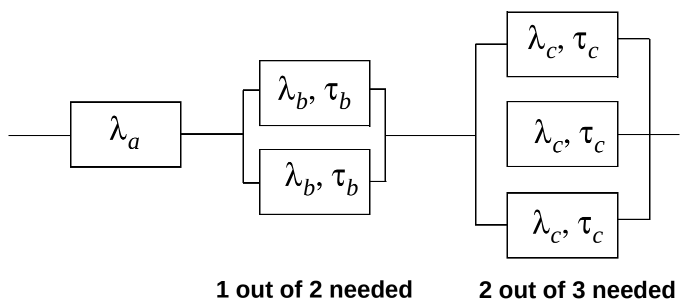


Figure 4-9. Reliability Block Diagram

Then, the system failure rate can be written down by inspection of the diagram. It is:

Equation

$$\lambda_S = \lambda_a + 2\lambda_b^2\tau_b + 6\lambda_c^2\tau_c \quad \text{(4.12e)}$$

The corresponding MTTF (θ_S) is simply $1/\lambda_S$.

Had no repairs been possible, then the task of obtaining an expression for system MTTF could be quite complicated. The starting point would be to obtain an expression for system reliability $R_S(t)$. Such an expression is given by:

Equation

$$R_S(t) = e^{-\lambda_a \cdot t} \cdot (2 \cdot e^{-\lambda_b \cdot t} - e^{-2 \cdot \lambda_b \cdot t}) \cdot (3 \cdot e^{-2 \cdot \lambda_c \cdot t} - 2 \cdot e^{-3 \cdot \lambda_c \cdot t}) \quad \text{(4.12f)}$$

To obtain an expression for the system MTTF, the above expression would have to be integrated from $t = 0$ to $t = \infty$ (not recommended). However, the answer is:

$$\frac{[(\lambda_a^3 + 6 \cdot \lambda_a^2 \cdot \lambda_b + 10 \cdot \lambda_a^2 \cdot \lambda_c + 11 \cdot \lambda_a \cdot \lambda_b^2 + 45 \cdot \lambda_a \cdot \lambda_b \cdot \lambda_c \ \ldots \ + 31 \cdot \lambda_a \cdot \lambda_c^2 + 6 \cdot \lambda_b^3 + 45 \cdot \lambda_b^2 \cdot \lambda_c + 75 \cdot \lambda_b \cdot \lambda_c + 30 \cdot \lambda_c^3]}{[(\lambda_a + \lambda_b + 3 \cdot \lambda_c) \cdot (\lambda_a + 2 \cdot \lambda_b + 3 \cdot \lambda_c) \cdot (\lambda_a + \lambda_b + 2 \cdot \lambda_c) \cdot (\lambda_a + 2 \cdot \lambda_b + 2 \cdot \lambda_c)]}$$

From the foregoing, it should be apparent that analysing quite complicated RBDs is easily accomplished by simply listing the single, then double, then triple… failure combinations and assigning to each combination terms similar to those given in expressions (4.12b), (4.12c) and (4.12e). However, when doing this, the remarks in “Cautionary Remarks” on page 4-39 must be kept very much in mind.

5. Fault Tree Analysis

Introduction

Reliability and safety analysis, particularly of complex and high-risk systems like nuclear power plants, large chemical plants, space vehicles, etc., have assumed ever-increasing importance in recent years, particularly after two major accidents in the history of nuclear power generation:

- Three Mile Island-2 in the United States.
- Chernobyl-4 in the Soviet Union.

Other events that have shaken the confidence of reliability and safety analysts as well as the public at large include:

- The release of a large amount of toxic gas in the Union Carbide factory in Bhopal, India, which resulted in the death of several thousands of people.
- The failure of the space shuttle Challenger, which resulted in the loss of millions of dollars and the death of a team of astronauts.

Although, for these systems, the techniques presented earlier on reliability block diagrams (RBDs) can be used adequately, **fault tree analysis** (FTA) offers a comparatively simple and powerful approach for reliability and safety analysis under the most general frame of assumptions.

FTA is an **event-oriented** analysis in contrast to RBD anlayis, which is structure-oriented and allows only hardware failure considerations. The advantage of event-oriented methods is that they consider not only hardware failures but also any undesirable events that may occur on account of software, human errors, operation and maintenance errors, environmental influences on the system, etc..

A **fault tree** is a pictorial representation of a system and shows how various events may lead towards a single (usually undesired) event. FTA is most often used for:

- Identifying safety-critical components.
- Verifying product requirements.
- Certifying product reliability.

- Assessing product risk.
- Investigating accidents or incidents.
- Evaluating design changes.
- Displaying the causes and consequences of events.
- Identifying common-cause failures.

FTA is a deductive analysis method that begins with a general conclusion (a system-level undesirable event) and then attempts to determine the specific causes of this conclusion. Based on a simple set of rules and logic symbols from probability theory and Boolean algebra, FTA uses a top-down approach to generate a logic model that provides for both qualitative and quantitative evaluation of system reliability.

The undesirable event at the system level is referred to as the **top event**. It generally represents a system failure mode or hazard for which predicted reliability data is required. The lowest-level events in each branch of a fault tree are referred to as **basic events**. They represent hardware, software and human failures for which the probability of failure is given based on historical or predicted data. Basic events are linked via logic symbols (gates) to one or more undesirable top events.

Another basic difference between the techniques described earlier and the fault tree methodology is that while the earlier techniques use a **success frame of consideration**, FTA uses a **failure frame of consideration**. In other words, the earlier analyses are based on an optimistic view of system operation whereas FTA is based on a pessimistic view point. However, it is interesting to observe that both the approaches have certain identifiable landmarks that are equivalent in the success-failure domains.

Figure 5-1 depicts the failure/success domain concept.

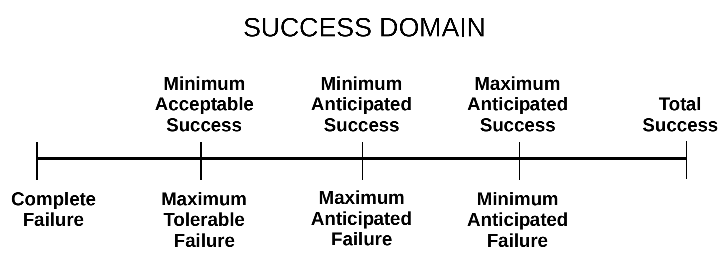


Figure 5-1. Failure/Success Domain Concept

NOTE Certain identifiable points in the success domain coincide with certain analogous points in the failure domain. For instance, “Maximum Anticipated Success” in the success domain coincides with “Minimum Anticipated Failure” in the failure domain. Although the inclination may be to select the optimistic view of the system (success rather than failure), it is often easier to agree on what constitutes a failure rather than a success. And, the size of the population in the failure domain is hopefully and generally far less than the size of the population in the success domain. This tends to occur because FTA typically concentrates on single failure units. When analysing for success, all aspects of a system are included.

FTA is one of the most widely used methods in system reliability analysis. It is a deductive procedure for determining the various combinations of hardware and software failures and human errors that could result in the occurrence of specified undesired events, referred to as **top events**, at the system level. A **deductive** analysis begins with a general conclusion, then attempts to determine the specific causes of this conclusion. This is often described as a **top-down** approach. This is in contrast to a Failure Mode and Effects Analysis (FMEA), which is considered an **inductive**, or **bottom-up**, approach.

The main purpose of FTA is to evaluate the probability of the top event using analytical or statistical methods. FTA has the capability of providing useful information concerning the likelihood of a failure and the means by which such a failure could occur. Efforts to improve system safety can be focused and refined using FTA results.

Fault Tree Construction

Fault trees show the logical connections between failure events in relation to defined top events. Fault trees can also be used to quantify the top event probabilities in much the same way as RBDs can provide the probabilty of success.

System Definition

System definition is an essential stage of FTA. Usually, a diagram defining all functional interconnections and components of the system is used as the system definition. The system definition must also include the dependencies between the components, their reliability parameters and conditions when the components are considered to have failed.

It is important that the description of the top event be both clear and concise. It sets the tone for the series of questions that must be considered when constructing the fault tree. For instance, if a top event is too vague, it can make the fault tree far too large and complex, resulting in a very unfocused fault tree. In determining the top event, it is often necessary to define not only the **what** (meaning what the specific fault is), but also to become more descriptive by including a description of **when**. The *when* in a top event may specify a specific mission phase or portion of the mission to which the top event applies. The fault tree results are more concise if the top event is descriptive rather than vague.

NOTE It may be necessary to construct a number of fault trees when considering the design of a system because a number of undesired events can exist in the system.

Top Event Occurrence Logic

A fault tree is a diagrammatic representation of the relationship between the lower-level events that may represent hardware failures, software failures, human error, etc., and a system-level event. The fault tree depicts the propagation of the lower-level events that cause a system-level undesired or top event. It is made up of successive levels such that each event is generated from lower levels via various logic operators (gates). The lowest-level events in each branch of the tree are generally referred to as **primary events** or **basic events**, but they may also be referred to as **terminal events**.

The primary events of a fault tree are those events that, for one reason or another, have not been further developed. Probabilities for these events must be provided if the fault tree is to be used for computing the probability of the top event. There are four types of primary events:

- Basic event.
- House event.
- Conditional event.
- Undeveloped event.

In addition, a Spare event is included in the literature to model spare components. For additional information, refer to “Events and Gates” below.

Events and Gates

Various symbols are used in the construction of a fault tree to represent events and gates. Each of these symbols is described in the sections that follow.

Basic Event

A basic event is either a component level event that is not further resolved. A basic event is at the lowest level in a tree branch and terminates a fault tree path. Component level events can include hardware or software failures, human errors and sub-system failures.

House Event

A house event is used to represent an event that is normally expected to occur. A house event can be turned on or off. When a house event is turned on (TRUE), that event is presumed to have occurred, and the probability of that event is set to 1. When a house event is turned off (FALSE), that event is presumed not to have occurred, and the probability is set to 0. House events are useful in making parts of a fault tree functional or non-functional. House events are also referred to as **trigger events**or **switching events**.

Conditional Event

A conditional event is used to indicate specific conditions or restrictions that apply to any logic gate, although they are most often used with Inhibit gates. For additional information, refer to “Inhibit Gate” on page 5-7.

Undeveloped Event

An undeveloped event is used if further resolution of that event does not improve the understanding of the problem or if further resolution is not necessary for proper evaluation of the fault tree. It is similar to a basic event, but is shown as a different symbol to signify that it could be developed further but that the analysis has not yet been done or need not be done for the sake of the analysis in question. Undeveloped events may changed to some other event type and broken down into associated gates and events if it is later deemed necessary.

Spare Event

A spare event is used to specify spares in dynamic fault trees. Spare events are similar to basic events in functionality; however, they allow only rates as inputs. The dormancy factor of the spare indicates the ratio of failure rate in the spare mode and the failure rate in the operational mode. Spare events can have a spares pool, which represents the number of identical instances of that event. For example, if a spares pool of an event is two, there are two identical spare components of that spare event. Spare events are restricted to use as either spares to SPARE gates or as dependent events to Functional Dependency gates.

AND Gate

The AND gate is used to indicate that the output occurs if and only if all the input events occur. The output of an AND gate can be the top event or any intermediate event. The input events can be basic events, intermediate events (outputs of other gates) or a combination of both.

Logic Summary

All events must be true (T) for the output to be true (T). If any event is false (F), then the output is false (F). Table 5-1 shows example inputs and outputs for an AND gate with two inputs.

Input A	Input B	Output
T	T	T
T	F	F
F	T	F
F	F	F

Table 5-1. Truth Table for AND Gate

OR Gate

The OR gate is used to indicate that the output occurs if and only if at least one of the input events occur. The output of an OR gate can be the top event or any intermediate event. The input events can be basic events, intermediate events or a combination of both. There should be at least two inputs to an OR gate.

Logic Summary

If at least one event is true (T), the output is true (T). If all events are false (F), then the output is false (F). Table 5-2 shows example input and output events for an OR gate with two inputs.

Input A	Input B	Output
T	T	T
T	F	T
F	T	T
F	F	F

Table 5-2. Truth Table for OR Gate

Voting Gate

The Voting (*M*/*n*) gate is used to indicate that the output occurs if and only if *M* out of the *n* input events occur. The output occurs when at least *m* input events occur. When *M* = 1, the Voting gate behaves like an OR gate. The output of a Voting gate can be a top event or an intermediate event. The input events can be basic events, intermediate events or a combination of both.

Logic Summary

If *M* = 2 and *n* = *3*, two (2) input events must be true (T) for the output to be true (T). If only one input event is true (T), then the output is false (F). Table 5-3 shows the input and output events for a 2 out-of-3 Voting gate.

Input A	Input B	Input C	Output
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	F
F	T	T	T
F	T	F	F
F	F	T	F
F	F	F	F

Table 5-3. Truth Table for 2-out-of-3 Voting Gate

Inhibit Gate

The Inhibit gate is used to indicate that the output occurs when the input events (l1 and l2) occur and the input condition (C) is satisfied. The output of an Inhibit gate can be a top event or an intermediate event. The input events can be basic events, intermediate events or a combination of both.

Logic Summary

If all input events and the input condition are true (T), then the output is true (T). Table 5-4 shows the input and output events for an Inhibit gate.

I1	I2	C	Output
T	T	T	T
T	T	F	F
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	F
F	F	T	F
F	F	F	F

Table 5-4. Truth Table for Inhibit Gate

Exclusive OR Gate

The Exclusive OR (XOR) gate is used to indicate that the output occurs if and only if one of the two input events occurs and the other input event does not occur. An XOR gate can only have two inputs. The output of an Exclusive OR gate can be the top event or an intermediate event. The input events can be basic events, intermediate events or a combination of both. The presence of an XOR gate may give rise to **non-coherent trees**, where the non-occurrence of an event causes the top event to occur.

Logic Summary

If one and only one input event is true (T), the output is true (T). If more than one input is true (T), then the output is false (F). Table 5-5 shows the input and output events for an Exclusive OR gate.

Input A	Input B	Output
T	T	F
T	F	T
F	T	T
F	F	F

Table 5-5. Truth Table for Exclusive OR Gate

NOT Gate

The NOT gate is used to indicate that the output occurs when the input event does not occur. The presence of a NOT gate may give rise to non-coherent trees, where the non-occurrence of an event causes the top event to occur. There is only one input to a NOT gate.

Logic Summary

The output is the opposite of the input gate or event. Table 5-6 shows the input and output events for a NOT gate.

Input A	Output
T	F
F	T

Table 5-6. Truth Table for NOT Gate

NOR Gate

The NOR gate functions like a combination of an OR gate and a NOT gate. The NOR gate is used to indicate that the output occurs when all the input events are absent. The output of a NOR gate can be the top event or an intermediate event. The input events can be basic events, intermediate events or a combination of both. The presence of a NOR gate may give rise to non-coherent trees, where the lack of one or more events causes the top event to occur.

Logic Summary

If there is at least one true input event, the output is false. Table 5-7 shows the input and output events for a NOR gate.

Input A	Input B	Output
T	T	F
T	F	F
F	T	F
F	F	T

Table 5-7. Truth Table for NOR Gate

NAND Gate

The NAND gate functions like a combination of an AND gate and a NOT gate. The NAND gate is used to indicate that the output occurs when at least one of the input events is absent. The output of a NAND gate can be the top event or an intermediate event. The input events can be basic events, intermediate events or a combination of both. The presence of a NAND gate may give rise to non-coherent trees, where the non-occurrence of an event causes the top event to occur.

Logic Summary

If there is at least one false (F) event, the output is true (T). Table 5-8 shows the input and output events for a NAND gate.

Input A	Input B	Output
T	T	F
T	F	T
F	T	T
F	F	T

Table 5-8. Truth Table for NAND Gate

Priority AND Gate

The Priority AND (PAND) gate is used to indicate that the output occurs if and only if all input events occur in a particular order. The order is the same as that in which the inputs events are connected to the PAND gate from left to right. The PAND gate is a dynamic gate, which means that the order of the occurrence of input events is important to determining the output.

The output of a PAND gate can be the top event or an intermediate event. The inputs can be basic events or outputs of any AND gate, OR gate, or dynamic gate, which includes the SPARE gate, PAND gate, sequence-enforcing (SEQ) gate and functional dependency (FDEP) gate. (These gates should have the inputs from basic events or other AND gates and OR gates.) The items that enter a PAND gate need to fail in temporal order from left to right to trigger the event. The PAND gate also supports a single input. When only a single input exists, then occurrence of that input will trigger the event.

Logic Summary

All input events must be true (T) for the output to be true (T) and the events must occur from left to right in the temporal order. Table 5-9 shows the input and output events for a PAND gate.

Input A	Input B	Output
T(1)	T(2)	T
T(2)	F(1)	F
T	F	F
F	T	F
F	F	F

Table 5-9. Truth Table for PAND Gate

Functional Dependency Gate

The Functional Dependency (FDEP) gate is used to indicate that all dependent basic events are forced to occur whenever the trigger event occurs. The separate occurrence of any of the dependent basic events has no effect on the trigger event. The FDEP gate has one trigger event and can have one or more dependent events. All dependent events are either basic events or spare events. The trigger event can be a terminal event or output of any AND gate, OR gate or dynamic gate, which includes the SPARE gate, PAND gate, Sequence-Enforcing gate (SEQ) and FDEP gate.

Dependent events are repeated events that are present in other parts of the fault tree. The FDEP gate is a dynamic gate, which means the temporal order of the occurrence of events is important to analyse this gate. Generally, the output of the FDEP gate is not that important; however, it is equivalent to the status of its trigger event.

The FDEP gate can also be used to set the priorities for SPARE gates. For example, if multiple spares are connected to a FDEP gate, after the occurrence of the trigger event, all spares that are connected to the FDEP gate will fail. Upon failure of these spares, the next available good spares in those SPARE gates will replace the failed spares. If there exists a conflict in choosing the next available spare between multiple SPARE gates, the priority will be based on the order of the connection of these spares in the FDEP gate from left to right.

Logic Summary

When the trigger event is true (T), then dependent events are forced to become true (T). The trigger event must be true (T) for the output to be true (T). Table 5-10 shows a truth table for a FDEP gate.

Trigger	Output	Dependent Event A	Dependent Event B
T	T	T	T
F	F	T/F	T/F

Table 5-10. Truth Table for FDEP Gate

Sequence Enforcing Gate

The Sequence-Enforcing (SEQ) gate forces events to occur in a particular order. The input events are constrained to occur in the left-to-right order in which they appear under the gate. That means that the left-most event must occur before the event on its immediate right, which must occur before the event on its immediate right is allowed to occur. The SEQ gate is used to indicate that the output occurs if and only if all input events occurs, when the input events are constraint to occur in a particular order.

The SEQ gate is a dynamic gate, which means the occurrence of the inputs follows a sequential order. In other words, an event connected to a SEQ gate will be initiated immediately after occurrence of its immediate left event. Therefore, if the left-most input is a basic event, then the SEQ gate works like a cold SPARE gate. The SEQ gate can be contrasted with the PAND gate in that the PAND gate detects whether events occur in a particular order (but the events can occur in any order), whereas the SEQ gate allows the events to occur only in the specified order. The first input (left-most input) to a SEQ gate can be a terminal event or outputs of any AND gate, OR gate or dynamic gate, which includes the SPARE gate, PAND gate, FDEP gate or SEQ gate). Only basic events are allowed for all other inputs.

Logic Summary

The output is true (T) if and only if all input events are true (T). However, the input events must occur in a particular order. Table 5-11 shows a truth table for a SEQ gate.

Input1 A	Input 2 B	Input 3 C	Output
F	F	F	F
F	F	T	Not Possible
F	T	F	Not Possible
F	T	T	Not Possible
T	F	F	F

Table 5-11. Truth Table for SEQ Gate

Input1 A	Input 2 B	Input 3 C	Output
T	T	F	F
T	T	T	T

Table 5-11. Truth Table for SEQ Gate (Continued)

SPARE Gate

The SPARE gate is used to model the behaviour of spares in the system. The SPARE gate is used to indicate that the output occurs if and only if all input spare events occur. All inputs of a SPARE gate are spare events. A SPARE gate can have multiple inputs. The first event (left-most event) is known as the primary input, and all other inputs are known as alternative inputs. The primary event is the one that is initially powered on, and the alternative inputs and are initially in standby mode.

After a failure, the active/powered unit that is the first available spare from left to right will be chosen to be active. If all units are failed, then the spare will be considered as failed (output occurred). Depending on the dormancy factor of spares, spares can fail even in standby mode.

If the dormancy factor of all spares connected to a SPARE gate are 0, then the spare acts like a cold spare. If the dormancy factor of all spares connected to a SPARE gate is 1, then the spare acts like a hot spare. If the dormancy factor of all spares connected to a SPARE gate are the same (and are between 0 and 1), then the spare acts like a warm spare. If the dormancy factors of its inputs are different, then it handles generalised situations. The SPARE gate is a dynamic gate, which means the temporal order of the occurrence of events is important to analyse this gate.

Transfer Gate

The Transfer gate is a symbol used to link logic in separate areas of a fault tree. There are two primary uses of Transfer gates. First, an entire fault tree may not fit on a single sheet of paper. (Or, to better view and organise them, the preference is to keep the individual trees small.) Second, the same fault tree logic may be used in different places in a fault tree. Through the use of Transfer gates, this logic can be defined once and then used in several places. To use a Transfer gate, a Transfer In gate is inserted in a fault tree and then linked to a Transfer Out gate, which represents the top gate of another fault tree.

Remarks Gate

The Remarks gate is used for the entry of comments. A Remarks gate has no calculation data associated with it, and, therefore, has no effect on calculations. However, the tree branch may continue after a Remarks gate. There can only be one input to a Remarks gate.

Pass-Through Gate

The Pass-Through gate is used for visually aligning the events and gates in a fault tree. A Pass-Through gate extends a vertical connector for visual alignment. A Pass-Through gate has no calculation data associated with it, and, therefore, has no effect on calculations. However, the tree branch may continue after a Pass-Through gate. There can be only one input to a Pass-Through gate.

Fault Tree Example

Some of the basic aspects of a fault tree construction can be explained through an example of a d.c. motor circuit.

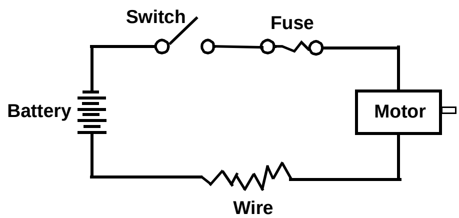


Figure 5-2. Schematic Circuit Diagram for the Operation of a D.C. Motor

The following steps indicate how a fault tree is constructed for a motor circuit when it does not operate when the switch is closed.

1. Decide what the undesired event of this system is and define it:

   Top event = `Motor does not operate when the switch is closed`.

2. Next, deductively determine the reasons why the motor may not operate. Such reasons may be:

   – Some internal faults exist within the motor itself, which is a basic motor failure. (Because this is a primary fault, it does not have to be developed any further in the fault tree.)

- The motor is not receiving any current. This fault event can be further developed to determine the causes for why the motor may not be receiving any current. Possible causes include:
  (1) The fuse may be in an open circuit failure mode due to over current in the circuit.
  (2) The switch may be in an open circuit.
  (3) The battery may have failed. (Because this is a basic event, it does not have to be developed any further in the fault tree.)
  (4) The connecting wire of the circuits may be open. (Because this is a basic event, it does not have to be developed any further in the fault tree.)

3. Decide the logic connecting the above events. In this example, an OR gate connects these particular events.
4. Determine if any of the causes need to be further developed. For example, a fuse can open if there is an over current in the circuit. However, the fuse does not open unless the over current is sufficient to melt the fuse. Therefore, fuse failure can be due to two reasons.
   - Secondary fuse failure is caused by bad fuse design or the selection of an inappropriate size of fuse wire.
   - Primary fuse failure is caused by an overload in the circuit. This fault event can be further developed to determine the causes for the overload. Possible causes include:
     (1) The lead wire to the motor terminals shorts.
     (2) The power supply voltage to the motor may be suddenly very high.

NOTE In the following figure, the event, `Switch Open`, is not developed further because sufficient information is not available. Therefore, it is an undeveloped event.

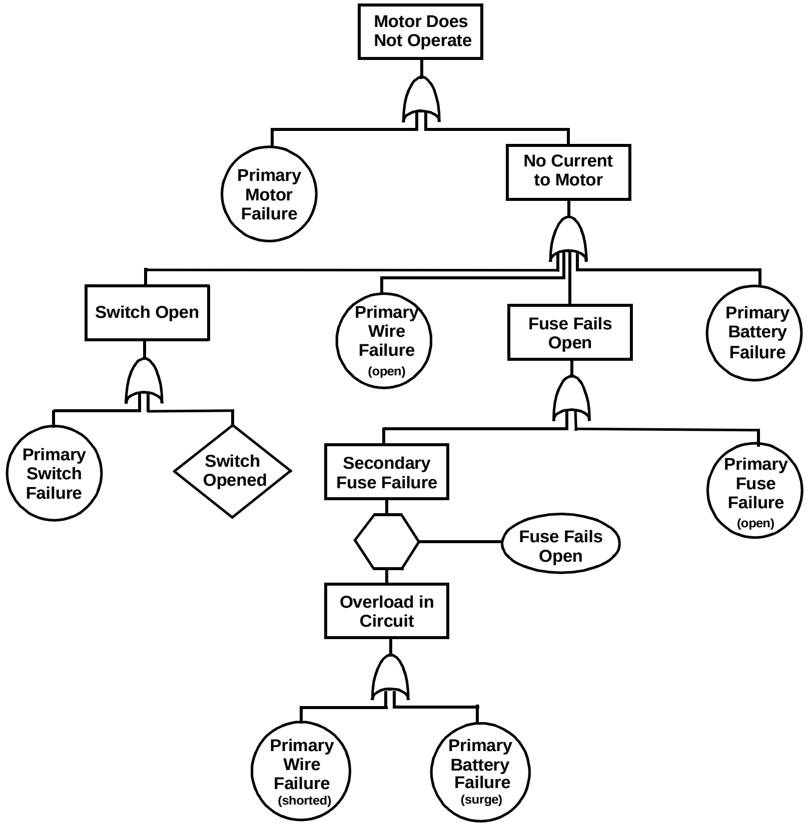


Figure 5-3. Fault Tree for "Motor Does Not Operate" When Switch is Closed

Analysis Methods

The main purposes of FTA are to evaluate the probability of the occurrence of the top event and show the chain of events that may cause the top event to occur. Prior to numeric information being entered into a fault tree, a qualitative analysis may be performed. To determine the probability of occurrence of the top event, however, system quantitative reliability and maintainability information such as failure probability, failure rate or repair rate must be used.

Qualitative Analysis

Qualitative analysis determines the **minimal cut sets** of your fault tree based on the gate logic. A **cut set** is a set of events that cause the top event to occur. A minimal cut set (MCS) is the smallest set of events, which, if they all occur, cause the top event to occur. If you remove any of the basic events from a minimal cut, the cut set would not remain. The basic events that belong to the cut sets provide information such as single point failures and the relative contribution of each cut set. Generally, cut sets that have the highest probability of occurrence are the ones that have the least number of basic events.

Quantitative Analysis

It is often desirable to be able to quantify the probability of occurrence of the top event and each of the minimal cut sets. To perform this task, reliability and maintainability information such as failure probability, failure rate or repair rate is used. Information about the minimal cut sets obtained in the qualitative stage of the analysis can then be used for computing the unavailability and unreliability of the system. In fault tree analysis, unavailability and unreliability values (rather than availability and reliability) are used because fault trees are organised around failures, unlike reliability block diagrams, which are organised around successes.

There are various quantitative methods that are used in quantitative analysis of fault trees, including:

- **Bottom-up method**. This is a very simple and fast method. It first finds the probabilities of all basic events, and then it uses these probabilities to find the probabilities of the lowest level gates. Similarly, it uses the lowest level gate probabilities to find next higher level gate probabilities, continuing this process until the top event probability is calculated. This method cannot be used to find the exact top event probability when repeated events exist because it assumes the independence of all sub-trees of the fault tree.
- **Top-down method**. This is also a very simple and fast method. It is based on recursion. The top event probability is calculated using the probabilities of the gates or events that are connected to the top event. Similarly, this process continues until the required information for performing this recursion is obtained. This method can not be used to find the exact top event probability when repeated events exist because it assumes the independence of all sub-trees of the fault tree.
- **Simulation**. This method is conceptually simple and can handle any type of fault tree. However, it takes more time in analysing complex systems to arrive at reasonably accurate results. This method first generates random numbers associated with each event, and then determines whether that event has occurred or not. The status of individual events, that is occurrence and non-occurrence informa-

tion (also the times if temporal order of events is important), is used to find the status of the top event (occurrence or non-occurrence). This process will be continued for many iterations. Then, the probability of the top event is calculated by finding the ratio of the number of top event occurrences and total number of simulation trials.

- **Cut Sets Method**. This method is useful for finding the exact results of the top event probability, particularly when repeated events exist. It is also useful to find results with a prescribed accuracy. The cut sets method first finds the minimal cut sets of the fault tree and uses these minimal cut sets to find the top event probability of the fault tree.

- **Shannon's Expansion**. Shannon's expansion method uses conditional probabilities recursively to find the top event probability. Consider a fault tree with events *A*, *B* and *C*. The top event probability can be expressed as: $Pr\{A\} \cdot Pr\{top|A\} + Pr\{\sim A\} \cdot Pr\{top|\sim A\}$, where $Pr\{A\}$ and $Pr\{\sim A\}$ are the probability of the occurrence of event *A* and the probability of non-occurrence of event *A* respectively. $Pr\{top|A\}$ is the probability of the top event given that event *A* has occurred. Similarly, $Pr\{top|\sim A\}$ is the probability of the top event given that event *A* has not occurred. Now, $Pr\{top|A\}$ and $Pr\{top|\sim A\}$ are calculated as a sum of conditional probabilities based on the occurrence of other events. This process is continued until the conditional probabilities are known.

- **Disjointing Method**. Top-down and bottom-up methods can be applied only for modular fault trees (for example, a fault tree without repeated events). If repeated events exist, then these methods do not produce correct results and should not be used. Alternative methods for when repeated events exist include simulation, the cut set method, Shannon's expansion method and the disjointing method. Simulation and the cut set method are time-consuming and cannot be applied for large systems. Shannon's expansion method uses conditional probability (total probability concept), continuing the process until all conditional probabilities are known. Thus, it may not be very effective when only a few repeated events are present. To overcome this difficulty, conditional probabilities and modularization concepts are used like in RBDs. A module of a fault tree is a subtree when none of its events are present in other parts of the fault tree. In this method, fault trees are disjointed as in Shannon's expansion method; however, they are conditioned on repeated events. For example, if there is a repeated event in the fault tree (say it is event A), the top event probability can be calculated using $Pr\{A\} \cdot Pr\{top|A\} + Pr\{\sim A\} \cdot P\{top|\sim A\}$. Because there is only one repeated event in this example, calculating $Pr\{top|A\}$ and $P\{top|\sim A\}$ do not involve any repeated events as the resultant event does not contain event A. Because the resultant fault tree is a module (contains no repeated event), its probability can be obtained using modular techniques (bottom-up approach). Therefore, the number of computations in this process are far fewer than when Shannon's expansion method is used.

- **Binary Decision Diagrams**. Binary decision diagrams are based on Shannon's expansion. The main advantage of binary decision diagrams over Shannon's expansion is that it eliminates the redundant computation in the process of finding the conditional probabilities. Therefore, it takes much less time to find the top event probability.
- **Sequential Analysis Using Stochastic Processes**. All of the above analytical methods except simulation are applicable only for combinatorial analysis and can not be used for sequence dependent situations such as the presence of dynamic gates. In such cases, the problem cannot be solved using combinatorial methods. If the events have exponentially distributed failure/occurrence and repair times, then top event probability can be found using Markov models. To perform this, the fault tree must be converted into an equivalent Markov model. For additional information, see "Markov Modelling" on page 8-1. If the distributions are not exponential, non-homogeneous Markov models or Semi-Markov models are needed. Because all dynamic fault trees cannot be converted to equivalent Markov models or Semi-Markov models, simulation methods may be required.
- **Hybrid Approach**. It is understandable that no method is suitable for all type of fault trees. Although, simulation can be used for any type of fault tree, it takes lots of time. Therefore, it is better to solve each module (independent sub-tree) of the fault tree separately, using an appropriate method, and then combine the results to find the top event probability.

Additional topics in this chapter contain more information about the bottom-up and disjointing methods.

Bottom-Up Method

This method first calculates the probabilities of the bottom most gates first, and then it uses this information to find the next higher-level gates. The following equations are used for calculating the probabilities of various gates.

AND Gate

If $A_1, A_2, ..., A_n$ are the inputs and A is the output of an AND gate, then the probability of (occurrence of the output of) the gate is:

$$Pr\{A\} = Pr\{A_1\} \cdot Pr\{A_2 | A_1\} \cdot .... \cdot Pr\{A_n | A_1, A_2, ..., A_{n-1}\}$$

If all events are independent, then:

$$Pr\{A\} = Pr\{A_1\} \cdot Pr\{A_2\} \cdot .... \cdot Pr\{A_n\}$$

Example Events A and B are independent and are connected to an AND gates. Given that the probabilities of these events are 0.1 and 0.2 respectively, then the gate probability is:

$$(0.1) \cdot (0.2) = 0.02$$

OR Gate

If $A_1, A_2, ..., A_n$ are the inputs and A is the output of an OR gate, then the probability of (occurrence of the output of) the gate is:

$$Pr\{A\} = Pr\{A_1\} + Pr\{A_2| \sim A_1\} + ... + Pr\{A_n| \sim A_1, \sim A_2, ..., \sim A_{n-1}\}$$

If all events are independent, then:

$$Pr\{A\} = Pr\{A_1\} + Pr\{A_2\} \cdot Pr\{\sim A_1\} + ... + Pr\{A_n\} \cdot Pr\{\sim A_1\} \cdot Pr\{\sim A_2\} \cdot ... \cdot Pr\{\sim A_{n-1}\}$$

$$= Pr\{A_1\} + Pr\{A_2\} \cdot (1-Pr\{A_1\}) + ...$$

$$+ Pr\{A_n\} \cdot (1-Pr\{A_1\}) \cdot (1-Pr\{A_2\}) \cdot ... \cdot (1-Pr\{A_{n-1}\})$$

$$= 1 - (1-Pr\{A_1\}) \cdot (1-Pr\{A_2\}) \cdot ... \cdot (1-Pr\{A_n\})$$

Example Events A and B are independent and are connected to an OR gate. Given that the probabilities of these events are 0.1 and 0.2 respectively, then the gate probability is:

$$1 – (1-0.1) \cdot (1-0.2) = 0.28$$

Voting Gate

If $A_1, A_2, ..., A_n$ are the independent inputs and A is the output of a Voting gate (k-out-of-n), then the probability of the gate is:

$Pr\{A\}$ = Probability of all combinations of events that events that have at least k success events.

If all events are statistically independent and identical, and the probability of each event is r, then:

$$Pr\{A\} = {}^nC_k\,(r)^k\,(1-r)^{n-k} + ... + {}^nC_n\,(r)^n\,(1-r)^{n-n}$$

NOT Gate:

If A_1 is the input and A is the output of a NOT gate, then the probability of the gate is:

$$Pr\{A\} = Pr\{\sim A_1\} = 1 - Pr\{A_1\}$$

XOR Gate:

If A_1 and A_2 are the inputs and A is the output of an XOR gate, then the probability of the gate is:

$$Pr\{A\} = Pr\{A_1 \text{ and } \sim A_2\} + Pr\{A_2 \text{ and } \sim A_1\}$$

If the events are independent, then:

$$Pr\{A\} = Pr\{A_1\} \cdot Pr\{\sim A_2\} + Pr\{A_2\} \cdot Pr\{\sim A_1\}$$
$$= Pr\{A_1\} + Pr\{A_2\} - 2 \cdot Pr\{A_1\} \cdot Pr\{A_2\}$$
$$= Pr\{\sim A_1\} + Pr\{\sim A_2\} - 2 \cdot Pr\{\sim A_1\} \cdot Pr\{\sim A_2\}$$

Example Consider a fault tree with four basic events: *A*, *B*, *C* and *D*. The top event is *T*. The events *A* and *B* are connected to an OR gate named *Gate1*. The events *C* and *D* are connected to an XOR gate named *Gate2*. The gates *Gate1* and *Gate2* are connected to the top event using an AND gate. Figure 5-4 shows this fault tree.

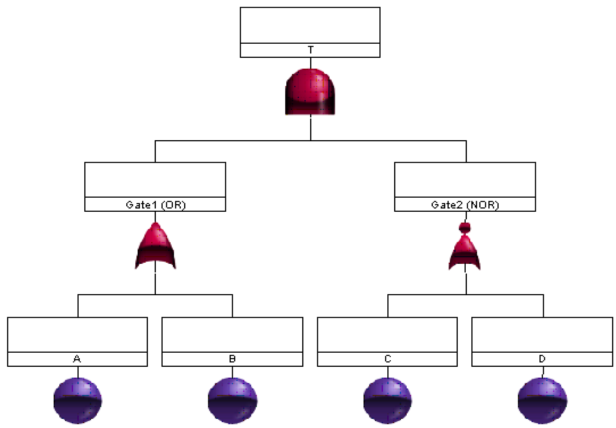


Figure 5-4. Fault Tree with Four Basic Events

Assuming that the probabilities of the basic events are:

$Pr\{A\} = 0.1$

$Pr\{B\} = 0.2$

$Pr\{C\} = 0.3$

$Pr\{D\} = 0.5$

Then:

$$Pr\{Gate1\} = 1 - (1 - Pr\{A\}) \cdot (1 - Pr\{B\})$$
$$= 1 - (1-0.1) \cdot (1-0.2)$$
$$= 0.28$$

$$Pr\{Gate2\} = Pr\{C\} (1 - Pr\{D\}) + (1 - Pr\{C\}) \cdot Pr\{D\}$$
$$= 0.3 \cdot (1-0.5) + 0.5 \cdot (1-0.3)$$
$$= 0.5$$

$$Pr\{top\ gate\} = Pr\{T\} = Pr\{Gate1\} \cdot Pr\{Gate2\}$$

$$= (0.28) \cdot (0.5)$$

$$= 0.14$$

Disjointing Method

This section illustrates the disjointing method, which uses the Bayes theorem while solving the fault tree. Thus, this method is similar to the method explained in the "Bayes Theorem" topic on page 4-11. The top event of the fault tree shown in Figure 5-5 represents the failure of this same power supply.

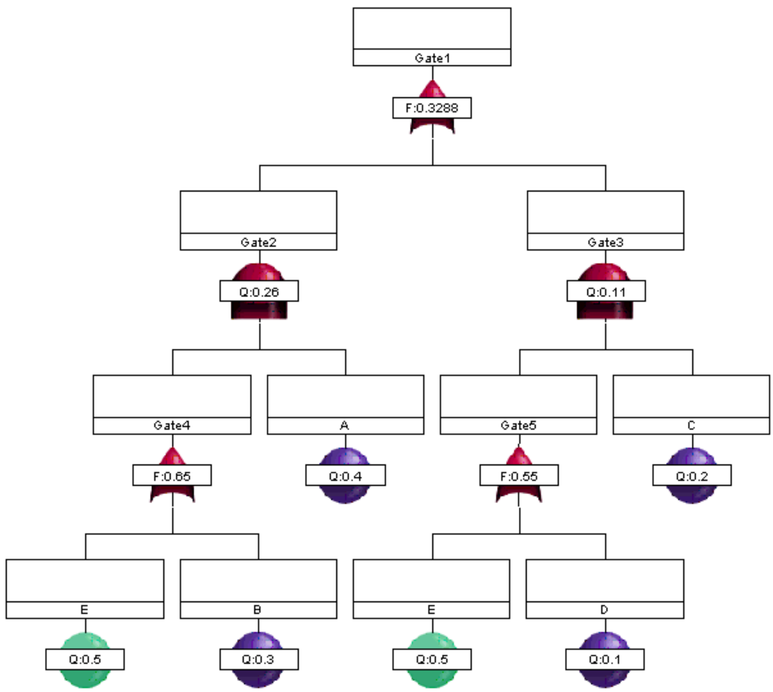


Figure 5-5. Power Supply Failure Fault Tree

In this example, event E is a repeated event. The following steps are performed for the disjointing method:

1. Calculate the top event probability twice:

   a. The first time, assume that event E has occurred (assume $Pr\{E\}$ as 1). Denote this probability as $Pr\{T|E = 1\}$.

b. The second time, assume that event E has not occurred (assume $Pr\{E\}$ as 0). Denote this probability as $Pr\{T|E = 0\}$.

2. Calculate $Pr\{T\}$ as $Pr\{E\} \cdot Pr\{T|E\} + Pr\{\sim E\} \cdot Pr\{T|\sim E\}$.

Calculation of $Pr\{T|E\}$

$Pr\{\mathrm{T}|E\}$ is the probability of the top event of the fault tree shown in Figure 5-6. This figure is simplified based on the condition that Event E has already occurred.

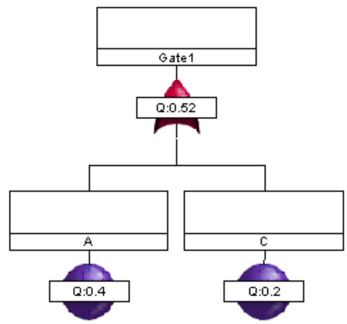


Figure 5-6. Power Supply Fault Tree When Event E Has Already Occurred

Thus:

$$Pr\{\mathrm{T}|E\}= 1 - (1-Pr\{A\}) \cdot (1-Pr\{\mathrm{C}\})$$

Similarly, $Pr\{\mathrm{T}|\sim E\}$ is the probability of the top event of the fault tree shown in Figure 5-7. This figure is simplified based on the condition that Event E has not occurred.

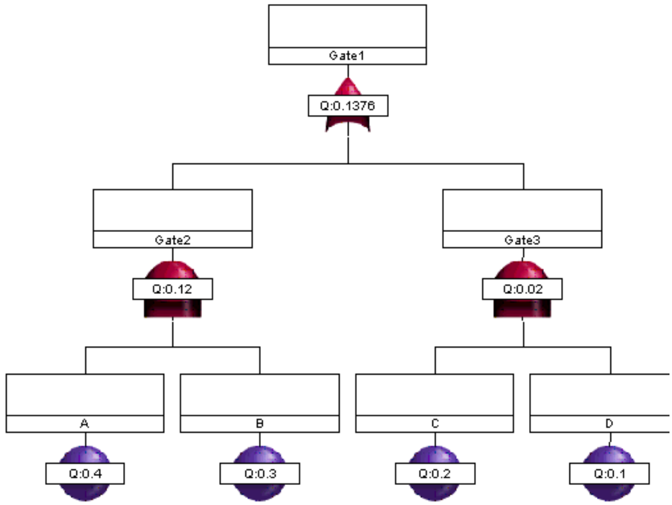


Figure 5-7. Power Supply Fault Tree When Event E Has Not Occurred

Thus:

$Pr\{T|\sim E\} = 1 - (1 - Pr\{A\} \cdot Pr\{B\}) \cdot (1 - Pr\{C\} \cdot Pr\{D\})$

Finally, the top event probability, *Pr{T}* is given below:

$Pr\{T\} = Pr\{E\} \cdot (1 - (1 - Pr\{A\}) \cdot (1 - Pr\{C\})) + Pr\{\sim E\} \cdot (1 - (1 - Pr\{A\} \cdot Pr\{B\}) \cdot (1 - Pr\{C\} \cdot Pr\{D\})$.

Assuming that the probabilities of the basic events are:

$Pr\{A\} = 0.4$

$Pr\{B\} = 0.3$

$Pr\{C\} = 0.2$

$Pr\{D\} = 0.1$

$Pr\{E\} = 0.5$

Then:

The top event probability is 0.3288.

This means that system unreliability is 0.3288 and hence system reliability is $1 - 0.3288 = 0.6712$.

Lambda-Tau Calculations

The Lambda-Tau method is an alternative way to analyse a fault tree. It can be used to determine availability or short-term reliability when the age of a component or system is unknown or indeterminate. Lambda-Tau calculations are very good to use in the case of a system that is well-maintained and routinely undergoes preventative maintenance. In such systems, the age of specific components is difficult to determine, or the components have reached steady-state behaviour.

There are various situations where Lambda-Tau calculations may be applied. In all these situations, Lambda signifies the failure rate of the system or component. Tau can represent the inspection interval, repair time or mission time of the system, depending on the type of model in use. Table 5-12 describes various Lambda-Tau models and their calculations.

Model	Description
Lambda Tau	This model approximates the probability of failure and asymptotic unavailability. $A = \lambda\tau$ τ = mission time to MTTR
Average Unavailability (approximately)	This model approximates the average unavailability. $A = \frac{\lambda\tau}{2}$ τ = time between tests (inspection interval)
Probability of Failure	This model uses Tau as the mission time. $A = 1 - exp\{-\lambda\tau\}$ τ = mission time to MTTR
Asymptotic Unavailability	This model uses asymptotic behaviour. $A = \frac{\lambda\tau}{\lambda\tau + 1}$ τ = MTTR
Average Unavailability	This models uses average unavailability over 0 and Tau. $A = 1 + \frac{exp\{-\lambda\tau\} - 1}{\lambda\tau}$ τ = time between tests (inspection interval)

Table 5-12. Lambda-Tau Models

Common Cause Failures

An event or mechanism that can cause two or more failures (basic events) simultaneously is called a **common cause**, and the failures themselves are called **common cause failures**. Because common causes can induce the failure of multiple components, they have the potential to increase system failure probabilities. The elimination of these common causes can appreciably improve system reliability.

Designers must recognise the failure sources that are responsible for common cause failures and implement specific solutions to deal with them. A list of frequently encountered causes, which are not in any specific order, follows:

- Mechanical Causes:
  - Abnormally high or low temperature.
  - Abnormally high or low pressure.
  - Stress above design limits.
  - Impact.
  - Vibration.
- Electrical Causes:
  - Abnormally high voltage.
  - Abnormally high current.
  - Electromagnetic interference.
- Chemical Causes:
  - Corrosion.
  - Chemical reaction.
- Other Causes:
  - Earthquake.
  - Tornado.
  - Flood.
  - Lightning.
  - Fire.
  - Radiation.
  - Moisture.

- Dust.
- Design or production defect.
- Test/maintenance/operation error.

Common Cause Analysis

There are several models for quantifying systems subject to common cause failures. Some of the popular models are:

- Beta Factor model.
- Multiple Greek Letter (MGL) model.
- Alpha model.
- Beta Binomial Failure Rate (BFR) model.

Example The following example is provided as an aid in understanding the mechanism of the handling of common cause failure (CCF) events in a fault tree. Assume that there are four basic events *A*, *B*, *C* and *D* belonging to a CCF group. When an analyst does the minimal cut set analysis of the fault tree, the following CCF events should be created corresponding to the basic events:

AB, *AC*, *AD*, *BC*, *BD*, *CD*, *ABC*, *ABD*, *ACD*, *BCD* and *ABCD*

For calculation purposes, each of the four original basic events (*A*, *B*, *C* or *D*) is replaced with an OR gate. The inputs to the OR gate include the individual basic event and CCF events that contain that basic event. For example, event *A* is replaced by an OR gate with *A* (individual failure), *AB*, *AC*, *AD*, *ABC*, *ABD*, *ACD* and *ABCD* as its inputs.

The following parameters are used in calculating CCF events:

Q_t = Total unavailability of each basic event in the CCF group.

Q_k = Unavailability of the CCF event of order *k*, which is a common cause failure involving *k* components.

n = Number of basic events in the CCF group.

Beta Factor Model

The Beta Factor model is the most basic model. It assumes that all components belonging to a CCF group fail when that common cause occurs. By definition, this model distinguishes between individual failures and CCFs, with the assumption that if the CCF occurs, all components fail simultaneously by a common cause. Multiple independent failures are neglected. The input parameter and calculations for the unavailabilty of CCF events for the Beta Factor model are:

Input Parameter: β

Unavailability of CCF events:

$$Q_1 = (1-\beta)Q_t$$

$$Q_k = 0 \qquad k = 2, 3, \ldots, n\text{-}1$$

$$Q_n = \beta Q_t$$

If $n = 4$, then the input parameter and calculations for the unavailability of CCF events would be:

Input Parameter: β

Unavailability of CCF events:

$$Q_1 = (1-\beta)Q_t$$

$$Q_2 = 0$$

$$Q_3 = 0$$

$$Q_4 = \beta Q_t$$

Multiple Greek Letter Model

The Multiple Greek Letter (MGL) model is a generalisation of the Beta Factor model. The input parameters and calculations for the unavailabilty of CCF events for the Multiple Greek Letter model are:

Input Parameters: $\rho_1 = 0, \rho_2 = \beta, \rho_3 = \gamma, \rho_3 = \delta, \ldots, \rho_n, \rho_{n+1} = 0$

Unavailability of CCF events:

$$Q_k = \frac{(\Pi_{i=1}^{k}\rho_i)(1-\rho_{k+1})Q_t}{\binom{n-1}{k-1}} \quad (k = 1, 2, \ldots, n)$$

ρ_i is the conditional probability that the cause of failure of a specific component will be shared by at least i additional components. If $n = 4$, then the input parameter and calculations for the unavailability of CCF events would be:

Input Parameters: β, γ, δ

Unavailability of CCF events:
$$Q_1 = (1-\delta)Q_t$$
$$Q_2 = \frac{\beta}{3}(1-\gamma)Q_t$$
$$Q_3 = \frac{\beta\gamma}{3}(1-\gamma)Q_t$$
$$Q_4 = \beta\gamma\delta Q_t$$

Alpha Factor Model

The input parameters and calculations for the unavailabilty of CCF events for the Alpha Factor model are:

Input Parameters: $\alpha_1, \alpha_2, \ldots, \alpha_n$

Unavailability of CCF events:
$$Q_k = \frac{n}{\binom{n}{k}}\frac{\alpha_k}{\mu_\alpha}Q_t$$

$$\mu_\alpha = \sum_{k=1}^{n} k\alpha_k$$

α_k is the probability of having a failure of multiplicity k. Therefore, $\Sigma_k\alpha_k = 1$. If n = 4, then the input parameter and calculations for the unavailability of CCF events would be:

Input Parameters: $\alpha_1, \alpha_2, \alpha_3, \alpha_4$

Unavailability of CCF events:
$$Q_1 = \frac{\alpha_1}{\mu_\alpha}Q_t$$
$$Q_2 = \frac{2\alpha_2}{3\mu_\alpha}Q_t$$
$$Q_3 = \frac{\alpha_3}{\mu_\alpha}Q_t$$
$$Q_4 = \frac{4\alpha_4}{\mu_\alpha}Q_t$$
$$\mu_\alpha = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4$$

Binomial Failure Rate Model

The Binomial Failure Rate model is also known as a **shock model**. The input parameters and calculations for the unavailabilty of CCF events for the Binomial Failure Rate model are:

Input Parameters: $p = \beta_1, Q_{SH} = \beta_2, Q_{LH} = \beta_3, Q_I$

Unavailability of CCF events: $Q_1 = Q_I + Q_{SH} \cdot (1-p)^n \equiv Q_1 + \beta_2(1-\beta_1)^n$

$$Q_k = Q_{SH} \cdot p^k(1-p)^{n-k} \equiv \beta_2\beta_1^k(1-\beta_1)^{n-k}$$
$(k = 2, 3, \ldots, n - 1)$

$$Q_n = Q_{SH} \cdot p^n + Q_{LS} \equiv \beta_2 B_1^m + \beta_3$$

Q_1 is the independent failure probability of each component, p is the conditional probability of failure of each component (given a non-lethal shock), Q_{SH} is the occurrence probability of non-lethal shock, and Q_{LS} is the occurrence probability of lethal shock. Therefore, $Q_t = Q_I + p \cdot Q_{SH} + Q_{LS}$.

If $n = 4$, then the input parameter and calculations for the unavailability of CCF events would be:

Input Parameters: $\beta_1, \beta_2, \beta_3$

Unavailability of CCF events: $Q_1 = Q_I + \beta_2\beta_1(1-\beta_1)^3$

$$Q_2 = \beta_2\beta_1^2(1-\beta_1)^2$$

$$Q_3 = \beta_2\beta_1^3(1-\beta_1)$$

$$Q_4 = \beta_2\beta_1^4 + \beta_3$$

Importance Measures

Reliability importance measures attempt to identify the event whose improvement will yield the most improvement in system performance. The three most popularly used importance measures are:

- Birnbaum.
- Criticality.
- Fussell-Vesely.

Birnbaum Importance

The Birnbaum importance measure is defined as:

$$I_B(A) = P\{X|A\} - P\{X|\sim A\}$$

Where:

A indicates that the event whose importance is being measured occurred.

$\sim A$ indicates that this event did not occur.

X indicates the top event.

The Birnbaum importance measure for the event A is the difference in the probability of the top event given that the event A did occur minus the probability of the top event given that the event A did not occur. This is one measure of the increase in the probability of the top event due to the event A.

Consider a top event X, which is the result of event A and event B being connected by an OR gate. The fault tree would define the top event X to be $X = \{A \text{ or } B\}$. Assume that the probability of event A is 0.1 and that of event B is 0.2.

Let $P\{X|A\}$ denote the probability of the top event X given that the basic event A occurred. Clearly, if A occurs, $\{A$ or $B\}$ occurs, so that X occurs. Therefore:

$$P\{X|A\} = 1.0$$

Also, let $P\{X|\sim A\}$ denote the probability of the top event given that the basic event A does not occur. Here, given that A does not occur, X only occurs if the event B occurs. Therefore:

$$P\{X|\sim A\} = P\{B\}$$

Where $P\{B\} = 0.2$

Thus, the Birnbaum importance measure equals:

$$I_B(A) = (P\{X|A\} - P\{X|\sim A\}) = (1.0 - P\{B\}) = (1.0 - 0.2) = 0.8$$

Criticality Importance

The Birnbaum importance measure, $I_B(A)$, is useful, but it does not directly consider how likely the event A is to occur. For instance, in the previous example, $I_B(A) = (1.0 - P\{B\})$ does not even involve the probability of the event A. This could lead to assigning high importance values to events that are very unlikely to occur and may be very difficult to improve. Remember, an event with a low probability of occurring in a fault tree is an event that has already been improved, so further improvement may be difficult to obtain. Therefore, in an attempt to focus only on those events that truly are important (which not only lead to the top event but also are more likely to occur and may reasonably be improved), a modified Birnbaum importance measure known as a Criticality importance measure is used.

The Criticality importance measure is defined as:

$$I_c(A) = (I_B(A)) \cdot \frac{P\{A\}}{P\{X\}}$$

$$= (P\{X|A\} - P\{X|\sim A\}) \cdot \frac{P\{A\}}{P\{X\}} \quad \text{where } X \text{ is the top event.}$$

The Criticality importance measure modifies the Birnbaum importance measure by:

- Adjusting for the relative probability of the basic event A to reflect how likely the event is to occur and how feasible it is to improve the event (which makes it easier to focus on the truly important basic events).
- Conditioning on the occurrence of the top event X to restrict the measure to evaluating the effect of the basic event A, not the probability of the top event X (which makes it possible to compare basic events between fault trees).

Now, the Criticality importance measure, $I_B(A)$, for the earlier OR gate example, where $P\{A\} = 0.1$ and $P\{B\} = 0.2$, is to be calculated. The probability of the top event, the event $X = \{A \text{ or } B\}$ is first calculated:

$P\{X\}$ is the probability of the top event occurring.

$P\{A\}$ is the probability of event A occurring.

$P\{\sim A\}$ is the probability of event A not occurring.

$P\{A \text{ and } B\}$ is the probability of both events A and B occurring.

$P\{A \text{ or } B\}$ is the probability of either event A or event B or both events occurring.

If events A and B are independent, then $P\{A \text{ and } B\} = (P\{A\}) \cdot (P\{B\})$. Therefore:

$$P\{X\} = P\{A \text{ or } B\}$$

$$= P\{A\} + P\{B\} - (P\{A\}) \cdot (P\{B\})$$

$$= 0.1 + 0.2 - (0.1) \cdot (0.2)$$

$$= 0.28$$

Based on earlier calculations:

$I_B\{A\} = 0.8$,

$P\{A\} = 0.1$ and

$P\{X\} = 0.28$.

Therefore, the Criticality importance measure is given by:

$$I_C(A) = \frac{(I_B\{A\}) \cdot (P\{A\})}{(P\{X\})} = \frac{(0.8) \cdot (0.1)}{(0.28)} = 0.2857143$$

Similar calculations for event *B* yields:

$I_B(B) = 0.9$

And:

$$I_C(B) = \frac{I_B\{B\} \cdot (P\{A \cdot B\})}{(P\{X\})} = \frac{(0.9) \cdot (0.2)}{(0.28)} = 0.6428571$$

Now, consider the Criticality importance measure for the AND gate, where:

$P\{A\} = 0.1$,

$P\{B\} = 0.2$ and

$P\{X\} = P\{A \text{ and } B\}$

$= (P\{A\}) \cdot (P\{B\})$

$= (0.1) \cdot (0.2)$

$= 0.02$, by independence of the basic events *A* and *B*.

Here:

$P\{X \mid A\} = P\{A \text{ and } B|A\}$

$= P\{B\} \cdot P\{X|{\sim} A\}$

$= P\{A \text{ and } B|{\sim} A\} = 0.0$ and

$I_B(A) = P\{X|A\} - P\{X| \sim A\} = P\{B\} - 0.0 = P\{B\}$

Thus:

$$I_C(A) = \frac{I_B\{A\} \cdot P\{A\}}{P\{X\}} = \frac{P\{B\} \cdot P\{A\}}{P\{X\}} = \frac{P\{X\}}{P\{X\}} = 1.0$$

Similarly,

$I_B(B) = P\{X|B\} - P\{X| \sim B\} = P(A) - 0.0 = P\{A\}$

So that:

$$I_C(B) = \frac{I_B\{B\} \cdot P\{B\}}{P\{X\}} = \frac{P\{A\} \cdot P\{B\}}{P\{X\}} = \frac{P\{X\}}{P\{X\}} = 1.0$$

Given independence of the basic events, all of the basic events under an AND gate will have the same Criticality importance measure. Thus, the Criticality importance measure is uninformative for AND gates.

Fussell-Vesely Importance

The Fussell-Vesely importance measure is calculated quite differently than the Birnbaum or Criticality importance measures. It is constructed using minimal cut sets. A cut set is a set of basic events whose occurrence causes the top event to occur. A minimal cut set is a cut set that would not remain a cut set if any of its basic events were removed.

For example, the set of all the basic events is a cut set (or else the fault tree would be meaningless). If the fault tree consists of a single AND gate, then the cut set consisting of all the basic events is the only cut set and the minimal cut set. This is because all events leading into an AND gate must occur in order for the AND gate to be activated.

If the fault tree consists of a single OR gate, then the cut set consisting of all the basic events is not a minimal cut set unless there is only one basic event. This is because only one event leading into an OR gate needs to occur for the OR gate to be activated. In this case, any collection of basic events is a cut set. Therefore, given an OR gate, only those cut sets containing a single basic event are minimal cut sets.

Minimal cut sets are important in fault trees because they may be used to calculate the probabilities of events, including the top event. For example, the probability of the top event is given by the probability of the union of all the minimal cut sets.

Another interesting probability associated with the basic event *A* is the probability of the union of all minimal cut sets containing the basic event *A*. This is because the probability of the union of all minimal cut sets containing the basic event *A* is the probability that the top event is caused by a cut set containing the event *A*. This is a measure of the association of the basic event *A* with the top event *X*. It does not directly measure the probability that the top event *X* was caused by the basic event *A*, but it does indicate the potential importance of the basic event *A*.

A useful fact is that the probability of the union (OR) of sets is equal to the sum of the probabilities of the sets when the sets are mutually exclusive. If the sets are “nearly” mutually exclusive and, in addition, the basic events are independent and their probabilities are small, then this equality is approximately satisfied. For example, suppose that two minimal cut sets, C_1 and C_2, are given by $C_1 = \{A \text{ and } B \text{ and } C\}$ and $C_2 = \{A \text{ and } D\}$.

Then, exactly:

$$P\{C_1 \text{ or } C_2\} = P\{C_1\} + P\{C_2\} - P\{C_1 \text{ and } C_2\}$$

$$= P\{C_1\} + P\{C_2\} - \{P(A \text{ and } B \text{ and } C) \text{ and } (A \text{ and } D)\}$$

$$= P\{C_1\} + P\{C_2\} - P\{A \text{ and } B \text{ and } C \text{ and } D\}$$

$= P\{C_1\} + P\{C_2\} - P\{A\} \cdot P\{B\} \cdot P\{C\} \cdot P\{D\}$,which is approximately equal to $P\{C_1\} + P\{C_2\}$ when the probability of each of the basic events is small.

This idea is used in calculating the Fussell-Vesely importance measure. This measure considers the ratio of the probability of the union of all minimal cut sets containing the basic event *A*, divided by the probability of the union of all minimal cut sets. In practice, the numerator is replaced by the approximating sum of the probabilities of all minimal cut sets containing the basic event *A*, and the denominator uses the exact calculation, which is simply the probability of the top event *X*.

With the Fussell-Vesely importance measure, the fact that there is only one cut set for an AND gate leads to the uninformative result that all of the basic events leading to an AND gate will have the same value for the Fussell-Vesely importance measure.

Now, consider the previous example of the fault tree with an OR gate. Two minimal cut sets exist: $C_1 = \{A\}$ and $C_1 = \{B\}$. Recall that $P\{A\} = 0.1$, $P\{B\} = 0.2$, and that $P\{X\} = P\{A \text{ or } B\} = 0.28$. Note that C_1 is the only minimal cut set containing the basic event *A*, and C_2 is the only minimal cut set containing the basic event *B*. Also, $P\{C_1\} = P\{A\} = 0.1$, and $P\{C_2\} = P\{B\} = 0.2$. Therefore, the Fussell-Vesely importance measures for the basic events *A* and *B* are given by:

$$I_{FV}(A) = \frac{P\{C_1\}}{P\{X\}} = \frac{0.1}{0.28} = 0.3571429 \quad \text{and}$$

$$I_{FV}(B) = \frac{P\{C_2\}}{P\{X\}} = \frac{0.2}{0.28} = 0.7142857$$

Importance Measure Usage

The previous paragraphs have shown how to calculate the three importance measures (Birnbaum, Criticality and Fussell-Vesely). Also, they have shown how to use each importance measure by rank ordering the basic events by the values of the importance measures and then considering improving first that basic event with the highest importance measure value.

If all three importance measures yield the same rank ordering of basic events, then the strategy for using the importance measures is straightforward. However, when the three importance measures yield different rank orderings of basic events, the following guidelines suggest how to select an appropriate solution:

- Keep in mind that the goal is to assist in selecting the next basic event to consider for improvement. It cannot be concluded definitively that a particular basic event must receive the next improvement effort.
- Ensure the correct **primary time point** is chosen. The rank ordering of the importance measures may be different at different time points.
- Consider averaging the three-way ranking of the three importance measure rank orderings for each basic event. This may indicate a consensus of the three measures. (An example follows.)

- Study the sequential ranking, first by ranking by the Fussell-Vesely or Criticality importance measure and then break ties within the ranking by the Birnbaum importance measure.
- When in doubt or when calculation performance is an issue, the Criticality importance measure is probably a reasonable single measure to use. It considers the probability of the basic event (an improvement over the Birnbaum importance measure). However, if this is a problem with uninformative results caused by AND gates (as can happen with the Fussell-Vesely importance measure), then use the Birnbaum importance measure.

Example A possible procedure for determining the **average rank order** when the three importance measures assign different orderings to the basic events follows. Refer to Appendix C for detailed application information.

1. For each of the three importance measures, assign the rank ordering number to each basic event.
2. For each basic event, average these three rankings.
3. Rank these averages to get an overall ranking for each basic event. The example in Appendix C yields the following values for the three importance measures.

Event	Birnbaum	Criticality	Fussell-Vesely
A_1	0.7407952	0.7408114	1.0000000
A_2	0.7407952	0.7408114	1.0000000
A_3	0.0000743	0.0000071	0.1903293
B_1	0.0000141	0.0000141	0.1903293
B_2	0.0000743	0.0000071	0.1042212
B_3	0.0000743	0.0000071	0.1042212

Table 5-13. Importance Measure for Time *t = 100*

4. Create a rank ordering by assigning the number of the ranking to the basic event.

NOTE If two or more basic events are tied (i.e., they have the same importance measure values), then assign each one of them the average of the rankings that they would have received if these ties had been ignored. This yields the following rank orderings and their rank ordering numbers:

Birnbaum Rank Ordering: $A_1 = A_2 > A_3 = B_2 = B_3 > B_1$

Birnbaum Rank Ordering Number: $5.5 = 5.5 > 3.0 = 3.0 = 3.0 > 1.0_1$

Criticality Rank Ordering: $A_1 = A_2 > B_1 > A_3 = B_2 = B_3$

Criticality Rank Ordering Number: $5.5 = 5.5 > 4.0 > 2.0 = 2.0 = 2.0_3$

Fussell-Vesely Rank Ordering: $A_1 = A_2 > A_3 = B_1 > B_2 = B_3$

Fussell-Vesely Rank Ordering Number: $5.5 = 5.5 > 3.5 = 3.5 > 1.5 = 1.5$

These rank ordering numbers can be rearranged by events to make it easier to tabulate. Note that the sum of the ranks of N basic events should be:

$$\frac{(N) \cdot (N+1)}{2}$$

In this case, $N = 6$, so the sum of the ranks should be:

$$\frac{(6) \cdot (6+1)}{2} = 21$$

This serves as a check on both the arithmetic and tabulation, as shown in Table 5-14:

Event	Birnbaum	Criticality	Fussell-Vesely	Average Rank
A_1	5.5	5.5	5.5	5.5
A_2	5.5	5.5	5.5	5.5
A_3	3.0	2.0	3.5	2.8
B_1	1.0	4.0	3.5	2.8
B_2	3.0	2.0	1.5	2.2
B_3	3.0	2.0	1.5	2.2
Check Sum	21.0	21.0	21.0	21.0

Table 5-14. Importance Measures

Thus, the average ranking orders the effort for improvement in basic events as follows:

$$A_1 = A_2 > A_3 = B_1 > B_2 = B_3$$

Earlier, an ad hoc ordering of the basic events concluded with this ordering:

$$A_1 = A_2 > A_3 > B_1 > B_2 = B_3$$

It can be seen that the mechanical average ranking ordered the basic events essentially the same as the ad hoc reasoning ordered them, and it ordered the basic events exactly as Fussell-Vesely ordered them. For additional information, refer to “Application of Importance Measures” on page C-1.

6. Failure Mode and Effects Analysis

Introduction

Failure Modes and Effects Analysis (FMEA) is one of the most widely used and effective tools for developing quality designs, processes and services.

NOTE When criticality is considered, FMEA is often times referred to as FMECA (Failure Modes, Effects and Criticality Analysis). For additional information, refer to “Criticality Analysis” on page 6-21. In this document, the term FMEA is used in a general sense to include both FMEAs and FMECAs.

Developed during the design stage, FMEAs are procedures by which:

- Potential failure modes of a system are analysed to determine their effects on the system.
- Potential failure modes are classified according to their severity (FMEAs) or to their severity and probability of occurrence (FMECAs).
- Actions are recommended to either eliminate or compensate for unacceptable effects.

When introduced in the late 1960s, FMEAs were used primarily to assess the safety and reliability of system components in the aerospace industry. During the late 1980s, FMEAs were applied to manufacturing and assembly processes by Ford Motor Company to improve production. Today, FMEAs are being used for the design of products and processes as well as for the design of software and services in virtually all industries. As markets continue to become more intense and competitive, FMEAs can help to ensure that new products, which consumers demand be brought to market quickly, are highly reliable, safe and affordable.

The principle objectives of FMEAs are to anticipate the most important design problems early in the development process and either to prevent these problems from occurring or to minimise their consequences as cost effectively as possible. In addition, FMEAs provide a formal and systematic approach for design development and actually aid in evaluating, tracking and updating both design and development efforts.

Because the FMEA is typically begun early in the design phase and is maintained throughout the life of the system, the FMEA becomes a diary of the design and all changes that affect system quality and reliability.

Types of FMEAs

All FMEAs focus on design and assess the impact of failure on system performance and safety. However, FMEAs are generally categorised based on whether they analyse product design or the processes involved in manufacturing and assembling the product.

- **Product FMEAs**. Examine the ways that products (typically hardware or software) can fail and affect product operation. Product FMEAs indicate what can be done to prevent potential design failures. As a result, product FMEAS are also called **design FMEAs**.
- **Process FMEAs**. Examine the ways that failures in manufacturing and assembly processes can affect the operation and quality of a product or service. Process FMEAs indicate what can be done to prevent potential process failures prior to the first production run.

Although FMEAs can be initiated at any system level and use either a top-down or bottom-up approach, today's products and processes tend to be complex. As a result, most FMEAs use an inductive, bottom-up approach, starting the analysis with the failure modes of the lowest level items of the system and then successively iterating through the next higher levels, ending at the system level. Regardless of the direction in which the system is analysed, all potential failure modes are to be identified and documented on FMEA worksheets (hard copy or electronic), where they are then classified in relation to the severity of their effects.

In a very simple product FMEA, for example, a computer monitor may have a capacitor as one of its components. By looking at the design specifications, it can be determined that if the capacitor is open (failure mode), the display appears with wavy lines (failure effect). And, if the capacitor is shorted (failure mode), the monitor goes blank (failure effect). When assessing these two failure modes, the shorted capacitor would be ranked as more critical because the monitor becomes completely unusable. On the FMEA worksheet, ways in which this failure mode can either be prevented or its severity lessened would be indicated.

Approaches to FMEAs

Product and process FMEAs can be further categorised by the level on which the failure modes are to be considered.

- **Functional FMEAs**. Focus on the functions that a product, process or service is to perform rather than on the characteristics of the specific implementation. When developing a functional FMEA, a functional block diagram is used to identify the top-level failure modes for each functional block on the diagram. For example, two potential failure modes for a heater would be: “Heater fails to heat” and “Heater always heats.” Because FMEAs are best begun during the conceptual design phase, long before specific hardware information is available, the functional approach is generally the most practical and feasible approach by which to begin a FMEA, especially for large, complex products or processes that are more easily understood by function rather than by the details of their operation. When systems are very complex, the analysis for functional FMEAs generally begins at the highest system level and uses a top-down approach.

- **Interface FMEAs**. Focus on the interconnections between system elements so that the failures between them can be determined and recorded and compliance to requirements can be verified. When developing interface FMEAs, failure modes are usually developed for each interface type (electrical cabling, wires, fibre optic lines, mechanical linkages, hydraulic lines, pneumatics lines, signals, software, etc.). Beginning an interface FMEA as soon as the system interconnections are defined ensures that proper protocols are used and that all interconnections are compliant with design requirements.
- **Detailed FMEAs**. Focus on the characteristics of specific implementations to ensure that designs comply with requirements for failures that can cause loss of end-item function, single-point failures, and fault detection and isolation. Once individual items of a system (piece-parts, software routines or process steps) are uniquely identified in the later design and development stages, FMEAs can assess the failure causes and effects of failure modes on the lowest level system items. Detailed FMEAs for hardware, commonly referred to as piece-part FMEAs, are the most common FMEA applications. They generally begin at the lowest piece-part level and use a bottom-up approach to check design verification, compliance and validation.

Variations in design complexity and data availability (along with time and money) will dictate the analysis approach to be used. Some cases may require that part of the analysis be performed at the functional level and other portions at the interface and detailed levels. In other cases, initial requirements may be for a functional FMEA that is to later progress to an interface FMEA, and then finally progress to a detailed FMEA. Thus, FMEAs completed for more complex systems often include worksheets that employ all three approaches to FMEA development.

FMEA Standards

FMEA standards commonly used by government, military and commercial organisations are described in this section.

US MIL-STD-1629

US MIL-STD-1629, *Procedures for Performing a Failure Mode, Effects and Criticality Analysis*, is a long-recognised FMEA standard used by government, military and commercial organisations worldwide. Originally published in 1980, US MIL-STD-1629 provides procedures for identifying failure modes and effects and then extending FMEA analysis to include criticality, maintainability and vulnerability assessments. Although each of these different tasks, which are listed and described in Table 6-1, are similar to each other, they analyse different data.

Title	Description
Task 101: Failure Mode and Effects Analysis	A qualitative method used to study the effects of item failure on system operation and to classify each potential failure according to its severity.
Task 102: Criticality Analysis	Criticality analysis extends a FMEA to include the combined influence of the severity classification and its probability of occurrence to provide a quantitative criticality rating for the component or function.
Task 103: FMEA Maintainability Information	FMEA maintainability information supplies early criteria for maintenance planning, logistics support analysis, test planning, and inspection and checkout requirements, and identifies maintainability design features that require corrective actions.
Task 104: Damage Mode and Effects Analysis	Damage Mode and Effects Analysis (DMEA) provides early criteria for survivability and vulnerability assessments. Because DMEA is primarily applicable to weapon systems, it is not addressed in this document. For additional information on DMEAs, refer to Task 104 in MIL-STD-1629.

Table 6-1. MIL-STD-1629 Tasks

IEC 60812 (1985-07)

Published by the International Electrotechnical Commission (IEC), IEC 60812 (1985-07), *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*, describes both FMEAs and FMECAs. It gives guidance as to how they may be applied by:

- Providing the procedural steps necessary to perform an analysis.
- Identifying appropriate terms, assumptions, criticality measures and failure modes.
- Determining ground rules.
- Providing examples of the necessary forms.

Automotive FMEAs

The Society of Automotive Engineers (SAE), the Automotive Industry Action Group (AIAG) and Ford Motor Company have all generated documents for performing FMEAs within the automotive industry. For the sake of simplicity, these different standards are referred to as Automotive FMEAs in this document. Automotive FMEAs categorise the FMEA analysis by whether it is for a design or a process.

SAE ARP 5580 FMEA Standard

In an effort to define a broad, widely accepted standard for performing FMEAs, the Society of Automotive Engineers (SAE) published ARP 5580. Created by a sub-committee of professionals that included representatives of government, industry and academia, this FMEA standard reflects not only commercial practices but also meets the strict guidelines of the Department of Defense (DoD).

By combining the capabilities of MIL-STD-1629 and the Automotive FMEAs, this sub-committee was able to produce a FMEA standard that is widely accepted across military and commercial barriers. The most notable difference in ARP 5580 is the support of fault equivalence groups, which allow the focus to be on the management of failure consequences rather than on individual failure modes.

Although the traditional approach of analysing individual failure modes is very systematic and complete, it can become very tedious, especially when performing a FMEA on a large or complex system. To automate and simplify the development of any FMEA, ARP 5580 suggests grouping failure modes that exhibit identical consequences together and assigning them to the same Fault Identification Number (FIN). The failure modes having the same FIN all must have exactly the same consequences, including the same local effect, next effect, end effect and severity. Using fault equivalence groups can greatly reduce repetition and improve consistency.

Advantages and Limitations of FMEAs

FMEAs can be developed for single items or for systems that consist of thousands of parts. Although FMEAs were once created by manually completing worksheets, they are now often generated using computerised spreadsheets or software packages designed specifically for FMEA development. Moving FMEA development from paper to computer has provided for:

- Generating FMEAs more quickly and accurately.
- Editing and updating information easily as the design changes.
- Modifying design options, viewpoints and input assumptions.
- Automating report preparation, including sensitivity analyses.
- Interacting with other software for graphic presentation, word-processing and the use of databases containing reliability information.
- Ranking effects in criticality order, at different system levels, in different phases of system operation or from different viewpoints.

FMEA software programs provide for creating, storing, retrieving and modifying common FMEA data elements, using uniform terminology and documentation templates for consistency, and applying changes globally. And, most importantly, FMEA software programs free engineers to concentrate on the engineering principles required for FMEAs rather than on formatting and consistency issues. The "down-side" of this is that the analyst sometimes loses sight of the underlying technical issues in the design itself while concentrating on data input. Sometimes the "numbers" become over-important at the expense of common sense.

Advantages of FMEAs

Effective FMEAs identify all failure modes and their effects and indicate how critical failure modes can either be eliminated or their effects lessened to make designs more reliable and safe. In addition to providing quality and safety enhancements, other advantages of FMEAs include:

- Increased customer satisfaction due to better products and processes.
- More robust designs that consider poor customer habits and less than ideal operating environments.
- Earlier preparation of diagnostic routines (such as check lists, flow charts and fault-finding tables) for fault recovery, fault tolerance, and failure detection and isolation.
- More efficient test and production planning based on the possibility of product-induced failures.

- Better design of built-in test (BIT), failure indications and redundancy (where applicable and necessary).
- Earlier determination of the automatic or manual test equipment needed to economically test hardware, particularly electronic sub-assemblies and systems, and diagnose failures.
- Superior placement of performance monitoring and fault-sensing equipment or test points.
- Earlier development of software for automatic test and BIT.
- Better preventative maintenance requirements based on the significance of failure effects.
- Fewer engineering changes in the prototyping and manufacturing stages of product development, where costs can be more significant.
- Comprehensive design documentation that formally records safety and reliability analysis in case evidence is ever required by customers or for product safety litigation.

By focusing attention on design weaknesses and what can go wrong in the manufacturing and support of a product, FMEAs play a central role in product or process design.

Limitations of FMEAs

FMEAs consider only non-simultaneous failure modes. Each failure mode is considered individually, assuming that all other system items are performing as designed. Because of this, FMEAs provide limited insight into anomalous behaviours such as:

- Effects of multiple component failures on system functions.
- Latent manifestations of defects such as timing, sequencing, etc..
- Effects on redundant items.

Other analysis techniques, such as fault tree analysis, sneak circuit analysis, Markov analysis and computer-aided simulation, can be used when such anomalous behaviours occur. For additional information, refer to “Fault Tree Analysis” on page 5-1 and “Markov Modelling” on page 8-1.

Also, the prioritization of failure modes in FMEAs for determining corrective actions can be highly subjective. However, clearly defining the method for assessing risk and developing FMEAs using a team approach greatly reduce their subjectiveness.

Corporate FMEA Standards

The usefulness of FMEAs is dependent upon the effectiveness with which analysis is communicated for early design attention. Thus, prior to beginning FMEA development, organisations should develop and implement a corporate FMEA standard that documents the internal procedures to be followed. Also, if data elements needed for FMEA analysis are predefined in electronic databases, information on using and maintaining these data elements should be included in the corporate standard.

To receive the greatest benefits from FMEAs, the corporate standard for managing the FMEA process should:

- Provide procedures for implementing the specified requirements of the corporate standard.
- Supply guidelines on how the analysis method is to be selected, how the FMEA is to be constructed and later updated to reflect design changes, and how analysis results are to provide design guidance.
- Give examples of the various FMEA worksheets that are used for the different FMEA approaches and indicate where these worksheets reside.
- Describe the nomenclature and coding system to be used in FMEAs so that results are repeatable, traceable (to programme drawings, design documentation and other analyses) and maintainable.
- Indicate how failure rates and probabilities are to be applied consistently to failure modes if analysis is extended to include criticality.
- Demonstrate how the analysis is to be exchanged for approval or between team members.
- Establish rating procedures for severity, occurrence and detection that are tailored to the industry and systems being analysed and clarify when each scale is to be implemented.
- Furnish a glossary of terms used in FMEA development.
- Explain how cost/benefit analysis should be performed to determine whether the FMEA can be completed at a reasonable cost within the needed time frame.

To gain even greater benefits from FMEAs, organisations should consider implementing a team approach. By including effective representation from all groups that influence the final design or process and who are affected by it—including reliability, test, logistics, quality assurance, suppliers and customers, the knowledge of all subject matter experts is collected, and the chances of identifying and preventing potential failure modes are greatly increased.

A team approach to developing FMEAs also ensures integration of the product and process planning, and provides for communication between departments. The team leader, who is the engineer responsible for the design, ensures that all team members understand the corporate FMEA standard and preserves team dynamics throughout the FMEA development.

The FMEA Process

The extent of effort and the approach used in a FMEA depend upon the nature and requirements of the individual programme. To contribute meaningfully to a programme, a FMEA must be initiated as early as possible during the design process and be tailored to the programme requirements as it progresses through three distinct stages:

- **FMEA Planning**. Construct a FMEA plan from experience and source requirements during the conceptual design phase.
- **FMEA Construction**. Identify and analyse system failure modes in worksheets that become, along with an introduction and summary analysis, a stand-alone FMEA report. (If analysis is extended to include criticality, maintainability and vulnerability assessments, these worksheets are also included in the FMEA.)
- **FMEA Post-Analysis**. Use test results and field data collected during the design verification and validation stage and even after the product is in use to maintain the accuracy of the FMEA.

FMEA Planning

Companies who spend more time planning a design traditionally have much lower development costs than those companies who use the “find-and-fix” method during prototyping. By starting FMEAs as soon as initial design information becomes available and iteratively performing them as designs evolve, potential failures can be detected and prevented early. When FMEAs are begun after designs are well beyond the conceptual stage, correcting potential faults identified by FMEAs often is too costly, resulting in the production of products that are either unreliable or perform poorly. Because product failures can cause extreme customer dissatisfaction, which ultimately diminishes a company’s reputation and its market share, the development of well-defined FMEA plans should take place during the conceptual design phase.

System Definition

System definition requires a review of all available design information. The information for defining the system is likely to be found in the following technical specifications and development plans:

- Customer specifications.
- Engineering specifications.
- Quality specifications.
- Reliability specifications (necessary for criticality analysis).
- Engineering drawings.
- Computer-aided design (CAD) data.
- Predecessor history, including:
  – Trade-off studies.
  – Stress analysis results.
  – Test results.

In addition to stating system objectives, the above resources specify design and test requirements for operation, reliability and maintainability, and give acceptable performance limits under specified operational and environmental conditions. These documents also generally define what constitutes a failure and describe what contributes to the various types of system failure.

The existing technical specifications and development plans are used to write functional narratives for each mission, mission phase and operational mode. These functional narratives, which reference the existing technical specifications and development plans as data sources, identify:

- Primary and secondary mission objectives.
- Mission functions and operational modes using a top-down approach.
- Alternative operational modes if more than one method for performing a function exists.
- All multiple functions using different equipment or groups of equipment.
- Functional outputs for each system level.
- Conditions that constitute system and part failure.
- Profiles of anticipated environmental conditions for each mission and mission phase.
- Amount of time an item spends operating in each operational mode during different mission phases or when only its function is required.

Once functional narratives are written, they serve as detailed system definitions for the FMEA plan and are used in the summary of the final FMEA report.

Functional and Reliability Block Diagrams

Functional block diagrams and reliability block diagrams are critical to the success of FMEAs. Functional block diagrams illustrate the operation and interrelationships between functional entities of a system as defined in engineering data and schematics, thereby providing functional flow sequences for the systems and each indenture level of analysis.

NOTE **Indenture levels** identify or describe the relative complexity of a function or assembly. Indenture levels progress from the more complex (system) levels to the simpler (part) divisions.

Reliability block diagrams define the series dependence or independence of all functions of a system or functional groups for each life-cycle event, thereby providing identification of interdependencies that can be used for functional FMEAs. If functional block diagrams and reliability block diagrams are not developed for each item configuration in a system during system definition, they must be generated immediately after the system has been defined.

To present the system as a breakdown of its major functions, several functional and reliability block diagrams are usually required, especially if alternative modes of operation must be displayed. These diagrams must show and clearly label all system inputs and outputs, and each block must be assigned a consistent and logical item number that reflects the functional system breakdown order. These numbers are used during the preparation of the FMEA and provide for tracing failure mode effects through all levels of indenture during the analysis as well as when maintaining its accuracy after the system is produced and in use.

Ground Rules and Assumptions

While the FMEA objective is to identify all potential failure modes within a design, the emphasis must be on the early identification of catastrophic and critical failure possibilities so that they can be eliminated or minimised quickly through early design correction. Consequently, the FMEA can begin at the higher system levels as soon as preliminary design information is available and then be extended to the lower system levels as more information becomes available.

To ensure that all team members share a common understanding of the level to which the analysis is to be performed and the time line by which it must be completed, an analysis approach (functional, interface or detailed) for each item must be identified and a schedule established. A well-designed FMEA plan will also include guidelines and assumptions for each of the topics in Table 6-2.

Topic	Topic Intent
Worksheet Format	Indicates which FMEA worksheet is to be used for each approach, based on those defined in the corporate FMEA standard.
Indenture Level	Indicates the lowest indenture level at which failure modes must be documented. For example, MIL-STD-1629 indicates that the lowest level for Task 101 is based on three criteria: • Lowest level specified for logistics support analysis • Lowest indenture level at which items are assigned a severity classification of catastrophic or critical • Specified or intended maintenance and repair level of items assigned a severity classification of marginal or minor
Coding System	Indicates how the system functions and equipment are to be consistently labelled on the FMEA worksheets so that they can be used to track failure modes. This coding system must be consistent with the numbering used on the functional and reliability block diagrams and must demonstrate the relationship of each failure mode with the system.
Failure Definition	Provides general statements of what constitutes a failure for each item, in terms of performance parameters and allowable limits for each specified output; also notes acceptable degradation limits.
Rating Scales	Indicates the assessment ratings to be used for severity, occurrence (if criticality analysis is to be performed) and detection. Standard classifications exist for use in the military, aerospace and automotive industries. The number of classifications and their descriptions can, however, be tailored to the industry and systems being analysed. If more than one set of rankings is to be used, a cross-reference mapping must be provided so that all scales can be merged.

Table 6-2. Guidelines and Assumptions for a FMEA Plan

Topic	Topic Intent
Coordination of Effort	Indicates how FMEA results are to be used by other departments to support reliability, maintainability, safety, and survivability and vulnerability programmes.

Table 6-2. Guidelines and Assumptions for a FMEA Plan (Continued)

Although every effort to identify and record all ground rules and assumptions must be made prior to beginning the analysis, both ground rules and assumptions may need to be added or changed as design requirements are modified. Communication of such changes to all involved, however, is critical to the success of the FMEA.

Cost/Benefit Analysis

To ensure that value is added to the design process, cost/benefit analysis should be performed to indicate whether the FMEA can be completed within the needed time frame and at a reasonable cost. Costs for implementing a FMEA include the time needed for training, meetings, analysis and implementation of the recommended prevention and detection measures. Also to be determined and considered are:

- Costs for implementing the FMEA process, which has been tailored to the complexity of the system.
- Impact on product development costs due to late design modification or over design.
- Impact on operating costs of the product due to product maintenance and reliability issues of any remaining fault potentials.

Other FMEA Guidelines

As FMEA worksheets are completed, the following general guidelines should be kept in mind:

- Analyse different design options separately to ensure that reliability implications can be considered when deciding on which option to choose.
- If the system operates in more than one phase in which different functional relationships or operating modes exist, conduct analyses for all phases and modes of system application. For example, when performing a functional FMEA for an aircraft, a failure with the landing gear does not adversely impact the plane while it is cruising but does have a very negative impact during landing. Failure consequences that are different for the various modes of operation must be considered.

- If redundant sub-systems exist, consider the effects of redundancy by evaluating the effects of failure modes when the redundant sub-system is available and is not available.
- Determine and state the viewpoint(s) being considered in the FMEA analysis. Different viewpoints include safety, mission success, availability, repair cost, failure mode, effect detectability, etc.. Otherwise, a safety-related FMEA, for example, might give a low criticality number to an item whose reliability seriously affects availability but which is not safety critical.
- If the system under development is similar to an existing system, look at field and experience data, including warranty information, benchmarking studies, risk analysis results, customer feedback and historical quality data from the field to gain additional insights.
- As the design evolves, update the FMEA so that it can be used to influence the design and provide comprehensive documentation upon design completion. This includes using test results to update the analysis throughout the implementation and production stages.

The goal of FMEAs is to get correct results using the fastest, least expensive approach. As a result, consider for complete evaluation in a FMEA only those potential failure modes that are real or legitimate issues. For a new design, particularly when the effects of failure seriously affect safety, reliability, high warranty costs, etc., the FMEA should take into account the failure modes of all components. For an existing design, the FMEA may need to consider only functional failure modes of sub-assemblies, particularly for modular components in electronic systems where design details are not known. When failure modes present unacceptable consequences, the design must either be modified to comply with supplied requirements, or recommendations for fixing or improving the design must be fed back into the analysis.

FMEA Construction

FMEA construction begins by selecting the appropriate worksheet from the many variations that are available, keeping in mind the analysis objective, design data availability and item indenture level. The heading of a FMEA worksheet can contain fields for subject line, team leader, team members and dates for the project deadline as well as for update and maintenance revisions. In MIL-STD-1629, the worksheet for Task 101 has the header information in Table 6-3. The Task 101 worksheet is shown in Figure 6-1.

Header Field	Description
System	Item for which the FMEA worksheet is being completed.
Indenture Level	Level at which the item resides within the system hierarchy.
Reference Drawing	Drawings used to determine and document the failure modes and effects for the item.
Mission	Tasks to be performed and the mode of operation for performing these specific functions.
Date	Date on which the FMEA worksheet is developed, or dates on which worksheet was last updated.
Sheet ___ Of ___	Number of FMEA worksheet pages for the item.
Compiled By	Team member(s) responsible for developing the FMEA worksheet.
Approved By	Person authorised to approve the FMEA worksheet.

Table 6-3. Header Information for Method 101 Worksheet

FAILURE MODE AND EFFECTS ANALYSIS

SYSTEM____________________
INDENTURE LEVEL____________________
REFERENCE DRAWING ____________________
MISSION____________________

DATE ____________________
SHEET______OF____________
COMPILED BY________________
APPROVED BY________________

IDENTIFICATION NUMBER	ITEM/FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	FAILURE EFFECTS			FAILURE DETECTION MODE	COMPENSATING PROVISIONS	SEVERITY CLASS	REMARKS
					LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				

Figure 6-1. MIL-STD-1629 Worksheet for Task 101

General descriptions of the columns in the Task 101 worksheet appear in Table 6-4. Although worksheets for analysing failure modes and their effects do vary, they all request the same information for assessing how system operation is affected.

Field	Description
Identification Number	Serial number or other unique reference designator that has been assigned for traceability purposes. This identification number is consistent with those used on the functional and reliability block diagrams for this item. These block diagrams are referenced in the **Reference Drawing** field in the worksheet header.
Item/Functional Identification (Nomenclature)	Name of the item or system function for which failure modes and effects are to be identified. Schematic diagram symbols or drawing numbers are used to identify the item or function properly.
Function	Concise statement of all the functions that the item is supposed to perform to accomplish its intended purpose to the satisfaction of the customer. Included are both inherent functions of the item and its relationships to interfacing items. Within a functional FMEA, the function is a description of the task, duty, action or operation performed by a group of elements at the functional block level.
Failure Modes and Causes	Potential failure modes that have been identified for each indenture level to be analysed based on stated requirements and failure definitions. To uncover potential failure modes, examine the item outputs and functional outputs in the applicable block diagrams and schematics, and review historical field and test data; if a team approach is being used, hold a brainstorming session to see if additional failure modes and causes can be identified. Causes for the failure mode, which are either the reasons for the failure or those which initiate the processes that lead to the failure (design defects, quality defects, part misapplication, physical process, chemical process, etc.). Multiple causes can be assigned to each failure mode.

Table 6-4. Columns on Task 101 Worksheet

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Mission Phase/ Operational Mode</td><td>Mission phase and operation mode in which the failure occurs. If the sub-phase, event or time can be defined from the system definition and mission profiles, include timing information for the failure occurrence.</td></tr>
<tr><td>Failure Effects</td><td>Consequences of the failure mode on the operation, function or status of an item as they are likely to be experienced by the customer. (Often times, historical field data from a similar design can be used to compile a list of effects.) Because the failure mode under consideration may affect the system at several levels, failure effects are related to the functions at the next higher level of the design, continuing progressively to the top or system-level functions.
Local Effects. Consequences that the failure mode has on the local operation, function or status of the specific item that is being analysed. Describe the fault condition in sufficient detail so that it can be used to determine the next higher level effects and end effects.
Next Higher Level. Consequences that a failure mode has on the operation, function or status of the items in the indenture level above the one under consideration.
End Effects. Consequences that a failure mode has on the operation, function or status of the highest indenture level.</td></tr>
<tr><td>Failure Detection Method</td><td>Techniques for detecting the failure mode or corresponding causes, including design reviews, process control plans, test plans, reliability plans, etc..</td></tr>
</table>

Table 6-4. Columns on Task 101 Worksheet (Continued)

Field	Description
Compensating Provisions	Design provisions or operator actions that can be taken to circumvent or mitigate the effect of a failure on a system but do not prevent its occurrence. Design provisions include redundant items that allow safe operation to continue in the event of failure, safety or relief devices such as monitors or alarms that permit effective operation or limits damage, and adding alternative modes of operation such as backup or standby items or systems. Operator provisions include providing operating procedures and installing built-in test (BIT), monitors, fault detectors and gauges.
Severity Classifications	Provides a qualitative measure of how serious the consequences of the failure mode are on the system, mission or application. Severity classifications for Task 101 are Catastrophic, Critical, Marginal and Minor. Rating scales should be tailored to fit the specific industry or organisation based on customer perception. The corporate FMEA standard should describe all ranking scales that can be used, and the FMEA plan should indicate which of these ranking scales are to be used for the given system. When determining which failure modes to address, prioritization is dependent upon severity (FMEA) or severity and criticality (FMECA). For detailed information on determining the most critical failures modes, refer to “Criticality Analysis” on page 6-21.

Table 6-4. Columns on Task 101 Worksheet (Continued)

Field	Description
Remarks	Comments pertaining to and clarifying other columns in the current line of the worksheet, including notes about unusual conditions, failure effects of redundant items and recognition of particular critical design features. Recommendations for design improvements to be pursued based on the quality or reliability payback for the customer, organisation and society. Keep in mind that the goal is to eliminate the root causes of a failure mode, which include: incorrect material specification, overstressed components, insufficient lubrication, inadequate maintenance instructions, poor protection from environment, incorrect algorithms, software design errors, etc.. Only notes regarding recommended corrective actions and their importance need to appear here. Recommended corrective actions are to be fully described in the summary of the finalised FMEA report. When the recommended corrective actions require significant resources or high risk, they must be investigated further and cost/benefit studies must be performed. Comparing estimated warranty costs to development costs of the proposed change to the current design can determine the appropriate corrective action. When design changes are not possible, compensating provisions must be identified.

Table 6-4. Columns on Task 101 Worksheet (Continued)

NOTE Most designs have more than one failure mode. To avoid debating whether an event is a mode, effect or cause, express the failure mode as the function in a negative sense. For example, if the function is that the item is to heat, the failure mode is that it does not heat.

Although the primary goal of FMEAs is to prevent potential failure modes, reducing the effects from failures (based on severity and possibly detection) must be carefully considered so that unnecessary costs are not incurred for failure modes having little negative impact on the customer. As severity and occurrence decrease, it is generally less expensive to provide detection than to investigate alternatives to improve the design.

Criticality Analysis

One of the most important results from a FMEA is the assessment of failure mode and effect criticality. Criticality analysis determines the significance of individual failure modes and helps to prioritize them for corrective actions. To extend a FMEA to include criticality analysis, a method for measuring criticality must be defined. Qualitative approaches include Risk Priority Numbers (RPNs), risk levels, criticality matrices and Pareto rankings. Quantitative approaches include using failure rate data to compute failure mode criticality and item criticality.

When criticality is considered, the FMEA worksheet includes columns for indicating how often a failure mode is likely to occur. When failure rate data is not available, a qualitative approach to criticality is used. When failure rate data is available, a quantitative approach to criticality is generally used. Larger criticality values indicate more critical failure modes. In the FMEA report, criticality analysis worksheets should follow the failure mode and effects worksheets for the same indenture level.

Qualitative Approach to Criticality

According to Task 102 in MIL-STD-1629, the availability of specific parts configuration data and failure rate data determine whether a qualitative or quantitative approach to criticality is to be used. The qualitative approach groups individual failure mode probabilities of occurrence into distinct, logically defined groups that establish the criticality value to be entered in the appropriate column of the FMEA worksheet. Table 6-5 defines the criticality groups for Task 102 when a qualitative approach is used.

Criticality Group	Probability Criteria
Level A - Frequent	Single failure mode probability is greater than 0.20 of the overall probability of failure during the item operating time interval.
Level B - Reasonably Probable	Single failure mode probability is greater than 0.10 but less than 0.20 of the overall probability of failure during the item operating time.
Level C - Occasional	Single failure mode probability is greater than 0.01 but less than 0.10 of the overall probably of failure during the item operating time.

Table 6-5. Qualitative Approach to Criticality Analysis

Criticality Group	Probability Criteria
Level D - Remote	Single failure mode probability is greater than 0.001 but less than 0.01 of the overall probability of failure during the item operating time.
Level E - Extremely Unlikely	Single failure mode probability is less than 0.001 of the overall probability of failure (essentially zero) during the item operating time.

Table 6-5. Qualitative Approach to Criticality Analysis (Continued)

RPNs

When Automotive FMEAs consider criticality, values of 1 to 10 are assigned to severity, detection and occurrence, with 10 being the most severe, the least detected or the most frequently occurring item. A criticality value known as a Risk Priority Number (RPN) is then calculated for each failure mode by taking the product of these three values:

$$\text{RPN} = \text{Severity} \cdot \text{Detection} \cdot \text{Occurrence}$$

When standard rating scales are used, RPNs have values between 1 and 1000. Higher RPNs indicate more critical failure modes. Therefore, RPNs should be sorted from highest to lowest values so that immediate attention can be given to those failure modes with the highest RPNs values. The RPN results can then be used for analysis.

Important! When detection values are high, RPNs may be high for failure modes that are less than critical in respect to quality, reliability and safety.

Risk Levels

In *Failure Modes and Effects Analysis*, Paul Palady describes how detection is reactive and explains that failures modes should be prioritized based only on severity and occurrence, which are proactive. To assess criticality, Palady recommends plotting the severity and occurrence values of all failure mode effects on an area chart and then dividing this chart into three regions of risk: high, medium and low.

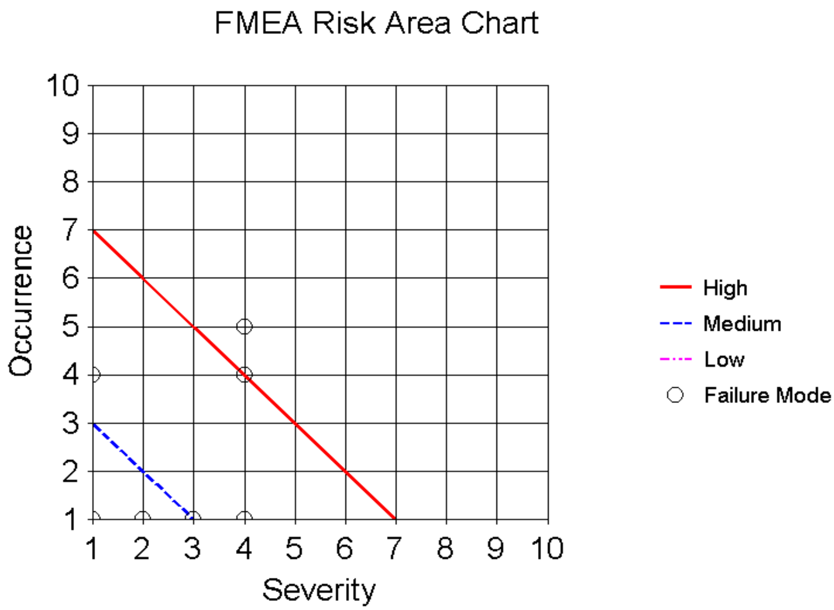


Figure 6-1. Risk Level Area Chart

Failure modes are then assigned a risk level based on where they appear on the area chart. Failure modes plotted above the high risk line are tagged as high risk, failure modes between the lines are tagged as medium risk, and failure modes below the low risk line are tagged as low risk.

Criticality Matrices

Traditionally, failure modes have been graphed after criticality has been assessed (rather than to determine criticality as in Palady's area charts above) in what are known as criticality matrices. Although the axes of a criticality matrix are user-definable, the X-axis is usually based on severity, and the Y-axis is usually based on the probability of occurrence (which are occurrence ranking values when analysis is qualitative and calculated probability values when analysis is quantitative). Report versions of criticality matrices list individual items by identifiers that fall under each criticality rank.

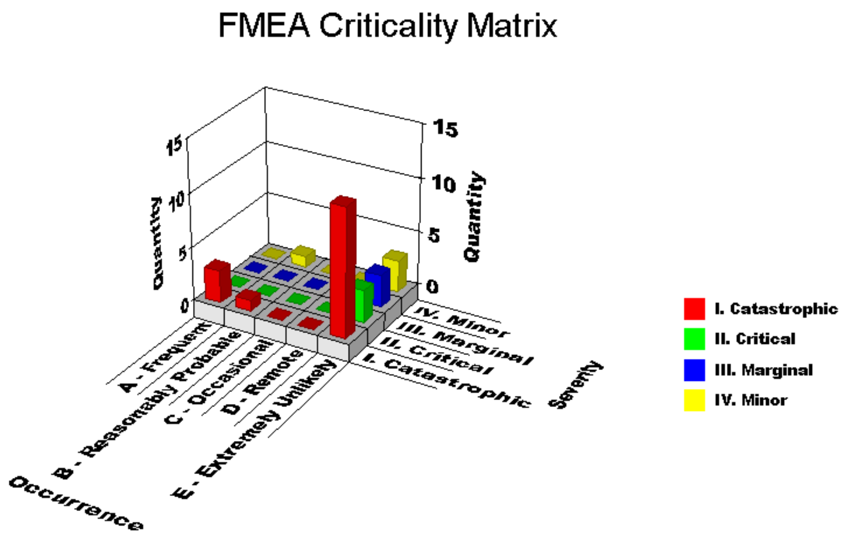


Figure 6-2. Criticality Matrix

Pareto Rankings

The criticality procedure in SAE ARP 5580 is based on a multi-criteria, Pareto ranking system. In this FMEA standard, rank is defined by going through all of the failure modes and finding non-dominated failure modes, which are failure modes that are not outranked in terms of severity and probability of occurrence. The first set of non-dominated failure modes is assigned a rank of 1, then the next level of non-dominated failure modes is assigned a rank of 2, etc.. This procedure continues until all sets of failure modes are ranked. The most critical failure modes are those assigned the highest ranking value.

Quantitative Approach to Criticality

A **quantitative approach** to criticality analysis uses the same failure rate data sources as other reliability and maintainability analyses. When system-specific failure rate data is not available, Task 102 of MIL-STD-1629 indicates that base failure rates and all failure rate adjustment factors are to be derived from MIL-HDBK-217 wherever possible.

NOTE Although MIL-HDBK-217 is no longer being supported by the U.S. military, it is still heavily used by both military and commercial manufacturers.

The Task 102 worksheet in Figure 6-2 applies a quantitative approach to criticality analysis.

CRITICALITY ANALYSIS

SYSTEM ____________________
INDENTURE LEVEL ____________________
REFERENCE DRAWING ____________________
MISSION ____________________

DATE ____________________
SHEET ______ OF ______
COMPILED BY ____________________
APPROVED BY ____________________

IDENTIFICATION NUMBER	ITEM/FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	SEVERITY CLASS.	FAILURE PROBABILITY FAILURE RATE DATA SOURCE	FAILURE EFFECT PROBABILITY β	FAILURE RATE MODE α	FAILURE RATE λ_P	OPERATING TIME t	FAILURE MODE CRIT # $C_m = \beta\alpha\lambda_p t$	ITEM CRIT # $C_R = \Sigma(C_M)$	REMARKS

Figure 6-2. MIL-STD-1629 Worksheet for Method 102

Although similar to the Task 101 worksheet, the Task 102 worksheet displays columns necessary for calculating the probability of a failure mode occurring for each possible cause. These failure probability columns are described in Table 6-6.

Column	Description
Failure Probability/ Failure Rate Data Sources	Failure rate probability of occurrence is listed when failure modes are assessed in terms of probability of occurrence. When failure rate data is used in the calculation of criticality numbers, list the data sources of these failure rates.
Failure Effect Probability (β)	Failure effect probability (β) values are the conditional probability that the failure effect will result in the identified criticality classification, given that the failure mode occurs. Guidelines for assigning β values for Task 102 appear in MIL-STD-1629.
Failure Mode Ratio (α)	Fraction of the item failure rate (λ_p) apportioned to the failure mode under consideration. The failure mode ratio, which is expressed as a decimal fraction, is best obtained from field data representative of the particular item in application. However, generic component failure rate data or failure rate data from lab or simulation studies (or from similar systems/processes) can be used. When failure mode data is not available, the α values shall represent the analyst's judgment based upon an analysis of the item's functions. Assuming that failure modes are mutually exclusive and complete, the sum of the failure mode ratios equal 1.0. If the modes are non-exclusive, the sum of failure mode ratios can be greater than 1.0.
Failure Rate (λ_p)	Part failure rate (λ_p) from the appropriate reliability prediction or as calculated using the procedure described in MIL-HDBK-217. Where appropriate, application factors (π_A), environmental factors (π_E) and other pi factors that may be required to adjust for differences in operating stresses shall be applied to the base failure rates (λ_b) obtained from handbooks or other reference materials. List values of all pi factors used in computing λ_p.

Table 6-6. Failure Probability Columns for Task 102 Worksheet

Column	Description
Operating Time (t)	Operating time in hours or number of operating cycles of the item per mission as derived from the system definition.
Failure Mode Criticality $C_m = \beta\alpha\lambda_p t$	Value of the failure mode criticality number C_m, which is the portion of the criticality number for the item due to one of its failure modes under a particular severity classification. The formula for calculating C_m is explained more fully after this table.
Item Criticality $C_r = \Sigma C_m$	The second criticality number calculation for the item under analysis, which is the number of system failures of a specific type expected due to the item's failure modes. The formula for calculating C_r is explained more fully after this table.

Table 6-6. Failure Probability Columns for Task 102 Worksheet (Continued)

Failure Mode Criticality

Failure mode criticality is calculated by the formula:

Equation

$$C_m = \beta\alpha\lambda_p t \qquad (6.1)$$

Where:

C_m Represents the criticality number for the failure mode.

β Represents the conditional probability of loss of function or mission, or failure effect probability.

α Represents the failure mode ratio (for an item, $\Sigma_\alpha = 1$).

λ_p Represents the part failure or hazard rate.

t Represents duration of applicable mission phase, usually expressed in hours or number of operating cycles.

The $\lambda_p t$ can be replaced with the failure probability, $1 - exp(-\alpha\lambda_p t)$, if $\alpha = 1$ and $\lambda_p t \ll 1$.

Item Criticality

Equation Item criticality is calculated by the formula:

$$C_r = \Sigma(C_m) \qquad (6.2)$$

Where:

C_r Represents the criticality number for the item.

C_m Represents the criticality number for the failure mode.

The specific type of system failure is expressed by the severity classification of the item's failure modes. For a particular severity classification and mission phase, the C_r for an item is the sum of the failure mode criticality numbers, C_m, under the severity classification. Item criticality may also be calculated using the following formula:

Equation

$$C_r = \sum_{n-1}^{j} (\beta\alpha\lambda_p t)n \qquad (6.3)$$

Where:

C_r Represents the criticality number for the failure mode.

n Represents the failure modes in the items that fall under a particular criticality classification (1, 2, 3, … , j).

j Represents the last failure mode in the item under the criticality classification.

β Represents the conditional probability of loss of function or mission, or failure effect probability.

α Represents the failure mode ratio (for an item, $\Sigma_\alpha = 1$).

λ_p Represents the part failure or hazard rate.

t Represents duration of applicable mission phase, usually expressed in hours or number of operating cycles.

NOTE Worst-case or pessimistic reliability values should always be used as input assumptions for failure modes that are identified as critical, or which might be critical if the pessimistic assumptions prove to be realistic. Generally, the more critical the failure mode, the more pessimistic the worst-case reliability assumptions should be. Computerised FMEA software greatly facilitates this type of sensitivity analysis.

FMEA Maintainability Analysis

FMEA analysis can be extended to identify maintainability design features requiring corrective action and to establish early criteria for:

- Maintenance Planning Analysis (MPA).
- Logistics Support Analysis (LSA).
- Test planning.
- Inspection and checkout requirements.

To extend a FMEA to include maintainability analysis, use a worksheet that includes columns for indicating the maintenance activities to be performed. In MIL-STD-1629, the Task 103 worksheet displays columns necessary for maintenance planning. These columns are described in Table 6-7.

Column	Description
Failure Predictability	Indicates operational performance variations peculiar to the failure trends for this item that can be used to predict failures. Includes data that must be collected and explains how it is to be used to predict the failure. Identifies any tests or inspections that must be performed to detect evidence of conditions that cause the failure mode.
Failure Detection Means	Indicates how the failure mode is to be detected by the organisational level maintenance technician and to what indenture level it is to be localised. If more than one failure mode causes the same failure indication, presents the method by which ambiguities are to be resolved. Describes any monitoring or warning devices that indicate impending failure. Indicates any planned test or inspections that can detect occurrence of the failure mode.
Basic Maintenance Actions	Describes the basic actions that the maintenance technician must take to correct the failure. Identifies special design provisions for modular replacement and any adjustments and calibrations required after repair.

Table 6-7. Maintainability Columns for Task 103 Worksheet

In the FMEA report, maintainability analysis worksheets generally follow the failure mode and effects worksheets and the criticality analysis worksheets for the same indenture level.

NOTE Damage Mode and Effects Analysis (DMEA) is also an extension of a FMEA. For additional information on DMEAs, refer to Task 104 in MIL-STD-1629.

FMEA Report

During the FMEA process, drafts of the FMEA are periodically reviewed and discussed. By the end of the process, the FMEA should be a complete record of analysis, tracking product conception, failures attributable to poor design quality or poor manufacturing practices and corrective actions for either eliminating or lessening the severity of all critical design flaws. Prior to initiating the first phase of prototype development, the FMEA should be formally approved as a stand-alone report.

Detailed information on content to be included in the final FMEA report appears in the FMEA standards (MIL-STD-1629, IEC 60812 (1985-07), Automotive FMEAs, SAE ARP 5580, etc.). The FMEA report typically consists of an introduction, summary and detailed analysis results.

Report Introduction

The information that generally appears in the introduction to or on the cover of the FMEA report includes:

- Name and description of the system being analysed.
- Indenture level to which analysis was performed.
- Preparing organisation or list of team members.
- Descriptions of customer and end users.
- Type of analysis performed (Product or Process FMEA).
- Analysis approach used (Functional, Interface, Detailed).
- Types of worksheets completed (Failure Mode, Criticality, Maintainability, etc.).
- Date of FMEA approval.
- Signature of approving authority.

Report Summary

The information that generally appears in the summary of the FMEA report includes:

- System description in the form of system definition narratives.
- Lists of data sources and techniques used in performing analysis.
- Ground rules and assumptions forming the basis of the FMEA.
- Summary of the analysis results.
- List of problems that cannot be corrected by design, with identification of any special controls needed to reduce failure risk.
- List of items omitted from the FMEA with a rationale for each item's exclusion.
- Recommendations for eliminating or reducing failure risks based upon FMEA analysis.

Detailed FMEA Analysis Results

The information that generally appears in the detailed analysis of the FMEA report includes:

- Reliability and functional block diagrams for each indenture level analysed.
- Functional descriptions of the system and all items analysed.
- Descriptions of each mission and mission phase that identify tasks to be performed and operating modes.
- Descriptions of ranking scales used for severity, occurrences and detection (as necessary).
- Descriptions of risk priority method and criticality levels if critical analysis is performed.
- Detailed worksheets that capture the FMEA results of each item, with the highest indenture level presented first, followed by worksheets for decreasing system indenture levels.
- Copies of data sources used in FMEA development.

Post-FMEA Analysis

During the design verification and validation phase, when the system is being used and supported, the accuracy of the FMEA can be assessed using applicable test results and field data. Verification is the process of proving that the system complies with its formally established requirements as well as the process of proving by special engineering inspections, analyses, demonstrations or tests that the system satisfies the requirements of its development specifications. Validation is the process of confirming that the system conforms to accepted engineering principles.

Testing during the design verification and validation phase provides a measure of the accuracy of the FMEA. Test results may show that the ground rules and assumptions should be changed or that additional iterations of analysis are necessary to maintain the integrity of the FMEA. Additional analysis may also be required to ensure that:

- End-item consequences captured from fault inspection tests and operating field data match FMEA results.
- FMEA results are clearly summarised and comprehensive recommendations are provided.
- Actions are provided for reducing the risk of single point failures, critical items and areas needing built-in test (BIT).
- Compensating provisions identified in the FMEA do lessen failure effects.
- Monitoring provisions correctly isolate the possible causes of system failure.
- Any new failure modes and consequences identified are fully assessed.
- Analysis results are being effectively communicated to enhance other programme decisions (BIT design, critical parts, reliability prediction, derating, fault tolerance, etc.).
- Related sources (analysis database, fault isolation manual, etc.) are revised as necessary.

After the product is in use, modifications to the FMEA are made based on FRACAS (Failure Reporting, Analysis and Corrective Action System) information, which provides for reporting failures in the field and tracking them to ensure that corrective actions are taken to correct the problem. Continuing to modify the FMEA throughout the life of the system results in a comprehensive and accurate record of the design analysis.

7. Weibull Analysis

Introduction

Among all of the distributions available for reliability calculations, the Weibull distribution is the only one unique to the engineering field. Originally proposed in 1937 by Professor Waloddi Weibull (1887-1979), the Weibull distribution is one of the most widely used distributions for **failure data analysis**, which is also known as **life data analysis** because life span measurements of a component or system are analysed.

A Swedish engineer and mathematician studying metallurgical failures, Professor Weibull pointed out that normal distributions require that initial metallurgical strengths be normally distributed, which is not necessarily the case. He noted the need for a function that could embrace a great variety of distributions, including the normal.

When delivering his hallmark American paper in 1951, *A Statistical Distribution Function of Wide Applicability*, Professor Weibull claimed that life data could select the most appropriate distribution from the broad family of Weibull distributions and then fit the parameters to provide reasonably accurate failure analysis. He used seven vastly different problems to prove that the Weibull distribution could easily be applied to a wide range of problems.

The initial reaction to the Weibull distribution was generally that it was too good to be true. However, pioneers in the field of failure data analysis began applying and improving the technique, which resulted in the U.S. Air Force recognising its merit and funding Professor Weibull's research until 1975.

Today, **Weibull analysis** refers to graphically analysing probability plots to find the distribution that best represents a set of life data for a given failure mode. Although the Weibull distribution is the leading method worldwide for examining life data to determine best-fit distributions, other distributions occasionally used for life data analysis include the exponential, lognormal and normal. By "fitting" a statistical distribution to life data, Weibull analysis provides for making predictions about the life of the products in the population. The parameterised distribution for this representative sample is then used to estimate such important life characteristics of the product as reliability, probability of failure at a specific time, mean life for the product and the failure rate.

Advantages of Weibull Analysis

Weibull analysis is extensively used to study mechanical, chemical, electrical, electronic, material and human failures. The primary advantages of Weibull analysis are its ability to:

- Provide moderately accurate failure analysis and failure forecasts with extremely small data samples, making solutions possible at the earliest indications of a problem.
- Provide simple and useful graphical plots for individual failure modes that can be easily interpreted and understood, even when data inadequacies exist.
- Represent a broad range of distribution shapes so that the distribution with the best fit can be selected.
- Provide physics-of-failure clues based on the slope of the Weibull probability plot.

Although the use of the normal or lognormal distribution generally requires at least 20 failures or knowledge from prior experience, Weibull analysis works extremely well when there are as few as 2 or 3 failures, which is critical when the result of a failure involves safety or extreme costs. **WeiBayes**, a distribution in the Weibull family, can even be used with no failures when prior engineering knowledge is sufficient.

Weibull Probability Plots

Weibull analysis studies the relationship between the life span of a component and its reliability by graphing **life data** for an individual failure mode on a Weibull probability plot. Weibull analysis is most often used to describe the time to failure of parts. These can be light bulbs, ball bearings, capacitors, disk drives, printers or even people. Failure modes include cracks, fractures, deformations or fatigue due to corrosion, excessive physical stress, high temperature, infant mortality, wear-out, etc..

When plotting the time-to-failure data on a Weibull probability plot, engineers prefer using **median rank regression** as the parameter estimation method. Median rank regression finds the best-fit straight line by using least squares regression (curve fitting) to minimise the sum of the squared deviation (regressing X on Y). Median rank regression is considered the standard parameter estimation method because it provides the most accurate results on the majority of data sets.

Typically, the horizontal scale (X-axis) measures the component age, and the vertical scale (Y-axis) measures the cumulative percentage of the components that have failed by the failure mode under consideration.

A Weibull probability plot has a linear/nonlinear time-scale along the abscissa and another nonlinear scale for the distribution function along the ordinate. These nonlinear scales are selected in such a way that the model used for data is an appropriate one. If the scales match the data, the graph turns out to be a straight line. Because of their simplicity and usefulness, probability graphs have been used for many years in statistical analysis. However, it must be noted that the probability plotting methods to derive distribution parameters are independently and identically distributed. This is usually the case for non-repairable components and systems but may not be true with failure data from repairable systems.

In Figure 7-1, the Weibull probability plot considers the times to failure for a unique failure mode. When a number of parts are tested under normal operating conditions, they do not all fail at the same time for the same cause. The failure times for any one cause tend to concentrate around some average, with fewer observations existing at both shorter and longer times. Because life data is distributed or spread out like this, they are said to follow a distribution. To describe the shape of a distribution, which tends to depend upon what is being studied, statistical methods are used to determine a formula. If the plotted data points fall near the straight line, the Weibull probability plot is considered reasonable.

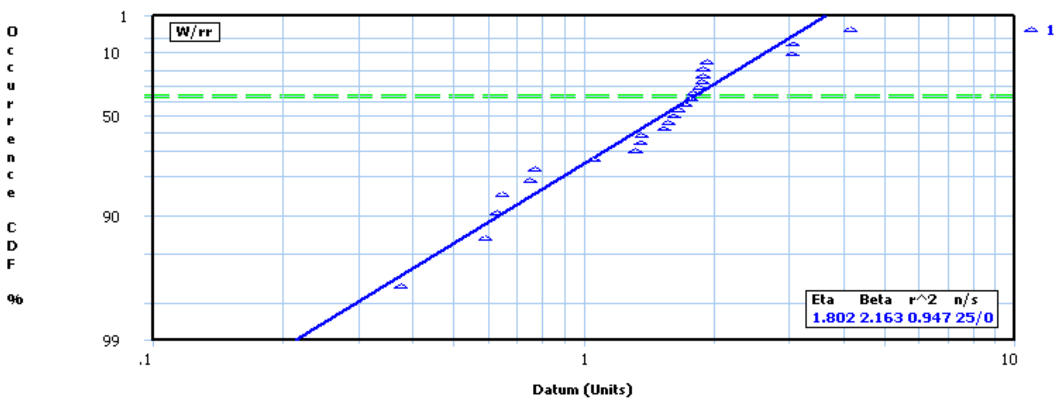


Figure 7-1. Weibull Probability Plot

NOTE Although the Y-axis values are probabilities that go from 1 to 99, the distances between the tick marks on this axis are not uniform. Rather than being based on point changes, the distances between tick marks on both the Y and X axes of the Weibull probability plot are based on percentage changes. Known as a logarithmic scale, the distance from 1 to 2, which is a 100 percent increase, is the same as the distance from 2 to 4, which is another 100 percent increase. A logarithmic scale provides for like-to-like comparisons of several series. In addition to offering more insight into the problem, this visual representation helps to identify the distribution method that best fits a straight line to the data set.

While the previous figure plots occurrences, it is very common to plot the age of components at failure. In these cases:

- The Y-axis is usually $ln\left\{ln\left[\frac{1}{1-F(t)}\right]\right\}$.
- The X-axis is $ln(t)$.
- The Y-axis intercept is $\beta \cdot ln(\eta)$.

Uses for Weibull Analysis

Weibull analysis has traditionally be used for analysing failure data for:

- Development, production and service.
- Quality control and design deficiencies.
- Maintenance planning and replacement strategies.
- Spare parts forecasting.
- Warranty analysis.
- Natural disasters (lightning strikes, storms, high winds, heavy snow, etc.).

New applications of Weibull analysis include medical research, instrument calibration, cost reduction, materials properties and measurement analysis.

Understanding Weibull Analysis

The two-parameter Weibull is by far the most widely used distribution for life data analysis:

$$R(t) = exp\left\{-\left(\frac{t}{\eta}\right)^{\beta}\right\}$$

Where:

$t \geq 0$, $\beta > 0$ and $\eta > 0$. Here, β and η are shape and scale (characteristic life) parameters of the distribution.

Because two-parameter Weibull distribution effectively analyses the life data from burn-in (infant mortality), useful life and wear-out periods, it can be used in increasing, constant and decreasing failure rate situations.

The first parameter defining the Weibull probability plot is the **slope**, beta (β), which is also known as the **shape parameter** because it determines which member of the Weibull family of distributions best fits or describes the data. The second parameter is the **characteristic life**, eta (η),which is also known as the **scale parameter** because it defines where the bulk of the distribution lies. The parameters β and η are estimated from the life data, which are always positive values. After Weibull analysis is completed, the Weibull probability plot visually indicates the slope and the goodness of fit.

NOTE A three-parameter Weibull distribution is also widely used. The third parameter, **location**, is a constant value that is added to or subtracted from the time variable, t. For additional information, refer to page 7-15.

The Weibull hazard function or **failure rate** depends upon the value of β. Because the β value indicates whether newer or older parts are more likely to fail, the Weibull hazard function can represent different parts of the bathtub curve:

- **Infant Mortality.** In electronics and manufacturing, infant mortality refers to a higher probability of failure at the start of the service life. When the β value is less than 1.0, the Weibull probability plot indicates that newer parts are more likely to fail during normal usage, which is known as a **decreasing instantaneous failure rate**. To end infant mortality in electronic and mechanical systems with high failure rates, manufacturers provide production acceptance tests, "burn-in" and environmental stress screenings prior to delivering such systems to customers. Providing that the part survives infant mortality, its failure rate should decrease, and its reliability should increase. In this case, because such parts tend to fail early in life, old parts are considered better than new parts. Overhaul of parts experiencing high infant mortality is generally not appropriate.
- **Random Failures**. Assuming that the Weibull probability plot is based on a single failure mode, a β value of 1.0 indicates that the failure rate is constant or independent of time. This means that of those parts that survive to time *t*, a constant percentage will fail in the next unit of time, which is known as a **constant hazard rate** or **instantaneous failure rate**. This makes the Weibull probability plot identical to the exponential distribution. Because old parts are assumed to be as good as new parts, overhaul is generally not appropriate. The only way to increase reliability for components or systems that experience random failures is by redesigning them.
- **Early Wear-out**. Unexpected failures during the design life are often due to mechanical problems. When the β value is greater than 1.0 but less than 4.0, overhauls or part replacements at low **B-lives** may be cost effective. B-lives indicate the ages at which given percentages of the population are expected to fail. For example, the B-1 life is the age at which 1 percent of the population is expected to fail, and the B-10 life is the age at which 10 percent of the population is expected to fail. Reliability and cost performance for parts experiencing early wear-out may be improved by optimizing the preventative maintenance schedule.
- **Rapid Wear-out**. Although a β value greater than 4.0 within the design life of a part is a major concern, most Weibull probability plots with steep slopes have a safe period within which the probability of failure is negligible, and the onset of failure occurs beyond the design life. The steeper the slope, the smaller variation in the times to failure and the more predictable the results. For parts that have significant failures, overhauls and inspections may be cost effective. Because scheduled maintenance can be costly, it is usually only considered when older

parts are more likely to wear out and fail, which is known as an **increasing instantaneous failure rate**.

Because different slopes imply different failure classes, the Weibull probability plot provides clues about what may be causing the failures. Figure 7-1 lists the failure causes that are most likely for each failure class.

β Value	Class	Description
β < 1.0	Infant Mortality	When β < 1.0, failures tend to be due to: • Inadequate burn-in or stress screening. • Quality problems in components. • Quality problems in manufacturing. • Improper installation, setup or use. • Problems in rework/refurbishment.
β = 1.0	Random Failures	When β = 1.0, failures tend to be due to: • Human error during maintenance. • Induced rather than inherent failures. • Accidents and natural disasters (foreign objects, lighting strikes, wind damage, etc.).
β > 1.0 and < 4.0	Early Wear-out	When β > 1.0 and < 4.0, failures tend to be due to such problems as: • Low cycle fatigue. • Bearing failures. • Corrosion/erosion. • Manufacturing process.
β > 4.0	Rapid Wear-out	When β > 4.0, failures tend to be due to rapid wear-out associated with old age or: • Inherent property limitations of materials (such as ceramic being brittle). • Severe problems in manufacturing process. • Minor variability in manufacturing or in material.

Table 7-1. Failure Classes and Likely Causes by Slope Values

Statisticians, mathematicians and engineers have formulated statistical distributions to mathematically model or represent certain behaviours. Compared to other statistical distributions, the Weibull distribution fits a much broader range of life data. The Weibull **probability density function** (pdf) is the mathematical function that describes the fitted curve over the data. The pdf is represented either mathematically or on a plot where the X-axis represents times. Different members of the Weibull family have widely different shaped pdfs. The **cumulative density function** (cdf) is the area under the curve of the pdf. The cdf for the Weibull distribution is given by:

Equation

$$F(t) = 1 - exp\left\{-\left[\frac{t}{n}\right]^{\beta}\right\} \qquad (7.1)$$

Where:

η represents the characteristic life (scale parameter).

β represents the slope (shape parameter).

The cdf gives the probability of failure within time, *t*. The parameters η and β are estimated from the failure times. If the failure data comes from a Weibull distribution, the values of η and β can be plugged in the cdf formula to find the fraction of parts expected to fail within a certain time.

Characteristic life, η, and the Mean Time To Failure (MTTF) are related. The characteristic life shows the point in the life of the part or system where the failure probability is independent of the parameters of the failure distribution. For all Weibull distributions, η is defined as the age at which 63.2 percent of the units can be expected to have failed.

For $\beta = 1$, MTTF and η are equal. The relationship between MTTF and η is gamma function:

Equation

$$MTTF = \eta \cdot \Gamma\left[1 + \frac{1}{\beta}\right] \qquad (7.2)$$

When $\beta < 1$, MTTF > η.

When $\beta = 0.5$, MTTF = 2η.

When $\beta = 1$, MTTF = η, the exponential distribution.

When $\beta > 1$, MTTF < η.

Although Professor Weibull originally proposed using the mean or average value to plot MTTF values on the Y-axis of Weibull probability plots, the standard engineering method is now to rank the life data by the median value of the failure times. Table 7-2 displays a Median Ranks table (50%) for a sample size of 10, which was generated using Leonard Johnson’s Rank formula.

Because non-symmetrical distributions are so common in life data, median rank values are slightly more accurate than mean values. Once β and η are known, the probability of failure at any time can easily be calculated.

Rank Order	1	2	3	4	5	6	7	8	9	10
1	50.00	29.29	20.63	15.91	12.94	10.91	9.43	8.30	7.41	6.70
2		70.71	50.00	38.57	31.38	26.44	22.85	20.11	17.96	16.23
3			79.37	61.43	50.00	42.14	36.41	32.05	28.62	25.86
4				84.09	68.62	57.86	50.00	44.02	39.31	35.51
5					87.06	73.56	63.59	55.98	50.00	45.17
6						89.09	77.15	67.95	60.69	54.83
7							90.57	79.89	71.38	64.49
8								91.70	82.04	74.14
9									92.59	83.77
10										93.30

Table 7-2. Median Ranks (50%)

Performing Weibull Analysis

In addition to indicating whether newer or older parts are more likely to fail, the Weibull distribution can be applied to a number of different analyses, including reliability and maintenance analysis, probabilistic design, distribution analysis, cost reduction and design comparison. Weibull software, which is any program capable of using the Weibull distribution to calculate the reliability of a component or system in the future based on its past performance, analyses field or laboratory data. Using Weibull software to predict reliability basically consists of six steps:

1. Gather “good” life data.
2. Select the distribution type.
3. Specify the estimation method.
4. Indicate the confidence values.
5. Generate the analysis.
6. Interpret the results.

Gathering “Good” Life Data

The first and most difficult step in Weibull analysis is the gathering of “good” life data. Because the results from Weibull analysis can only be as good as the data on which it is based, data-related tasks must be performed carefully.

Determine the Failure Usage Scale

In Weibull analysis, the units for age depend entirely upon part usage and the failure mode under consideration. Product lifetimes can be measured in hours, miles, cycles or any other metric that applies to a period of successful operation for a particular product. For example, the age of an automobile tire is likely to be measured in the number of miles or kilometers for which the tire has been used. The age of a burner and turbine is likely to be measured in either the amount of time spent operating at a high temperature or the number of cold-to-hot-to-cold cycles. Thus, component age can be measured in distance, time, mission cycles, duty cycles, number of revolutions, etc., depending upon the failure mode in question.

The best results from Weibull analysis are achieved when each failure mode is analysed separately and the time origin and scale for the age of the component has been attentively considered. Because the best data analysis methods cannot improve bad data, thoroughly investigate data sources to find the root cause of reported difficulties, keeping in mind that a single part can have many failure modes. If the data set contains a mixture of failure modes, tag individual data points to indicate the appropriate failure mode. After the life data is manually entered or automatically imported into Weibull software, distributions can then be fitted to each failure mode.

Although the failure mode generally dictates the most appropriate unit for age, uncertainty about the best age parameter may occasionally exist. For such situations, Weibull probability plots can easily be generated for each alternative age parameter. The best age parameter would then be the one used in the Weibull probability plot that most closely fits the data points to a straight line. Weibull software often provides for automatic selection of the best distribution and optimizes the scale for the life data being analysed.

Because Weibull probability plots usually provide significant knowledge from very little data, graphing what is viewed as “bad” data can even be informative. When operating data is not available or obtainable, for example, the age parameter can be based on calendar intervals. For a failed furnace, the most appropriate age parameter would probably be either operating hours or operating cycles; however, the only data available may be initial shipment and return dates. Although using calendar time for the age parameter may result in a poorer fit and increased uncertainty, a measure of the goodness of fit can easily be calculated to determine if the resulting Weibull probability plot is accurate enough to provide valuable analysis.

When material characteristics such as creep, stress rupture and fatigue are considered, the age parameter is often stress, load or temperature. Although these parameters do not truly indicate age, the resulting Weibull probability plots are interpreted as if they were component ages. Prior to collecting component age for any probability plot, however, ensure that:

- The single failure mode to be analysed is clearly defined.
- The time origin for component age is clearly defined.
- The scale for measuring the passage of time is agreed upon.

Arrange the Data

As life data is collected, it must be arranged so that the lowest failure time (earliest-occurring failure) is listed first and the highest failure time (latest-occurring failure) is listed last. This ranking sets up the plotting positions for the time (t) axis and the ordinate, $F(t)$, in percentage values. Each failure is to be plotted at its time-to-failure (t) and an estimate of $F(t)$, the percentage of the total population failing before it.

Identify Suspensions

Units that have not failed by the failure mode under investigation are called **suspensions** or **censored units**. Suspensions have either not failed at all or have failed by an entirely different failure mode. Suspensions are categorised based on how their ages compare to the length of service (or age) that the component has so far attained. In engineering, suspensions generally refer to units with true times to failures greater than the oldest age for the failure mode under consideration. However, other types of suspensions exist and are categorised based on age:

- **Early suspensions**. Units whose failure age is less than the earliest failure age for the failure mode in question. Early suspensions have little effect on the Weibull probability plot. Also known as **left-censored data**, early suspensions are not often found in engineering data. During a medical prevention study, left-censored data is created when a person joins the study after learning that he or she already has the disease. Because contraction of the disease occurred prior to joining the prevention study, this occurrence has an age that is less than the first failure (occurrence) that develops during the course of the study.
- **Intermediate suspensions**. Units that have random failure ages for failure modes other than the failure mode in question. Intermediate suspensions, also known as **random suspensions** or **progressive suspensions**, tend to shift the Weibull line somewhere between the early and late suspensions.
- **Late suspensions**. Units whose failure age is greater than the oldest failure age for the failure mode in question. Late suspensions may reduce the slope of the

Weibull probability plot. Also known as **right-censored data**, late suspensions are a concern in engineering data. During life testing, right-censored data is created by the removal of a part before failure. While it is known that the part operated successfully for a given period of time, the length of time it may have continued to operate is unknown.

Although not weighted as much as failures, all identified suspensions must be included in the sample data set. Because suspensions have no effect on adjusted ranks or median ranks until after they occur, the procedure is to rank the data with the suspensions first and then to adjust the ranks. While adding suspensions generally has little effect on the slope (β), it does tend to increase characteristic life (η). Thus, failing to include suspensions can yield results that are too pessimistic.

Identify the Data Type

When the precise failure or suspension time for each point in the data set is known, the data is **point-by-point**. Considered the standard type of data for Weibull analysis, point-by-point data is classified into **occurrences** (failures) and **suspensions**. For an occurrence, the failure age or event is recorded precisely at a point on the time scale (*t*). For a suspension, the removal of the unfailed unit is recorded precisely at a point on the time scale, even though its true time to failure is actually greater than the age attained so far ($> t$). Most controlled test data is point-to-point because the length of the testing period and the time of failures are known. When all failure times are known and good estimates can be made of suspension times, warranty data can also be classified as point-by-point.

When exact failure and suspension times are not known, the data is **grouped** by failure intervals (or number of units). Grouped data is considered **dirty** because it causes the uncertainty of the analysis to increase. When handled in monthly counts of failures without exact failure and suspension times, warranty data is considered grouped data. Terms used to better describe grouped data include:

- **Interval data**. Involves benign (or dormant) failure modes that are only found when the component or system is shut down and inspected at periodic intervals. When a benign failure mode is found upon first inspection, it is called a **discovery.** The true time to failure for the failed part is actually less than the age recorded at the first inspection ($< t$). A benign failure that occurs after the last inspection time (*t1*) but is not discovered until the next inspection time (*t2*) has a true time to failure greater than the previous inspection age but less than the detection age.
- **Coarse data**. Related to interval data, coarse data has less precise time to failures because the intervals between data collections are too long, perhaps even months rather than days or hours.
- **Probit data**. Also known as **destructive inspection data,** probit data is obtained when every part is inspected at every inspection due to the additional uncertain-

ties that are related to detecting or finding failures during inspection. For probit data, each observation is either considered to be a suspension or a failure. For example, when bombs and missiles are tested (or eddy currents are inspected), they either do or do not work.

Because the type of life data determines which distribution type is best, Table 7-3 describes the selections that are commonly found in Weibull software for indicating how data points are collected.

Type	Description
Point-by-point	Provides for entering the failure and suspension data when the precise failure or suspension time is known for each point in the data set. When 20 or fewer of such data points exist, the standard method is to select the Weibull distribution and use median rank regression as the parameter estimation method.
Point-by-point/Inspect	Provides for entering the failure and suspension data when the data is specified in periodic inspection intervals. This classification also provides for defining the interval frequency.
Grouped, Probit 2	Provides for entering the failure and suspension data from repeated tests on the same units **by occurrences**. This method compares the cumulative number of failures to the number of inspected units at various points in time. When a new unit replaces a unit that failed in a previous inspection, it is added to the number of failed units as well as to the number of inspected units. This classification also provides for entering a varying number of inspected units at different ages.

Table 7-3. Data Types and Descriptions

Type	Description
Grouped, Probit 3	Provides for entering the failure and suspension data from non-repeated tests on varying sizes of units tested at different times **by percentages**. This method compares the cumulative percentage of failures to the number of inspected units at various points in time. Such tests are sometimes found in destructive inspections. Because the cumulative failure distribution is an increasing function in time, the cumulative percentage failed tends to increase with time for most destructive tests. However, considering the random nature of failures, this may not always be the case. This classification also provides for using the varying number of inspected units at different ages.
Grouped, Kaplan-Meier	Provides for entering the failure and suspension data when the exact failure time defines the intervals, which means that failures and suspensions occur at the end of the interval. This method can also be used for intervals that are not same, especially if actuarial corrections are used when entering the data. This method accurately estimates the cumulative distribution without making any distribution assumptions.
Interval MLE	Provides for entering the failure and suspension data in a generalised data format for when Maximum Likelihood Estimation (MLE) or Modified Maximum Likelihood (MMLE) is the parameter estimation method. (Refer to “Specifying the Estimation Method” on page 7-18.) Occurrence, suspension, discovery and intervals for the data set can be specified, and the interval can be defined.

Table 7-3. Data Types and Descriptions (Continued)

Select the Distribution Type

The Weibull family of distributions can be applied in a variety of forms, including one-parameter, two-parameter, three-parameter and mixed Weibull. On occasion, the normal and lognormal distributions, which are not members of the Weibull family, are also used for life data analysis. The distribution that is most appropriate to a particular data set is chosen based on the quantity and quality of the data, past experience and goodness-of-fit tests. Table 7-4 describes the distributions in the Weibull family.

Two-Parameter Weibull	The required parameters for the two-parameter Weibull distribution are the slope and characteristic life. This Weibull distribution provides reasonably accurate failure analysis and failure forecasts with extremely small samples. It has the special capability to diagnose failure types, such as infant mortality (particularly for electronics), age-independent failures (accidents and natural occurrences) or wear-out type mechanisms (bearings, filters, etc.). The two-parameter Weibull distribution is recommended if the failure rate decreases (burn-in period) or increases (wear-out period) over time, or if the failure rate remains constant (random failure period).
Exponential	The only parameter required for the exponential distribution is the failure rate. The exponential distribution can be viewed as a special case of the Weibull distribution, where the β value is known to equal 1. When the failure rate for a component is constant, then its reliability is best described by the Weibull or exponential distribution. A constant failure rate leads to the memoryless property, which states that the remaining life of a used component is independent of its current age, thereby declaring that a used component as good as a new component. (The Weibull distribution is memoryless only when the β value equals 1.) Because the exponential distribution assumes that there is no infant mortality or wear-out period, the field data must be carefully tested to ensure that such assumptions are valid. For the exponential distribution, the MTTF is the reciprocal of the failure rate.
Rayleigh	The only parameter required for the Rayleigh distribution is the characteristic life. The Rayleigh distribution can be viewed as a special case of the Weibull distribution, where the β value is known to equal 2. It is, however, an important distribution in its own right, finding application not only in reliability problems but also in noise problems associated with communication systems. A single-parameter distribution similar to the exponential distribution, the Rayleigh distribution can be used to describe the root-mean-square (RMS) value of error sources. The Rayleigh distribution is recommended if the failure rate increases linearly with time.

Table 7-4. Distributions in the Weibull Family

WeiBayes	The only parameter required for the WeiBayes distribution is characteristic life. Also known as the **one-parameter Weibull distribution**, WeiBayes is a special case of the Weibull distribution where the slope parameter (β) is defined based on prior knowledge. Related to Bayesian assumption, the WeiBayes distribution is a powerful method developed to solve the problems that occur when traditional Weibull analysis has large uncertainties. The WeiBayes distribution is more accurate than two-parameter Weibull distributions when the sample has fewer than 10 failures, and it is the only distribution that can be used when there are 0 failures. For example, after a design change corrects an existing failure mode, success data from tests can be used to determine a lower confidence bound for the Weibull line for the new design called a WeiBayes line. When parts exceed their design life, a Weibull analysis with no failures can be constructed to extend their life. Because the WeiBayes distribution can be used without the requirement of testing to failure, it is of extreme importance in situations where failures involve safety or extreme costs.
Three-Parameter Weibull	In addition to slope and characteristic life parameters, the three-parameter Weibull distribution requires a location parameter, **t-zero** (t_0), that defines the location of the distribution in time. This third parameter provides for shifting the origin of the age scale and is only used if earlier two-parameter Weibull analysis has shown that it is appropriate. (For additional information, refer to "Curved Data on Weibull Probability Plots" on page 7-26.) When using the location parameter, the t_0 value is either subtracted from or added to each age value prior to generating the Weibull probability plot. For example, if the probability of failure is zero for some given period of time, the origin of the age scale should be shifted from zero to time t_0 to reflect this **guaranteed failure-free period**. The correction, t_0, would be a positive value equal to the minimum time necessary for a failure to occur. To provide for some loss of life (reliability) before service officially begins, t_0 can be a negative value. Negative corrections are helpful for situations where spare parts deteriorate while in storage. Rubber parts, chemicals and ball bearings, for example, all deteriorate with prolonged storage. When the t_0 value applied to the data is correct, the resulting plot follows a straight line. Without prior experience, at least 20 failures are usually needed to do a distribution analysis using the three-parameter Weibull distribution.

Table 7-4. Distributions in the Weibull Family (Continued)

Gumbel	In the 1920s, E. J. Gumbel was the first to seriously investigate extreme values in failure data, finding that there are only six separate extreme value distributions. His Type III smallest extreme value distribution is the same as the Weibull distribution. The **Gumbel- (lower) distribution**, which is also known as a **Type I lower extreme value distribution**, is an extreme minimum value distribution. The **Gumbel+ (upper) distribution**, which is also known as a **Type I upper extreme value distribution**, is an extreme maximum value distribution. Gumbel distributions are recommended when failure data is a result of rare events and failure values are extreme. Examples include natural disasters and maximum guest loads. Because Gumbel distributions (and normal distributions) can predict negative life for high reliability requirements, an impossibility with life data, care must be taken when using them to model life data.

Table 7-4. Distributions in the Weibull Family (Continued)

Statistical Concerns

Although statisticians oppose the use of extremely small samples, cases of safety and extraordinary financial loss prevent the collection of additional data. When only a few failures exist, Weibull analysis can provide usable results because:

- Wear-out failures tend to occur in the oldest units. This results in most failures being plotted in the B-0.1 to B-1 lives, which is in the lower left corner of the Weibull probability plot, the area in which engineering is most interested.
- Both failures and suspensions are included. Although suspensions are not weighted as heavily as failures, thousands of suspensions may exist, contributing to more accurate engineering predictions in the B-0.1 to B-1 lives.

The Weibull distribution applies to situations where there are multiple opportunities to fail and the first failure is of extreme interest. The Weibull distribution also applies to system deterioration that is linear rather than accelerating. When deterioration is non-linear but rather a function of the current deterioration, the lognormal distribution applies. Table 7-5 describes the normal and lognormal distributions because they are occasionally used for the parametric analysis of life data even though they are not members of the Weibull family. Most Weibull software provides for quickly generating all distributions and automatically picking the best fit for a data set.

Normal (or Gaussian)	The two parameters required for the normal distribution are the mean and standard deviation. Normal distributions, which are always symmetric and commonly called **bell curves**, are important and widely used in the field of statistics and probability. Normal distributions are frequently used to describe equipment that has increasing failure rates with time. The normal distribution is recommended only if failure times can be expressed as a summation of some other random variables. Although the normal distribution is a handy tool for describing all sorts of different data, it allows observations to be negative. Because parts cannot fail before time $t = 0$, life data is always positive. As a result, the normal distribution does not usually describe life data very well. Most analysts do not even bother to check for a normal fit because life data that follow the normal distribution also generate good Weibull probability plots.
Lognormal	The two parameters required for the lognormal distribution are the mean and standard deviation. Although the lognormal distribution is similar to the normal distribution, it assumes that the logarithm of the values of random variables is normally distributed rather than the values themselves. Thus, all values are positive, and the distribution is skewed to the left. The lognormal distribution is probably the most significant competitor to the Weibull distribution. It is frequently used in engineering for metal-fatigue testing, maintainability data (time to repair), chemical-process equipment failures and repairs, some material characteristics and non-linear, accelerating deterioration. When the time to failure results from the multiplication of effects, the lognormal distribution is recommended. For example, in the case of progressive deterioration, a crack forms due to stress, and the stress increases as the crack grows. Non-engineering applications of the lognormal distribution include the analysis of personal incomes, inheritances and bank deposits.

Table 7-5. Non-Weibull Distributions for Failure Data Analysis

Specifying the Estimation Method

To fit a statistical model to a life data set, parameters for making the life distribution most closely fit the data are estimated. Although there are several estimation methods to choose from, based on the data type and number of data points being analysed, various forms of rank regression and Maximum Likelihood Estimation (MLE) are used most frequently. This is because only they work with all data types and for all distributions. Based on the parameter estimations, the resulting Weibull probability plot indicates how well the selected distribution fits the data set being analysed.

Rank Regression

Rank regression is a method of fitting a line (or curve) to data. To fit a statistical model to a life data set, estimates are made for the parameters of the life distribution that will make the function most closely fit the data. The parameters control the scale, shape and location of the pdf function. For example, in the three-parameter Weibull distribution:

- The slope parameter, β, defines the shape of the distribution.
- The scale parameter, η, defines where the bulk of the distribution lies.
- The location parameter, t_0, defines the location of the distribution in time.

In almost all cases, the best estimation method is *median rank regression*, which estimates the Weibull parameters β and η using the method of least squares to best fit a straight line through the failure times and median ranks graphed on the Weibull probability plot. Once you have gathered good life data for a single, well-defined failure mode, Weibull software generates the Weibull probability plot by:

1. Ranking the times of both failures and suspensions from the earliest occurrence to the last occurrence. (Although suspensions are not weighted as much as failures, they must be included in the data set.)
2. Calculating the adjusted ranks for the failures. (Suspensions are not plotted.)
3. Converting the adjusted ranks to median ranks using Benard's approximation.
4. Converting median ranks to percentages for graphing on Weibull probability plots.
5. Plotting the failure times on the X-axis and the median ranks on the Y-axis.
6. Displaying confidence bounds if confidence parameters are specified.
7. Estimating the characteristic life by reading the B-63.2 life from the Weibull probability plot.
8. Estimating the slope as the ratio of the rise.

Median rank regression seems to be the most accurate parameter estimation method for samples that contain fewer than 100 failures.

Maximum Likelihood Estimation

Maximum Likelihood Estimation (MLE) is an alternative method that most statisticians prefer. It finds the values of β and η that maximise the **likelihood** of obtaining β and η given the observed data. The likelihood function consists of the product of the pdfs written once for each data point, with the distribution parameters unknown. Evaluated in logarithms, this function has many terms and is quite complicated. With two parameters, the log likelihood is a three-dimensional surface shaped like a mountain. The top of the mountain locates the maximum likelihood values. The MLE values are the **most likely** to be the true values. When the data set to be analysed contains 100 or more failures and has either many suspensions or data that is **dirty** or deficient, MLE tends to be more accurate than median rank regression. However, engineers, who like to see data plotted, find MLE deficient because of its inability to provide a good graphic display.

Parameter Estimation Methods

In addition to the data type and the number of data points, parameter estimation methods can be selected based on computational time and fit quality of the analysis line. Table 7-6 describes the rank regression and MLE methods that are usually available in Weibull software.

Method	Description/Advantages	Disadvantages
Median Rank Regression	Finds the best-fit straight line by using least squares regression (curve fitting) to minimise the sum of the squared deviation (regressing X on Y). Median regression is considered the standard parameter estimation method because it provides the most accurate results on the majority of data sets. In addition to using the simplest method, the Weibull probability plots that this method generates are easily understood.	Cannot be used with a single failure. Statisticians, who prefer MLE, claim that median regression is not rigorous enough.
Mean Regression	A regression method based on mean values (as originally proposed by Weibull) rather than median values.	Because of the non-symmetrical nature of life data, mean values are generally not as accurate as median values.

Table 7-6. Parameter Estimation Methods

Method	Description/Advantages	Disadvantages
Mean Regression Special	A regression method based on mean values instead of median values, where the percentage of failure is the dependent variable and time is the independent variable (regressing Y on X).	Because of the non-symmetrical nature of life data, mean values are generally not as accurate as the median values. Regressing Y (component age) on X (time to failure) is generally not as accurate as regressing X on Y. This is because the times to failure are much more scattered and have more error than the component ages.
Hazen Regression	A regression method based on midpoint values instead of median values.	Cannot be used with a single failure.
Hazen Regression Special	A method that uses the midpoint to calculate rank regression, where the percentage of failure is the dependent variable and time is the independent variable.	Regressing Y (component age) on X (time to failure) is generally not as accurate as regressing X on Y. This is because the times to failure are much more scattered and have more error than the component ages.
Binomial Regression	An exact method that uses binomial distribution to find the median rank values. This is generally the default parameter estimation method in Weibull software.	Calculations are intensive.
Binomial Regression Special	An exact method that uses binomial distribution to find the rank values, where the percentage of failure is the dependent variable and time is the independent variable.	Calculations are intensive. Regressing Y (component age) on X (time to failure) is generally not as accurate as regressing X on Y because the times to failure are much more scattered and have more error than the component ages.
Benard Regression	An approximation method to binomial regression that requires less computational time to determine median rank values.	Approximations are used.

Table 7-6. Parameter Estimation Methods (Continued)

Method	Description/Advantages	Disadvantages
Benard Regression Special	A simplified approximation method to binomial regression, where the percentage of failure is the dependent variable and time is the independent variable.	Approximations are used. Regressing Y (component age) on X (time to failure) is generally not as accurate as regressing X on Y because the times to failure are much more scattered and have more error than the component ages.
Maximum Likelihood Estimation (MLE)	Finds the β and η values that maximise the probability or "likelihood" of obtaining the observed data. MLE is probably the best practice to use with 500 or more failures; however, if the right suspensions exist, MLE can be used with a single failure. If inspection intervals are not the same with all units, MLE should be used.	Calculations are complex and iterative, and convergence does not always occur. Generally requires more than 500 failures for accurate results. Smaller samples are likely to be biased and yield results that are overly optimistic. Lacks a good method for plotting the data to produce the graphic data displays important to engineers.
Modified Maximum Likelihood Estimation (MMLE)	To reduce the bias of the estimation, uses the square root of an unbiased estimate of variance, SQR(Var-U), rather than the MLE of the standard deviation from the normal distribution. MMLE is considered the best method if a large sample has many suspensions or dirty data.	All of the disadvantages for MLE apply to MMLE. Although the square root is less biased for small sample than the standard deviation of the normal distribution, small sample bias still exists.

Table 7-6. Parameter Estimation Methods (Continued)

Specifying Confidence Values

The results from Weibull analysis are estimates based on the observed lifetimes of a very small sample. Because the sample size is generally very limited, uncertainty about the results exist. Thus, the **degree of confidence**, which is a measure of statistical precision, can be used to gauge the accuracy of the resulting analysis. Specified prior to looking at the data points and performing the Weibull analysis, the degree of confidence is a percentage value that is entered. The higher the percentage value, the higher the desired confidence of the results.

A **confidence interval** is used to show the range within which the true analysis value is expected to fall a certain percentage of the time (the degree of confidence). The confidence interval quantifies the uncertainty due to sampling error by expressing the confidence that a specific interval contains the quantity of interest. Whether a specific interval actually contains the quantity of interest, however, is unknown.

NOTE **Assurance** refers to when the value entered for the degree of confidence is equal to the reliability.

Confidence intervals can have either one or two bounds. The type of confidence bound selected is dependent upon the application. One-sided bounds are used to indicate that the quantity of interest is above the lower bound or below the upper bound with a specific confidence. A one-sided lower bound is used when predicting reliability. A one-sided upper bound is used for predicting the percentage of components failing under warranty.

Two-sided bounds are used to indicate that the quantity of interest is contained within the bounds with a specific confidence. Two-sided bounds are used for predicting the parameters of a distribution. Confidence interval calculations can be used on all distributions and parameter estimation methods. To find the confidence interval, the confidence method, the type of confidence interval and the degree of confidence must all be assigned. Table 7-7 describes the confidence methods available in most Weibull software.

Confidence Method	Description
Modified Fisher Matrix	Produces almost instantaneous results with reasonable accuracy when 10 or more failures are included in the sample. This method assumes B-lives for input percentages are normally distributed and produces a full plot (extrapolated bounds). The Modified Fisher Matrix method is considered the best confidence method when rank regression is the selected parameter estimation method for larger samples with few suspensions. The Modified Fisher Matrix method has various versions that include: • **Gumbel Truncated**. The original (unmodified) Fisher Matrix method uses some of the Gumbel terms but does not use all of the second-partial derivative terms. It also has significant small sample bias. Although this has no effect when MLE is the estimation method, differences in solution parameters are significant when rank regression is the estimation method. • **Weibull Full**. This Fisher Matrix method is significantly biased for rank regression and small samples. It uses all second-partial derivative terms.

Table 7-7. Confidence Methods Commonly Available

Confidence Method	Description
Modified Fisher Matrix (Continued)	• **Gumbel Full**. This Fisher Matrix method is based upon all of the Gumbel terms and is less biased for smaller samples. Consequently, it is considered the standard Fisher Matrix method.
Likelihood Ratio	When MLE or MMLE is the selected parameter estimation method, the likelihood ratio can be used to compare designs for significant differences, compensating for the small sample bias so often found in life data. The likelihood ratio method produces a full plot (extrapolated bounds) and provides the amount of differences between two data sets. In addition to comparing a new design to an old design, the likelihood ratio method can be used to compare supplier A against supplier B, application C against application D, etc.. It is accurate when 30 or more failures are included in the sample and is the best practice for data with suspensions. However, this method takes significant computer time and the results are almost identical to the Fisher Matrix method, which are calculated almost instantaneously.
Beta-Binomial	This method is evaluated at each occurrence point and is best used for determining bounds for probit analysis. Although beta-binomial bounds give more conservative results, they require more calculation time than the Fisher Matrix method.
Monte Carlo	This method is a special technique for simulation based upon the pivotal statistic method. Made possible only by today's fast computers, Monte Carlo simulation is used as a prediction tool and can provide a reference for analytical techniques. When used for generating confidences, Monte Carlo simulation generates random data samples to add to existing data sets with very few data points so that more accurate correlation p-values, confidence limits for B-lives and parameters can be generated. Producing generally conservative results, the Monte Carlo method is considered the best practice for confidence estimation for distributions without exact derivations. Because Monte Carlo simulations are performed for each confidence point, this method requires a great deal of calculation time. Unless the confidence seed value is kept the same, recalculating for the same conditions produces slightly different results each time, giving an indication of actual variability. Monte Carlo simulation is the recommended method for generating confidence intervals for data sets with 10 or fewer data points or for data sets with random suspensions.

Table 7-7. Confidence Methods Commonly Available (Continued)

Confidence Method	Description
Greenwood's Variance	This method is best used for determining bounds for Kaplan-Meier models, which are described in "Related Quantitative Models" on page 7-29.

Table 7-7. Confidence Methods Commonly Available (Continued)

Although increasing the sample size can reduce uncertainty, testing more units to failure can be very costly and even impossible in cases that risk safety. A more cost-effective method of reducing sample uncertainty is to employ prior experience with the subject failure mode. If a Weibull library has been built, the Weibull probability plots can be reviewed for the failure modes of the current design prior to starting a new design. In addition to probability plots, the ideal Weibull library contains failure analysis and corrective analysis reports from a FRACAS (Failure Reporting, Analysis and Corrective Action System), root cause analyses, statements indicating how designs or processes could be changed to avoid a failure mode in the future, materials laboratory analyses, failure modes and effects analyses (FMEAs), fault tree analyses and all other related reports. The WeiBayes distribution, which requires only one parameter, can then use an entered slope value based on engineering experience and the Weibull probability plots from earlier designs. For small samples, defining the slope for the WeiBayes distribution can reduce uncertainty by factors of two or three.

Goodness of Fit

When data points cluster around a straight line, the selected distribution is good; however, the **goodness of fit** cannot be gauged easily when the samples are very small. Although there are several complex statistical measures for determining the most appropriate distribution for a set of data, Table 7-8 describes the simple measures that are generally used to evaluate Weibull probability plots.

Measure	Description
Correlation Coefficient (r)	Measures the strength of a linear relationship between two variables. The correlation coefficient is always a number between -1 and +1, depending on the slope. Because Weibull probability plots always have positive slopes, they will always have positive correlation coefficients. The closer r is to 1, the better the fit.

Table 7-8. Goodness of Fit Measures

Measure	Description
Correlation Coefficient Squared (r^2)	Measures the proportion of the variation in the data that is explained by the fit to the distribution. For example, if r^2 equals 0.93, it implies that 93 percent of the variation in the data is explained by the fit. The r^2 is also known as the **coefficient of determination**.
Critical Correlation Coefficient (CCC)	Measures the distribution of the correlation coefficient from ideal Weibull probability plots based upon simulations of median rank plotting positions. The 90 percent CCC is then compared to the correlation coefficient. If r is greater than the CCC, the fit is good fit. If r is smaller than the CCC, the data is significantly different from a Weibull distribution, and the fit is bad. CCC is considered the best statistical practice for determining how well the distribution fits the data set.
Critical Correlation Coefficient Squared (CCC^2)	Measures the proportion of variation for the regression fit method. A good fit occurs when r^2 is greater than or equal to CCC^2.

Table 7-8. Goodness of Fit Measures (Continued)

To compare the fit of one distribution with another, you generally need to have 20 or more data points in the sample, and you must know the P value for the correlation coefficient (r) for each distribution. The distribution with the highest P value is the best statistical choice.

Conducting Analyses and Interpreting Results

Many analysts automatically assume that the underlying distribution of life data is Weibull. However, the resulting Weibull probability plot should be reviewed to determine if this assumption is accurate. If the plotted data points fall along a straight line, the life data actually does come from a Weibull distribution. If, however, the plotted data points do not fall along a straight line, the bad fit may be related to either the physics of the failure, the quantity or quality of the data, or the selection of an inappropriate distribution.

Weibull Probability Plots with Steep Slopes

A steep plot often hides problems in the data. In such plots, all messages that are available from the data, such as curves, outliers and “doglegs” tend to disappear. What appears to be a good Weibull probability plot may have a poor fit. In such cases, the failure data should be carefully reviewed to ensure that it is appropriate.

Curved Data on Weibull Probability Plots

When the points graphed on a Weibull probability plot appear to curve, the selected distribution is considered a poor fit. The causes for this poor fit can be due to poor quality data or to the origin of the age scale not being appropriately located, as explained below:

- **Concave downward plots**. May reflect the manufacturer's failure to include the early failures that occurred during burn-in, stress screening or production acceptance. May also suggest the existence of a guaranteed failure-free period, where it is physically impossible for the failure mode to produce failures instantaneously or early in life. For example, a bearing cannot fail due to spalling or imbalance until bearing rotation has caused sufficient damage.
- **Concave upward plots**. Much more unusual and difficult to explain, may reflect either shelf life or shipping deterioration of spare parts or the mixture of failure modes.

When curved data appears on a Weibull probability plot and the cause is that the origin of the age scale is inappropriately located, a three-parameter Weibull distribution can be used to shift the scale by the value entered for the location parameter, **t-zero** (t_0). To estimate the t_0 value that is needed to straighten the Weibull probability plot, you can "eyeball" a curve through the two-parameter Weibull probability plot and use the point where it intersects the horizontal time scale.

Computerised three-parameter Weibull analysis iterates on the t_0 value until the correlation coefficient is maximised. The t_0 value will always be less than the first failure time and either be added to or subtracted from the failure values. Providing that the t_0 value is correct, the plot resulting from the three-Weibull distribution should follow a straight line. If shifting the origin does not correct the curved data on the Weibull probability plot, the lognormal distribution, which is not a member of the Weibull family, may be better suited for analysing this particular set of life data.

Weibull Probability Plots with Batch Problems

When plotted points show an unexpected concentration of failures, a **batch problem** is likely to have been caused by changes made to:

- Production or assembly processes.
- Maintenance or overhaul schedules.
- Increases in service usage.

Other indications that a batch problem exists are the presence of many late suspensions and the closeness of serial numbers of failed parts. The Weibull probability plot is likely to show a steep slope followed by a shallow slope (which may be followed by another steep slope if the period of time being analysed is long enough).

Weibull Probability Plots with Corners and Doglegs

Data collection is often less than perfect. When the Weibull probability plot shows sharp corners or **dogleg** bends, the cause is likely to be the mixture of multiple failure modes or failure sources in the data set. For example, many hydro-mechanical components show infant mortality from production and quality problems, followed by wear-out later in life as competing failure modes. The resulting Weibull probability plot is likely to have a shallow slope followed by a steep slope.

Known as a **classic bi-Weibull**, results for both the infant mortality and wear-out failure mechanisms are shown on one probability plot. Such bi-Weibull probability plots often occur in the analysis of warranty data. Although failure and suspension times are identified, the modes of failure often are not. In such cases, the life data should be examined to determine the different failure modes that exist, and the failures from modes other than the one being plotted should be tagged as suspensions.

In cases where the failure modes cannot be physically separated, Weibull software often provides a technique for separating failure modes statistically by analysing the data for competing risks. This means that the software searches the data set for two possible failure modes by evaluating ordered combinations. Separate Weibull probability plots are then generated for each failure mode identified, with the failures from a second failure mode (B) treated as suspensions for the first failure mode under consideration (A).

When warranty data suffers from mixed failure modes, the **Kaplan-Meier** model can be used to predict life based on the age of the units. Or, the **Crow-AMSAA** model can be used to predict life based on test or calendar time. The Kaplan-Meier and Crow-AMSAA models are further described in “Related Quantitative Models” on page 7-29.

When a data set mixes many failure modes for a system or component, the doglegs disappear, the slope tends toward 1 and the Weibull distribution has a better fit. However, using a Weibull probability plot with a mixture of many failure modes is the equivalent of assuming that the exponential distribution applies. The best procedure is to perform careful analysis of the root causes for failure and avoid mixing failure modes together. An effort to categorise the data into separate, more accurate failure modes should be made.

Weibull Probability Plots for System Models

System models combine tens or hundreds of failures modes. Although system models may be represented by lognormal or even binomial distributions, the Weibull distribution is used most often. The combination can be done by Monte Carlo simulation or by analytical methods. If the data cannot be segregated into individual failure modes or if early data is missing, the Crow-AMSAA or the Kaplan-Meier models may be applied to provide trending and failure forecasting.

System models are useful for predicting spare parts usage, availability, module returns to depot and maintainability support costs. System models are frequently updated with the latest Weibull probability plots. Past predictions may be compared with actual results to estimate the model uncertainties and fine tune the model.

For complex systems, early failure modes are likely to “cover” later failure modes. This means that unless early failure modes are eliminated, later failure modes are never identified. For this reason, complex systems that involve safety are exposed to accelerating testing well beyond their design life to uncover and eliminate any later failure modes that may be catastrophic. Because all problems are never found or solved, there are always unknown failure modes that will occur in the future.

Updating Weibull Probability Plots

If the fit of the line on a Weibull probability plot is not good, the initial analysis parameters should be altered and new probability plots generated until an acceptable fit is found. Once this occurs, results from the Weibull analysis can be used to accurately predict the trends in the data set and estimate future failures. As time goes on, Weibull probability plots can be based on larger failure samples. Although the Weibull parameters, β and η, will be different for each Weibull probability plot, they will gradually stabilise and approach the true Weibull. With the appropriate fit, however, the important engineering inferences about B-21 life and the failure forecasts do not change significantly as the sample size increases. With complete samples (no suspensions), β and η oscillate around the true unknown value.

Plots

Once Weibull software has fitted the selected distribution to the data, it can display the results graphically in the form of various plots:

- **Probability Plot**. A plot of the probability of failure over time based on a specific distribution. For life data analysis, these plots are usually called Weibull probability plots.
- **Reliability vs. Time Plot**. A plot of the reliability over time.
- **PDF Plot**. A plot of the probability density function (pdf).
- **Failure Rate vs. Time Plot**. A plot of the failure rate over time.
- **Contour Plot**. When MLE is the parameter estimation method, a graphical representation of the possible solutions to the likelihood ratio equation for comparing different data sets.

Calculations

Once the parameters for fitting a life distribution to a particular data set have been estimated, calculated results available from the Weibull analysis can include:

- **Reliability Over Time**. The probability that a product will operate successfully over a given period of time (or number of cycles) without any failures. For example, there is a 94 percent chance that the product will operate successfully after 7 months of operation.
- **Probability of Being in a Failed State at a Given Time**. If the component is non-repairable, then it is equivalent to the probability that a product is in a failed state at a particular point in time. Also known as **unreliability**, the probability of failure is 1.00 minus the reliability. For example, there is a 6 percent chance (1.00 - 0.94) that the above product will have failed after 7 months of operations (and a 94 percent chance that it will operate successfully).
- **Mean Life**. The average time that the products in the population are expected to operate before failure. This metric is referred to as the Mean Time to Failure (MTTF).
- **Failure Frequency**. The number of failures per unit time that can be expected to occur for the product.
- **Failure Rate**. The rate of occurrence of failures. This value is normally expressed as failures per million hours, but it can also be expressed as a FIT Rate (Failures in Time) or failures per billion hours. Failure rate is basically the anticipated number of times that an item fails in a specified period of time. For example, if a component has a failure rate of 2 failures per million hours, then it is anticipated that the component fails 2 times in a million hour time period.
- **Warranty Time**. The estimated time when the reliability will be equal to a specified goal. For example, the estimated time of operation is 9 months for a reliability of 96 percent.
- **B-Life**. The estimated time when the probability of failure will reach a specified point. For example, if 10 percent of the products are expected to fail by 3 years of operation, then the B-10 life is 3 years. (This is the equivalent to a warranty time of 3 years for a 90 percent reliability.)

Related Quantitative Models

Quantitative models related to the Weibull distribution include the Binomial, Poisson, Kaplan-Meier and Crow-AMSAA. Table 7-9 provides general descriptions of each of these models.

Model	Description
Binomial	Discovered in 1663 by John Newton, the simple formula for the binomial distribution requires only that the proportion that each of two outcomes is expected and the number of samplings or trials that are to be made are known. The binomial distribution applies to counted events that can have only two outcomes. It is used extensively in quality control and test planning, and it can be used in all discrete situations, such as yes/no, on/off, good/bad, pass/fail, etc.. An example of binomial distribution is coin tossing.
Poisson	Often used as an approximation for the binomial distribution when the values are within appropriate limits, the Poisson distribution is used to model rare events in a continuum. Requiring only one-parameter, the average or mean value, the Poisson distribution is based on counted events that are random in time. The Poisson distribution is used for nuclear emissions, accidents, spare parts prediction for low-demand components, etc.. An example of Poisson distribution is a lightning strike.
Kaplan-Meier	Long-used in the medical industry, the Kaplan-Meier survival function estimates the cumulative survival distribution **without making any distribution assumptions**. This method is non-parametric, meaning that it does not assume a distribution that uses parameters like the β and η in the Weibull distribution. The Kaplan-Meier estimate of the survivor curve looks like a stair pattern rather than a smooth curve. It works well for grouped, uncensored or right-censored data. Each time you have a failure, you multiply by a fraction. The fraction is determined by the total units at the start of the test, minus the number that are no longer on test after time *t* (failures and censored observations), divided by the number at risk of failure before *t*. A tie is taken into account in the fraction by the numerator. If you do not know what distribution the data comes from and do not want to assume a distribution, consider using the Kaplan-Meier method. It is the best practice for snapshot data and is often useful for tracking warranty data by age as well as for analysing inspection data.

Table 7-9. Related Quantitative Models

Model	Description
Crow-AMSAA	The Crow-AMSAA model is used to track the growth of reliability in a development programme as a function of time. Requiring less information than Weibull analysis, the Crow-AMSAA model indicates instantaneous failure rate changes by plotting a straight line on a log-log plot. Although may reliability growth models are available, the Crow-AMSAA model is considered the best practice because of the powerful statistical capabilities that Dr. Larry Crow added to J. T. Duane's postulate for learning curve modelling. The charts note trends that are used to forecast failures as a function of additional test time or calendar time, thereby making spares ordering and maintainability planning easier. This model can be used to track critical parameter rates such as warranty claims, outages, fires and accidents. It is also now being applied to tracking maintainability for fleets of repairable systems and ranking significant management events. It can handle mixed failure modes and well as missing portions of data.

Table 7-9. Related Quantitative Models (Continued)

Beyond Weibull Analysis

Other techniques related to Weibull analysis include risk analysis, probabilities analysis, optimal parts replacement and process reliability.

Risk Analysis

Risk analysis is a forecast of the number of failures expected to occur in a specified time period so that priorities can be set and resources for corrective action allocated. Also known as **expected quality forecasting**, risk analysis is extremely useful for determining the purchasing policy for spare parts and for identifying batch problems. In addition to life data, risk analysis requires:

- Age of the components in service.
- Usage rate per unit per a specified time period.
- Introduction rate of new units subject to the failure mode.
- Indication as to whether failed parts are replaced with zero time parts.

Keeping in mind that the failure forecast is dependent on the quantity and quality of the data, and that uncertainty increases as the time span for the forecast increases, the following can be predicted:

- Failures expected at the current time.

- Failures expected in the future when failed units are replaced.
- Failures expected in the future when failed units are not replaced.

Probabilistic Analysis

Probabilistic analysis reduces the chance of failure for a new design. To accomplish this, the probability of the applied stress being larger than the strength for each load application is measured. Estimates of the distribution of stress and the distribution of load are used to estimate the probability of failure within the specified confidence level. This technique also applies to life distribution versus usage distribution.

Optimal Part Replacement Intervals

A replacement interval indicates how long equipment remains in service before it is retired and new equipment substituted. The optimum replacement interval is the service time associated with the smallest cost per unit. If a part wears out and the cost of an unplanned failure is greater than the cost of the planned replacement, an optimal replacement interval exits. Replacing the part any sooner than this interval results in replacement costs that are too high. Replacing the part later than this interval increases the odds of a breakdown, which generates failures costs that are too high. The optimal interval is the age with the minimum ratio of the mean cost to the mean time to failure.

Process Reliability

Process reliability is defined as the maximum reliability point where the data indicates that a mechanical or production process is under control. Analysing existing processes can uncover inefficiencies or poor design techniques that could be improved. These improvements could result in more efficient manufacturing, increased reliability and overall cost reduction.

The Barringer process, developed by Paul Barringer, is a reliability technique for identifying problems that have significant opportunities for improvements. This technique uses failure rate distribution for analysis and presents important facts as an engineering graphic, which is useful for solving business problems. This analysis provides the evidence needed for root cause analysis for the process.

Parameters to be defined for the production line represent the demonstrated capability (volume, wattage, etc.) of the process as it is plotted among the higher production output values, especially those consistently close to a straight line on the probability plot. It shows normal production with respect to time when all is functioning properly. Parameters are also entered for maximum production capacity of the factory under ideal operation and control (design capacity). Such values are required for calculating efficiency and utilisation losses, and minimising costs and maximising product integrity.

8. Markov Modelling

Introduction

The reliability models explored in previous chapters assume **independence** between system components, meaning that the failure or repair of a component is not affected by what is going on with any other component. Consequently, the system failure state is expressed as a combination of component failures. For example, in a series system, if any component fails, then the system fails; in a parallel system, if all components fail, then the system fails. For these models, it is important to know the set of failed components; however, the order in which the components failed is not significant.

For complex systems that are modelled using Reliability Block Diagrams (RBDs) or Fault Trees, there may exist a set of component failure combinations that lead to a failed system state. In most cases, it is assumed that these component failures are independent, meaning that the failure of one component does not affect the failure times or behaviours of any other component. However, in shared load systems, the failure of a component can increase the load on other components, thereby increasing the failure rate of the system. In addition, a common cause failure, whose occurrence can lead to the failure of one or more components in the system, can arise. Examples of common cause failures include the loss of a common power supply, earthquakes, extreme weather conditions, etc..

Although the previous chapters provide formulas to compute such reliability-related measures as reliability, availability and MTTF for standby systems, they do not provide methods for deriving these equations. For example, in a system with cold standby components, components cannot fail in the standby mode, but they can fail when they are in operation. Thus, the failure rate (or failure time distribution) in these two modes are different. The time to keep the standby component in operation depends on the failure time of the active unit. This means that component failures depend on the failure times of other components. In such cases, components cannot be assumed to be statistically independent. In addition to considering the set of component failure states, the order in which components fail must be considered.

Also, the previous chapters assume that all components are non-repairable. The equations given for system availability are based on the availability of individual components. The equations not only assume that component failure times are independent, but they also assume that the component repair times are independent. This means that the repair time of a component is independent of the states of other system components. This may not be true if a common-repair facility (group of repair technicians) exists for a set of components because a failed component may have to wait for a repair crew, who is busy repairing some other failed component.

In most cases, it is assumed that a **good** component operates continuously, even during system failure. This assumption is generally valid. However, when such independence between component failures and/or repairs should not be assumed, stochastic processes (rather than RBDs, fault trees or other combinatorial models) should be used. And, even when failure and repair times of all components are independent, cases exist where stochastic processes are necessary.

For example, exact reliability evaluation of a parallel system with repairable components cannot be performed using combinatorial models because the reliability of this system depends not only on the set of component states at a specified time but also on the history of component failure and repair events. Most combinatorial models do not even provide formulas for approximating the reliability of a repairable system. Moreover, combinatorial models cannot directly calculate the availability of a single component because all of the possible sequences of failures and the repairs of that component must be considered.

Stochastic processes can handle all of these complex and sequence-dependent situations. Stochastic processes can also accurately and completely model such dynamic system behaviours as:

- Repairs.
- Shocks (shared loads and induced failures).
- Common cause and dependent failures.
- Sequence/state-dependent failure rates (standby components).
- Variable configurations.
- Complex error handling and recovery mechanisms (common pool of repair technicians).
- Phased mission requirements.

Because of their flexibility, generalized stochastic processes can be used to specify various complex system behaviours. Thus, they are widely used to assess system reliability and related characteristics in mission critical systems and research-oriented projects. However, their complexity makes them much harder to understand than combinatorial models. Consequently, generalized stochastic processes are not used in all industries.

Stochastic Processes

The **stochastic process** has a number of states that describe the behaviour of a set of random variables. The behaviour of the stochastic process varies with respect to an index. In reliability engineering, the index is generally **system time**. This means that the stochastic process is used to describe the dynamics of a system with respect to time.

State space is the set of all possible states of a process, and **index space** is a set of all possible index values. At a particular time (index value), a system will be in one of its possible states. In each state, a set of events can occur. The occurrence distribution of each state depends on the history of the system (all previous events and state transition times).

In reliability engineering, the state space is generally discrete. For example, a system might have two states: good and failed. There are, however, applications in which state space can be continuous. Examples include the water level in a tank (where tank failure characteristics depend on the water level), the load on a shaft, the waiting time for repair, etc.. If the state space is discrete, then the process is called a **chain**.

Similarly, the state index can be discrete or continuous. In most reliability engineering applications, the state index (time scale) is continuous, which means that component failure and repair times are random variables. However, cases exist where the state index is discrete. Examples include time-slotted (synchronous) communication protocol, shifts in equipment operation, etc..

Given a continuous-time process, it is often useful to embed a discrete time process by considering only those points at which certain events (like state changes) happen within the process. In such an embedded process, the discrete points are generally not equally spaced in real time. However, such details are not included in this document.

Markov Processes

Markov processes are a special class of stochastic processes that uniquely determine the future behaviour of the process by its present state. This means that the distributions of events (rates of occurrences) are independent of the history of the system. Furthermore, the transition rates are independent of the time at which the system arrived at the present state. Thus, the basic assumption of the Markov process is that the behaviour of the system in each state is **memoryless**. The transition from the current state of the system is determined only by the present state and not by the previous state or the time at which it reached the present state. Before a transition occurs, the time spent in each state follows an exponential distribution.

In reliability engineering analysis, these conditions are satisfied if all events (failures, repairs, switch-overs, etc.) in each state occur with constant occurrence rates (failure rate, repair rate, switch-over rate, etc.). Because the basic behaviour of the process is time-independent, these processes are also called **Time Homogeneous Markov processes** or simply **Homogeneous Markov processes**. However, failure and repair rates of a component can depend upon the current state. Because of constant transition rate restriction, the Homogenous Markov process should not be used to model the behaviour of systems that are subjected to component wear-out characteristics. General stochastic processes should be used instead.

In most cases, special classes of the stochastic processes that are generalizations to the Homogenous Markov processes are used. The corresponding models include:

- **Semi-Markov models**. Although very similar to Homogeneous Markov models, the transition times and the probabilities (distributions) depend on the time at which the system reached the present state. This means that the transition rates in a particular state depend on the time already spent in that state, but that they do not depend on the path by which the present state was reached. Thus, transition distributions can be non-exponential.
- **Non-homogeneous models**. Although very similar to Homogeneous Markov models, the transition times depend on the global system time rather than on the time at which the system reached the current state.

NOTE A non-exponential distribution (such as normal or Weibull) can be approximated as a set of exponential distributions. In this case, even the distributions are non-exponential, and the homogeneous Markov models discussed in this chapter can be used. However, the results are approximate. Further information about this topic is beyond the scope of this document.

As noted earlier, Markov processes are classified based on state space and index space characteristics. Table 8-1 lists the characteristics of the four types of Markov processes and their corresponding model names.

State Space	Index Space	Common Model Name
Discrete	Discrete	Discrete Time Markov Chains
Discrete	Continuous	Continuous Time Markov Chains
Continuous	Discrete	Continuous State, Discrete Time Markov Processes
Continuous	Continuous	Continuous State, Continuous Time Markov Processes

Table 8-1. Markov Model Types

In most reliability engineering applications, the state space is discrete and the index space (time scale) is continuous. Thus, this chapter focuses on Discrete State Space, Continuous Index Space Homogenous Markov processes. Because the term **Markov chain** is generally used whenever state space is discrete, the above table refers to these models as **Continuous Time Markov Chains**. In many text books, these models are simply called **Continuous Markov Models**.

In addition to being an important concept in reliability analysis, Markov models find wide applications in other areas, including:

- Artificial music.
- Spread of epidemics.
- Traffic on highways.
- Occurrence of accidents.
- Growth and decay of living organisms.
- Emission of particles from radioactive sources.
- Number of people waiting in a line (queue).
- Arrival of telephone calls at a particular telephone exchange.

NOTE Markov models are included in this guide because they are the only accurate method for modelling complex situations. Although the complex proofs related to these models have not been included, they can be found in many reliability engineering handbooks and related publications.

Limitations of Homogeneous Markov Models

Homogeneous Markov models are limited by two major assumptions:

- The transitions (probabilities) of changing from one state to another are assumed to remain constant. Thus, a Markov model is used only when a constant failure rate and repair rate assumption is justified.
- The transition probabilities are determined only by the present state and not by the system's history. This means future states of the system are assumed to be independent of all but the current state of the system.

State Transition Diagrams

Markov state transition diagrams are graphical representations of system states and the possible transitions between these states. They provide a visual aid to help understand Markov models. A state transition diagram can graphically represent all:

- System states and their initial conditions.
- Transitions between system states and corresponding transition rates.

In some cases, analysts represent continuous Markov models in terms of their discrete equivalents. The transition rates are replaced with equivalent transition probabilities considering that the state transition time is very small (Δt). This leads to a situation where the system can remain in the current state after time Δt with some probability. Thus, in this case, the probabilities of remaining in the existing state (transition rates) are also shown in the diagram.

A given system configuration is considered, at any instant in time, to exist in one of several possible states. In a single diagram, all of the operational and failure states of the system and the possible transitions between them are shown. The state transition diagram displays system states as individual nodes and transitions as either arrows or arcs.

An Example of a Single-component System

Consider a non-repairable component with a constant failure rate (λ). The component has two states: good and failed. The states of the system are equivalent to the states of the component. Initially, assume that the component is good. The system reaches the failed state when the component fails. Once the system reaches a failed state, it will remain there forever because no events occur in the failed state. The state transition diagram of this single-component system can be represented as shown in Figure 8-1.

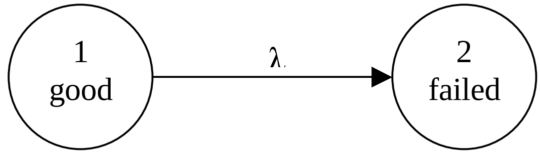


Figure 8-1. Single-component, Non-repairable System

NOTE Because state transition diagrams are more visual than mathematical matrix representations, they are much easier to interpret. However, for large systems, they can become unmanageable and difficult to analyse.

A state transition diagram is similar to a flow diagram representation that would be used in system analysis. It graphically represents the various system states and the rates associated with the transitions between the system states. Because a direction is associated with a transition, a state transition diagram can be viewed as a directed graph.

Construction of State Transition Diagram

The basic steps in constructing state transition diagrams are:

1. Define the failure criteria of the system.
2. Enumerate all of the possible states of the system and classify them into good or failed states.
3. Determine the transition rates between various states and draw the state transition diagram.

Example of a Two-component System

Assume that there are two components in a system (labelled A and B) and that these components are in parallel. Thus, the system will function properly as long as at least one of the two components is good. Also assume that λ_1 and λ_2 are the failure rates of component A and component B respectively. Therefore, the system has a total of four states (labelled $\mathbf{S_1}$, $\mathbf{S_2}$, $\mathbf{S_3}$ and $\mathbf{S_4}$):

- $\mathbf{S_1}$. Component A is good, and Component B is good. (The system is good.)
- $\mathbf{S_2}$. Component A is good, but Component B has failed. (The system is good.)
- $\mathbf{S_3}$. Component B is good, but Component A has failed. (The system is good).
- $\mathbf{S_4}$. Component B has failed, and Component A has failed. (The system has failed).

Of the four system states possible, only one, $\mathbf{S_4}$, is a failed state. The state transition diagram of this two-component system is shown in Figure 8-2.

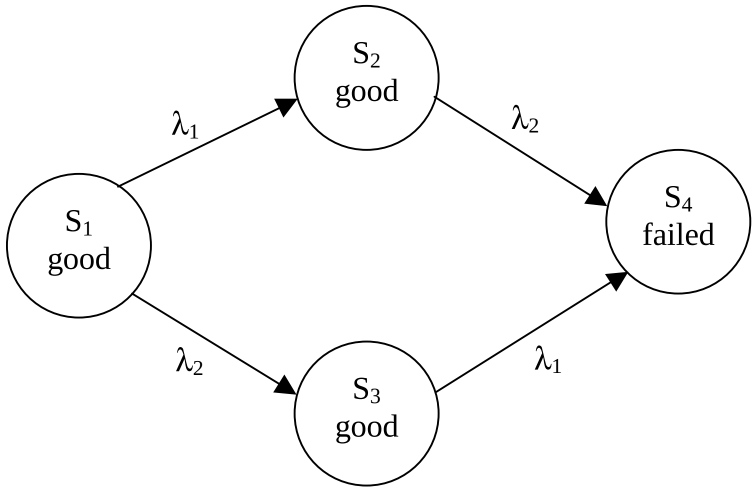


Figure 8-2. Two-component, Non-repairable System

NOTE Because the two components in this example are assumed to be independent and non-repairable, this problem can be solved using a combinatorial model such as an RBD.

Generally, the arrow representing the initial state is omitted from the diagram because:

- The initial state is generally where all components are in the good condition. In this example, $\mathbf{S_1}$ is the initial state.
- Multiple initial states can exist, such as when there are multiple phases of mission. In these cases, all initial states are assigned probabilities that are then represented by an initial state probability vector.

Now, assume that the components can be repaired as long as there is no system failure. This means that failed components can be repaired in state $\mathbf{S_2}$ and state $\mathbf{S_3}$. Also assume that μ_1 and μ_1 are the repair rates of component A and component B respectively. Figure 8-3 shows a state transition diagram that can represent this system. This problem cannot be solved using combinatorial models.

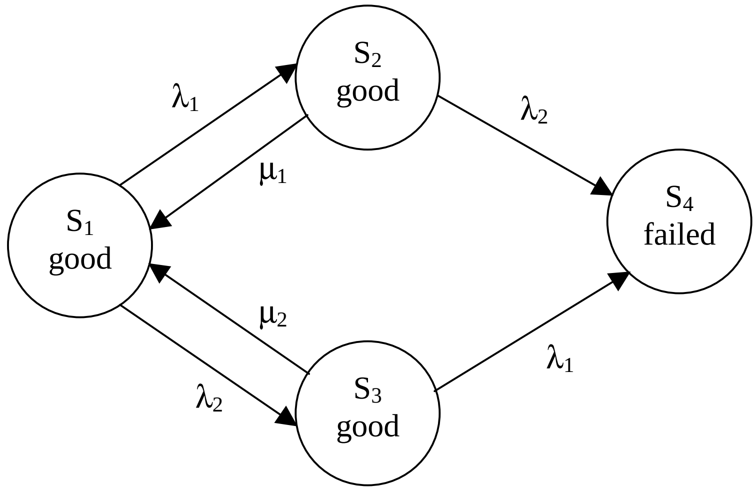


Figure 8-3. Two-component Non-repairable System with Repairable Components

In some text books, the state transition diagrams of continuous models are represented using their discrete equivalents. For example, if λ is the transition rate from state *i* to state *j*, then the probability of occurrence of that transition within Δt (a small increment of t, is approximately equivalent to $\lambda\Delta t$. If there are multiple events that can occur in that state and their summation is λ, then $\lambda\Delta t$ is equivalent to the probability of transition within Δt. This shows that $1 - \lambda\Delta t$ is the probability of no transition occurring within Δt. Figure 8-4 shows this state transition diagram.

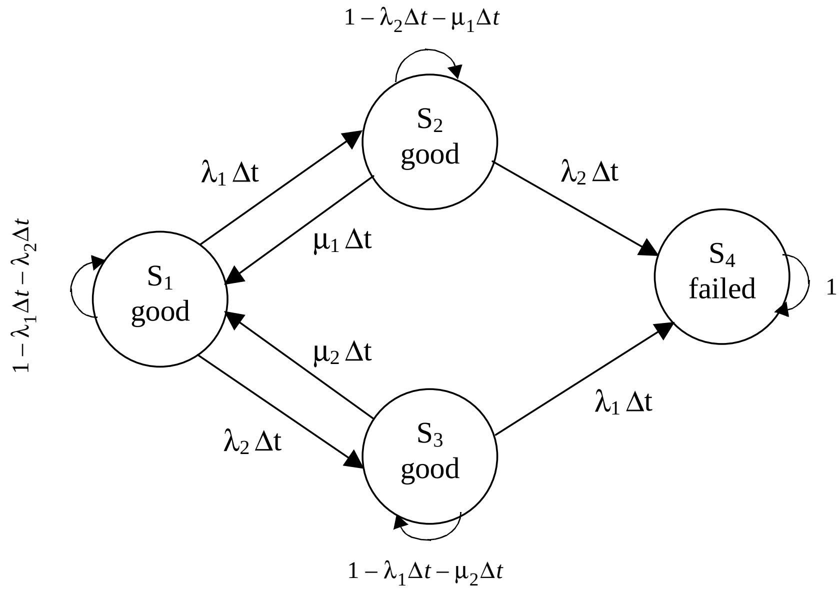


Figure 8-4. Two-component Non-repairable System with Comparable Components (in Terms of Transition Probabilities)

In all of the examples presented so far, it is assumed that the system state can be expressed as combinations of component states. However, in some cases, the order of the events (failures, for example) are important. Suppose that each of these states has a different effect on system reliability and fail-safety. The probability of component A failing before component B fails and the probability of component B failing before component A fails must then be known. For this example, five system states (labelled $\mathbf{S_1}$, $\mathbf{S_2}$, $\mathbf{S_3}$, $\mathbf{S_4}$ and $\mathbf{S_5}$) exist.

- $\mathbf{S_1}$. Component A is good, and Component B is good. (The system is good.)
- $\mathbf{S_2}$. Component A is good, but Component B has failed. (The system is good.)
- $\mathbf{S_3}$. Component B is good, but Component A has failed. (The system is good.)
- $\mathbf{S_4}$. Component A has failed, and then Component B has subsequently failed. (The system has failed in mode 1.)
- $\mathbf{S_5}$. Component B has failed, and then Component A has subsequently failed. (The system has failed in mode 2.)

Figure 8-5 shows a state transition diagram of this system without considering repairs. Problems considering sequence cannot be solved using combinatorial models.

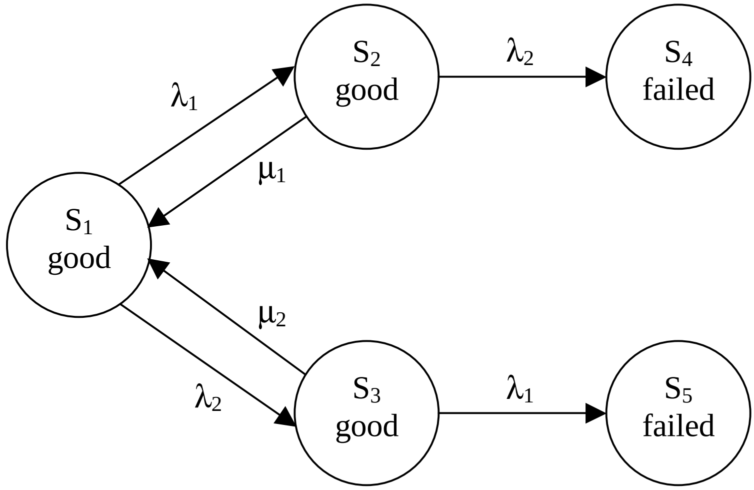


Figure 8-5. Two-component System, Sequence-dependent Failure Modes

The previous discussion shows that finding all of the system failure states may not always be simple. The following approach to constructing a state transition diagram is recommended:

1. Understand the system and the behaviours that are going to be modelled, drawing each system state in the state transition diagram.
2. Find the initial state of the system (which is generally where all components are in a good condition) and then classify each state (good, failed, etc.).
3. Determine all events that can occur in each state (component failures, repairs, external events such as common cause failures, etc.).
4. For each event that can occur in a state:
    a. Find the state that corresponds to the event's occurrence. If this state already appears in the state transition diagram, then draw a transition from the current (initial) state to the succeeding (next) state. Otherwise, create a new state and then draw the transition.
    b. Set the rate for this transition, which is the event occurrence rate (such as a failure rate or repair rate).
    c. Classify the state (good, failed, etc.).
5. Repeat steps 3 and 4 for each state. The state transition diagram is completed when all states are visited and there are no states left to create.

After constructing the state transition diagram, adding the following information can be useful.

- Initial condition. Generally the initial condition (state probability) is 1 for the perfect state of the system (which is where this example starts), and 0 for all other states.
- Capacity. The throughput or reward of the system. For additional information, refer to “Expected Capacity or Reward” on page 8-24.

The following information is also useful for constructing state transition diagrams:

- Results from Failure Mode and Effects Analysis (FMEA) can help to identify all possible failures of a component. For additional information, refer to “Failure Mode and Effects Analysis” on page 6-1.
- An **absorbing state** is a state in which no events can occur. Once a system reaches an absorbing state, it cannot visit any other state. Therefore, there are no outward transitions from this state. Generally, all absorbing states are failed states.
- Between one state and another, there can be only one transition. If multiple events make this transition, all transition rates between these two states should be added together and then this value assigned to the transition.
- Similar states are generally merged to reduce the state space and keep the state transition diagrams neat and readable. Any two states having the same transitions going out from them are treated as if they had the same set of succeeding states and corresponding transitions rates.
- All failed and absorbing states can be merged to a single state if there is no interest in analysing individual failures, i.e., when all failed states are of the same type.
- If the sequence in which failures occur is important to identifying the type of state (good, failed, etc.), states should not be merged based on the combination of component failures. Otherwise, states can be merged on this basis.

Diagram Simplification

To limit state transition diagrams to a reasonable size without a major sacrifice in accuracy, longer paths between the initial operational state and the system failure state may be truncated. For example, when the number of faults exceeds five, it may be desirable to truncate the paths. However, when truncation is used, the effect of this approximation in the final model must be examined.

Transition Rates

In reliability models, state transition rates are typically obtained from failure rates and repair rates. The failure rates of components can be calculated using prediction models. These calculations should consider the base failure rate as well as the appropriate environmental stress factors.

After examining the operational equipment associated with each state in the state transition diagram, corresponding failure rates can be calculated using failure rate handbooks available for commercial or military products (such as Telcordia [formerly Bellcore] and MIL-HDBK-217 respectively). Because these handbooks are so well respected and widely used, numerous software programs that calculate failure rates based on them are available.

Where several states can be reached from a single state, the equipment failure rate is apportioned among the possible transitions as indicated by the FMEA. For additional information, refer to “Failure Mode and Effects Analysis” on page 6-1.

Maintenance-related state transitions are calculated from repair times. Calculations for repair time can be based on generic maintenance procedures or accepted standards (such as MIL-HDBK-472 Procedures 2, 5A and 5B). The most common maintainability calculation is MTTR (Mean Time To Repair), which is basically the average time required to perform repairs or maintenance on a system.

Reliability Characteristics

The various reliability characteristics that can be calculated using Markov models are described in this section.

Reliability Characteristics of a Non-repairable System

The reliability characteristics of a non-repairable system include:

- Transient/Time-dependent Indices:
  - Reliability, $R(t)$.
  - Unreliability, $F(t)$.
  - Individual state probabilities, $P_i(t)$.
  - Time-specific failure frequency, $v(t)$.
  - Frequency of visits to a particular state at time t, $v_i(t)$.
  - Time-specific capacity/reward, $C(t)$ (see “Expected Capacity or Reward” on page 8-24).
- Steady-state and Asymptotic Indices:

- Expected time spent in a particular state before reaching a failed (absorbing) state.
- MTTFF (Mean Time To First Failure) or MTTF (Mean Time to Failure).

Reliability Characteristics of a Repairable System

The reliability characteristics of a repairable system include:

- Transient/Time-dependent Indices:
  - Reliability, $R(t)$.
  - Time-specific availability, $A(t)$.
  - Time-specific unavailability, $U(t)$.
  - Time-specific individual state probabilities, $P_i(t)$.
  - Time-specific failure frequency, $v(t)$.
  - Frequency of visits to a particular state at time t , $v_i(t)$.
  - Time-specific capacity/reward, $C(t)$.
- Time-independent Indices:
  - Steady-state Availability, A .
  - Steady-state Failure Frequency, v .
  - MTTF (Mean Time to First Failure).
  - MTBF (Mean Time Between Failures).
  - MTTR (Mean Time to Repair).

Markov Analysis

This section describes the Markov analysis for a single-component repairable system.

Availability and State Probabilities

Assume that the system has only two states: state 1 is good, and state 2 is failed. Initially, the system is in a good state. The system reaches a failed state immediately after the single component fails. Repair of the component will start immediately after failure. Let λ and μ be the failure and repair rates of the single component. Figure 8-6 shows the state transition diagram for this system.

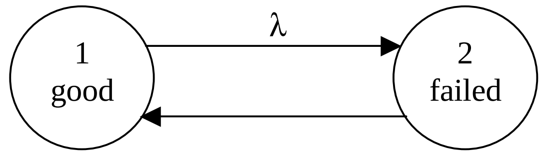


Figure 8-6. Single-component Repairable System

The information in the state transition diagram above can be represented in matrix form:

Equations

$$T = \begin{bmatrix} 0 & \lambda \\ \mu & 0 \end{bmatrix} \quad (8.1)$$

The matrix T is called a state transition rate matrix. The elements t_{ij} (row i and column j) represent the transition rate from state i to state j.

Note: The matrix T is a square matrix of order $n \times n$ (where n is the total number of states), and all elements in the diagonal are zeros. In this example, n = 2.

Let $P_i(t)$ be the probability of state i at time t. Alternatively, $P_i(t)$ is the probability that the system would be found in state i at time t. From the initial condition, it is known that the system is initially in state 1. Therefore, $P_1(0) = 1$ and $P_2(0) = 0$.

The initial state vector can also be represented in the matrix (vector) form:

$$\begin{aligned} P(0) &= [P_1(0), P_2(0)] \\ &= [1, 0] \quad (8.2) \end{aligned}$$

Where:

$P(0)$ = The initial state vector, which is a row vector.

According to the definition, $P_1(t + \Delta t)$ is the probability of state i at time $t + \Delta t$. Let Δt be very small, such that probability of occurrence of more than one event within this time interval (Δt) is negligible. Therefore, $P_1(t + \Delta t)$ can be expressed as the sum of the following two mutually exclusive events.

- E_1. The system is in state 1 at time t and continues to remain in state 1 throughout the interval Δt.
- E_2. The system is in state 2 at time t and it transitions to state 1 during the interval Δt.

Therefore:

$$P_1(t+\Delta t) = Pr\{E_1\} + Pr\{E_2\} \quad \text{(8.3)}$$

Where:

$Pr\{E_i\}$ = The probability of event E_i.

According to the definition of the transition rates, if Δt is very small, the probability that the system transitions to state 2 from state 1 within Δt is $\lambda \Delta t$. Using this same logic for the transition from state 2 to state 1 results in:

$$Pr\{E_1\} = P_1(t) \cdot [1 - \lambda \Delta t]$$
$$Pr\{E_2\} = P_2(t) \cdot \lambda \Delta t \quad \text{(8.4)}$$

Therefore:

$$P_1(t+\Delta t) = P_1(t) \cdot [1 - \lambda \Delta t] + P_2(t) \cdot \mu \Delta t \quad \text{(8.5)}$$

Similarly, $P_2(t+\Delta t)$ can be expressed as:

$$P_2(t+\Delta t) = P_2(t) \cdot \lambda \Delta t + P_2(t) \cdot [1 - \mu \Delta t] \quad \text{(8.6)}$$

These equations for $P_i(t+\Delta t)$ are known as **Chapman-Kolmogorov difference equations**.

Rearranging equations (8.5) and (8.6) results in:

$$\frac{P_1(t+\Delta t) - P_1(t)}{\Delta t} = -\lambda \cdot P_1(t) + \mu \cdot P_2(t)$$
$$\frac{P_2(t+\Delta t) - P_2(t)}{\Delta t} = \lambda \cdot P_1(t) - \mu \cdot P_2 t \quad \text{(8.7)}$$

If $\Delta t \to 0$, then equation (8.7) can be represented in the form of differential equations:

$$P'_1(t) = -\lambda \cdot P_1(t) + \mu \cdot P_2(t)$$
$$P'_2(t) = \lambda \cdot P_1(t) - \mu \cdot P_2(t) \quad \text{(8.8)}$$

Equation (8.8) can be represented in matrix form:

$$[P'_1(t), P'_2(t)] = [P_1(t), P_2(t)] \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix} \quad \text{(8.9)}$$

In a compact form, the equation is:

$$P'(t) = P(t) \cdot Q \quad \text{(8.10)}$$

Where $P'(t)$ and $P(t)$ are the row vectors.

The matrix Q is known as an infinitesimal generator matrix of the Continuous Time Markov Chain (CTMC). It can be obtained directly from the transition matrix, T. Let q_{ij} and t_{ij} be elements of row i and column j of matrix Q and T respectively.

Then:

$$q_{ij} = t_{ij} \quad i \neq j$$

$$= -\sum_{j=1}^{n} t_{ij} \quad i \neq j \quad \text{(8.11)}$$

Equation (8.10) is known as a **Kolmogorov (Forward) differential equation**. The probability vector $P(t)$ can be solved using the initial state probability vector $P(0)$ and equation (8.10).

Similarly, the **Kolmogorov (Backward) differential equation** can be used to show the relationship between state probabilities. Equation (8.9) can be written as:

$$\begin{bmatrix} P'_1(t) \\ P'_2(t) \end{bmatrix} = \begin{bmatrix} -\lambda & \mu \\ \lambda & -\mu \end{bmatrix} \begin{bmatrix} P_1(t) \\ P_2(t) \end{bmatrix} \quad \text{(8.12)}$$

In a compact form, the equation is:

$$P'(t) = Q^T \cdot P(t) = B \cdot P(t) \quad \text{(8.13)}$$

Where $P'(t)$ and $P(t)$ are the column vectors.

In some reference books, the symbol Q is used in the place of Q^T. Therefore, to avoid confusion, B is used to represent Q^T. The matrix B is also known as the coefficient matrix of the Markov differential equations.

In this chapter, the Kolmogorov backward differential equations are shown as in equation (8.13). There are various methods to solve this equation. This section presents the procedure to compute the probabilities analytically.

Taking a Laplace transform to equation (8.8) results in:

$$sP_1(s) - P_1(0) = -\lambda \cdot P_1(s) + \mu \cdot P_2(s)$$

$$sP_2(s) - P_2(0) = \lambda \cdot P_1(s) - \mu \cdot P_2(s) \quad \text{(8.14)}$$

Where:

$P_i(s)$ = The Laplace transform of $P_i(t) = \int_0^{\infty} P_i(t) e^{-st} dt$.

After solving equation (8.14), the following equations can be obtained:

$$P_1(s) = \frac{s + \mu}{s(s + \lambda + \mu)} \quad \text{(8.15)}$$

$$P_2(s) = \frac{\lambda}{s(s + \lambda + \mu)} \quad \text{(8.16)}$$

$P_i(t)$ can be obtained after taking an inverse Laplace transform of $P_i(s)$.

Therefore:

$$P_1(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} exp\{-(\lambda+\mu)t\} \qquad (8.17)$$

$$P_2(t) = \frac{\lambda}{\lambda+\mu} - \frac{\lambda}{\lambda+\mu} exp\{-(\lambda+\mu)t\} \qquad (8.18)$$

Because the system is operational only in state 1, the availability of the system is $A(t) = P_1(t)$. Similarly, the reliability of the system, $R(t)$, can be calculated as indicated in the next section.

Reliability

Reliability is the probability that the system operates (is in a good state) continuously over the specified period. Therefore, it can be viewed as the probability that the system is in a good state and that there are no system repairs (or system failures). This means, once the system reaches a failed state, it cannot be repaired. Hence, to compute system reliability, the transitions that correspond to repairs in a failed state need to be removed.

In the single-component example, state 2 is a failed state. To compute reliability, repairs should not be considered in this state. Therefore, the transition from state 2 to state 1 will not be there (or the transition rate for it will be zero). Figure 8-7 shows the resulting state transition diagram.

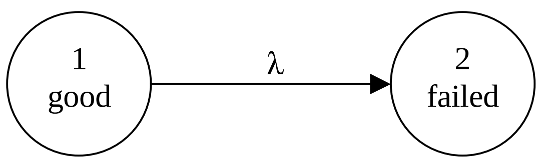


Figure 8-7. Single-component System Without System Repair

Hence, the matrices, T, Q, B and C, are:

Equations

$$T = \begin{bmatrix} 0 & \lambda \\ 0 & 0 \end{bmatrix} \qquad (8.19)$$

$$Q = \begin{bmatrix} -\lambda & \lambda \\ 0 & 0 \end{bmatrix} \qquad (8.20)$$

$$B = Q^T = \begin{bmatrix} -\lambda & 0 \\ \lambda & 0 \end{bmatrix} \qquad (8.21)$$

$$C = s \cdot I - B = \begin{bmatrix} s+\lambda & 0 \\ -\lambda & s \end{bmatrix} \qquad (8.22)$$

Therefore:

$$P_1(s) = \frac{\Delta_1}{\Delta} = \frac{s}{s(s+\lambda)} = \frac{1}{s+\lambda} \quad (8.23)$$

$$P_2(s) = \frac{\Delta_2}{\Delta} = \frac{\lambda}{s(s+\lambda)} = \frac{1}{s} - \frac{1}{s+\lambda} \quad (8.24)$$

Thus, system reliability, $R(t)$, is:

$$R(t) = P_1(t) = L^{-1}[P_1(s)] = e^{-\lambda t} \quad (8.25)$$

The above procedure shows that Markov analysis is difficult in comparison with the RBD method and fault tree analysis. The above procedure is used to find analytical solutions. However, the numerical solutions of Markov chains are also relatively easy to find. It should be noted that Markov models are the only correct models for highly dependable complex systems.

MTTF

Mean Time to Failure (MTTF) of a system can be obtained by integrating the system reliability $R(t)$:

Equations

$$MTTF = \int_0^{\infty} R(t)dt \quad (8.26)$$

If the system reliability expression is in the following form:

$$R(t) = \sum_{i=1}^{m} a_i e^{-b_i t} \quad (8.27)$$

Then, MTTF of the system is:

$$MTTF = \sum_{i=1}^{m} \frac{a_i}{b_i} \quad (8.28)$$

For example, the reliability of the two-unit parallel system is:

$$R(t) = 2e^{-\lambda t} - e^{-2\lambda t} \quad (8.29)$$

Hence, MTTF is:

$$MTTF = \frac{2}{\lambda} - \frac{1}{2\lambda} = \frac{3}{2\lambda} \quad (8.30)$$

To find MTTF using equation (8.26), first, system reliability must be computed as already shown. In general, computing $R(t)$ is difficult. However, this section provides an easy method for computing MTTF.

To calculate MTTF, it is necessary to classify the states. This section presents only the details that are required to analyse the MTTF and other commonly used reliability characteristics. A Markov process is called an **Ergodic Markov process** if it is homogeneous (time-independent) and the final value of the probability (probability at infinity) of a state is independent of the initial state.

This is possible only when there are no absorbing states. In reliability analysis, this means that system is repairable. Therefore, a non-trivial (non-zero) solution for system steady-state availability is possible only when there are no absorbing states in the system (the system is repairable). However, if the system is non-repairable (at least for some type of failures), then there exist absorbing as well as non-absorbing (transient) states. Further, as in case of reliability analysis, we should consider all failed states as absorbing states to compute system MTTF.

Consider that there are r absorbing states (failed states) in the system and $(n-r)$ non-absorbing (transient) states in the system. For example, consider the system in Figure 8-3. The corresponding matrices, T and $Q = B^T$ are as follows:

$$T = \begin{bmatrix} 0 & \lambda_1 & \lambda_2 & 0 \\ 0 & 0 & 0 & \lambda_2 \\ 0 & 0 & 0 & \lambda_1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{.......(8.31)}$$

$$Q = \left[\begin{array}{ccc:c} -(\lambda_1+\lambda_2) & \lambda_1 & \lambda_2 & 0 \\ 0 & -\lambda_2 & 0 & \lambda_2 \\ 0 & 0 & -\lambda_1 & \lambda_1 \\ \hdashline 0 & 0 & 0 & 0 \end{array}\right] \quad \text{.......(8.32)}$$

For this example, state 4 is absorbing state; hence, $r = 1$. It should be noted that all elements in a row of Q that correspond to an absorbing state are 0s. We can partition matrix Q. (Although this partition is not necessary to compute MTTF, it is helpful for finding other system characteristics.)

$$Q = \begin{bmatrix} Q_t & R_t \\ 0 & 0 \end{bmatrix} \quad \text{.......(8.33)}$$

Where:

Q_t = The square matrix of size $(n-r)$. It is called the truncated transition matrix associated with T.

For this example:

$$Q_t = \begin{bmatrix} -(\lambda_1+\lambda_2) & \lambda_1 & \lambda_2 \\ 0 & -\lambda_2 & 0 \\ 0 & 0 & -\lambda_1 \end{bmatrix} \quad \text{.......(8.34)}$$

$$S_t = \begin{bmatrix} 0 \\ \lambda_2 \\ \lambda_1 \end{bmatrix} \quad \text{.......(8.35)}$$

Find the matrix M, which is the inverse of $-Q_t$:

$$M = -Q_t^{-1} = \begin{bmatrix} (\lambda_1+\lambda_2) & -\lambda_1 & -\lambda_2 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_1 \end{bmatrix}^{-1}$$

$$= \frac{1}{\lambda_1\lambda_2(\lambda_1+\lambda_2)} \begin{bmatrix} \lambda_1\lambda_2 & \lambda_1^2 & \lambda_2^2 \\ 0 & \lambda_1(\lambda_1+\lambda_2) & 0 \\ 0 & 0 & \lambda_2(\lambda_1+\lambda_2) \end{bmatrix} \quad (8.36)$$

It should be noted that the element m_{ij} of the matrix represents the amount of time spent in state j before reaching an absorbing state when the system is initially in state i. Therefore, when the system is initially in state 1, the sum of all the elements of row 1 is the MTTF of the system.

Therefore, for this system:

$$MTTF = \frac{\lambda_1\lambda_2 + \lambda_1^2 + \lambda_2^2}{\lambda_1\lambda_2(\lambda_1+\lambda_2)}$$
$$= \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1+\lambda_2} \quad (8.37)$$

It should be noted that if MTTF is finite (if there are some absorbing states), then MTTF can also be found directly using $-Q^{-1}$ (if $-Q^{-1}$ exists). Further, if the initial state probability is specified (if there are multiple initial states), then MTTF is the sum of all elements of the vector ζ:

$$\zeta = -P(0) \cdot Q^{-1} \quad (8.38)$$

Absorbing State Probabilities

If there are absorbing states (for example, failed states) in the system, then the system eventually reaches one of the absorbing states. This shows that system reliability at infinite time is zero. In some cases, the consequences of (damage due to) different failure modes may be different. In order to evaluate the system further (to find overall failure cost for example), the probability of reaching each absorbing state must be found. This can be achieved by solving individual state probabilities at infinite time. However, this can be more easily found using the following procedure.

Find matrix A, which is the product of matrix $M = -Q_t^{-1}$ and matrix S_t:

Equations

$$Z = M \cdot S_t \quad (8.39)$$

It should be noted that the element z_{ij} of matrix Z represents the probability that the system eventually reaches absorbing state j when the system is initially in state i.

Consider the 2-unit series system shown in Figure 8-8. State 2 (3) presents system failure due to the failure of component 1 (2).

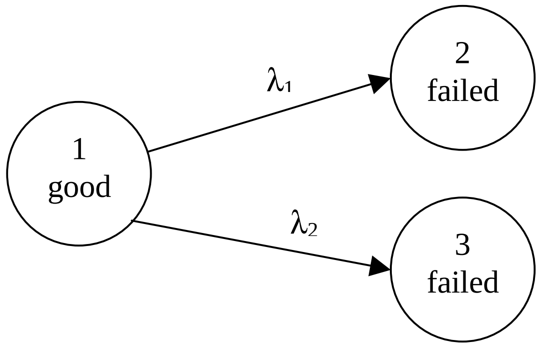


Figure 8-8. Two-unit Series System with Two Failure States

Therefore:

$$Q = \begin{bmatrix} -(\lambda_1+\lambda_2) & \lambda_1 & \lambda_2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad (8.40)$$

$$M = -Q_t^{-1} = \frac{1}{\lambda_1+\lambda_2} \qquad (8.41)$$

$$S_t = [\lambda_1, \lambda_2] \qquad (8.42)$$

$$Z = M \cdot S_t = \left[\frac{\lambda_1}{\lambda_1+\lambda_2}, \frac{\lambda_2}{\lambda_1+\lambda_2}\right] \qquad (8.43)$$

It shows that $\lambda_1/(\lambda_1+\lambda_2)$ is the probability that the system reaches a failed state due to the failure of component 1. Similarly, $\lambda_2/(\lambda_1+\lambda_2)$ is the probability that the system reaches a failed state due to the failure of component 2.

Frequency Parameters

This section describes three frequency parameters:

- Frequency of transition.
- Frequency of visits to a state.
- Failure frequency.

Frequency of Transition

Frequency of transition is the expected number of occurrences of a particular transition per unit time (at a specified time or at a steady state). This may be useful to know the total number of occurrences of an event (transition) within a specified time. Frequency of a transition from state i to state j can be found by multiplying $P_i(t)$ and t_{ij} (transition rate). For example, consider the system shown in Figure 8-6. The frequency of transition from state 2 to state 1 is $P_2(t) \cdot \mu$. The expected number transitions can be found by integrating the frequency of transition over a specified interval.

Frequency of Visits to a State

It should be noted that the number of outward transitions in a state is the sum of the frequencies of all transitions that can occur in that state. For example, consider the system shown in Figure 8-2. The frequency of outward transition in state 1 is $P_1(t) \cdot (\lambda_1 + \lambda_2)$.

Similarly, the frequency of inward transitions to a state can be found by summing the frequencies of all inward transitions. This frequency is equivalent to the frequency of visits to a particular state. For the system in Figure 8-2, the frequency of visits of state 4 is $P_2(t) \cdot \lambda_2 + P_3(t) \cdot \lambda_1$.

Under steady-state conditions, the frequency of inward transitions is equivalent to the frequency of outward transitions. This information can be used to find steady-state probabilities (also availability) as well as system MTBF.

Failure Frequency

System failure frequency is a very useful measure in reliability engineering. The cost of a system not only depends on the system downtime but also on the number of failures. Total number of failures within an interval can be found by integrating the failure frequency over that interval. Further, frequency can be used to find the approximate reliability of complex systems.

Failure frequency is the summation of frequencies of all transitions from good states to failed states. This means that all of the transitions that lead to system failure are summed. For example, consider the system shown in Figure 8-2. The system failure frequency is $P_2(t) \cdot \lambda_2 + P_3(t) \cdot \lambda_1$.

Using this same method, system recovery (repair) frequency can also be found. In this case, however, the transitions from failed states to good states should be considered. Under steady-state conditions, system failure frequency is equivalent to system recovery (success) frequency.

Expected Capacity or Reward

Consider that each state of the system has some (throughput) capacity or reward. For example, consider the two-state system shown in Figure 8-6. Assume a gain of 100 units (dollars, for example) can be obtained from the system when it is in state 1 per time unit. Similarly, assume a loss of 25 units (dollars) when the system is in state 2. Therefore, the expected gain from state i per unit time (at a specified time point t) is $c_i \cdot P_i(t)$, where c_i is the gain (or capacity or reward) from state i per unit time. Therefore, the total gain of the system can be obtained by summing the gains of all states of the system. Integrating this over a specified time interval gives the total gain within that interval.

Steady-state Availability and State Probabilities

As time progresses, the system availability and the individual state probabilities reach stable values. This means that the change in these probabilities are negligible or zero. Theoretically, this happens at an infinite time. However, in most calculations, this can be observed at a reasonably large system time. This condition is known as the **steady-state** condition or long-run behaviour of the system. The probabilities (or availability) can be found by substituting infinity (∞) for the time t. For example, consider the system shown in Figure 8-6. The availability of the system is:

Equations

$$A(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} exp\{-(\lambda + \mu)t\} \quad \text{.........}(8.44)$$

Hence, by substituting ∞ for t, the steady-state availability can be obtained:

$$A = A(\infty) = \frac{\mu}{\lambda + \mu} \quad \text{.........}(8.45)$$

To apply this procedure, the analytical availability expression must first be found. As demonstrated earlier, this process is cumbersome. The remainder of this topic shows how steady-state solutions can be more easily found.

Note: In order to have a non-trivial solution (non-zero availability), there should be no absorbing state in the system. In other words, the Markov process should be an Ergodic Markov process.

According to the above discussion, at steady-state conditions, the change in state probabilities are zero. This means $P'_i(t) = 0$. Further, if there is no absorbing state in the system, the steady-state values are independent of the initial state of the system.

Therefore, equation (8.10) becomes:

$$P \cdot Q = P(\infty) \cdot Q = 0 \quad \text{.........}(8.46)$$

Similarly, equation (8.13) is equivalent to:

$$B \cdot P(\infty) = 0$$

For example, equation (8.8) is:

$$-\lambda \cdot P_1 + \mu \cdot P_2 = 0$$

$$\lambda \cdot P_1 - \mu \cdot P_2 = 0 \qquad (8.47)$$

These are a set of linear equations. Therefore, steady-state probabilities can be obtained by solving these equations. However, both of the equations are the same. Hence, effectively, there is only one equation with two variables (P_1 and P_2). This is because these two equations are not independent. In fact, if there are n states in the system, $n-1$ independent equations can be found. But, at any time, the sum of the probabilities of all states is equivalent to 1. This information can be used to make the number of unknowns and equations the same:

$$\sum_{1}^{n} P_i = 1 \qquad (8.48)$$

Any one of the above equations can be replaced with equation (8.48).

For the example:

$$-\lambda \cdot P_1 + \mu \cdot P_2 = 0$$

$$P_1 + P_2 = 1$$

Solving this equation gives:

$$A = P_1 = \frac{\mu}{\lambda + \mu}$$

$$U = 1 - A = P_2 = \frac{\lambda}{\lambda + \mu} \qquad (8.49)$$

These steady-state probability results can be used to find both steady-state frequencies and rewards.

MTBF

MTBF (Mean Time Between Failure) of a system is the time between two successive failures of the system. It is the sum of the MDT (Mean Down Time) and MTTF (Mean Time to Failure). Assume that the MTBF of the system is six months and that there are on average two failures in a year. The frequency of failure of the system is two per year. There exists a reciprocal relationship between MTBF and failure frequency (which is discussed on page 8-23.) Therefore, if ν is the steady-state failure frequency of the system, then:

Equations

$$MTBF = \frac{1}{\nu} \qquad (8.50)$$

For the example problem:

$$\nu = \frac{\mu}{\lambda + \mu} \cdot \lambda \qquad (8.51)$$

Therefore:

$$MTBF = \frac{1}{\nu} = \frac{\lambda + \mu}{\lambda \cdot \mu} = \frac{1}{\lambda} + \frac{1}{\mu} \quad (8.52)$$

If $\lambda \ll \mu$, then $MTBF = 1/\lambda$. This relationship is commonly employed elsewhere in this document.

Once MTBF has been obtained, MTTF and MTTR can easily be found:

$$MTTF = A \cdot MTBF = \frac{\mu}{\lambda + \mu} \cdot \frac{\lambda + \mu}{\lambda \cdot \mu} = \frac{1}{\lambda} \quad (8.53)$$

$$MTTR = (1 - A) \cdot MTBF = \frac{\lambda}{\lambda + \mu} \cdot \frac{\lambda + \mu}{\lambda \cdot \mu} = \frac{1}{\mu} \quad (8.54)$$

All of the methods provided in this section are exact methods. Approximate solutions are useful for solving large practical problems within a short time.

Examples

This section provides calculation examples for a two-component parallel system, an $(n-1)$-out-of-n system, a cold standby system, a two-component cold standby system with repair and a warm standby system.

Two-component Parallel System

Information on the various reliability characteristics that can be calculated for a two-component parallel system follow.

Availability

Consider a two-component repairable system in which the two components are identical. Initially, assume that both of the components are working (state 1). Either of the components leads the system to a state where there is only one working component (state 2). Because each component can fail with failure rate λ, failure of any one of the components is 2λ. (This is similar to the failure rate of a series system with two identical components.) This technique is known as state merging.

In state 2, two events can exist:

- The working component can fail, which causes the system to reach a failed state (state 3) where both components are failed.
- The failed component can be repaired, and the system returns to state 1.

In state 3, both the components are under repair. If either of the components is repaired, then the system reaches state 2. As in the case of failure rate, here, the effective transition rate is 2μ. Figure 8-9 shows the state transition diagram for the two-component parallel system.

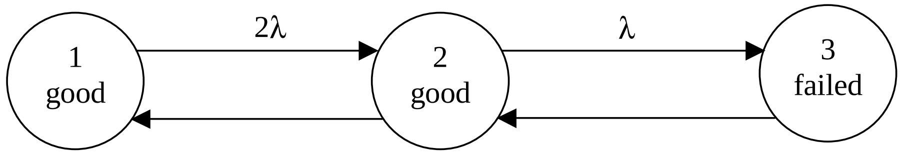


Figure 8-9. Two-component Parallel System

NOTE Although the availability of this system can be found using combinatorial models, the exact reliability cannot.

Using the previous procedures results in:

Equations

$$P_3(t) = \left[\left(\frac{\lambda}{\lambda+\mu}\right)(1 - exp\{-(\lambda+\mu)t\})\right]^2 \quad (8.55)$$

Because state 3 is the only failed state:

$$A(t) = 1 - P_3(t) = 1 - \left[\left(\frac{\lambda}{\lambda+\mu}\right)(1 - exp\{-(\lambda+\mu)t\})\right]^2 \quad (8.56)$$

If $\mu \gg \lambda$, then:

$$A(t) = 1 - \left[\frac{\lambda}{\mu}\right]^2 \quad (8.57)$$

Using the previous procedures, the availability of any system can be found. However, it is advisable to use combinatorial models whenever possible.

Reliability

As noted earlier, when performing reliability analysis, all failed states should be treated as absorbing states. Figure 8-10 shows a state transition diagram for a two-component parallel system without system repair.

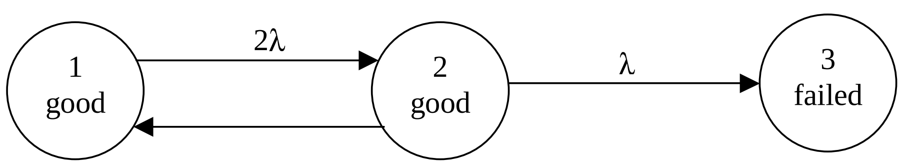


Figure 8-10. Two-component Parallel System Without System Repair

Following the procedure mentioned earlier, the Laplace transformation of $P_3(t)$ can be shown as:

Equations

$$P_3(s) = \frac{\Delta_3}{\Delta}$$

$$\Delta = s(s^2 + s(3\lambda + \mu) + 2\lambda^2) = s(s + s_1)(s + s_2) \quad (8.58)$$

$$\Delta_3 = 2\lambda^2 \quad (8.59)$$

Where s_1 and s_2 are negative and are the roots of the equation $s^2 + s(3\lambda + \mu) + 2\lambda^2$, where $s_1 \cdot s_2 = 2\lambda^2$.

This means:

$$s_2, s_1 = \frac{-(3\lambda + \mu) \pm \sqrt{(3\lambda + \mu)^2 - 8\lambda^2}}{2} \quad (8.60)$$

According to the above procedure:

$$P_3(t) = \frac{2\lambda^2}{s_1 \cdot s_2} - \frac{s_1 e^{s_2 t} - s_2 e^{s_1 t}}{s_1 - s_2} \quad (8.61)$$

Because state 3 is the only failed state and $s_1 \cdot s_2 = 2\lambda^2$, then:

$$R(t) = 1 - P_3(t) = \frac{s_1 e^{s_2 t} - s_2 e^{s_1 t}}{s_1 - s_2} \quad (8.62)$$

If $\mu \gg \lambda$, then s_2 will be numerically very much greater than s_1.

Specifically:

$$\sqrt{(3\lambda + \mu)^2} \approx 3\lambda + \mu - \frac{4\lambda^2}{3\lambda + \mu} \quad (8.63)$$

$$s_1 \approx 3\lambda + \mu - \frac{2\lambda^2}{3\lambda + \mu} \approx 3\lambda + \mu \quad (8.64)$$

$$s_2 \approx \frac{2\lambda^2}{3\lambda + \mu} \approx \frac{2\lambda^2}{\mu} \quad (8.65)$$

Therefore:

$$R(t) \approx e^{s_1 t} = exp\left\{-\frac{2\lambda^2}{\mu}t\right\} \quad (8.66)$$

Considering the same procedure, the reliability as well as the approximation of any system can be found.

MTTF

MTTF of the system can be found as described in “MTTF” on page 8-19.

Therefore:

Equations

$$M = -Q_t^{-1} = \frac{1}{2\lambda^2}\begin{bmatrix} \lambda + \mu & 2\lambda \\ \mu & 2\lambda \end{bmatrix} \quad (8.67)$$

$$MTTF = \frac{1}{2\lambda^2}(\lambda + \mu + 2\lambda) = \frac{3\lambda + \mu}{2\lambda^2} \quad (8.68)$$

If $\mu \gg \lambda$, then:

$$MTTF \approx \frac{\mu}{2\lambda^2} \qquad (8.69)$$

However, this can also be found by integrating the approximate reliability expression:

$$MTTF = \int_0^{\infty} exp\left\{-\frac{2\lambda^2}{\mu}t\right\} = \frac{\mu}{2\lambda^2} \qquad (8.70)$$

Steady-state Failure Frequency

Using the equation in "Steady-state Availability and State Probabilities" on page 8-24, failure frequency is:

$$\nu = P_2(\infty) \cdot \lambda = P_3(\infty) \cdot 2\mu \qquad (8.71)$$

$$= 2\mu \cdot \left(\frac{\lambda}{\lambda + \mu}\right)^2 \qquad (8.72)$$

If $\mu \gg \lambda$, then:

$$\nu \approx \frac{\mu}{2\lambda^2} \qquad (8.73)$$

MTBF

As discussed in "MTBF" on page 8-25, MTBF is the reciprocal of steady-state failure frequency. Therefore:

Equations

$$MTBF = \frac{1}{2\mu}\left(\frac{\lambda + \mu}{\lambda}\right)^2 \qquad (8.74)$$

If $\mu \gg \lambda$, then:

$$MTBF \approx \frac{\mu}{2\lambda^2} \qquad (8.75)$$

Mean Up Time

As discussed in "MTBF" on page 8-25, Mean Up Time (MUT) is the product of steady-state availability and MTBF. Therefore:

$$MUT = \left[1 - \left(\frac{\lambda}{\lambda + \mu}\right)^2\right] \cdot \left[\frac{1}{2\mu}\left(\frac{\lambda + \mu}{\lambda}\right)^2\right] \qquad (8.76)$$

If $\mu \gg \lambda$, then:

$$MUT \approx \frac{\mu}{2\lambda^2} - \frac{1}{\mu} \approx \frac{\mu}{2\lambda^2} \qquad (8.77)$$

Similarly, all other reliability characteristics can be found.

(*n*-1)-out-of *n* System

Consider a special k-out-of-n system, where $k = n - 1$. Examples of this system include 2-out-of-3 and 3-out-of-4 systems. Figure 8-11 shows a state transition diagram for such a system. It has only three states (versus n states because all failed states have been merged into a single state.) In other words, once the system reaches a failed state where there are exactly two failed components, it cannot be repaired. Because the system has already failed, it is not necessary to consider the events that can occur in that state and hence the states that follow it.

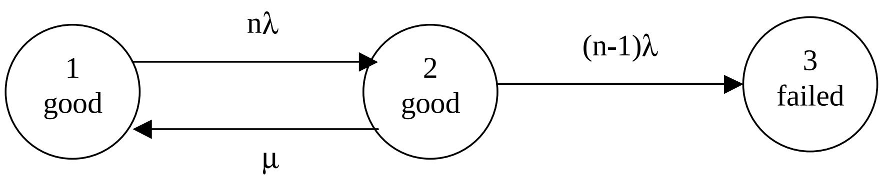


Figure 8-11. (*n*-1)-out-of-*n* System (Without System Repair)

Following the previous procedures:

Equations

$$\Delta = s[s^2 + \{s(2n-1)(\lambda + \mu)\} + n(n-1)\lambda^2] = s(s + s_1)(s + s_2) \quad (8.78)$$

$$\Delta_3 = n(n-1)\lambda^2 \quad (8.79)$$

The reliability expression for this system is similar to the reliability expression for the two-component parallel system. The only difference is that here, s_1 and s_2 are the roots of the equation $s^2 + s\{(2n-1)(\lambda + \mu)\} + n(n-1)\lambda^2$.

As in the case of the parallel system, the approximation to reliability is:

$$R(t) \approx e^{s_1 t} = exp\left\{-\frac{n(n-1)\lambda^2}{\mu}t\right\} \quad (8.80)$$

Therefore:

$$MTTF = \int_0^\infty R(t)dt = \frac{\mu}{n(n-1)\lambda^2} \quad (8.81)$$

Cold Standby System

Consider a cold standby system with two identical components. Initially, one component is working while the other is in standby. The failure rate of the standby component is zero. After a failure of the working component, the standby component will become operational. The system reaches a failed state after the failure of the second component. Figure 8-12 shows the state transition diagram for this system.

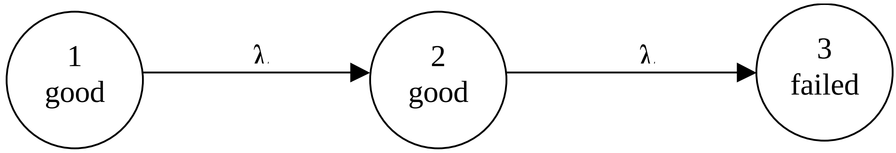


Figure 8-12. Two-component Cold Standby System

Following the previous procedures:

Equations

$$P_3(s) = \frac{\lambda^2}{s(s+\lambda)^2} = \frac{1}{s} - \frac{1}{(s+\lambda)^2} \quad (8.82)$$

$$R(t) = P_3(t) = e^{-\lambda t}(1+\lambda t) \quad (8.83)$$

Similarly, reliability of an n-component cold standby system (1 online, $n-1$ in standby) is:

$$R(t) = e^{-\lambda t}\sum_{i=0}^{n-1}\frac{(\lambda t)^i}{i!} \quad (8.84)$$

Therefore:

$$MTTF = \int_0^\infty R(t)dt = \frac{n}{\lambda} \quad (8.85)$$

The same procedure can be extended to a k-out-of-n cold standby system where initially there are k units in operation and $(n-k)$ units in standby:

$$R(t) = e^{-k\lambda t}\sum_{i=0}^{n-k}\frac{(k\lambda t)^i}{i!} \quad (8.86)$$

Therefore:

$$MTTF = \int_0^\infty R(t)dt = \frac{n-k+1}{k\lambda} \quad (8.87)$$

Consider a 1-out-of-n cold standby system with non-identical units. The failure rate of component i is λ_i. Figure 8-13 shows the state transition diagram for this system.

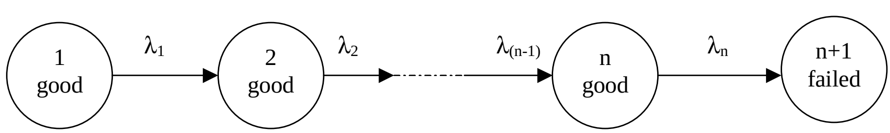


Figure 8-13. *n*-component Cold Standby System

Following the previous procedures, the reliability of the system is:

$$R(t) = \sum_{i=1}^{n} \left[\prod_{j=1, j \neq i}^{n} \frac{\lambda_j}{\lambda_j - \lambda_i} \right] e^{-\lambda_i t} \quad (8.88)$$

After simplification, the MTTF of the system is:

$$MTTF = \sum_{i=1}^{n} \frac{1}{\lambda_i} \quad (8.89)$$

Note: It should be noted that if n is large (preferably all failure rates are almost equal), then the failure time distribution follows the normal distribution with the mean (α) and standard deviation (σ), where:

$$\alpha = \sum_{i=1}^{n} \frac{1}{\lambda_i} \quad (8.90)$$

$$\sigma = \sqrt{\sum_{i=1}^{n} \frac{1}{\lambda_i^2}} \quad (8.91)$$

Therefore, the reliability of the system is:

$$1 - \Phi\left(\frac{t - \alpha}{\sigma}\right)$$

Where $\Phi(\,.)$ is the cumulative distribution function of the standard normal distribution. For additional information, refer to the numeric results in Table 3-2.

Two-component Cold Standby System with Repair

Consider a cold standby system with two identical components. Initially, one component is working while the other is in standby. The failure rate of the standby component is zero. After a failure of the working component, the standby component will become operational and the repair of failure component will be started. In this state, if the working component fails before the repair of the failed component, then the system will reach a failed state. If repair of the failed component is done before the failure of the working component, then it will be kept in the standby mode. Hence, the system reaches state 1 again. Figure 8-14 shows the state transition diagram for this system.

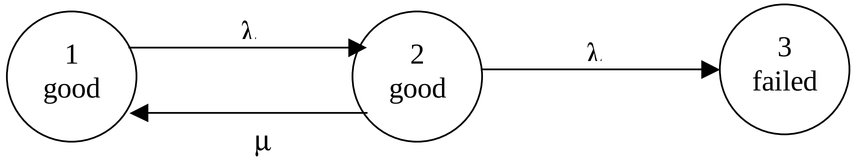


Figure 8-14. Two-component Cold Standby System with Repair

The reliability expression of this system is similar to the reliability expression of the two-component parallel system. The only difference is that here, s_1 and s_2 are the roots of the equation $s^2 + s(2\lambda + \mu) + \lambda^2 = 0$:

As in the case of the parallel system, the approximation to system reliability is:

$$R(t) = e^{s_2 t} = exp\left\{-\frac{\lambda^2}{\mu}t\right\} \qquad (8.92)$$

Therefore:

$$MTTF = \int_0^{\infty} R(t)dt = \frac{\mu}{\lambda^2} \qquad (8.93)$$

(*n*-1)-out-of-*n* Cold Standby System with Repair

Figure 8-15 shows the state transition diagram for an ($n-1$)-out-of-n cold standby system with repair.

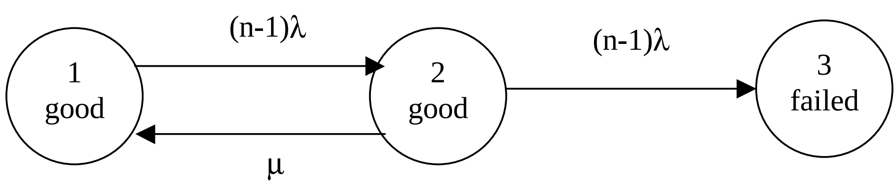


Figure 8-15. (n-1)-out-of-n Cold Standby System With Repair

Following the previous procedures, the approximation for system reliability is:

Equation

$$R(t) \approx exp\left\{-\frac{(n-1)^2\lambda^2}{2(n-1)\lambda + \mu}t\right\} \approx exp\left\{-\frac{(n-1)^2\lambda^2}{\mu}t\right\} \qquad (8.94)$$

Therefore:

$$MTTF \approx \frac{\mu}{(n-1)^2\lambda^2} \qquad (8.95)$$

Warm Standby System

Unlike cold standby components, warm standby components fail even during the standby mode. Generally, though, the failure rate during standby is much less than during operation. Assume that the failure rate of the standby mode is λ . Therefore, the system can reach state 2 due to either the failure of the operating unit or the failure of the standby component. Consequently, these failure rates can be added. Figure 8-16 shows the state transition diagram for a warm standby system.

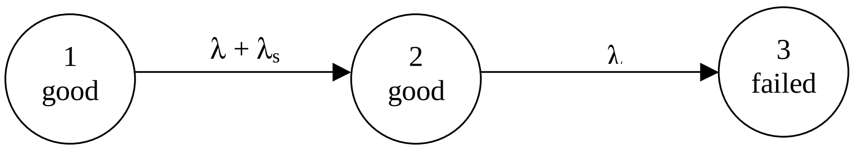


Figure 8-16. Two-component Warm Standby System

Using the procedures mentioned earlier:

$$R(t) = 1 - P_3(t) = \frac{(\lambda + \lambda_s)}{\lambda_s} e^{-\lambda t} - \frac{\lambda}{\lambda_s} e^{-(\lambda + \lambda_s)t} \quad \text{(8.96)}$$

Therefore:

$$MTTF = \int_0^\infty R(t)dt = \left(\frac{\lambda + \lambda_s}{\lambda_s} \cdot \frac{1}{\lambda}\right) - \left(\frac{\lambda}{\lambda_s} \cdot \frac{1}{\lambda + \lambda_s}\right) \quad \text{(8.97)}$$

$$= \frac{2\lambda + \lambda_s}{\lambda(\lambda + \lambda_s)} \quad \text{(8.98)}$$

The reliability of an n -unit warm standby can be found from equation (8.88) by substituting $\lambda_i = \lambda + (n - i) \cdot \lambda_s$, where $i = 1, ..., n$. Moreover, reliability of a k -out-of n warm standby system can be found by substituting $\lambda_i = k\lambda + (n - k + 1 - i) \cdot \lambda_s$, where $i = 1, ..., n - k + 1$ (In this case, the total number of states will be $n - k + 1$.)

A. Data Tables

References for Reliability Predictions

This appendix contains the data tables needed to carry out the calculations referred to in “Generic Parts Count Method” on page 3-6 and “Parts Stress Analysis Methods” on page 3-15.

Discrete Electronic and Electro-mechanical Components

Table A-1 provides base failure rates for discrete electronic and electro-mechanical components.

Table A-1. Discrete Electronic and Electro-mechanical Components

Component Description	Base Failure Rate λ_B $\frac{\text{failures}}{10^6\text{hrs}}$	K Factors						Predominant Failure Modes	
	G.1	G.2	S.1	S.2	A.1	A.2			
Part	**Ground Fixed**	**Ground Mobile**	**Ship Protected**	**Ship Exposed**	**Air Protected**	**Air Exposed**		**Mode**	**% Factor**
Accelerometers									
Accelerometer, General	22.00	3.00	1.70	3.00	5.00	6.00			
Accelerometer, Linear	18.00	3.00	1.70	3.00	5.00	4.00			
Accelerometer, Angular									
Accelerometer, Pendulum									
Accelerometer, Strain Gauge	32.00	3.00	1.70	3.00	5.00	4.00			
Accelerometer, Sintered-Ceramic, Piezo-Electric									
Actuators									

Table A-1. Discrete Electronic and Electro-mechanical Components

Component Description	Base Failure Rate λ_B failures/10^6hrs	K Factors						Predominant Failure Modes	
	G.1	G.2	S.1	S.2	A.1	A.2			
Part	**Ground Fixed**	**Ground Mobile**	**Ship Protected**	**Ship Exposed**	**Air Protected**	**Air Exposed**		**Mode**	**% Factor**
Actuator, Linear (Electrical)	1.20	2.00	1.50	2.70	2.20	4.00			
Actuator, Rotary (Electrical)	2.40	2.00	1.50	2.70	2.20	4.00			
Aerial	1.00	6.00	2.30	6.00	5.00	10.00		No Transmission	54
								Signal Leakage	21
								Spurious Transmission	25
Aerial Dish	3.00	4.00	1.70	4.00	3.00	6.00		Ditto	
Alternator	3.00	3.00	1.30	3.00	2.00	3.00			
Batteries	3.00	3.00	1.30	3.00	2.00	3.00			
Battery, Secondary, General	1.50	10.00	8.00	10.00	24.00	50.00			
Battery, Secondary, Lead Acid	0.50	2.50	1.80	4.00	1.80	7.60		Degraded Output	70
								Short Circuit	20
								Intermittent Output	10
Battery, Secondary, Nickel Cadmium	0.20	2.50	1.80	4.00	1.80	7.60		Degraded Output	72
								No Output	28
Battery, Secondary, Silver Zinc									
Battery, Lithium								Degraded Output	78
								Startup Delay	14
								Short Circuit	6
								Open Circuit	2
Cable, Electric, Interconnecting - per cable. (Semi-permanent Surface/ Air ground installation)	1.20	Not Applicable							
Capacitors, Fixed									
Aluminum Electrolytic	0.30	3.00	2.00	10.00	9.00	13.00		Short Circuit	50
								Open Circuit	30
Tantalum, Electrolytic, Foil	0.13	3.00	1.50	3.00	2.30	3.50		Short Circuit	75
								Open Circuit	25
Capacitors, Fixed (Continued)									

Table A-1. Discrete Electronic and Electro-mechanical Components (Continued)

Component Description	Base Failure Rate λ_B failures 10^6hrs	K Factors						Predominant Failure Modes	
	G.1	G.2	S.1	S.2	A.1	A.2			
Part	Ground Fixed	Ground Mobile	Ship Protected	Ship Exposed	Air Protected	Air Exposed		Mode	% Factor
Tantalum, Electrolytic, Sintered |Anode, Wet Electrolyte	0.12	2.40	2.30	2.40	4.80	5.00		Short Circuit	80
								Open Circuit	20
Tantalum, Electrolytic, Solid	0.08	2.30	2.00	2.30	4.00	6.00		Short Circuit	50
								Open Circuit	30
Ceramic	0.04	2.00	1.20	2.40	4.00	5.00		Short Circuit	50
								Open Circuit	30
Ceramic, Chip	0.10	2.00	1.20	1.80	1.50	2.50		Short Circuit	50
								Open Circuit	30
Mica	0.06	2.00	3.00	4.30	2.40	6.00			
Mica, Button									
Mica, Silvered									
Porcelain									
Paper, Metallized	0.06	2.00	2.70	8.00	2.00	10.00			
Paper, Foil	0.12	2.70	1.50	2.50	3.50			Short Circuit	90
								Open Circuit	5
Plastic Film (Synthetic Film)	0.05	3.00	1.70	3.00	3.00	7.00		Short Circuit	55
								Open Circuit	40
Capacitors, Variable									
Air	0.10	5.00	3.20	5.00	12.00	16.00			
Ceramic	0.14	12.00	3.00	12.00	9.00	15.00			
Glass	0.26	2.20	2.50	11.00	4.50	20.00			
Circuit Breakers									
Circuit Breaker, Magnetic	1.00	5.00	1.70	5.00	3.00	5.00			
Circuit Breaker, Thermal	2.00	2.70	1.40	2.70	2.20	7.00			
Clutch, Electro-Magnetic	3.50	3.00	2.00	3.00	4.00	5.00		Bearing Wear	30
								Coil Failure	20
								Contamination	25
								Lubrication failure	15
Connections									
Crimped	0.01								
Hand Soldered	0.00	Connection failure rates are greatly dependent on the level of process control employed. The quoted base failure rates are achievable in all environments provided the effect of vibration on lead connections is eliminated.							
Connections (Continued)									

Table A-1. Discrete Electronic and Electro-mechanical Components (Continued)

Component Description	Base Failure Rate λ_B failures/10^6hrs	K Factors						Predominant Failure Modes	
	G.1	G.2	S.1	S.2	A.1	A.2			
Part	**Ground Fixed**	**Ground Mobile**	**Ship Protected**	**Ship Exposed**	**Air Protected**	**Air Exposed**		**Mode**	**% Factor**
Flow Soldered	0.00								
Through-Plated, PCB	0.00								
Welded	0.00								
Wire Wrapped (Using tool)	0.00								
Connectors									
Connector, co-axial	0.17	2.00	1.40	2.30	2.00	3.40		Contamination / Corrosion	29
								Distortion	29
								Fracture	22
								Low Insulation	17
Connector, edge	0.01	2.00	1.40	2.30	2.00	3.40		Ditto	
Connector, non-hermetic	0.04	2.00	1.40	2.30	2.00	3.40		Ditto	
Connector, hermetic	0.03	2.00	1.40	2.30	2.00	3.40		Ditto	
Crystal Devices									
Crystal, Quartz	0.20	5.00	2.00	5.00	4.00	6.00		Open Circuit	80
Crystal Oscillator	0.76							No Oscillation	10
Diodes									
Germanium, general purpose	0.30	8.00	2.30	8.00	5.00	8.00		Short Circuit	75
								Open Circuit	5
								Intermittent	18
Rectifier, low power, <1W	0.12	2.50	1.80	2.50	2.00	4.00		Open Circuit	60
								Short Circuit	40
Rectifier, medium power, <20W	0.20	3.00	1.20	3.00	1.50	5.00		Ditto	
Rectifier, high power, >20W	0.50	3.00	1.20	3.00	1.50	5.00		Ditto	
Silicon, signal	0.05	4.00	3.00	4.00	3.00	6.00		Open Circuit	24
								Short Circuit	16
								Parameter Change	58
Silicon, Reference/Regulation (Zener, Avalanche)	0.07	2.50	2.00	3.50	2.00	5.50		Open Circuit	45
								Short Circuit	20
								Parameter Change	35
Diodes (Continued)									

Table A-1. Discrete Electronic and Electro-mechanical Components (Continued)

Component Description	Base Failure Rate λ_B failures 10^6hrs	K Factors						Predominant Failure Modes	
	G.1	G.2	S.1	S.2	A.1	A.2			
Part	**Ground Fixed**	**Ground Mobile**	**Ship Protected**	**Ship Exposed**	**Air Protected**	**Air Exposed**		**Mode**	**% Factor**
Microwave, Gunn Oscil-lator	0.50	4.00	1.70	4.00	3.00	5.00			
Microwave, Detector	1.20	7.00	7.50	10.20	7.50	15.00			
Microwave, Mixer	1.80	5.00	5.70	7.50	5.00	11.00			
Microwave, Schottky	0.50	5.00	4.00	6.00	4.00	9.00			
Step Recovery	0.30	5.00	6.00	8.00	5.00	11.00			
Tunnel	0.30	5.00	6.00	8.00	5.00	11.00			
Varactor Tuning	0.30	5.00	6.00	8.00	5.00	11.00			
P.I.N. (Intrinsic), Switching	0.50	2.00	1.30	2.00	2.00	3.00			
P.I.N. (Attenuation)	4.00	2.00	1.30	2.00	2.00	3.00			
Thyristor, Reverse blocking, 2 leads (Shockley)	0.40	2.25	2.50	3.50	3.00	5.00		Failed OFF	45
								Short Circuit	40
								Open Circuit	10
								Failed ON	5
Thyristor, Reverse blocking, 3 leads (Silicon Controlled Rectifier)	0.40	2.25	2.50	3.50	3.00	5.00		Open Circuit	2
								Short Circuit	
Thyristor, Bi-Directional, 2 leads, DIAC	0.40	2.25	2.50	3.50	3.00	5.00			
Thyristor, Bi-Directional, 3 leads, TRIAC	0.75	5.00	6.00	7.00	5.00	10.00		Failed OFF	90
								Failed ON	10
Surge Suppressor, Sele-nium	0.25	2.00	1.50	2.00	2.50	3.00			
Fuses									
Fuse, General	0.20	4.00	2.30	4.00	5.00	6.00		Fails to Open	49
								Slow to Open	43
								Premature Open	8
Fuse Link, Cartridge	0.10	5.00	2.00	5.00	4.00	8.00		Ditto	
Gyroscopes									
Gyroscope, displacement	12.00	3.00	2.00	3.00	4.00	4.00			
Gyroscope, free	14.00	3.00	2.00	3.00	4.00	4.00			
Gyroscope, rate	20.00	4.00	3.50	4.00	6.00	8.00			
Gyroscope, integrating	20.00	4.00	3.50	4.00	6.00	8.00			
Gyroscope, Laser									

Table A-1. Discrete Electronic and Electro-mechanical Components (Continued)

Component Description	Base Failure Rate λ_B $\frac{failures}{10^6 hrs}$	K Factors						Predominant Failure Modes	
	G.1	G.2	S.1	S.2	A.1	A.2			
Part	Ground Fixed	Ground Mobile	Ship Protected	Ship Exposed	Air Protected	Air Exposed		Mode	% Factor
Inductors (Coils and Chokes)									
L.F. Signal	0.11	8.00	2.70	8.00	6.00	10.00		Short Circuit	42
								Open Circuit	42
								Change in Value	16
L.F. Power	0.25	8.00	2.70	8.00	6.00	10.00		Ditto	
R.F. Signal	0.08	6.00	2.30	6.00	5.00	8.00		Ditto	
R.F. Power	0.15	6.00	2.30	6.00	5.00	8.00		Ditto	
R.F. Variable	0.20							Ditto	
Saturated	0.24							Ditto	
Inductors (Coils and Chokes) (Continued)									
Solenoid, Electrical	1.50	3.00	1.70	3.00	3.00	4.00		Fails to Operate	57
								Slow Move-ment	43
Solenoid, Rotary	1.50	3.00	1.50	3.00	2.50	4.00		Ditto	
Solenoid, Valve, General	6.40	3.00	1.70	3.00	3.00	4.00		Ditto	
Transformers									
High Power, Pulse and Power (>1kV)	0.16	0.34	0.13	0.45	0.27	0.45			
Low Power /Signal	0.02	0.05	0.02	0.07	0.04	0.05			
Audio	0.05	0.10	0.04	0.13	0.07	0.10			
Transistors									
Germanium	0.13	6.60	5.50	8.00	6.60	8.30		High Collector-Base Leakage current	59
								Low Collector-Emitter Break-down Voltage	37
NPN/PNP (f<200MHz)	0.05	4.40	4.70	6.30	6.80	8.80			
Power NPN/PNP (f<200MHz)	0.09	5.00	5.00	6.00	5.00	8.00			

Table A-1. Discrete Electronic and Electro-mechanical Components (Continued)

Component Description	Base Failure Rate λ_B failures 10^6hrs	K Factors					Predominant Failure Modes	
Part	G.1 Ground Fixed	G.2 Ground Mobile	S.1 Ship Protected	S.2 Ship Exposed	A.1 Air Protected	A.2 Air Exposed	Mode	% Factor
Transistors (Continued)								
Si FET (f £ 400MHz)							Short Circuit	51
							Output Low	22
							Parameter Change	17
							Open Circuit	5
							Output High	5
Si FET (f > 400MHz)							Ditto	
GaAs FET (P<100mW)							Open Circuit	61
							Short Circuit	26
							Parameter Change	13
GaAs FET (P³100mW)							Ditto	
Unijunction	0.10	5.50	5.90	8.80	5.50	12.00		
RF, Low Noise (f>200MHz, P<1W)							Parameter Change	50
							Short Circuit	40
							Open Circuit	10
RF, Power (P³1W)							Ditto	
Electrical Components								
Meter, Electrical, General	2.30	40.00	1.70	4.00	3.00		Contamination	71
							Mechanical Damage	23
Meter, Electrical, Moving Coil	3.00	2.70	1.40	2.70	2.20			
Meter, Electrical, Moving Iron								
Magneto	11.00	4.00	1.70	4.00	3.00	4.00		
Motors								
Motor, Electrical, AC	1.20	3.00	1.30	3.00	2.00	3.00	Bearing Failure	28
							Winding Failure	31
							Fails to Run After Start	23
							Fails to Start	18
Motor, Electrical, Stepper	0.50	4.00	1.70	4.00	3.00	4.00		
Motor, Fractional HP	3.30	2.30	1.20	2.00	1.50	5.50		
Motor, Full HP	0.90	4.50	1.80	4.00	35.00	13.00		
Motor, Servo (Servomotor)	1.50	3.00	1.70	3.00	3.00	4.00	Bearing Failure	45

Table A-1. Discrete Electronic and Electro-mechanical Components (Continued)

Component Description	Base Failure Rate λ_B failures/10^6hrs	K Factors						Predominant Failure Modes	
	G.1	G.2	S.1	S.2	A.1	A.2		
Part	**Ground Fixed**	**Ground Mobile**	**Ship Protected**	**Ship Exposed**	**Air Protected**	**Air Exposed**	**Mode**	**% Factor**
Motors (Continued)								
Motor, Servo (Servomotor) Integrating	6.00						Winding failure	50
Motor, Servo (Servomotor) Position	1.00							
Slip Ring and Brush (per pair)	3.20	5.00	2.60	5.00	6.00		Contamination	37
							Shorted Contact	26
							High Resistance	15
							Open Circuit	9
Motor, Synchro	3.00	2.00	1.30	2.00	2.00	3.00	Bearing Failure	33
							Winding failure	45
							Brush Failure	22
Dynamotor, (AC/DC Rotary Converter)	9.00	4.00	1.70	4.00	3.00	4.00		
Brush, Contact (per contact)	0.50	7.00	2.30	7.00	5.00	10.00		
Generators								
Generator, Electrical, AC	3.00	3.00	1.30	3.00	2.00	3.00	Degraded Output	60
							No Output	22
							Fails to Run After Start	9
							Loss of Control	9
Generator, Electrical, DC	7.00	4.00	1.70	4.00	3.00	4.00	Ditto	
Blower / Fan	4.00	3.60	6.25	22.00	10.00	25.00	Winding Failure	35
							Bearing Failures	50
							Slip-rings/Brushes	5

Table A-1. Discrete Electronic and Electro-mechanical Components (Continued)

Component Description	Base Failure Rate λ_B failures 10^6hrs	K Factors						Predominant Failure Modes	
	G.1	G.2	S.1	S.2	A.1	A.2			
Part	Ground Fixed	Ground Mobile	Ship Protected	Ship Exposed	Air Protected	Air Exposed		Mode	% Factor
Opto-Electronics									
Light Emitting (LED) Single Point	0.10	2.00	1.30	2.00	2.00			Open Circuit	100
Light Emitting Array	0.10 per element	2.00	1.30	2.00	2.00			Open Circuit	100
Photodiode (light sensors & counters)	2.00	2.00	1.30	2.00	2.00			Open Circuit	100
Opto-Isolator	0.27	4.00	1.70	4.00	3.00			Open Circuit	100
Laser Diode, GaAs/Al GaAs	16.00	5.00	2.40	7.50	5.00	7.00		Open Circuit	100
Laser Diode, In GaAs/In GaAsP	28.00	5.00	2.40	7.50	5.00	7.00		Open Circuit	100
Lamp, Filament	1.00	2.50	1.30	2.50	2.00	6.00		Open Circuit	90
								Breakage	10
Lamp, Neon	0.20	3.00	1.30	3.00	2.00	4.00			
Lens, Optical	0.40	3.00	2.00	3.00	4.00	6.00		Breakage	100
Fibre Optics									
Cable, Plastic coated, Silica Fibre									
Link, Single Fibre, Digital									
Link, Single Fibre, Analogue									
Transmitter, Digital									
Transmitter, Analogue									
Receiver, Digital									
Receiver, Analogue									
Printed Circuit Boards									
Double Sided	0.01	2.00	2.00	5.00	3.00	10.00		Open Circuit	76
								Short Circuit	24
Multi-Layer	0.13	2.00	2.00	5.00	3.00	10.00		Ditto	
Surface Mount Tech. Circuit Boards	0.37	4.80	4.80	114.00	17.00	95.00		Ditto	
Relays									
Relay, Armature (Electro-mechanical)	0.35	3.50	2.60	8.00	9.00	10.00		Coil faults	5
								Contact faults	75
								Mechanical faults	10
Relay, Crystal can	0.16	10.00	5.00	8.00	10.00	12.00			
Relay, Dry Reed (per contact pair)	0.15	7.00	8.00	13.00	9.00	11.00			

Table A-1. Discrete Electronic and Electro-mechanical Components (Continued)

Component Description	Base Failure Rate λ_B failures 10^6hrs	K Factors					Predominant Failure Modes	
	G.1	G.2	S.1	S.2	A.1	A.2		
Part	**Ground Fixed**	**Ground Mobile**	**Ship Protected**	**Ship Exposed**	**Air Protected**	**Air Exposed**	**Mode**	**% Factor**
Relays (Continued)								
Relay, Electro-Mechanical, Flat-Pack								
Relay, Electro-Mechanical, PCB								
Relay, Hybrid (Mechanical switch with Solid State circuitry)								
Relay, Mercury-wetted contact	1.00	7.00	4.00	7.00	9.50	11.00		
Relay, Mercury-wetted contact (per contact pair)	0.30							
Relay, Resonant Reed	0.35							
Relay, Time Delay	0.34	7.00	4.50	7.00	8.50	10.00		
Relay, Solid State (SSR)								
Relay, T05 Encapsulated								
Relay, Co-Axial								
Relay, Latching, Mechan-ical	0.45	3.00	3.00	6.00	3.50	5.00		
Relay, Latching, Magnetic								
Relay, Power	1.00	7.00	4.50	7.00	9.50	14.00		
Relay, Stepping								
Relay, Thermal	0.35	3.00	2.20	3.00	5.00	6.00		
Resistors - Fixed								
Fixed, Carbon Composition	0.015	6.00	2.00	6.00	3.00	6.00	Open Circuit	75
							Change of Value	20
Fixed, Carbon Film	0.02	7.00	2.00	10.00	9.00	12.00	Ditto	
Fixed, Cermet, Single Unit (thick film)								
Fixed, Carbon Film (High Stability)								
Fixed, Metal Film	0.016	2.50	1.50	3.50	1.50	3.60	Ditto	
Fixed, Oxide Film	0.02	4.00	1.70	4.00	3.00	4.00	Open Circuit	95
Fixed, Temperature Sensi-tive (Thermistor) Rod, Bead or Disc Type	0.18	3.00	1.50	2.00	1.40	2.00	Open Circuit	95
							Change in Value	5
Fixed, Voltage Sensitive (Varistor)							Open Circuit	95
							Change in Value	5

Table A-1. Discrete Electronic and Electro-mechanical Components (Continued)

Component Description	Base Failure Rate λ_B $\frac{\text{failures}}{10^6\text{hrs}}$	K Factors						Predominant Failure Modes	
	G.1	G.2	S.1	S.2	A.1	A.2			
Part	Ground Fixed	Ground Mobile	Ship Protected	Ship Exposed	Air Protected	Air Exposed		Mode	% Factor
Resistors - Fixed (Continued)									
Fixed, Wirewound, Precision	0.05	4.00	3.50	5.00	4.00	6.40		Open Circuit	65
								Change in Value	26
								Short Circuit	9
Fixed, Voltage Sensitive (Varistor)								Open Circuit	95
Fixed, Wirewound, Power	0.06	3.00	2.50	4.00	4.00	6.00		Ditto	
Resistors - Variable									
Variable, Carbon Composition	2.00	3.75	2.00	17.00	4.50	17.00		Erratic Operation	95
								Insulation Failure	5
Variable, Cermet	0.40	3.00	2.30	3.00	5.00	7.00			
Variable, Conductive Plastic	0.60	2.50	1.80	2.50	3.50	6.00		Excessive Contact Resistance	30
								Open Circuit track	60
Variable, Non-Wirewound	2.00	3.30	1.20	4.20	2.00	5.00		Erratic Operation	95
								Insulation Failure	5
Variable, Wirewound, Precision	1.00	5.80	2.30	9.00	5.70	11.00		Excessive Contact Resistance	30
								Open Circuit	40
Variable, Wirewound, Semi-Precision	2.00	8.50	8.60	10.00	6.40	10.00		Erratic Operation	55
Variable, Wirewound	0.75	11.00	3.30	11.00	8.00	11.00		Erratic Operation	55
								Open Circuit	40
Variable, Plastic Film Precision								Excessive Contact Resistance	30
								Open Circuit track	60
Resistors - Pre-Set									
Pre-Set, Carbon Composition	0.20	5.00	2.30	5.50	5.00	6.00			
Pre-Set, Cermet	0.15	6.50	2.70	7.00	6.00	8.00			

Table A-1. Discrete Electronic and Electro-mechanical Components (Continued)

Component Description	Base Failure Rate λ_B $\frac{failures}{10^6 hrs}$	K Factors						Predominant Failure Modes	
	G.1	G.2	S.1	S.2	A.1	A.2			
Part	**Ground Fixed**	**Ground Mobile**	**Ship Protected**	**Ship Exposed**	**Air Protected**	**Air Exposed**		**Mode**	**% Factor**
Resistors - Pre-Set (Continued)									
Pre-Set, Wirewound	0.15	2.60	2.40	4.30	4.00	5.00			
Pre-Set, Thick/Thin Film Network DIL	0.10	5.00	4.00	5.00	9.60	13.00		Open Circuit	92
								Short Circuit	8
Synchros									
Synchro-Generator (Transmitter)	2.00	3.00	1.70	3.00	3.00	4.00		Windings Shorted	50
								Windings Open	43
Synchromotor (Receiver)	2.00	3.00	1.70	3.00	3.00	4.00		Windings Shorted	50
								Windings Open	43
Switches									
Switch, Centrifugal	1.80								
Switch, Co-Axial	0.25								
Switch, Float (Liquid Level)	5.00				N/A				
Switch, Inertia	0.40	N/A	N/A	N/A	1.50	1.50			
Switch, Limit (Heavy Duty)	10.00	5.00	2.00	5.00	3.00	6.00			
Switch, Micro (Light Duty)	0.60	5.00	2.30	5.00	5.00	7.00		Contact Resistance High	60
								Open Circuit	27
Switch, Mercury									
Switch, Pressure	5.60	4.00	1.30	5.00	10.00	16.00			
Switch, Push Button	0.32	6.00	1.50	8.50	8.00	17.00		Open Circuit	60
								Short Circuit	7
								Sticking	33
Switch, Reed	0.10	1.50							
Switch, RF									
Switch, Rotary Wafer (per active contact)	0.12	3.00	1.70	3.00	3.00	4.00		Intermittent Contact (Spring fracture and contamination)	90
Switch, Sensitive (Non-Manually Operated	0.53	8.50	2.10	12.00	18.00	24.00		Contact Resistance High	60
								Open Circuit	27

Table A-1. Discrete Electronic and Electro-mechanical Components (Continued)

Component Description	Base Failure Rate λ_B failures 10^6hrs	K Factors						Predominant Failure Modes	
	G.1	G.2	S.1	S.2	A.1	A.2			
Part	Ground Fixed	Ground Mobile	Ship Protected	Ship Exposed	Air Protected	Air Exposed		Mode	% Factor
Switches (Continued)									
Switch, Stepping	0.22	2.50	2.00	3.00	3.00	N/A			
Switch, Thermostatic	2.00	3.00	1.30	3.00	2.60	3.00		Parameter Change	63
								Open Circuit	27
								No Control	8
								Short Circuit	2
Switch, Thermal Delay	0.50	3.00	2.20	3.00	5.00	6.00		Parameter Change	63
								Open Circuit	27
								No Control	8
								Short Circuit	2
Switch, Toggle	0.40	5.70	1.10	8.00	11.00	17.00		Open Circuit	65
								Short Circuit	16
								Sticking	19
Switch, Waveguide, General	2.00	3.00	1.70	3.00	3.00	4.00			

Table A-1. Discrete Electronic and Electro-mechanical Components (Continued)

Stress Ratio for Electronic and Electro-Mechanical Components

Table A-2 through Table A-35 provide temperature and electrical stress factors (K_S) for electronic and electro-mechanical components. These values are needed to carry out the calculations referred to in“Parts Stress Analysis Methods” on page 3-15.

Table A-2. Capacitor, Fixed Ceramic

Temp °C	0	25	50	65	75	100	125	140	150
Stress Ratio (Voltage)									
0.0	.26	.27	.28	.29	.30	.32	.34	.36	.37
0.1	.27	.29	.30	.31	.32	.34	.36	.38	.39
0.2	.34	.36	.38	.39	.40	.43	.45	.45	.50
0.3	.50	.55	.59	.59	.64	.64	.68	.73	.76
0.4	.85	.91	1.00	1.00	1.05	1.09	1.18	1.23	1.23
0.5	1.45	1.55	1.64	1.73	1.73	1.86	1.95	2.05	2.09
0.6	2.32	2.50	2.64	2.73	2.77	2.95	3.14	3.27	3.32
0.7	3.55	3.77	4.00	4.14	4.27	4.50	5.00	5.00	5.00
0.75	4.21	4.53	4.86	4.94	5.20	5.35	5.84	6.03	6.03
0.8	5.00	5.45	5.91	5.91	6.36	6.36	6.82	7.27	7.27
0.9	7.27	7.73	8.18	8.64	8.64	9.09	10.00	10.00	10.45
1.0	10.00	10.45	10.91	11.36	11.82	12.73	13.18	13.64	14.08

Table A-2. Capacitor, Fixed, Ceramic

Table A-3. Capacitor, Fixed Ceramic

Temp °C	0	25	50	65	75	100	125
Stress Ratio (Voltage)							
0.0	.04	.13	.38	.69	1.03	2.86	7.62
0.1	.05	.14	.39	.71	1.05	2.90	7.85
0.2	.05	.14	.40	.72	1.08	3.01	8.06
0.3	.05	.16	.44	.80	1.18	3.32	8.92
0.4	.08	.20	.35	1.00	1.51	4.09	10.75
0.5	.11	.28	.77	1.40	2.15	5.81	16.13
0.6	.16	.43	1.18	2.15	3.23	8.82	24.73
0.7	.25	.69	1.83	3.44	5.16	13.98	37.63
0.75	.32	.86	2.30	4.30	6.40	17.34	47.17
0.8	.39	1.06	2.90	5.38	7.96	21.51	59.14
0.9	.59	1.61	4.41	8.17	11.83	33.33	90.32
1.0	.88	2.37	6.56	11.83	18.28	49.46	129.03

Table A-3. Capacitor, Fixed, Glass

Table A-4. Capacitor, Fixed, Electrolytic, Aluminium Oxide

Temp °C	0	25	50	65	75	100	125
Stress Ratio (Voltage)							
0.0	.15	.23	.40	.65	.94	2.65	11.00
0.1	.15	.24	.42	.67	.97	2.78	11.67
0.2	.16	.25	.44	.72	1.00	3.06	12.73
0.3	.19	.28	.53	.81	1.17	3.33	13.89
0.4	.23	.36	.64	1.00	1.44	4.17	17.22
0.5	.31	.47	.83	1.33	1.89	5.56	22.78
0.6	.42	.64	1.17	1.83	2.58	7.50	30.56
0.7	.58	.89	1.58	2.50	3.61	10.56	41.57
0.75	.67	1.03	1.85	2.89	4.13	12.23	
0.8	.78	1.19	2.17	3.33	4.72	14.17	
0.9	1.06	1.58	2.78	4.44	6.39		
1.0	1.39	2.11	3.89	6.11	8.61		

Table A-4. Capacitor, Fixed, Electrolytic, Aluminium Oxide

Table A-5. Capacitor, Fixed, Mica

Temp °C	0	25	50	65	75	100	125
Stress Ratio (Voltage)							
0.0	.03	.09	.25	.45	.60	1.80	3.50
0.1	.04	.10	.27	.50	.71	2.00	4.59
0.2	.04	.11	.30	.55	.86	2.21	5.06
0.3	.05	.14	.38	.69	1.07	2.86	6.47
0.4	.07	.19	.54	1.00	1.43	4.00	8.82
0.5	.11	.29	.79	1.43	2.14	5.93	13.53
0.6	.16	.43	1.14	2.14	3.21	10.71	19.41
0.7	.23	.62	1.71	3.14	4.64	15.71	28.82
0.75	.27	.73	2.04	3.73	5.41	18.65	34.15
0.8	.32	.86	2.43	4.43	6.57	22.14	40.59
0.9	.44	1.21	3.29	6.07	9.29	30.00	55.88
1.0	.59	1.64	4.43	7.86	12.14	40.71	76.47

Table A-5. Capacitor, Fixed, Mica

Table A-6. Capacitor, Fixed, Mica Button

Temp °C	0	25	50	65	75	100	125	150
Stress Ratio (Voltage)								
0.0	.40	.42	.44	.46	.48	.58	.76	1.15
0.1	.41	.44	.48	.51	.54	.66	.86	1.29
0.2	.46	.49	.53	.57	.61	.71	1.00	1.43
0.3	.58	.61	.67	.71	.79	.93	1.21	1.79
0.4	.79	.860	.93	1.00	1.07	1.29	1.71	2.50
0.5	1.21	1.29	1.36	1.50	1.57	1.93	2.50	3.71
0.6	1.79	1.86	2.07	2.21	2.36	2.86	3.79	5.50
0.7	2.57	2.71	3.00	3.21	3.43	4.14	5.43	7.86
0.75	3.06	3.23	3.52	3.83	4.08	4.930	6.53	9.47
0.8	3.64	3.86	4.14	4.57	4.86	5.86	7.86	11.43
0.9	5.07	5.36	5.86	6.29	6.64	7.86	10.71	15.71
1.0	6.79	7.14	7.86	8.57	9.29	10.71	14.29	20.71

Table A-6. Capacitor, Fixed, Mica Button

Table A-7. Capacitor, Fixed, Tantalum - Non-solid, Solid and Foil

Temp °C	0	25	50	65	75	100	125
Stress Ratio (Voltage)							
0.0	.29	.32	.40	.19	.57	1.12	3.63
0.1	.30	.33	.41	.50	.59	1.16	3.73
0.2	.33	.36	.46	.56	.66	1.30	4.08
0.3	.42	.47	.57	.70	.85	1.66	5.25
0.4	.59	.66	.80	1.00	1.17	2.31	7.23
0.5	.87	.95	1.17	1.45	1.77	3.43	10.85
0.6	1.30	1.44	1.77	2.15	2.62	5.08	15.94
0.7	1.84	2.12	2.58	3.12	3.77	7.32	
0.75	2.21	2.51	3.01	3.72	4.46	8.66	
0.8	2.65	2.96	3.62	4.43	5.27	10.25	
0.9	3.65	4.00	4.96	6.08	7.23	14.29	
1.0	4.92	5.38	6.73	8.09	10.00		

Table A-7. Capacitor, Fixed, Tantalum - Non-solid, Solid and Foil

Table A-8. Capacitor, Fixed, Paper or Plastic

Temp °C	0	25	50	65	75	100	125
Stress Ratio (Voltage)							
0.0	.41	.41	.41	.45	.50	.91	5.00
0.1	.46	.46	.46	.50	.54	.96	5.38
0.2	.46	.46	.50	.54	.58	1.00	5.38
0.3	.54	.54	.58	.62	.69	1.19	6.54
0.4	.88	.88	.92	1.00	1.12	1.92	10.77
0.5	1.81	1.81	1.88	2.04	2.23	3.85	21.92
0.6	3.81	3.85	3.85	4.23	4.62	8.46	46.15
0.7	7.69	7.69	8.08	8.85	9.62	16.92	92.31
0.75	10.60	10.60	11.15	12.10	13.19	23.23	127.79
0.8	14.62	14.62	15.38	16.54	18.08	31.92	176.92
0.9	26.15	26.15	27.69	29.62	32.31	57.69	315.38
1.0	42.31	46.15	46.15	50.00	53.85	96.15	538.46

Table A-8. Capacitor, Fixed, Paper or Plastic

Table A-9. Capacitor, Variable, Ceramic

Temp °C	0	25	50	65	75	100	125
Stress Ratio (Voltage)							
0.0	.04	.04	.05	.06	.09	.09	.25
0.1	.07	.07	.08	.09	.10	.14	.30
0.2	.14	.15	.17	.19	.21	.30	.67
0.3	.35	.37	.42	.47	.51	.77	1.65
0.4	.77	.79	.88	1.00	1.09	1.67	3.49
0.5	1.42	1.51	1.67	1.86	2.07	3.26	6.74
0.6	2.33	2.56	2.79	3.26	3.49	5.35	11.40
0.7	3.72	3.95	4.42	5.12	5.58	8.37	18.14
0.75	4.56	4.89	5.46	6.17	6.83	10.25	22.50
0.8	5.58	6.05	6.74	7.44	8.37	12.56	27.91
0.9	8.14	8.37	9.53	10.23	11.63	17.67	37.21
1.0	10.93	11.63	13.02	14.42	16.05	23.26	51.16

Table A-9. Capacitor, Variable, Ceramic

Table A-10. Capacitor, Variable, Glass

Temp °C	25	50	65	75	100	125	140	150
Stress Ratio (Voltage)								
0.0	.10	.22	.35	.47	1.01	2.08	3.40	4.56
0.1	.11	.23	.36	.50	1.06	2.24	3.55	4.81
0.2	.13	.28	.44	.59	1.26	2.70	4.23	5.73
0.3	.19	.40	.62	.86	1.80	3.83	6.06	8.20
0.4	.30	.63	1.00	1.35	2.86	6.13	9.62	13.02
0.5	.47	1.01	1.61	2.17	4.61	10.09	15.49	20.97
0.6	.73	1.59	2.48	3.30	7.21	15.57	24.25	32.83
0.7	1.29	2.39	3.74	5.13	10.58	23.30	36.47	49.38
0.75	1.55	2.87	4.49	6.12	12.88	27.75	43.86	59.38
0.8	1.87	3.45	5.39	7.30	15.69	33.04	52.74	71.40
0.9	2.65	4381	7.65	10.44	21.91	47.39	73.62	99.68
1.0	3.57	6.52	10.35	13.91	29.67	63.91	99.70	135.00

Table A-10. Capacitor, Variable, Glass

Table A-11. Diode, Germanium, General Purpose

Temp °C	0	25	50	65	75	90
Stress Ratio (Voltage)						
0.0	.01	.04	.10	.20	.31	.78
0.1	.02	.06	.17	.31	.48	1.19
0.2	.03	.09	.23	.43	.69	
0.3	.04	.12	.31	.63	1.19	
0.4	.06	.16	.43	1.00		
0.5	.08	.21	.63			
0.6	.11	.28	1.00			
0.7	.14	.38				
0.8	.19	.54				
0.9	.25	.83				
1.0	.34	1.50				

Table A-11. Diode, Germanium, General Purpose

Table A-12. Diode, Silicon, General Purpose, Power

Temp °C	0	25	50	65	75	100	125	140	150
Stress Ratio (Voltage)									
0.0	.04	.07	.12	.15	.18	.34	.42	.59	1.21
0.1	.05	.09	.17	.22	.26	.41	.67	1.00	2.10
0.2	.07	.14	.22	.28	.35	.55	1.00	1.68	
0.3	.11	.18	.28	.38	.45	.76	1.68		
0.4	.15	.24	.38	.49	.60	1.16			
0.5	.20	.32	.49	.67	.86	2.10			
0.6	.26	.41	.67	1.00	1.37				
0.7	.35	.55	1.00	1.68					
0.8	.45	.76	1.68						
0.9	.60	1.16							
1.0	.86	2.10							

Table A-12. Diode, Silicon, General Purpose, Power

Table A-13. Diode, Silicon, General Purpose, Signal/Low Power

Temp °C	0	25	50	65	75	100	125	140	150	160
Stress Ratio (Voltage)										
0.0	.08	.14	.25	.34	.38	.68	.87	1.15	1.60	2.34
0.1	.09	.19	.34	.45	.53	.82	1.36	2.02	2.77	4.26
0.2	.14	.27	.45	.57	.64	1.06	2.02	3.40		
0.3	.19	.36	.57	.77	.92	1.53	3.40			
0.4	.25	.49	.77	1.00	1.21	2.34				
0.5	.34	.64	1.00	1.36	1.74	4.26				
0.6	.47	.83	1.36	2.02	2.77					
0.7	.64	1.11	2.02	3.40						
0.8	.83	1.53	3.40							
0.9	1.13	2.34								
1.0	1.49	4.26								

Table A-13. Diode, Silicon, General Purpose, Signal/Low Power

Table A-14. Diode, Microwave Detectors and Mixers (Silicon)

Temp °C	0	25	50	65	75	100	125	135
Stress Ratio (Voltage)								
0.0	.49	.52	.57	.63	.68	.73	.95	1.32
0.1	.54	.61	.68	.73	.78	.97	1.49	2.02
0.2	.57	.64	.72	.79	.85	1.14	2.29	
0.3	.61	.68	.77	.87	.97	1.49		
0.4	.64	.73	.85	1.00	1.14	2.29		
0.5	.68	.78	.97	1.17	1.49			
0.6	.73	.84	1.14	1.55				
0.7	.78	.97	1.49					
0.8	.86	1.14	2.29					
0.9	.97	1.49						
1.0	1.14	2.29						

Table A-14. Diode, Microwave Detectors and Mixers (Silicon)

Table A-15. Diode, Microwave Detectors and Mixers (Germanium)

Temp °C	0	25	40	50	60	65
Stress Ratio (Voltage)						
0.0	.43	.53	.66	.77	1.00	1.28
0.1	.45	.58	.73	.90	1.28	1.59
0.2	.45	.62	.78	1.07	1.59	
0.3	.50	.66	.89	1.22		
0.4	.51	.72	1.00	1.51		
0.5	.53	.75	1.20			
0.6	.55	.84	1.42			
0.7	.59	.98				
0.8	.63	1.12				
0.9	.68	1.34				
1.0	.73	1.65				

Table A-15. Diode, Microwave Detectors and Mixers (Germanium)

Table A-16. Thyristor, Power

Temp °C	0	25	50	65	75	100	125	140	160
Stress Ratio (Voltage)									
0.0	.04	.07	.12	.16	.20	.31	.51	.62	1.08
0.1	.05	.10	.17	.22	.28	.44	.75	1.00	1.83
0.2	.07	.13	.322	.30	.37	.60	1.00	1.58	
0.3	.11	.18	.30	.40	.49	.83	1.58		
0.4	.15	.25	.40	.54	.67	1.17			
0.5	.20	.32	.54	.75	.92	1.83			
0.6	.28	.44	.75	1.00	1.42				
0.7	.37	.60	1.00	1.58					
0.8	.49	.83	1.58						
0.9	.67	1.17							
1.0	.92	1.83							

Table A-16. Thyristor, Power

Table A-17. Thyristor, Signal/Low Power

Temp °C	0	25	50	65	75	100	125	140	160
Stress Ratio (Voltage)									
0.0	.06	.14	.22	.29	.37	.59	.95	1.15	1.69
0.1	.09	.19	.31	.42	.51	.82	1.39	1.85	2.62
0.2	.14	.25	.42	.55	.68	1.11	1.85	2.92	
0.3	.20	.34	.55	.74	.91	1.54	2.92		
0.4	.28	.46	.74	1.00	1.25	2.15			
0.5	.37	.60	1.00	1.39	1.69	3.38			
0.6	.51	.82	1.38	1.85	2.62				
0.7	.68	1.11	1.85	2.92					
0.8	.91	1.53	2.92						
0.9	1.25	2.15							
1.0	1.69	3.39							

Table A-17. Thyristor, Signal/Low Power

Table A-18. Diode, Zener and Avalanche, Power

Temp °C	0	25	50	65	75	100	125	140	160
Stress Ratio (Voltage)									
0.0	.21	.25	.31	.34	.37	.42	.57	.67	1.17
0.1	.24	.31	.38	.42	.46	.58	.79	1.00	1.80
0.2	.28	.35	.42	.48	.52	.68	1.00	1.50	
0.3	.32	.39	.48	.55	.61	.86	1.50		
0.4	.36	.44	.55	.64	.73	1.10			
0.5	.41	.50	.64	.79	.94	1.80			
0.6	.46	.58	.79	1.00	1.30				
0.7	.52	.68	1.00	1.50					
0.8	.61	.86	1.50						
0.9	.73	1.10							
1.0	.94								

Table A-18. Diode, Zener and Avalanche, Power

Table A-19. Diode, Zener and Avalanche, Signal/Low Power

Temp °C	0	25	50	65	75	100	125	140	150	160
Stress Ratio (Voltage)										
0.0	.16	.39	.48	.53	.58	.67	.89	1.05	1.34	2.03
0.1	.38	.49	.59	.66	.72	.91	1.23	1.56	2.03	2.81
0.2	.44	.55	.66	.75	.81	1.06	1.56	2.34		
0.3	.50	.61	.75	.86	.95	1.34	2.34			
0.4	.56	.69	.86	1.00	1.14	1.72				
0.5	.64	.78	1.00	1.23	1.47	2.81				
0.6	.72	.91	1.23	1.56	2.03					
0.7	.81	1.25	1.56	2.34						
0.8	.95	1.34	2.34							
0.9	1.14	1.78								
1.0	1.47	2.81								

Table A-19. Diode, Zener and Avalanche, Signal/Low Power

Table A-20. Diode, Varactor, Step Recovery or Tunnel

Temp °C	0	25	50	65	75	100	125	140	150	160
Stress Ratio (Voltage)										
0.0	.21	.28	.39	.45	.51	.64	.85	1.04	1.44	1.96
0.1	.26	.36	.49	.57	.66	.87	1.26	1.64	2.13	2.95
0.2	.33	.44	.57	.69	.77	1.06	1.64	2.46		
0.3	.39	.52	.69	.82	.92	1.38	2.46			
0.4	.46	.61	.82	1.00	1.15	1.80				
0.5	.56	.72	1.00	1.26	1.52	2.95				
0.6	.66	.87	1.26	1.64	2.13					
0.7	.77	1.06	1.64	2.46						
0.8	.92	1.38	2.46							
0.9	1.14	1.80								
1.0	1.52	2.95								

Table A-20. Diode, Varactor, Step Recovery or Tunnel

Table A-21. Resistor, Fixed, Composition

Temp °C	0	25	50	65	75	100	120
Stress Ratio (Voltage)							
0.0	.043	.054	.24	.40	.58	1.48	3.1
0.1	.050	.13	.31	.54	.78	1.85	3.85
0.2	.064	.16	.39	.66	.92	2.35	
0.3	.071	.19	.47	.78	1.21	2.92	
0.4	.086	.22	.57	1.00	1.42	3.71	
0.5	.11	.27	.70	1.21	1.78	4.64	
0.6	.12	.32	.86	1.50	2.21		
0.7	.13	.39	1.00	1.85	2.78		
0.8	.17	.46	1.29	2.28	3.42		
0.9	.20	.56	1.50	2.78	4.21		
1.0	.24	.67	1.86	3.42			

Table A-21. Resistor, Fixed, Composition

Table A-22. Resistor, Fixed, Film

Temp °C	0	20	50	65	75	100	125	140	160	170
Stress Ratio (Voltage)										
0.0	.34	.39	.54	.60	.66	.81	1.03	1.16	1.39	1.55
0.1	.38	.46	.60	.69	.75	.94	1.19	1.38	1.63	1.81
0.2	.42	.51	.69	.81	.88	1.06	1.38	1.63	1.94	
0.3	.46	.57	.75	.88	1.00	1.25	1.63	1.88	2.25	
0.4	.51	.63	.88	1.00	1.13	1.44	1.88	2.19		
0.5	.57	.69	.94	1.13	1.25	1.63	2.13	2.50		
0.6	.63	.81	1.06	1.31	1.44	1.88	2.50	2.94		
0.7	.69	.88	1.25	1.44	1.63	2.19	2.88	3.38		
0.8	.75	1.00	1.38	1.63	1.88	2.50	3.31			
0.9	.88	1.06	1.56	1.88	2.13	2.81	3.81			
1.0	.94	1.19	1.75	2.13	2.38	3.25	4.44			

Table A-22. Resistor, Fixed, Film

Table A-23. Resistor, Fixed, Film (Power)

Temp °C	0	30	50	65	80	100	130	150	180	210
Stress Ratio (Voltage)										
0.0	.69	.71	.75	.78	.78	.80	.88	.96	1.04	1.20
0.1	.71	.75	.78	.80	.80	.88	.96	1.04	1.12	1.28
0.2	.74	.79	.80	.88	.88	.96	1.04	1.12	1.20	
0.3	.78	.80	.88	.92	.96	1.04	1.12	1.20		
0.4	.80	.88	.96	1.00	1.04	1.12	1.20	1.36		
0.5	.88	.96	1.04	1.08	1.12	1.20	1.36			
0.6	.96	1.04	1.12	1.16	1.20	1.36				
0.7	1.04	1.12	1.20	1.28	1.36					
0.8	1.12	1.20	1.28							
0.9	1.20	1.36								
1.0	1.28									

Table A-23. Resistor, Fixed, Film (Power)

Table A-24. Resistor, Fixed, Wirewound, Precision

Temp °C	0	25	50	65	75	100	125	135	140
Stress Ratio (Voltage)									
0.0	.60	.62	.65	.68	.72	.95	1.05	2.08	2.30
0.1	.62	.64	.70	.74	.79	1.04	1.68	2.26	2.64
0.2	.66	.68	.74	.81	.87	1.13	1.87	2.45	3.02
0.3	.70	.75	.81	.89	.96	1.28	2.08	2.83	
0.4	.77	.83	.92	1.00	1.09	1.47	2.45	3.40	
0.5	.85	.92	1.04	1.15	1.26	1.74	3.02	3.96	
0.6	.94	1.06	1.21	1.34	1.49	2.08	3058		
0.7	1.08	1.21	1.42	1.58	1.77	2.45	4.53		
0.8	1.23	1.40	1.66	1.89	2.08	3.02	5.66		
0.9	1.42	1.64	2.08	2.26	2.64	3.77	7.17		
1.0	1.62	1.89	2.45	2.83	3.21	4.91	9.25		

Table A-24. Resistor, Fixed, Wirewound, Precision

Table A-25. Resistor, Fixed, Wirewound, Power

Temp °C	0	20	40	65	80	100	130	160	200	250	300
Stress Ratio (Voltage)											
0.0	.22	.26	.30	.35	.41	.48	.52	.78	1.30	2.60	4.50
0.1	.29	.33	.39	.47	.54	.64	.83	1.17	1.79	3.24	6.28
0.2	.35	.47	.49	.61	.69	.83	1.17	1.59	2.55	4.14	
0.3	.43	.51	.61	.79	.90	1.10	1.52	2.21	3.59	6.90	
0.4	.52	.63	.76	1.00	1.17	1.45	2.07	2.97	5.20		
0.5	.64	.76	.96	1.27	1.52	1.93	2.76	4.14			
0.6	.76	.96	1.24	1.62	1.93	2.55	3.72				
0.7	.96	1.17	1.52	2.07	2.55	3.31					
0.8	1.17	1.52	1.93	2.69	3.31						
0.9	1.45	1.86	2.41								
1.0	1.72	2.28									

Table A-25. Resistor, Fixed, Wirewound, Power

Table A-26. Resistor, Variable, Wirewound

Temp °C	0	25	50	65	75	100	125	140
Stress Ratio (Voltage)								
0.0	.37	.43	.54	.60	.68	.96	1.53	2.20
0.1	.40	.45	.59	.68	.77	1.09	1.77	2.55
0.2	.44	.55	.64	.77	.86	1.27	2.05	
0.3	.50	.59	.73	.86	1.00	1.45	2.68	
0.4	.55	.64	.82	1.00	1.14	1.68		
0.5	.59	.73	.91	1.09	1.27	1.91		
0.6	.68	.82	1.05	1.27	1.45	2.18		
0.7	.73	.91	1.18	1.41	1.64	2.50		
0.8	.82	1.00	1.32	1.59	1.86			
0.9	.91	1.14	1.50	1.82	2.14			
1.0	1.00	1.27	1.68	2.05	2.41			

Table A-26. Resistor, Variable, Wirewound

Table A-27. Resistor, Variable, Wirewound Precision

Temp °C	0	25	50	65	75	100	125	140
Stress Ratio (Voltage)								
0.0	.43	.53	.65	.78	.83	1.12	1.80	2.45
0.1	.45	.55	.68	.82	.91	1.27	2.00	2.73
0.2	.50	.59	.73	.86	1.00	1.41	2.27	
0.3	.50	.59	.77	.95	1.09	1.59	2.64	
0.4	.55	.64	.82	1.00	1.18	1.77		
0.5	.55	.68	.91	1.09	1.27	2.00		
0.6	.55	.73	.95	1.18	1.36	2.23		
0.7	.59	.73	1.00	1.27	1.50	2.45		
0.8	.29	.77	1.09	1.36	1.64			
0.9	.64	.82	1.18	1.50	1.77			
1.0	.64	.86	1.23	1.59	1.95			

Table A-27. Resistor, Variable, Wirewound Precision

Table A-28. Resistor, Variable, Composition

Temp °C	0	20	40	50	65	80	100	115
Stress Ratio (Voltage)								
0.0	.42	.44	.48	.52	.60	.71	.98	1.78
0.1	.43	.46	.52	.57	.67	.84	1.33	2.22
0.2	.44	.49	.57	.62	.76	1.00	1.75	
0.3	.48	.52	.62	.70	.87	1.17	2.06	
0.4	.49	.56	.68	.78	1.00	1.40	2.54	
0.5	.51	.59	.75	.86	1.14	1.59		
0.6	.54	.63	.81	.95	1.30	1.90		
0.7	.56	.67	.89	1.06	1.49	2.38		
0.8	.59	.71	.97	1.17	1.75	2.70		
0.9	.60	.76	1.06	1.48	1.90			
1.0	.63	.81	1.16	1.59	2.22			

Table A-28. Resistor, Variable, Composition

Table A-29. Transistor, Field Effect

Temp °C	0	25	50	65	75	100	125	140	150	160
Stress Ratio (Voltage)										
0.0	.22	.28	.40	.46	.51	.63	.86	1.15	1.47	1.88
0.1	.27	.35	.50	.59	.65	.85	1.26	1.71	2.24	2.84
0.2	.32	.44	.59	.68	.76	1.06	1.71	2.59		
0.3	.38	.53	.68	.82	.91	1.38	2.59			
0.4	.47	.62	.82	1.00	1.15	1.94				
0.5	.56	.71	1.00	1.26	1.53	2.94				
0.6	.65	.85	1.26	1.71	2.24					
0.7	.76	1.06	1.71	2.59						
0.75	.83	1.20	2.14							
0.8	.91	1.38	2.59							
0.9	1.15	1.94								
1.0	1.53	2.94								

Table A-29. Transistor, Field Effect

Table A-30. Transistor, Germanium (NPN and PNP)

Temp °C	0	25	50	65	75	85	90
Stress Ratio (Voltage)							
0.0	.06	.11	.20	.30	.40	.59	.74
0.1	.08	.14	.26	.41	.57	.90	1.18
0.2	.09	.18	.33	.52	.79	1.39	
0.3	.11	.21	.41	.70	1.17		
0.4	.14	.25	.52	1.00			
0.5	.16	.31	.70				
0.6	.20	.38	1.00				
0.7	.24	.47					
0.75	.26	.55					
0.8	.28	.64					
0.9	.34	.90					
1.0	.43	1.38					

Table A-30. Transistor, Germanium (NPN and PNP)

Table A-31. Transistor, Silicon, Power (NPN and PNP)

Temp °C	0	25	50	65	75	100	125	140	160
Stress Ratio (Voltage)									
0.0	.12	.16	.22	.25	.28	.35	.51	.67	1.10
0.1	.15	.21	.28	.32	.37	.48	.73	1.00	1.75
0.2	.19	.25	.32	.40	.44	.63	1.00	1.50	
0.3	.22	.30	.40	.47	.54	.82	1.50		
0.4	.27	.35	.47	.58	.67	1.15			
0.5	.31	.41	.58	.73	.89	1.75			
0.6	.37	.48	.73	1.00	1.28				
0.7	.44	.63	1.00	1.50					
0.8	.54	.82	1.50						
0.9	.67	1.15							
1.0	.89	1.75							

Table A-31. Transistor, Silicon, Power (NPN and PNP)

Table A-32. Transistor, Silicon, Signal/Low Power (NPN and PNP)

Temp °C	0	25	50	65	75	100	125	140	160
Stress Ratio (Voltage)									
0.0	.21	.28	.39	.44	.50	.61	.88	1.15	1.85
0.1	.26	.36	.49	.56	.64	.84	1.25	1.73	3.02
0.2	.32	.43	.56	.69	.76	1.09	1.73	2.60	
0.3	.38	.52	.69	.81	.93	1.42	2.60		
0.4	.46	.60	.81	1.00	1.14	1.98			
0.5	.54	.71	1.00	1.26	1.54	3.02			
0.6	.64	.84	1.25	1.73	2.22				
0.7	.76	1.09	1.73	2.60					
0.75	.84	1.25	2.15						
0.8	.93	1.42	2.60						
0.9	1.17	1.98							
1.0	1.54	3.02							

Table A-32. Transistor, Silicon, Signal/Low Power (NPN and PNP)

Table A-33. Transistor, Unijunction

Temp °C	0	25	50	65	75	100	125	140	150	160
Stress Ratio (Voltage)										
0.0	.11	.17	.28	.35	.42	.58	.91	1.26	1.58	2.09
0.1	.15	.23	.37	.47	.56	.84	1.35	1.93	2.56	3.49
0.2	.20	.30	.47	.61	.72	1.09	1.93	3.02		
0.3	.26	.40	.61	.77	.91	1.49	3.02			
0.4	.35	.51	.77	1.00	1.21	2.21				
0.5	.44	.65	1.00	1.35	1.70	3.49				
0.6	.56	.84	1.35	1.93	2.56					
0.7	.72	1.09	1.93	3.02						
0.75	.81	1.26	2.42							
0.8	.91	1.49	3.02							
0.9	1.21	2.21								
1.0	1.70	3.49								

Table A-33. Transistor, Unijunction

Table A-34. Relays

Temp °C	0	25	50	65	70	85	100	125
Component								
Relay								
Rated 85°C	0.51	0.61	0.74	1.00	1.13	2.15		
Rated 125°C	0.68	0.79	0.88	1.00	1.05	1.29	1.73	4.13

Table A-34. Relays

Table A-35. Synchros and Resolvers

Frame Temp °C	0	25	50	65	75	100	125	135
Component								
Synchros and Receivers	0.45	0.51	0.70	1.00	1.36	4.26	28.0	79.0

Table A-35. Synchros and Resolvers

Connectors

Table A-36 and Table A-37 provide cycling failure rates and active pin factors for connectors.

Table A-36. Connectors - Cycling Failure Rates

Connectors - Cycling Failure Rates (λ_{cyc})			
Cycling Rate (Cycles per 1000 Operating Hours)	**Cycling Failure Rate λ_{cyc} (Failures per 10^6 hours)**	**Cycling Rate (Cycles per 1000 Operating Hours)**	**Cycling Failure Rate λ_{cyc} (Failures per 10^6 hours)**
Less than 10	0.00		
10	0.0011	260	.0.135
20	0.0012	270	0.0149
30	0.0013	280	0.0164
40	0.0015	290	0.0182
50	0.0016	300	0.0201
60	0.0018	310	0.0222
70	0.0020	320	0.0245
80	0.0022	330	0.0271
90	0.0025	340	0.0300
100	0.0027	350	0.0331
110	0.0030	360	0.0366
120	0.0033	370	0.0404
130	0.0037	380	0.0447
140	0.0041	390	0.0494
150	0.0045	400	0.0546
160	0.0050	410	0.0603
170	0.0055	420	0.0667
180	0.0060	430	0.0737
190	0.0067	440	0.0815
200	0.0074	450	0.0900
210	0.0082	460	0.0995
220	0.0090	470	0.1099
230	0.0100	480	0.1215
240	0.0110	490	0.1343
250	0.0122	500	0.1484

Table A-36. Connectors - Cycling Failure Rates

Table A-37. Connectors - Active Pin Factors

Connectors - Active Pin Factors (K_P)			
Number of Active Pins (Contacts) N_P	K_P	Number of Active Pins (Contacts) N_P	K_P
1	1.00	65	13.20
2	1.36	70	14.60
3	1.55	75	16.10
4	1.72	80	17.69
5	1.87	85	19.39
6	2.02	90	21.19
7	2.16	95	23.10
8	2.30	100	25.13
9	2.44	105	27.28
10	2.58	110	29.56
11	2.72	115	31.98
12	2.86	120	34.53
13	3.00	125	37.22
14	3.14	130	40.07
15	3.28	135	43.08
16	3.42	140	46.25
17	3.57	145	49.60
18	3.71	150	53.12
19	3.86	155	56.83
20	4.00	160	60.74
25	4.78	165	64.85
30	5.60	170	69.17
35	6.46	175	73.70
40	7.42	180	78.47
45	8.42	185	83.47
50	9.50	190	88.72
55	10.65	195	94.23
60	11.89	200	100.00

Table A-37. Connectors - Active Pin Factors

Microelectronic Devices (Excluding Hybrids)

Table A-38 through Table A-48 provide information for all microelectronic devices, excluding hybrids.

Table A-38. Bi-Polar Beam Lead, ECL, All Linear and All MOS Devices - Generic Failure Rates, Environmental Factors and Failure Modes

Non-operational		Operational							
Base Failure Rate λ_b failures 10^6 hrs	Bipolar Beam Lead, ECL All Linear and MOS Devices	Base Failure Rate λ_b failures 10^6 hrs	Environmental Factors (K_E)					Predominant Failure Modes	
GFP		G.1	G.2	S.1	S.2	A.1	A.2	Mode	% Factor
Ground Fixed Protected	Circuit Complexity	Ground Fixed	Ground Mobile	Ship Protected	Ship Exposed	Air Protected	Air Exposed		
0.005	1- 20 Gates	0.05	2.5	2.9	5.2	2.5	5.0		
0.019	21- 50	0.19	1.8	2.3	4.8	1.8	4.2		
0.031	51 -l00	0.31	1.7	2.2	4.8	1.7	4.2		
0.082	101-500	0.82	1.6	2.1	4.8	1.6	3.9		
0.14	50l -l000	1.40	1.5	2.0	4.6	1.5	3.8		
0.31	1001-200	3.10	1.5	2.1	4.8	1.5	3.9		
0.84	2001-3000	8.40	1.5	2.0	4.9	1.5	3.9	Loss of Output	90
2.30	3001-4000	23.00	1.6	2.0	4.8	1.6	3.9		
6.2	4001-5001	62.00	1.6	2.1	4.8	1.6	3.9		
	Read-only Memories (ROM)								
0.009	<320 Bits	0.09	1.6	2.1	4.8	1.6	3.9	Open Input	10
0.013	321 - 576	0.13	1.5	2.1	4.8	1.5	3.9		
0.02	577 - 1120	0.20	1.6	2.1	4.9	1.6	4.0		
0.03	1121 - 2240	0.30	1.6	2.1	5.0	1.6	4.0		
0.046	2241 - 5000	0.46	1.6	2.1	4.8	1.6	3.9		
0.07	500l - 1l000	0.70	1.6	2.1	4.8	1.6	4.0		
0.11	11001 - 17000	1.10	1.5	2.0	4.7	1.5	3.9		
	Random Access Memories (RAM)								
0.032	<320 Bits	0.32	1.6	2.1	4.8	1.6	3.9		
0.046	321 - 576	0.46	1.5	2.1	4.8	1.5	3.9		
0.070	577 - 1120	0.70	1.6	2.1	4.9	1.6	4.0		
0.105	1121 - 2240	1.05	1.6	2.1	5.0	1.6	4.0		
0.161	2241 - 5000	1.61	1.6	2.1	4.8	1.6	3.9		
0.245	500l - l1000	2.45	1.6	2.1	4.8	1.6	4.0		
0.385	11001 - 17000	3.85	1.5	2.0	4.7	1.5	3.9		
0.032	<320 Bits	0.32	1.6	2.1	4.8	1.6	3.9		
0.005 Linear	< 32 Transistors	0.05	2.9	3.1	5.2	2.9	5.2		
0.011 Linear	33 - 100 Transistor	0.11	2.8	3.2	5.4	2.8	5.4		

Table A-38. Bi-Polar Beam Lead, ECL, All Linear and All MOS Devices - Generic Failure Rates, Environmental Factors and Failure Modes

Table A-39. Bi-Polar Digital Devices (TM and DTL) Generic Failure Rates, Environmental Factors and Failure Modes

Non-operational		Operational							
Base Failure Rate λ_b failures 10^6 hrs	Bipolar Digital Devices TTL and DTL	Base Failure Rate λ_b failures 10^6 hrs	Environmental Factors (K_E)					Predominant Failure Modes	
GFP		G.1	G.2	S.1	S.2	A.1	A.2	Mode	% Factor
Ground Fixed Protected	Circuit Complexity	Ground Fixed	Ground Mobile	Ship Protected	Ship Exposed	Air Protected	Air Exposed		
0.003	1- 20 Gates	0.03	3.1	3.2	4.1	3.1	4.8		
0.006	21- 50	0.06	2.6	2.7	3.7	2.6	4.0		
0.009	51 -l00	0.09	2.4	2.4	3.6	2.4	3.8		
0.022	101-500	0.22	2.0	2.2	3.2	2.0	3.3		
0.034	50l -l000	0.34	2.0	2.1	3.2	2.0	3.2		
0.078	1001-200	0.78	1.9	2.2	3.2	1.9	3.2		
0.210	2001-3000	2.10	1.9	2.1	3.2	1.9	3.2		
0.570	3001-4000	5.70	1.9	2.1	3.2	1.9	3.2		
1.600	4001-5001	16.00	1.9	2.1	3.1	1.9	3.1	High Output (1)	60
								Low Output (0)	30
	Read-only Memories (ROM)								
0.002	<320 Bits	0.02	1.9	2.2	3.2	1.9	3.2	Open Input	10
0.003	321 - 576	0.03	2.0	2.2	3.3	2.0	3.3		
0.005	577 - 1120	0.05	1.9	2.1	3.3	1.9	3.3		
0.008	1121 - 2240	0.08	2.0	2.2	3.2	2.0	3.3		
0.012	2241 - 5000	0.12	2.0	2.2	3.2	2.0	3.2		
0.018	500l - 1l000	0.18	2.1	2.3	3.3	2.1	3.4		
0.028	11001 - 17000	0.28	2.1	2.2	3.3	2.1	3.4		
	Random Access Memories (RAM)								
0.007	<320 Bits	0.07	1.9	2.2	3.2	1.9	3.2		
0.011	321 - 576	0.11	2.0	2.2	3.3	2.0	3.3		
0.018	577 - 1120	0.18	1.9	2.1	3.3	1.9	3.3		
0.028	1121 - 2240	0.28	2.0	2.2	3.2	2.0	3.3		
0.042	2241 - 5000	0.42	2.0	2.2	3.2	2.0	3.2		
0.063	500l - l1000	0.63	2.1	2.3	3.3	2.1	3.4		
0.098	11001 - 17000	0.96	2.1	2.2	3.3	2.1	3.4		

Table A-39. Bi-Polar Digital Devices (TM and DTL) - Generic Failure Rates, Environmental Factors and Failure Modes

Table A-40. Summary of Failure Rate Models, Factors and Data Tables

Linear	Digital: Small and Medium Scale Integration (SS/MSI) Less than 100 gates or 400 transistors	Digital: Large Scale Integration (LSI) and Micro-processor Devices More than 100 gates or 400 transistors (See Note 1 below)	Memories RAMS and CAMS; ROMS and PROMS Static and dynamic shift registers
$\lambda_p = K_Q(C_1 \cdot K_T + C_2 \cdot K_E)$	$\lambda_p = K_Q \cdot K_P(C_1 \cdot K_T + C_2 \cdot K_E)$		

Where:

λ_p = Total failure rate of the device in failures/10^6 operating hours.

K_Q = The Quality factor, obtained from Table A-41 for all devices.

K_E = The Environmental factor, obtained from Table A-42 for all devices.

K_T = The Temperature Acceleration factor, obtained from Table A-43 for all devices.

C_1 and C_2 = The Circuit Complexity failure rates, based on the number of transistors for linear devices, the number of gates for digital devices and the number of bits for memories. They are obtained from:

- Table A-44 for linear devices.
- Table A-45 for digital SSI/MSI devices.
- Table A-46 for digital LSI and microprocessor devices.
- Table A-47 for memories.

K_P = The Pin factor, obtained from Table A-45 through Table A-47 for devices as shown above.

Note 1: A J-K (grating) or R-S (set and re-set) flip-flop is equivalent to 8 gates when used as part of a complex circuit.

Note 2: For shift registers larger than dual 8-bit, the RAM model should be used. For smaller shift registers, the digital SSM/MSI model should be used.

Table A-40. Summary of Failure Rate Models, Factors and Data Tables

Table A-41. Quality Factors for Microelectronic Devices

Screening Level	BS 9000				
	S1	S2	S3	S4	Full Assessment
Quality Factor, K_Q	0.5	1.0	2.5	5.0	8.0

Table A-41. Quality Factors for Microelectronic Devices

Table A-42. Environmental Factors for Microelectronic Devices

Operational Environment (See Note1 below)		K_E
Ground Fixed	G1	1.0
Ground Mobile	G2	4.0
Ship Protected	S1	4.0
Ship Exposed	S2	5.0
Air Protected	A1	4.0
Air Exposed	A2	6.0
Note: The environments are described in Table A-57.		

Table A-42. Environmental Factors for Microelectronic Devices

Table A-43. Temperature Acceleration Factors Vs. Junction Temperature

$T_j(°C)$	K_{T1}	K_{T2}	$T_j(°C)$	K_{T1}	K_{T2}	$T_j(°C)$	K_{T1}	K_{T2}	$T_j(°C)$	K_{T1}	K_{T2}
25	.10	.10	51	.36	.89	77	1.1	5.7	103	2.8	29.0
27	.11	.12	53	.40	1.00	79	1.2	6.5	105	3.0	32.0
29	.12	.14	55	.44	1.20	81	1.3	7.5	110	3.6	42.0
31	.14	.17	57	.48	1.40	83	1.4	8.5	115	4.2	56.0
33	.15	.20	59	.52	1.60	85	1.5	9.6	120	4.9	73.0
35	.17	.24	61	.57	1.90	87	1.6	11.0	125	5.7	94.0
37	.19	.29	63	.62	2.20	89	1.7	12.0	135	7.6	155.0
39	.21	.34	65	.67	2.50	91	1.8	14.0	145	10.0	250.0
41	.23	.40	67	.73	2.90	93	2.0	16.0	155	13.0	393.0
43	.25	.47	69	.79	3.30	95	2.1	18.0	165	17.0	607.0
45	.28	.56	71	.86	3.80	97	2.3	20.0	175	22.0	918.0
47	.30	.65	73	.93	4.40	99	2.5	23.0			
49	.33	.76	75	1.00	5.00	101	2.6	25.0			

Notes:

1. K_{T1} is applicable to Bipolar digital devices, i.e., TTL and DTL, and to I^2L. It does not apply to Bipolar Beam Lead and Bipolar ECL. (See Note 2.)

2. K_{T2} is applicable to Bipolar and MOS Linear, Bipolar Beam Lead, Bipolar ECL and all other MOS devices.

3. In the table above, T_j is the worst-case junction temperature in $°C$. If T_j is unknown, use the following approximations for all microcircuit types except low power TTL and MOS:

   T_j = ambient $T(°C) + 10°C$ if the number of gates < 30 or the number of linear circuit transistors < 120.

   T_j = ambient $T(°C) + 25°C$ if the number of gates > 30 or the number of linear circuit transistors > 120 and for all memories.

   For low power TTL, MOS and I^2L, use the following approximations if T_j is unknown:

   T_j = ambient $T(°C) + 5°C$ if the number of gates < 30 or the number of linear circuit transistors < 120.

   T_j = ambient $T(°C) + 13°C$ if the number of gates > 30 or the number of linear circuit transistors > 120 and for all memories.

Table A-43. Temperature Acceleration Factors Vs. Junction Temperature

Table A-44. Linear Devices - Complexity Failure Rates

No. of Transistors	Failure/10^6 hrs		No. of Transistors	Failure/10^6 hrs		No. of Transistors	Failure/10^6 hrs	
	C1	C2		C1	C2		C1	C2
4	.0016	.0056	64	.013	.025	148	.025	.040
8	.0027	.0081	68	.014	.026	156	.026	.041
12	.0037	.010	72	.015	.027	164	.027	.042
16	.0046	.012	76	.015	.028	172	.028	.043
20	.0055	.013	80	.016	.029	180	.029	.045
24	.0063	.015	84	.016	.029	188	.030	.046
28	.0071	.016	88	.017	.030	196	.031	.047
32	.0079	.017	92	.618	.031	204	.032	.048
36	.0086	.018	96	.018	.032	220	.034	.050
40	.0093	.020	100	.019	.032	236	.036	.052
44	.010	.021	108	.020	.034	252	.038	.054
48	.011	.022	116	021	.035	268	.040	.055
52	.011	.023	124	.022	.036	284	.042	.057
56	.012	.024	132	.023	.038	300	.043	.059
60	.013	.024	140	.024	.039			

Table A-44. Linear Devices - Complexity Failure Rates

Table A-45. SSI/SMI Devices - Complexity Failure Rates and Pin Factors

No. of Gates	Failure/10^6 hrs		No. of Gates	Failure/10^6 hrs		No. of Gates	Failure/10^6 hrs	
	C1	C2		C1	C2		C1	C2
1	.0013	.0039	30	.013	.013	60	.021	.017
2	.0021	.0050	32	.013	.013	62	.021	.017
4	.0033	.0064	34	.014	.014	64	.022	.017
6	.0043	.0074	36	.015	.014	66	.022	.018
8	.0053	.0082	38	.015	.014	68	.022	.018
10	.0061	.0089	40	.016	.015	70	.023	.018
12	.0069	.0095	42	.0l6	.015	72	.023	.018
14	.0077	.010	44	.017	.015	74	.024	.018
16	.0084	.011	46	.017	.015	76	.024	.018
18	.0091	.011	48	.018	.016	78	.025	.019
20	.0098	.011	50	.018	.016	80	.025	.019
22	.010	.012	52	.019	.0l6	85	.026	.019
24	.011	.012	54	.019	.016	90	.027	.020
26	.012	.013	56	.020	.017	95	.028	.020
28	.012	.013	58	.020	.017	99	.029	.020

The pin factor, K_P, is based upon the number of pins (package leads) and is:

No. of Pins	K_P
< 24	1.0
24 to 40	1.1
41 to 64	1.2
> 64	1.3

Table A-45. SSI/SMI Devices - Complexity Failure Rates and Pin Factors

Table A-46. LSI Devices - Complexity Failure Rates and Pin Factors

No. of Gates	Failure/10^6 hrs		No. of Gates	Failure/10^6 hrs		No. of Gates	Failure/10^6 hrs	
	C1	C2		C1	C2		C1	C2
100	.029	.020	950	.13	.046	4200	3.4	1.1
150	.038	.024	1000	.14	.046	4400	4.2	1.4
200	.047	.026	1200	.17	.057	4600	5.1	1.7
250	.054	.028	1400	.21	.069	4800	6.2	2.1
300	.061	.030	1600	.25	.085	5000	7.6	2.5
350	.068	.032	1800	.31	.100	5200	9.2	3.1
400	0.75	.033	2000	.38	.130	5400	11.0	3.8
450	.081	.035	2200	.46	.150	5600	14.0	4.6
500	.087	.036	2400	.56	.190	5800	17.0	5.6
550	.092	.037	2600	.69	.230	6000	21.0	6.9
600	.098	.039	2800	.84	.280	6200	25.0	8.4
650	.100	.040	3000	1.0	.340	6400	31.0	10.0
700	.110	.041	320	1.3	.420	6600	37.0	13.0
750	.110	.042	3400	1.5	.510	6800	46.0	15.0
800	.120	.043	3600	1.9	.630	7000	56.0	19.0
850	.120	.044	3800	2.3	.760			
900	.130	.045	4000	2.8	.930			

The pin factor, K_P , is based upon the number of pins (package leads) and is:

No. of Pins	K_P
< 26	1.0
26 to 64	1.1
> 64	1.2

Table A-46. LSI Devices - Complexity Failure Rates and Pin Factors

Table A-47. Memories - Complexity Failure Rates and Pin Factors

No. of Bits	ROMS (including PROMS)		ROMS (including PROMS)	
	C1	C2	C1	C2
16	.0015	.00048	.0053	.00l7
32	.0023	.00075	.0080	.0026
64	.0035	.0012	.012	.0041
128	.0053	.0018	.019	.0064
256	.0081	.0029	.028	.010
320	.0092	.0033	.032	.011
512	.012	.0045	.043	.016
576	.013	.0049	.046	.017
1024	.019	.0070	.065	.024
1120	.020	.0075	.069	.026
1280	.021	.0081	.074	.028
2048	.028	.011	.099	.038
2240	.030	.012	.l0	.040
2560	.032	.013	.11	.044
4096	.043	.017	.15	.059
8192	.065	.027	.23	.093
9216	.070	.029	.24	.l0
10240	.075	.031	.26	.11
12288	.083	.035	.29	.12
14848	.093	.040	.33	.14
16384	.099	.042	.35	.14

The pin factor, K_P , is based upon the number of pins (package leads) and is:

No. of Pins	K_P
≤ 24	1.0
> 24	1.2

Table A-47. Memories - Complexity Failure Rates and Pin Factors

Microelectronic Hybrid Devices

Table A-48 through Table A-55 provide information for microelectronic hybrid devices.

Table A-48. Die Correction Factors

Component	Applicable to:	K_G
Integrated Circuits	All Linear devices, Digital devices < than 400 gates, and Memories < 4000 bits	0.6
	All Digital devices > 400 gates	0.8
	Memories > 4000 bits	0.4
Transistors		0.4
Diodes		0.2
Capacitor Chips		0.8

Table A-48. Die Correction Factors

Table A-49. Base Failure Rates for Chip and Substrate Resistors

Temperature of Hybrid Package °C	Base Failure Rate λ_r
Below 50 °C	0.00010
51 °C - 80 °C	0.00015
81 °C - 100 °C	0.00020
101 °C - 125 °C	0.00025
126 °C - 150 °C	0.00030

Table A-49. Base Failure Rates for Chip and Substrate Resistors

Table A-50. Base Failure Rates for Interconnections in a Hybrid Device

Hybrid Package Temperature °C	Base Failure Rate λ_t per 10^6 hours per bond	
	Bi-metal Bonds (Gold/Aluminium)	Single Metal Bonds (Aluminium/Aluminium) Gold/Gold or Solder)
25	0.000174	0.000174
30	0.000230	0.000218
35	0.000302	0.000271
40	0.000394	0.000334
45	0.000508	0.000410
50	0.000650	0.000499
55	0.000826	0.000604
60	0.00104	0.000727
65	0.00130	0.000871
70	0.00162	0.00103
75	0.00201	0.00123
80	0,00247	0.00145
85	0.00302	0.00170
90	0.00367	0.00199
95	0.00444	0.00231
100	0.00534	0.00268
105	0.00639	0.00310
110	0.00762	0.00356
115	0.00904	0.00409
120	0.0106	0.00467
125	0.0125	0.00531
130	0.0147	0.00603
135	0.0171	0.00682
140	0.0199	0.00770
145	0.0231	0.00866
150	0.0266	0.00971
Note: If metal system is unknown, assume bi-metal bonds.		

Table A-50. Base Failure Rates for Interconnections in a Hybrid Device

Table A-51. Base Failure Rates for Hybrid Packages

	Package Temperature $^{\circ}C$								
Seal Perimeter (inches)	25 $^{\circ}C$ 70 $^{\circ}C$	30 $^{\circ}C$ 90 $^{\circ}C$	35 $^{\circ}C$ 90 $^{\circ}C$	40 $^{\circ}C$ 100 $^{\circ}C$	45 $^{\circ}C$ 110 $^{\circ}C$	50 $^{\circ}C$ 120 $^{\circ}C$	55 $^{\circ}C$ 130 $^{\circ}C$	60 $^{\circ}C$ 140 $^{\circ}C$	65 $^{\circ}C$ 150 $^{\circ}C$
1.75	0.0011 0.0113	0.0015 0.0174	0.0020 0.0261	0.0026 0.0383	0.0034 0.0551	0.0044 0.0778	0.0056 0.1081	0.0072 0.1478	0.0090 0.1990
2.00	0.0017 0.0167	0.0023 0.0257	0.0030 0.0385	0.0039 0.0566	0.0051 0.0815	0.0065 0.1151	0.0084 0.1599	0.0106 0.2186	0.0134 0.2944
2.25	0.0024 0.0235	0.0032 0.0362	0.0042 0.0543	0.0055 0.0798	0.0071 0.1148	0.0092 0.1622	0.0118 0.2253	0.0149 0.3079	0.0188 0.4148
2.50	0.0032 0.0319	0.0043 0.0491	0.0057 0.0736	0.0075 0.1081	0.0097 0.1556	0.0125 0.2199	0.0160 0.3054	0.0202 0.4175	0.0255 0.5642
2.75	0.0042 0.0420	0.0057 0.0645	0.0075 0.0968	0.0098 0.1421	0.0127 0.2045	0.0164 0.2890	0.0210 0.4014	0.0266 0.5487	0.0335 0.7390
3.00	0.0054 0.0537	0.0073 0.0825	0.0096 0.1239	0.0126 0.1819	0.0163 0.2618	0.0210 0.3700	0.0268 0.5138	0.0341 0.7024	0.0429 0.9461
3.25	0.0068 0.0673	0.0091 0.1034	0.0120 0.1551	0.0157 0.2278	0.0204 0.3279	0.0263 0.4633	0.0336 0.6435	0.0427 0.8797	0.0537 1.1848
3.50	0.0084 0.0827	0.0112 0.1270	0.0147 0.1906	0.0193 0.2800	0.0251 0.4030	0.0323 0.5694	0.0413 0.7908	0.0524 1.0810	0.0660 1.4560
3.75	0.0101 0.0999	0.0135 0.1536	0.0178 0.2305	0.0233 0.3384	0.0303 0.4871	0.0391 0.6883	0.0499 0.9559	0.0634 1.3067	0.0798 1.7600
4.00	0.0120 0.1191	0.0161 0.1830	0.0212 0.2746	0.0278 0.4032	0.0361 0.5804	0.0465 0.8201	0.0595 1.1390	0.0755 1.5569	0.0951 2.0971
4.50	0.0165 0.1629	0.0220 0.2503	0.0291 0.3757	0.0381 0.5517	0.0494 0.7940	0.0637 1.1219	0.0814 1.5582	0.1033 2.1300	0.1301 2.8690
5.00	0.0216 0.2138	0.0287 0.3286	0.0381 0.4932	0.0500 0.7242	0.0649 1.0424	0.0836 1.4728	0.1069 2.0456	0.1356 2.7963	0.1708 3.7663
5.50	0.0275 0.2713	0.0366 0.4170	0.0484 0.6258	0.0634 0.9191	0.0823 1.3228	0.1061 1.8691	0.1356 2.5959	0.1721 3.5485	0.2168 4.7795
6.00	0.0339 0.3347	0.0452 0.5143	0.0597 0.7720	0.0782 1.1336	0.1016 1.6317	0.1308 2.3054	0.1673 3.2020	0.2122 4.3770	02674 5.8954
6.50	0.0408 0.4030	0.0544 0.6193	0.0719 0.9295	0.0942 1.3650	0.1223 1.9646	0.1575 2.7759	0.2014 3.8554	0.2555 5.2702	0.3220 7.0985
7.00	0.0481 0.4753	0.0642 0.7304	0.0848 1.0962	0.1111 1.6097	0.1442 2.3170	0.1858 3.2737	0.2375 4.5468	0.3014 6.2153	0.3797 8.3714
7.50	0.0557 0.5505	0.0743 0.8460	0.0982 1.2697	0.1286 1.8646	0.1671 2.6838	0.2152 3.7920	0.2751 5.2666	0.3491 7.1993	0.4398 9.6968
8.00	0.0635 0.6277	0.0847 0.9647	0.1120 1.4478	0.1467 2.1262	0.1905 3.0603	0.2454 4.3239	0.3137 6.0055	0.3491 8.2093	0.4398 11.0572

Table A-51. Base Failure Rates for Hybrid Packages

Table A-52. Circuit Function Factors

Type of Hybrid Circuit	Circuit Function Factor K_F
Digital	1.0
Linear or Linear- Digital Combination	1.25

Table A-52. Circuit Function Factors

Table A-53. Environmental Factors For Resistors, Interconnections and Packages in a Hybrid Device

Operational Environment (See Note1 below)		K_E
Ground Fixed	G1	1.0
Ground Mobile	G2	2.0
Ship Protected	S1	2.0
Ship Exposed	S2	3.0
Air Protected	A1	3.0
Air Exposed	A2	36.0
Note: The environments are described in Table A-57.		

Table A-53. Environmental Factors For Resistors, Interconnections and Packages in a Hybrid Device

Table A-54. Quality Factors for a Hybrid Device

Screening Level	BS 9000				
	S1	S2	S3	S4	Full Assessment
Quality Factors, K_Q	0.5	1.0	2.5	5.0	8.0

Table A-54. Quality Factors for a Hybrid Device

Table A-55. Density Factors for a Hybrid Device

Density Factors (K_D) for a Hybrid Device

$$Density = \frac{\text{Number of Interconnections}}{(A_S + 0.10)}$$

Where A_S = area of substate (sq. inches)

$$K_D = 0.2 + (0.15\sqrt{Density})$$

Density	K_D	Density	K_D
15	0.78	160	2.10
20	0.87	165	2.13
25	0.95	170	2.16
30	1.02	175	2.18
35	1.09	180	2.21
40	1.15	185	2.24
45	1.21	190	2.27
50	1.26	195	2.29
55	1.31	200	2.32
60	1.36	205	2.35
65	1.41	210	2.37
70	1.45	215	2.40
75	1.50	220	2.42
80	1.54	225	2.45
85	1.58	230	2.47
90	1.62	235	2.50
95	1.66	240	2.52
100	1.70	245	2.55
105	1.74	250	2.57
110	1.77	255	2.60
115	1.81	260	2.62
120	1.84	265	2.64
125	1.88	270	2.66
130	1.91	275	2.69
135	1.94	280	2.71
140	1.97	285	2.73
145	2.01	290	2.75
150	2.04	295	2.78
155	2.07	300	2.80

Note: The density parameter is intended as a measure of the mechanical complexity of the hybrid microcircuit as a whole.

Table A-55. Density Factors for a Hybrid Device

Mechanical Devices

Table A-56 provides information for mechanical devices.

Table A-56. Mechanical Items - Base Failure Rates, Environmental Factors and Failure Mode Data

Non-operational	Item Description	Operational							
Base Failure Rate λ_b failures 10^6 hrs		**Base Failure Rate λ_b failures 10^6 hrs**	**Environmental Factors (K_E)**					**Predominant Failure Modes**	
GFP		**G.1**	**G.2**	**S.1**	**S.2**	**A.1**	**A.2**	**Mode**	**% Factor**
Ground Fixed Protected		**Ground Fixed**	**Ground Mobile**	**Ship Protected**	**Ship Exposed**	**Air Protected**	**Air Exposed**		
0.53	Accumulator, Hydraulic	35.0	1.5	1.3	1.5	2.0	4.5		
0.29	Actuator, Hydraulic	15.0	3.5	3.3	3.5	6.0	8.0		
0.06	Actuator, Pneumatic	15.0	5.5	2.5	7.5	5.0	8.0		
1.2	Barometric Capsule	1.2	N/A	N/A	N/A	2.0	4.0	Distortion	50
								Porosity	50
0.1	Bearing, Ball, Light Duty	2.3	3.0	2.0	3.0	2.0	4.0	Lubrication Failure	45
								Contamination	25
0.04	Bearing, Ball, Heavy Duty	4.5	2.2	1.2	2.2	1.5	3.2	Lubrication Failure	45
								Contamination	25
0.002	Bearing, Jewel	0.4	3.0	1.3	3.0	2.0	4.0	Contamination	60
								Distortion	20
								Lubrication	12
0.005	Bearing, Rotary, Roller	1.2	3.0	2.5	3.0	2.2	3.5		
0.005	Bearing, Rotary, Sleeve	3.0	7.0	3.0	7.0	8.0	10.0		
0.0005	Bearing, Spherical	1.0	5.0	3.0	5.0	6.4	l0.0		
0.0002	Bearing, Translatory, Sleeve	0.2	6.0	2.3	6.0	5.0	10.0		

Table A-56. Mechanical Items - Base Failure Rates, Environmental Factors and Failure Mode Data

Non-operational Base Failure Rate λ_b failures 10^6 hrs	Item Description	Operational Base Failure Rate λ_b failures 10^6 hrs	Environmental Factors (K_E)					Predominant Failure Modes	
GFP		G.1	G.2	S.1	S.2	A.1	A.2		
Ground Fixed Protected		Ground Fixed	Ground Mobile	Ship Protected	Ship Exposed	Air Protected	Air Exposed	Mode	% Factor
0.0005	Bearing, Bush	0.4	6.0	2.3	6.0	5.0	10.0		
1.0	Bellows	9.5	5.0	4.0	5.0	10.0	12.0		
0.0002	Bracket, Mounting	0.1	4.0	1.5	4.0	2.0	6.0		
0.01	Brake Assembly, Mechanical, Friction	1.5	3.0	1.3	3.0	2.0	3.0		
0.0001	Cam and Follower	1.8	5.0	1.2	5.0	1.5	6.0	Lubrication Faults	33
								Adhesive Bond	27
								Failure Distortion	33
	Carburetor								
0.0005	Clutch, Dog	0.5	3.0	2.7	3.0	6.0	9.0		
0.05	Clutch, Friction	3.5	6.2	2.6	6.0	4.0	8.0	Contamination Lubrication	20
								Failure	15
								Mechanical Degradation	50
0.005	Clutch, Magnetic	5.0	3.0	2.0	3.0	4.0	5.0		
0.05	Clutch, Slip	2.4	6.0	2.0	6.0	4.0	7.0		
0.0001	Connections, Hydraulic	0.35	2.5	1.5	3.0	3.5	4.3		
0.0001	Connections, Pneumatic	0.4	2.5	1.5	3.0	3.5	5.0		
0.05	Counter, Mechanical	2.0	5.0	2.0	5.0	4.0	5.0	Lubrication Failure	58
								Contamination	21
0.004	Coupling, Flexible Drive	1.25	5.0	4.0	5.0	10.0	13.0		

Table A-56. Mechanical Items - Base Failure Rates, Environmental Factors and Failure Mode Data

Non-operational	Item Description	Operational							
Base Failure Rate λ_b failures 10^6 hrs		Base Failure Rate λ_b failures 10^6 hrs	Environmental Factors (K_E)					Predominant Failure Modes	
GFP		G.1	G.2	S.1	S.2	A.1	A.2	Mode	% Factor
Ground Fixed Protected		Ground Fixed	Ground Mobile	Ship Protected	Ship Exposed	Air Protected	Air Exposed		
0.002	Coupling, Rotary Shaft	0.2	2.0	1.3	2.0	2.0	3.0		
	Diaphragm, Metal	5.0					6.0		
	Diaphragm, Rubber	8.0							
	Drive, Belt	34.0					5.3		
	Drive, Cable	3.2					6.0		
	Drive, Chain	0.8							
	Drive, Constant Speed								
	(Pneumatic)	20.0					7.0		
	Drive, Pulley	1.3					6.0		
	Duct	2.0					12.0		
0.0001	Filter, Fuel	3.0					11.0		
0.0001	Filter, Hydraulic Fluid	3.25					8.0		
0.001	Filter, Pneu-matic	1.5					6.5		
0.01	Gasket, Cork	0.5					6.5		
0.01	Gasket, Paper	1.0					6.8		
0.01	Gasket, Monel Mesh	0.4					6.25		
0.01	Gasket, 0 Ring	0.16	2.0	1.5	2.0	2.5	6.25	Deterio-ration	90
0.01	Gasket, Phenolic	0.4					6.25		
0.01	Gasket, Rubber	0.16					6.25	Deterio-ration	65
0.05	Gauge Pres-sure (Bourden Tube)	9.5	2.0	1.5	2.0	2.0	2. 4		
	Gear Train, per Mesh	0.03	4.0	2.7	4.0	6.0		Contam-ination	21
								Mechan-ical Failure	21
								Misalign ment	29

Table A-56. Mechanical Items - Base Failure Rates, Environmental Factors and Failure Mode Data

Non-operational		Operational								
Base Failure Rate λ_b failures 10^6 hrs	**Item Description**	**Base Failure Rate λ_b failures 10^6 hrs**	**Environmental Factors (K_E)**						**Predominant Failure Modes**	
GFP		**G.1**	**G.2**	**S.1**	**S.2**	**A.1**	**A.2**	**Mode**	**% Factor**
Ground Fixed Protected		**Ground Fixed**	**Ground Mobile**	**Ship Protected**	**Ship Exposed**	**Air Protected**	**Air Exposed**		
								Lubrication Inadequate	29
	Gear Train, Anti-Backlash, per Mesh	1.0	3.0	2.0	3.0	4.0			
	Gear Box	12.0					2.5		
	Heat Exchanger	0.9	4.0	1.8	2.0	1.2	3.5		
0.001	Hose, Heavy Stress	25.0					4.0	Deterioration	85
								End Fitting Failure	10
0.005	Hose, Flexible	1.5					2.2	Deterioration	85
								End Fitting Failure	10
0.005	Hose, Pneumatic	10.0					15.0	Deterioration	85
								End Fitting Failure	10
	Hose, Coolant (I.C. Engine)	22.0				N/A	N/A	Deterioration	85
	Insert, Wire, Screwthread	0.1							
0.01	Jack, Hydraulic								
0.18	Motor, Hydraulic Mount, Anti-Vibration	5.0	8.0	2.7	8.0	10.0			
0.0001	Mirror	0.1	3.0	2.0	3.0	4.0			
	Plugs, Spark, I.C. Engine								
0.18	Pump, Engine Driven, Hydraulic	8.0	5.0	2.0	5.0	4.0	10.0		
0.06	Pump, Fuel, Engine Driven	12.0	2.0	1.5	2.0	2.5	3.0		

Table A-56. Mechanical Items - Base Failure Rates, Environmental Factors and Failure Mode Data

Non-operational Base Failure Rate λ_b failures 10^6 hrs	Item Description	Operational Base Failure Rate λ_b failures 10^6 hrs	Environmental Factors (K_E)					Predominant Failure Modes	
GFP		G.1	G.2	S.1	S.2	A.1	A.2		
Ground Fixed Protected		Ground Fixed	Ground Mobile	Ship Protected	Ship Exposed	Air Protected	Air Exposed	Mode	% Factor
	Pump, Vacuum, Engine Driven	9.0	2.0	1.5	2.0	5.0	6.0		
0.002	Piston, Hydraulic	1.3	5.0	2.0	5.0	4.0	6.0		
0.0004	Prism	0.4	3.90	2.0	3.0	4.0			
0.003	Radome	8.0	2.0	N/A	2.0	N/A	3.0		
0.01	Reducer, Pneumatic Pressure	0.3	2.0	1.5	2.0	2.5	3.0		
0.01	Regulator, Hydraulic Pressure	2.3	3.0	2.0	3.0	4.0	5.0		
0.01	Reservoir, Hydraulic	2.4	3.0	2.0	3.0	4.0	5.0		
	Seal, Sliding	3.0	3.0	2.0	3.0	3.5	6.25		
0.01	Seal, 0 Ring	0.16	2.0	1.5	2.0	2.5	3.0		
	Seal, Rotating	7.0	3.0	2.0	3.0	3.5	5.0		
	Seal, Rubber Strip, Bonded	0.09	2.0	1.5	2.0	2.5	3.0		
	Shaft, Gear, Extension	0.35	2.0	1.5	2.0	2.5	3.0		
	Spring, Calibration, Sensitive	2.0	4.0	2.3	4.0	5.0	6.0	Distortion	30
								Fracture	67
	Spring, Simple Return Force	0.32	3. 0	1.5	3.0	2.5	3.0	Distortion	30
	Spring, Valve, I.C. Engine	9.6	1.5	1.0	1.5	N/A	N/A	Distortion	30
								Fracture	67
	Tank, Fuel, Integral (Wing)	13.0	N/A	N/A	N/A	N/A	10.0		
0.24	Tank, Small, SP	2.0	2.0						
0.24	Tank, Small, LP	1.5	2.0						
0.05	Timer, Mechanical	2.0	5.0	2.7	5.0	6.0	7.0		
	Valve, Air	1.7	3.0	4.0	5.0	4.0	6.0		
0.17	Valve, Butterfly	1.32							

Table A-56. Mechanical Items - Base Failure Rates, Environmental Factors and Failure Mode Data

Non-operational		Operational							
Base Failure Rate λ_b failures 10^6 hrs	Item Description	Base Failure Rate λ_b failures 10^6 hrs	Environmental Factors (K_E)					Predominant Failure Modes	
GFP		G.1	G.2	S.1	S.2	A.1	A.2	Mode	% Factor
Ground Fixed Protected		Ground Fixed	Ground Mobile	Ship Protected	Ship Exposed	Air Protected	Air Exposed		
	Valve, Filler and Charging (Gas)	0.9	3.0	2.0	4.0	4.0	6.0		
	Valve, Float, Fuel	15.0	2.0	1.5	2.0	3.0	4.0		
0.24	Valve, Fuel, Check	1.3	1.4	1.25	1.4	2.2	3.0		
0.28	Valve, Hydraulic, Ball	0.6	2.3						
0.002	Valve, Hydraulic, Check	2.0	6.0						
0.005	Valve, Hydraulic, Control								
0.01	Valve, Hydraulic, Pressure Regulator	3.5	2.4	8.0					
0.002	Valve, Hydraulic, Relief	10.0					3.0		
	Valve, Hydraulic, Restrictor	2.0					10.0		
0.66	Valve, Hydraulic, Servo	48.0				3.3			
	Valve, Hydraulic, Shut-off	6.0					3.0		
	Valve, Hydraulic, Shuttle	9.0					6.0		
	Valve, Hydraulic, Spool	55.0	3.5	3.0	3.5	3.0	6.0		
	Valve, Pneumatic, Bleed								
0.22	Valve, Pneumatic, Check	1.2			6.0				
0.02	Valve, Pneumatic, Control	0.6	3.0	1.8	3.0	7.0	9.0		

Table A-56. Mechanical Items - Base Failure Rates, Environmental Factors and Failure Mode Data

Non-operational		Operational								
Base Failure Rate λ_b failures 10^6 hrs	**Item Description**	**Base Failure Rate λ_b failures 10^6 hrs**	**Environmental Factors (K_E)**						**Predominant Failure Modes**	
GFP		**G.1**	**G.2**	**S.1**	**S.2**	**A.1**	**A.2**			
Ground Fixed Protected		**Ground Fixed**	**Ground Mobile**	**Ship Protected**	**Ship Exposed**	**Air Protected**	**Air Exposed**	**Mode**	**% Factor**
	Valve, Pneumatic, Pressure Regulator	2.0	10.0				58.0		
0.001	Valve, Pneumatic, Relief	1.6	2.5	6.0	10.0	17.0	31.0		
	Valve, Pneumatic, Selector								
	Valve, Pneumatic, Shut-off	52.0				1.4	2.0		
0.03	Valve, Solenoid, General	6.4	3.0	1.7	3.0	3.0	4.0		

Table A-56. Mechanical Items - Base Failure Rates, Environmental Factors and Failure Mode Data

Operational Environments

Table A-57 lists all categories of operational environments.

Table A-57. Categories of Operational Environments

Category	Symbol	Description of Operational Environment
Ground Fixed	G1	Equipment protected from the weather and high levels of humidity, vibration, shock and excessive temperature variations. Maintained by military personnel.
Ground Mobile	G2	Conditions more severe than conditions G1, mostly due to vibration and shock. Cooling air may also be more limited and maintenance less uniform.
Ship Protected	S1	Equipment protected from rain, high humidity levels and excessive temperature variations. Subjected to the vibration and shock levels relative to the main region of a ship.
Ship Exposed	S2	Conditions more severe than condition S1, mostly due to the increased vibration and shock levels associated with the bows, aft and masthead regions of a ship.
Air Protected	A1	Equipment situated in typical cockpit conditions and protected from the environmental extremes of pressure, temperature, shock and vibration.
Air Exposed	A2	Equipment bay, tail, nose or wing installations with environmental extremes of pressure, temperature, shock and vibration.

Table A-57. Categories of Operational Environments

Non-operational Environments

Table A-58 lists non-operational environmental factors.

Table A-58. Non-operational Environmental Factors

Category	Description of Non-operational Environment	Environmental Factor (K_E)
Ground Fixed Protected (GFP)	Fixed Ground storage in permanent buildings providing adequate protection against excessive temperature variation and high humidity.	1 (Base Condition)
Deep Storage (DS)	Deep Storage, i.e., conditions similar to Fixed Ground Storage but additionally equipment is stored in its own protective container (possibly pressurised with an inert gas.	0.5
Ground Fixed Exposed (GFE)	Fixed Ground Storage in semi-tropical regions. Ambient temperatures less than 45 °C and relative humidity approaching 100% four months of the year.	2
Ground Mobile (GM)	Ground Mobile transportation of non-operating equipment.	10
Ship Protected (SP)	Storage (or inactive) in areas of a ship protected from rain, high humidity levels and excessive temperature variations. Vibration and shock levels relative to the main region of the ship.	2
Ship Exposed (SE)	Storage (or inactive) in areas of a ship which experience more severe environmental conditions than SP above, e.g., increased vibration and shock levels associated with the bows, aft and masthead regions of a ship.	4
Air Protected (AP)	Air transportation of non-operating equipment.	5
Air Exposed (AE)	Air exposed on wing, pylon or other external fixture.	15
Workshop Storage (WS)	Storage in Depot / Base / Workshop.	2
Ready-Use Storage (RUS)	Storage in a Ready-Use Store.	2

Table A-58. Non-operational Environmental Factors

One-shot Devices

Table A-59 lists reliability data for one-shot devices.

Table A-59. Reliability Data for One-shot Devices

One-shot Device	Reliability (i.e., Probability of Successful Operation)	95 Confidence Limits	Failures per 10^6 Trials (See Note 1)
Acutator, hot gas	0.9983	0.9992 0.9960	1750
Cartridge, Ejector Release Unit	0.9992	0.9998 0.9972	760
Cartridge, Cover Removal	0.9897	0.9965 0.9700	10350
Expansive Motor: Motor, Gas Piston, Thruster	0.9998	0.9999 0.9992	150
Flare, guided missile	0.9994	0.9999 0.9986	566
Gas Generator (actuator or remote gyro)	0.9988	0.9990 0.9985	1154
Gyro assembly, remote (efflux of remote gas generator impinges on buckets cut into rotor periphery. Reliability of gas generator and igniter not included)	0.9991	0.9999 0.9976	928
Gyro assembly, integral (cordite charge built into periphery of rotor; Catherine wheel principle)	0.9936	0.9964 0.9889	6359
Note 1: All data (except *) includes failures in associated electrical power supplies, including electrical wiring, switches, plug/socket connectors, etc..			

Table A-59. Reliability Data for One-Shot Devices

One-shot Device	Reliability (i.e., Probability of Successful Operation)	95 Confidence Limits	Failures per 10^6 Trials (See Note 1)
Igniter, electric, bridge wire	0.9996	0.9999 0.9990	430
Igniter, fuzehead	0.9983	0.9991 0.9969	1700
Ignition and Safety Arming Unit (Rocket Motor)	0.9903	0.9939 0.9851	9745
*Rocket Motor, case-bonded type (less igniter and electrical supply failures)	0.9993*	0.9997* 0.9983*	666*
Rocket Motor, loose-cartridge type (includes igniter and electrical supply failures)	0.9988	0.9993 0.9978	1246
Switch, fusible link	0.9992	0.9999 0.9957	735
Thermal Battery, cup and cover type	0.9996	0.9999 0.9985	400
Thermal Battery, Pellet: Siconium/barium Chloarte pyrotechnic	0.9997	0.9999 0.9982	320
Thermal Battery, Pellet: Iron/Potassium Perchlorate pyrotechnic			
Note 1: All data (except *) includes failures in associated electrical power supplies, including electrical wiring, switches, plug/socket connectors, etc..			

Table A-59. Reliability Data for One-Shot Devices (Continued)

One-shot Device	Reliability (i.e., Probability of Successful Operation)	95 Confidence Limits	Failures per 10^6 Trials (See Note 1)
Typical Warhead Initiation Train, (surface-to-air or air-to-air), consisting of: • Electrical power and wiring • Safety and Arming Unit (Single Channel, Mechanical Shutter) • Pressure Delay Unit or Accelerometer • Infra Red Fuze • Warhead	0.9929	0.9979 0.9768	7100
Wire Guidance Mechanism	0.9986	0.9991 0.9978	1400
Note 1: All data (except *) includes failures in associated electrical power supplies, including electrical wiring, switches, plug/socket connectors, etc..			

Table A-59. Reliability Data for One-Shot Devices (Continued)

B. Preparation of Reliability Block Diagrams

Introduction

The level and detail of a Reliability Block Diagram (RBD), or set of RBDs, will vary and, in general, reflect a customer's requirements in respect to the bid or project requirement.

All reliability and maintainability data used within this appendix should be obtained from the predictions.

System design and configuration information necessary for the preparation of RBDs shall be obtained from the appropriate project manager who will have designated system design engineers responsible for major sub-systems of the equipment.

Elements of Reliability Block Diagrams

Figure B-1 demonstrates typical elements of an RBD. These key elements can be considered as:

- Presentation.
- Sub-system identification.
- Serial item modelling.
- Parallel item modelling (redundancy).
- Non-operational sub-systems.
- System failure rate and mean time between failures.

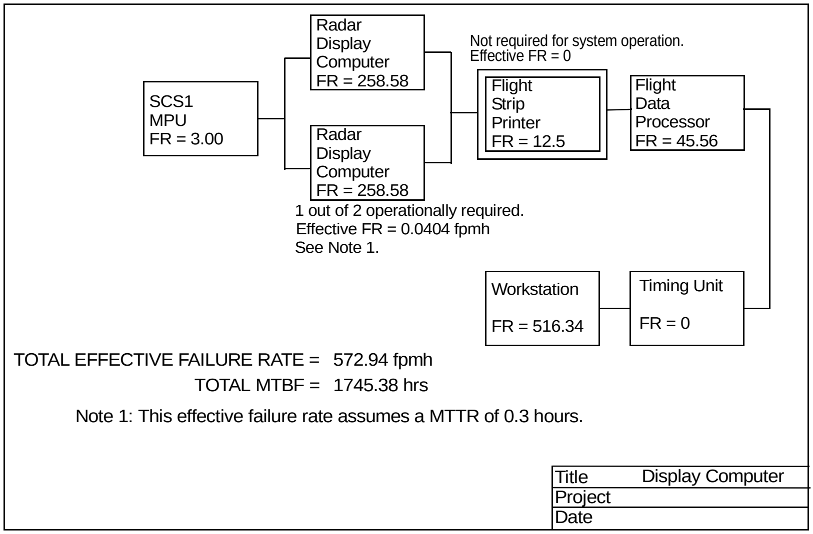


Figure B-1. Sub-system RBD

Presentation

RBDs are typically presented directly to potential and existing customers. Therefore, a clear, neat and unambiguous presentation is essential. The format shown in Figure B-1 is a representative example, not a mandatory requirement.

Sub-System Identification

Figure B-1 shows a series of blocks that represent sub-systems of the main system. For example, it shows a Display Computer comprising of a SCS1 MPU, Radar Display Computer (2 off), Flight Strip Printer, Flight Data Processor Timing Unit and Workstation.

The correct identification of these sub-systems is an important aspect of the RBD. Each sub-system would normally be limited to a list of **Line Replaceable Units** (LRUs) to enable the calculation of the sub-system failure rate.

RBDs are not intended to emulate the technical layout of the system. Therefore, the order in which sub-systems are placed on the diagram is irrelevant.

Serial Item Modelling

If a sub-system is essential for the mission success of the overall system, it should be modelled as a series item, e.g., SCSI MPU, Flight Data Processor, Timing Unit and Workstation in Figure B-1). In Figure B-2, the RBD displaying serial items is indicating that a failure in a serial item will mean a total system failure.

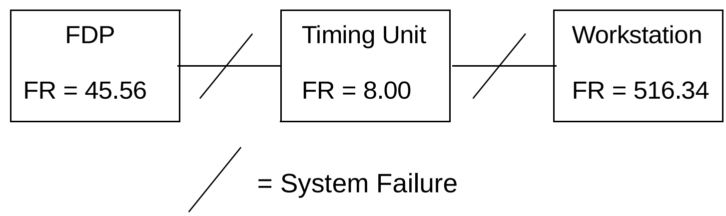


Figure B-2. Series RBD

The logic of serial modelling in an RBD is similar to that of an electrical circuit. If a serial component fails, then the entire circuit will fail.

Parallel Item Modelling (Redundancy)

Sub-systems that are modelled in a parallel configuration (Figure B-3) indicate that the primary function of that sub-system is duplicated, thus allowing switch over to the active redundant unit in the event of failure.

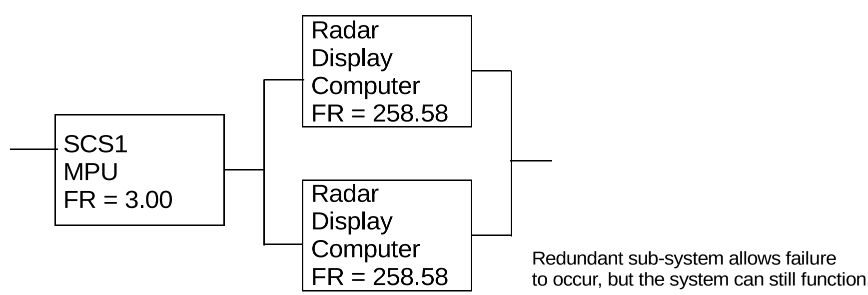


Figure B-3. Radar Display Computer RBD

Again, this logic follows that of an electrical circuit; if one parallel component fails, the circuit continues to operate because there is another route for the current to follow.

Figure B-1 shows an effective failure rate of the redundant Radar Display Computer Sub-system of 0.0404 failures per million hours. This effective failure rate has been calculated using equations from the Rome Air Development Centre “Reliability Engineers Tool-kit”. (See Figure B-4.)

Example **Linear Device**

Data: Radar Data Computer λ = 258.58.
One out of two required for system operation.
Mean Time to Repair (MTTR) = 0.3 hours.

What is the effective failure rate?

Solution:

Step 1: Using equation 1 in Figure B-4:

$$\lambda = \frac{2!(2.58 \cdot 10-4)^{2}}{(2-1-1)!(3.3)^{1}} \text{ failures per } 10^{6} \text{ hours}$$

Step 2: Effective failure rate is:

$$0.00004 \cdot 10^{-3} \text{ failures per hour}$$

$$= 0.04 \text{ failures per million hours}$$

Redundancy Equations

With Repair	Without Repair
All units are active on-line with equal unit failure rates. (n-q) out of n required for success. **Equation 1** $$\frac{\lambda_{(n-q)}}{n} = \frac{n!(\lambda)^{q+1}}{(n-q-1)!(\mu)^{q}}$$	**Equation 4** $$\frac{\lambda_{(n-q)}}{n} = \frac{\lambda}{\sum_{i=n-q}^{n} \frac{1}{i}}$$
Two active on-line units with different failure and repair rates. One of two required for operation. **Equation 2** $$\lambda_{1/2} = \frac{\lambda_A\lambda_B[(\mu_A+\mu_B)+(\lambda_A+\lambda_B)]}{(\mu_A+\lambda_B)\cdot(\mu_B+\lambda_A)+\lambda_A(\mu_B+\lambda_A)+\lambda_B(\mu_A+\lambda_B)}$$	**Equation 5** $$\lambda_{1/2} = \frac{\lambda_A^2\lambda_B+\lambda_A\lambda_B^2}{\lambda_A^2+\lambda_B^2+\lambda_A\lambda_B}$$
One standby off-line unit with n active on-line units required for success. Off-line spare is assumed to have a failure rate of zero. On-line units have equal failure rates. **Equation 3** $$\lambda_{n/(n+1)} = \frac{n[n\lambda+(1-P)\mu]\lambda}{\mu+n(P+1)\lambda}$$	**Equation 6** $$\lambda_{n/(n+1)} = \frac{n\lambda}{(P+1)}$$

Key:

$\lambda_{x/y}$ = The effective failure rate of the redundant configuration where x of y units are required for success.

n = Number of active on-line units. $n!$ is n factorial (e.g., $5! = 5\cdot4\cdot3\cdot2\cdot1 = 120$, $1! = 1$, $0! = 1$.

λ = Failure rate of an individual on-line unit (failures/hour).

q = Number of on-line active units that are allowed to fail without system failure.

μ = Repair rate ($\mu = 1/M_{ct}$, where M_{ct} is the mean corrective maintenance time in hours).

P = Probability switching mechanism will operate when needed ($P = 1$ with perfect switching).

Notes:

1. Assumes all units are functional at the start.
2. The approximations represent time to first failure.
3. **CAUTION**: Redundancy equations for repairable systems should not be applied if delayed maintenance is used.

Figure B-4. Redundancy Equations

Thanks are extended to the Rome Laboratory, Reliability Analysis Centre, for allowing this table to be reproduced.

Non-operational Sub-systems

Figure B-1 shows a Flight Strip Printer that is modelled as a serial item; however, it is not required for system operation. The block diagram indicates that a failure of the Flight Strip Printer will not prevent the system from completing its mission. The effective failure rate of this sub-system is therefore zero and is normally included in the total failure rate for the system.

A sub-system not required for system operation is often shown with a shaded outline and an explanatory note as displayed in Figure B-1.

System Failure Rate and Mean Time Between Failures

Upon completion of sub-system identification, serial and parallel configuration, etc., the final failure rate and Mean Time Between Failures (MTBF) of the system can be calculated. This calculation consists of the simple addition of the failure rates of each sub-system.

NOTE Only add effective failure rates in the case of parallel and non-operational sub-systems.

A total effective failure rate is often given in the diagram. (See Figure B-1.) The MTBF of the system can also be calculated by:

$$\text{System MTBF} = \frac{10^6}{\text{Total Effective Failure Rate}}$$

if Failure Rate has units of FPMH or 10^9 if in FITS).

C. Application of Importance Measures

This section explains how the Birnbaum, Criticality and Fussell-Vesely importance measures are applied in a typical fault tree analysis.

Equal Event Probabilities

OR Gate

Let's consider the simplest example, which is two equally probable events connected by an OR gate (or in parallel). Assume a constant probability of 0.1 for both events *A* and *B*. Because the events have equal probability, it is expected that each event would have the same importance measure.

Using the formulae presented earlier in this document for importance measures, the Birnbaum importance measure for both events *A* and *B* is 0.9. Similarly, the Criticality and Fussell-Vesely importance measures are the same for both of these identical events. Therefore, for this system, the importance measures are the same for both events.

AND Gate

If these two equally probable events are connected by an AND gate, the identical events are still equally important. For example, the Birnbaum importance measure would be 0.1 for both events *A* and *B*.

Unequal Event Probabilities

Recall that a fault tree is a negative outcome analysis, which means that improvement in a system reduces the probability of the top event. Suppose now that event *A* has a probability of 0.1, and event *B* has a probability of 0.2. Event *B* is now more likely to happen than event *A*.

It would follow that these events would have different values of a given importance measure. However, which event will have the higher importance measure value? That is, to lower the probability of occurrence of the top event, which event should receive more effort for improvement? Also, does the system structure determine the values of the importance measures? That is, will it matter whether the events are connected by an OR gate or an AND gate?

OR Gate

In considering the answer to the last question, assume that events *A* and *B* are connected by an OR gate. Then, the top event, event *X*, occurs if either event *A* or event *B* occurs. Also assume that the development efforts cost the same for a given improvement of either event, that is, for a given reduction in the probability of occurrence of either event *A* or event *B*. The more probable event, event *B* in this example, is the event that more often leads to the occurrence of event *X*. In this case, placing the development efforts into reducing the occurrence of event *B* (the more probable event) can reduce the occurrence of event *X* more than an equal effort spent reducing the occurrence of event *A*.

The Birnbaum importance measure for event *A* is 0.8, and the Birnbaum importance measure for event *B* is 0.9. This indicates that development effort should be directed toward reducing the occurrence of event *B* because it yields the maximum reduction in the occurrence of event *X*, the top event. Similarly, the Criticality and the Fussell-Vesely importance measures also both give event *B* the greater importance.

To reinforce this, take the probabilities of events *A* and *B* to their respective extremes. Let *A* have a probability of 0.01 (it hardly ever occurs), and let *B* have a probability of 0.99 (it nearly always occurs). Then, development efforts directed at event *A* are wasted (because it hardly ever causes the occurrence of the top event). All of the development effort should obviously be directed towards improving (or reducing the probability of) event *B*.

AND Gate

Now, assume that events *A* and *B* are now connected by an AND gate instead of an OR gate. The top event, event *X*, occurs only if both events *A* and *B* occur. Assume once again that the development efforts cost the same for a given improvement of either event. The least probable event, event *A* in this example, is the event that more often leads to the non-occurrence of event *X*. That is, *X* can only occur if *A* occurs. (Of course, *B* must also occur in order for *X* to occur.) Here, a greater reduction in the occurrence of event *X* is gained by placing development efforts into further reducing the occurrence of event *A* (the least probable event) than by placing development efforts into reducing the occurrence of event *B*.

If the Birnbaum importance measure for event *A* is calculated, it is now 0.2 while this value for event *B* is 0.1. This indicates that to maximise the reduction in the occurrence of event *X*, the top event, development effort should be directed at reducing the occurrence of event *A*. In the case of the AND gate, for reasons discussed later in this section, the Criticality and the Fussell-Vesely importance measures both give event *A* and event *B* the same importance.

Again, to reinforce this, take the probabilities of events *A* and *B* to their respective extremes. Assume that *A* has the probability of 0.01 (it hardly ever occurs), and *B* has the probability of 1.0 (it always occurs). Then, development efforts directed at eliminating that last 0.01 probability of event *A* is the best course of action because it ensures that the top event never occurs. No development effort should be directed towards improving event *B*.

To this point, it will be seen that with an OR gate, development effort is devoted to reducing the probability of occurrence of the most likely to occur event. This is the event with the highest importance measure and is most likely to cause the occurrence of the top event.

Also, it has been shown that with an AND gate, development effort is directed towards reducing the probability of occurrence of the event that is least likely to occur. This is the event with the highest importance measure and is most likely to single-handedly prevent the occurrence of the top event.

Because the importance measures say a different thing in each case, these conclusions may, at first, seem counter intuitive. However, consider an argument by analogy with the RBD. In a series system (OR gate in fault tree), the importance measures indicate that the least reliable component should be improved to reduce the differences between components in the system. The natural thought about engineering is to focus on improving the worst component, until every component works **perfectly**.

However, in a parallel system (AND gate in fault tree), the importance measures invite one to improve the most reliable component, increasing the differences between components in the system. Assuming equal development costs, this makes sense. In a parallel system (an AND gate in fault tree), the most reliable component (that event which is least likely to occur) is the component that is most likely to be the last component to fail (event to occur) before the system fails (the top event occurs).

Assumptions

Keep in mind that these theoretical conclusions about importance measures are based upon assumptions. One of the assumptions is that the cost of improvement is constant, both across components and within a component across reliability of that component. This is a rather strong assumption.

For example, consider the constant cost of improvement assumption across components by reflecting on the relative cost of improving a turbine blade in a jet engine versus improving a rubber O-ring. It is likely to be much more expensive to get a slight improvement out of a turbine blade redesign as compared to upgrading the quality of an O-ring.

Also, consider the constant cost of improvement assumption within a component across reliability improvement. At the early stages of component development, reliability is lower but incremental improvements are generally much cheaper to introduce than in the later stages of component development. Therefore, importance measures should be used only as guides to selecting which components should be considered for improvement, not as a hard and fast rule that generates fixed decisions.

It is clear from the OR gate and AND gate examples that system structure and events are combined to determine the relative importance of each event. Also, it is clear that different importance measures (Birnbaum, Criticality and Fussell-Vesely) can assign different relative importance to each event.

Typically, an engineer chooses a given importance measure, such as Birnbaum, and then ranks or sorts the basic events in the fault tree on the basis of this important measure's value. Those events with the largest importance measure values are then improved to reduce the chance of their occurrence. This improvement could be either a re-design of the basic component or sub-assembly or the introduction of redundancy at the component or sub-assembly level.

One reasonable question remains: *Is the rank order of the chosen importance measure determined by the system structure and the events?*

To answer this question, consider a system of six basic events, A_1, A_2, A_3, B_1, B_2 and B_3:

- The events A_1, A_2 and A_3 are connected to gate *A*, a 2::3 Voting gate.
- The events B_1, B_2 and B_3 are connected to gate *B*, also a 2::3 Voting gate.
- The gates *A* and *B* are connected to the top gate, an OR gate.

Assume that all of the basic events have exponential distributions with the Mean Time Between Failures (MTBF) given in Table C-1:

Event	MTBF
A_1	10
A_2	10
A_3	1000
B_1	10
B_2	1000
B_3	1000

Table C-1. Event and MTBF

Table C-2 shows the Birnbaum importance measures for the top gate of this fault tree at time $t = 1$:

Event	MTBF	Measure
A_1	10	0.0959535
A_2	10	0.0959535
A_3	1000	0.1721804
B_1	10	0.0019786
B_2	1000	0.0950862
B_3	1000	0.0950862

Table C-2. Birnbaum Importance Measure at Time *t* = 1

Ordering: $A_3 > A_1 = A_2 > B_2 = B_3 > B_1$

Therefore, improve A_3 first, then A_1, A_2, etc.

Table C-3 shows the Birnbaum importance measures for the top gate of this fault tree at time $t = 100$:

Event	MTBF	Measure
A_1	10	0.7407952
A_2	10	0.7407952
A_3	1000	0.0000743
B_1	10	0.0000141
B_2	1000	0.0000743
B_3	1000	0.0000743

Table C-3. Birnbaum Importance Measure at Time *t* = 100

Ordering: $A_1 = A_2 > A_3 = B_2 = B_3 > B_1$

Therefore, improve A_1 and A_2 first, then A_3, etc.

Thus, the system structure and events **do not by themselves** determine the rank order of the chosen importance measure. Because event probabilities are used in determining the importance measures, and because event probabilities can change with time, the ranking of basic events by the importance measure will change over time for the same system and events. In this example, the rankings changed as follows:

Rank Ordering at time $t = 1$: $A_3 > A_1 = A_2 > B_2 = B_3 > B_1$

Rank Ordering at time $t = 100$: $A_1 = A_2 > A_3 = B_2 = B_3 > B_1$

Now, it has been shown that the rank ordering of a given importance measure can be affected by:

- The basic events.
- The system structure.
- The time of evaluation.

Also, this last example illustrates the fact that for a given set of basic events, a given system and a given time of evaluation, **the rank orderings of different importance measures can be different.**

For example, from the previous window for time $t = 100$, the importance measure values in Table C-4 were found:

Event	Birnbaum	Criticality	Fussell-Vesely
A_1	0.7407952	0.7408114	1.0000000
A_2	0.7407952	0.7408114	1.0000000
A_3	0.0000743	0.0000071	0.1903293
B_1	0.0000141	0.0000141	0.1903293
B_2	0.0000743	0.0000071	0.1042212
B_3	0.0000743	0.0000071	0.1042212

Table C-4. Importance Measure for Time *t = 100*

These importance measure values yield the following rank orderings:

Birnbaum Rank Ordering: $A_1 = A_2 > A_3 = B_2 = B_3 > B_1$

Criticality Rank Ordering: $A_1 = A_2 > B_1 > A_3 = B_2 = B_3$

Fussell-Vesely Rank Ordering: $A_1 = A_2 > A_3 = B_1 > B_2 = B_3$

All three importance measures indicate that A_1 and A_2 should be the first and second choices for improvement. It is not so clear that B_2 and B_3 should be the last choices for improvement because only two of the three measures place them as least important. Even so, B_2 and B_3 would probably be the last events to target for improvement.

The events A_3 and B_1 are the middle candidates for improvement. Because A_3 is third ranked twice and fourth ranked once, it is probably the third choice for improvement. However, B_1 is much more difficult to classify. Although B_1 is sixth place for the Birnbaum importance measure, it is third place for the Criticality importance measure and the fourth place for the Fussell-Vesely importance measure. Given that B_1 ranks in front of B_2 and B_3 on two out of the three importance measures, B_1 would probably be the fourth choice for improvement.

D. Bibliography

Reference	Publication
1	RPM 80
2	Rome Air Development Centre “Reliability Engineers Tool-kit”
3	RADC-TR-89-299 “Reliability and Maintainability Operational Parameter Translation II”
4	MIL-HDBK-217
5	BS 9002 and BS CECC Qualified Products List

Table D-1. List of References

Index

D

E

F

G

H

I

J

K

L

M

Q

R

S

T

U

V

W